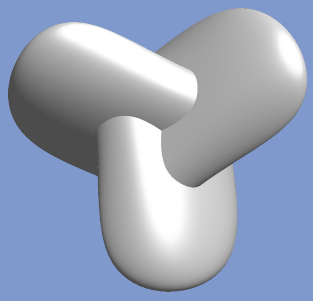


Publicaciones Matemáticas del Uruguay

Volumen 15, Junio 2016

Publicaciones Matemáticas del Uruguay

Publicada por:

CMAT — Facultad de Ciencias
IMERL — Facultad de Ingeniería

Universidad de la República

http://pmu.uy/

ISSN: 0797-1443

Créditos:

Diseño de tapa: J. Rodriguez Hertz
Editor LaTeX: G. Tornaría

Publicaciones Matemáticas del Uruguay

Volumen 15 Junio 2016

Prefacio

El presente volumen de las Publicaciones Matemáticas del Uruguay contiene un artículo arbitrado y notas correspondientes a cursos y conferencias del 2do Coloquio Uruguayo de Matemática, del XXIII Encuentro Rioplatense de Álgebra y Geometría Algebraica, y del 4to Coloquio Uruguayo de Matemática.

Su publicación contó con el apoyo de la Comisión Sectorial de Investigación Científica (CSIC) de la Universidad de la República.

Diego Armentano
Jana Rodriguez Hertz
Gonzalo Tornaría
Armando Treibich
José L. Vieitez

Montevideo, Junio 2016.

NOTAS DE CURSOS

2do Coloquio Uruguayo de Matemática (2009)

Publicaciones Matemáticas del Uruguay
Volumen 15, Junio 2016, Páginas 1–15
S 0797-1443

COMPUTABILIDAD E INCOMPUTABILIDAD EN ÁLGEBRA Y COMBINATORIA

ANTONIO MONTALBÁN

Introducción

Este artículo está basado en un curso de tres días dado durante el Segundo Coloquio Uruguayo de Matemática en Diciembre del 2009. El objetivo del curso, y de este artículo, es transmitir las ideas básicas de la teoría de la computabilidad y la matemática computable, y no contiene resultados originales. Todos sabemos que en matemática hay construcciones o demostraciones que son más complicadas que otras. Matemática computable es el área de la teoría de la computabilidad donde uno estudia la complejidad de construcciones, procesos, demostraciones y estructuras matemáticas. Hay varias formas de medir la complejidad de una construcción. La que usaremos en este artículo se basa en la idea de que un proceso que es computable, es decir uno que puede ser efectuado de forma totalmente mecánica, es un proceso *simple*, y que los procesos más complejos son los que no pueden ser efectuados por computadores. Esta noción es adecuada para estudiar la complejidad de objetos infinitos. En algunas situaciones, uno puede estar interesado en otras nociones de complejidad, como por ejemplo en ciencias de la computación donde los procesos que son considerados simples son los que son computables en tiempo polinomial.

Este artículo esta dividido en tres secciones. En la primera desarrollamos los conceptos básicos de la teoría de la computabilidad. En las siguientes secciones estudiamos la complejidad de construcciones concretas en combinatoria y en álgebra. En la segunda sección estudiaremos problemas relacionados al problema de la parada, y en la tercera sección estudiaremos el lema de König sobre caminos en árboles binarios.

Hemos incluido varias demostraciones, pero no de todos los resultados que mencionamos. Además, muchas de las demostraciones omiten varios detalles que dejamos para que el lector verifique.

1. Computabilidad

La noción de *algoritmo* ya era conocida por los griegos cuando se preguntaban si ciertas construcciones geométricas, o de teoría de números, pueden hacerse mecánicamente. Un ejemplo de algoritmo, ya usado por lo griegos hace más de 2000 años, es el algoritmo de Euclides para calcular el máximo común divisor de dos números. Un algoritmo no es más que una receta de cocina. Es simplemente un método claramente determinado por una serie de instrucciones para calcular algo. Esta idea intuitiva es clara para la mayoría de los matemáticos: todos reconocemos un algoritmo cuando lo vemos.

Para poder trabajar con esta idea intuitiva deberíamos explicitar claramente a qué nos referimos con "un algoritmo totalmente mecánico." Hay varias definiciones posibles, y la mayoría son un poco técnicas, por lo cual no nos detendremos en detalles. Recomendamos al lector que desea ver una definición formal consultar los primeros capítulos de [4] o [1]. Para los que ya conocen algún lenguaje de programación, imaginen que por algoritmo nos referimos a cualquier programa que pueda escribirse en ese lenguaje, y que tenemos tanto tiempo y memoria como sea necesario para correr el programa. La elección del lenguaje de programación a usar no es importante, ya que todos son equivalentes desde nuestro punto de vista. La definición más usada en los cursos de complejidad se basa en el lenguaje de las máquinas de Turing. Éstas son máquinas muy simples, y son universales en el sentido que pueden hacer lo mismo que cualquier otra máquina mecánica. El que puedan hacer los mismos cálculos que cualquier otra máquina mecánica es la conocida *tesis de Church-Turing*. En la década del 30, Turing propuso una justificación para su tesis, pero la tesis no se puede demostrar rigurosamente, ya que no tenemos una definición rigurosa de "máquina mecánica." Actualmente, la tesis de Church-Turing es globalmente aceptada.

1.1. Conjuntos computables.

Definición 1.1. Un conjunto $A \subseteq \mathbb{N}$ es *computable* si existe un algoritmo totalmente mecánico que, dado $n \in \mathbb{N}$, decide si $n \in A$ o no. O sea, el algoritmo recibe n como entrada, y produce una salida de 1 o 0, dependiendo de si $n \in A$ o no.

Antiguamente se usaba la palabra "recursivos" para definir estos conjuntos.

Ejemplo 1.2. Los siguientes conjuntos son computables:

- El conjunto de los números pares;
- El conjunto de los números primos;
- El conjunto de los programas escritos correctamente de acuerdo a las reglas del lenguaje.

¿Por qué nos restringimos solamente a subconjuntos de $\mathbb{N}$? Porque es suficiente. Todo objeto finito puede ser codificado con un número natural. Y nos referimos a cualquier tipo de objeto finito, como un grafo, un complejo simplicial, un grupo, una representación finita de un grupo infinito, etc. La codificación pude ser hecha de varias maneras, y es irrelevante cual método se usa en la codificación. Todos sabemos que las computadoras modernas codifican todas los objetos que manejan en código binario: el mismo método serviría, cualquiera que sea.

Ahora presentamos tres ejemplos de conjuntos no computables.

1.1.1. El problema de la palabra. Consideremos el conjunto de grupos que pueden ser definidos usando un conjunto finito G de generadores y un conjunto finito R de relaciones entre los generadores. Por ejemplo, si tenemos dos generadores $G = \{a, b\}$, y la relación $R = \{aba^{-1}b^{-1} = 1\}$, tenemos el grupo $\mathbb{Z}^2$. El conjunto de pares (G, R) de generadores-relaciones que determinan un grupo no-trivial (i.e. con más de un elemento) no es computable. La razón es que para saber si un elemento del grupo (y en particular un generador) es equivalente a la identidad, uno tiene que aplicar las relaciones dadas de alguna manera hasta llegar a 1, pero no hay forma de anticipar el número de aplicaciones que uno puede llegar a necesitar.

1.1.2. Variedades simplemente conexas. Este problema esta directamente conectado con el anterior. Como ya dijimos, cada complejo simplicial finito se puede representar con un número natural. El conjunto de lo números que representan complejos simpliciales simplemente conexos no es computable. Si un complejo simplicial es simplemente conexo, entonces en un número finito de pasos podemos encontrar las homotopías de todos las curvas generadoras con la identidad. Pero si no, no hay forma de saber que hemos revisado todas la homotopías posibles.

1.1.3. El décimo problema de Hilbert. El conjunto de los polinomios con coeficientes enteros, y en varias variables, que tienen raíces enteras no es computable. Este era el décimo problema de la famosa lista que Hilbert propuso en el año 1900, antes de que existiese una noción formal de que significa ser computable. Este problema fue resulto en 1970 por Matiyasevich, usando resultados previos de M. Davis, Putnam y Robinson.

1.2. Funciones parciales computables. Todo programa define una función parcial. Por lo tanto, nos sera útil estudiar las funciones parciales que son computables.

Definición 1.3. Todo programa de computadora (i.e. algoritmo totalmente mecánico) p, cuya entrada y salida es un número natural, representa a una función parcial $p\colon \mathbb{N} \rightharpoonup \mathbb{N}$, donde el valor de $p(n)$ puede estar indefinido en caso que el programa p con entrada n no se detenga nunca. Nótese que hay programas que entran en loops infinitos, o que se quedan haciendo cálculos para siempre, y nunca se detienen. En este caso escribimos $p(n)\uparrow$. Si p, con entrada n, sí se detiene con salida m, luego, obviamente $p(n) = m$. En este caso escribimos $p(n)\downarrow$, o $p(n)\downarrow = m$, o simplemente $p(n) = m$.

Una función parcial $f\colon \mathbb{N} \rightharpoonup \mathbb{N}$ (o sea una función que puede estar indefinida en algunos valores) es una *función parcial computable* si está asociada a un programa p como en el parágrafo anterior. Cuando nos referimos a *función computable*, nos referiremos a una función *total* (i.e. definida en todos los valores), que es computable.

Como los programas son secuencias finitas de caracteres, podemos ordenarlos en una lista (digamos en orden lexicográfico). Sea $\varphi_0, \varphi_1, \varphi_2, \ldots.$ una enumeración de todos los programas que uno puede escribir que tienen como entrada y como salida un número natural. A cada programa φ_e asociamos la función parcial $\varphi_e\colon \mathbb{N} \rightharpoonup \mathbb{N}$. Como la enumeración de los programas es totalmente efectiva, podemos escribir un programa p, cuya entrada son dos números naturales, tal que $p(e, n) = \varphi_e(n)$. O sea que p primero busca el e-ésimo programa de la lista, y luego lo corre con entrada n. Usando una biyección computable entre $\mathbb{N} \times \mathbb{N}$ y $\mathbb{N}$, (como por ejemplo $\frac{1}{2}((n+m)^2 + 3n + m)$), podemos suponer que la entrada de p es sólo un número natural y no dos.

1.2.1. El problema de la parada. El ejemplo más usado de conjunto no computable es el problema de la parada.

Definición 1.4. Llamamos el *problema de la parada* al conjunto K de los programas que, con entrada 0, se detienen en algún momento.

$$K = \{e \in \mathbb{N} : \varphi_e(0)\downarrow\}.$$

Teorema 1.5. *(Turing* [5]*) El problema de la parada no es computable.*

La única manera mecánica de saber si un programa eventualmente se detiene o no es correrlo. El problema es que si el programa nunca se detiene, nunca lo sabremos.

Demostración. Supongamos que K es computable, y que el programa $p\colon \mathbb{N} \to \{0,1\}$ es tal que $p(e) = 1$ si y sólo si el e-ésimo programa φ_e con entrada 0 se detiene eventualmente. Consideremos el siguiente programa q:

> Con entrada i, primero buscamos un programa φ_e tal que $\varphi_e(n) = \varphi_i(i+n)$, y luego si $p(e) = 0$, paramos el programa $q(i)$ dando alguna respuesta (digamos $q(i) = 0$), y si $p(e) = 1$, dejamos que $q(i)$ entre en un loop infinito. Nótese que $p(e) = 1$ si y sólo si $\varphi_i(i)$ se detiene. O sea que $q(i)$ se detiene si y sólo si $\varphi_i(i)$ no se detiene.

Como q es un programa, existe e tal que $\varphi_e = q$. Luego, por definición de q, $\varphi_e(e)$ se detiene si y sólo si $\varphi_e(e)$ no se detiene. Esta contradicción muestra que K no puede ser computable. □

1.3. Computabilidad relativa. Sea B un conjunto, preferiblemente no computable, al que llamamos *oráculo*. Supongamos ahora que cuando queremos computar un conjunto o una función, podemos usar B en nuestro algoritmo. Es decir, dentro del algoritmo tenemos una función, que asumimos como primitiva, tal que dado n nos responde si $n \in B$ o no, y dependiendo de la respuesta continuamos el algoritmo de una forma u otra. Esto nos permite computar una cantidad mayor de conjuntos.

Definición 1.6. Dados $A, B \subseteq \mathbb{N}$, decimos que A *es computable en* B (y escribimos $A \leq_T B$) si hay un programa que, con entrada n y usando a B como oráculo, responde si $n \in A$ o no. Decimos que A y B son *Turing equivalentes* (y escribimos $A \equiv_T B$) si $A \leq_T B$ y $B \leq_T A$.

Ejemplo 1.7. Los siguientes conjuntos son Turing-equivalentes.

- El problema de la parada;
- El problema de la palabra;
- El conjunto de complejos simpliciales finitos simplemente conexos;
- El conjunto de los polinomios con coeficientes enteros, y en varias variables, que tienen raíces enteras.

Luego, por ejemplo, consideremos el conjunto de los pares (G, R) de generadores y relaciones que generan grupos de torsión. Este conjunto es mayor, en el sentido de $\leq_T$, que todos estos conjuntos recién mencionados, pero no puede ser computado en ninguno de ellos. El conjunto (que llamamos $Th(\mathbb{N})$) de todas las sentencias de lógica de primer orden que son verdaderas sobre los números naturales es aún $\leq_T$-mayor.

Definición 1.8. Las clases de equivalencia de la relación $\equiv_T$ se llaman *grados de Turing*. Nótese que los grados de Turing forman un orden parcial, al ser ordenados por $\leq_T$.

$$\mathbf{D} = \frac{2^{\mathbb{N}}}{\equiv_T} \quad \text{y} \quad \mathcal{D} = (\mathbf{D}, \leq_T).$$

Para cada $A \in 2^{\mathbb{N}}$, el conjunto $\{B \in 2^{\mathbb{N}} : B \leq_T A\}$ es numerable, porque hay una cantidad numerable de programas que uno puede escribir. Por lo tanto cada clase de equivalencia es numerable, y $\mathbf{D}$ tiene tantas clases de equivalencia como $\mathbb{R}$ tiene números reales. La segunda observación importante sobre $\mathcal{D}$ es que tiene un

grado que es $\leq_T$-menor que todos los demás. Este grado, que denotamos 0, es la clase de equivalencia de los conjuntos computables: los conjuntos computables son Turing-equivalentes entre ellos y son computables en cualquier otro conjunto.

Entender la forma y las propiedades del orden parcial de los grados de Turing es uno de los temas de investigación de la Teoría de la Computabilidad. En los años 60 se buscaba caracterizar este orden parcial como el único orden con alguna propiedad de densidad o alguna otra propiedad. Luego de varios años, todos los intentos de encontrar una caracterización de esa forma fueron fallando. En los años 80 hubo un cambio de dirección, y en vez de buscar alguna propiedad que muestre la simpleza de los grados de Turing, se empezaron a buscar propiedades que muestren que este orden parcial es muy complicado, lo más complicado que puede llegar a ser.

1.4. Conjuntos computablemente enumerables. Una clase importante de conjuntos, es la de los conjuntos computablemente enumerables.

Definición 1.9. Un conjunto $A \subseteq \mathbb{N}$ es *computablemente enumerables (c.e.)* si existe una función computable $f\colon \mathbb{N} \to \mathbb{N}$ cuya imagen es A (i.e. $A = \{f(0), f(1), \dots\}$). El conjunto vacío también es considerado un conjunto c.e. a pesar de no cumplir esta condición.

Los conjuntos c.e. no tienen por que ser computables. Por ejemplo, el problema de la parada es c.e. ya que podemos correr todos los programas, una cantidad finita a la vez, y cada vez que encontramos uno que se detiene lo enumeramos. Nótese que cuando enumeramos un conjunto $A = \{f(0), f(1), f(2), ...\}$, no tenemos porque hacerlo en orden creciente.

Teorema 1.10. *Sea $A \subseteq \mathbb{N}$. Los siguientes enunciados son equivalentes.*

- *A es c.e.*
- *Existe un programa φ tal que para $n \in \mathbb{N}$, $n \in A$ si y sólo si φ se detiene con entrada n.*
- *Existe un programa φ tal que para $n \in \mathbb{N}$, $n \in A$ si y sólo si existe m tal que $\varphi(m)$ se detiene y $\varphi(m) = n$.*

Teorema 1.11. *$A \subseteq \mathbb{N}$ es computable si y sólo si A y $\mathbb{N} \setminus A$ son ambos c.e. (donde $\mathbb{N} \setminus A$ es el complemento de A).*

El problema de la parada K no es un conjunto c.e. cualquiera: es universal entre los conjuntos c.e.

Teorema 1.12. *Para todo conjunto c.e. A existe una función computable $f\colon \mathbb{N} \to \mathbb{N}$ tal que $\forall n \in \mathbb{N}$,*

$$n \in A \iff f(n) \in K.$$

Por lo tanto, todo conjunto c.e. es computable en K.

1.5. El salto de Turing. La definición del problema de la parada puede hacerse relativa a cualquier oráculo.

Definición 1.13. Dado $B \subseteq \mathbb{N}$, definimos B' como el conjunto de índices e de los programas que, con entrada 0 y oráculo B, se detienen. Si denotamos como φ_e^B el e-ésimo programa con oráculo B, y usamos $\varphi_e^B(n)\downarrow$ para decir que φ_e^B con entrada n se detiene, tenemos que

$$B' = \{e \in \mathbb{N} : \varphi_e^B(0)\downarrow\}.$$

B' es llamado el *salto de Turing* de B.

Teorema 1.14. *Para todos $A, B \subseteq \mathbb{N}$,*

- *$A \leq_T B$ implica $A' \leq_T B'$.*
- *$B <_T B'$.*

Con respecto a los ejemplos de 1.7, tenemos que $K \equiv_T 0'$, que $T \equiv_T 0''$, y que $Th(\mathbb{N}) >_T 0^{(n)}$ para todo n, donde $0^{(n)}$ es la n-ésima iteración del salto de Turing. De aquí en adelante usaremos $0'$ en lugar de K.

2. El problema de la parada en matemáticas

Ya mencionamos el problema de la parada en la Secciones 1.2.1 y 1.5. El aspecto más interesante de este problema es su complejidad. Conjuntos con la misma complejidad aparecen de forma natural en muchas áreas de matemática. El siguiente teorema es bien conocido y se debe a varios autores.

Teorema 2.1. *Sea $A \subseteq \mathbb{N}$. Los siguientes enunciados son equivalentes.*

1. *$0' \leq_T A$;*
2. *El oráculo A puede decidir si un grupo dado por (generadores, relaciones) es no-trivial;*
3. *El oráculo A puede decidir si un polinomio en $\mathbb{Z}[X_1, X_2, ...]$ tiene raíces en $\mathbb{Z}$;*
4. *El oráculo A puede computar la componente conexa de un vértice dado en cualquier grafo computable G;*
5. *Todo anillo computable tiene un ideal maximal computable en A;*
6. *Toda secuencia creciente acotada y computable de números racionales tiene limite cuya representación decimal es computable en A;*

Demostraremos la equivalencia entre (1), (4) y (5).

Como ya dijimos, el objetivo de la matemática computable es estudiar la complejidad de de las construcciones, procesos, demostraciones y estructuras que manejamos regularmente en matemática. Los resultados más interesantes son los que relacionan propiedades computacionales con propiedades estructurales o algebraicas.

La mejor forma de entender a que nos referimos con "estudiar la complejidad" de construcciones matemáticas es viendo ejemplos. Empezaremos estudiando algunas construcciones básicas sobre grafos y demostrando la equivalencia entre (1) y (4).

2.1. Grafos. Un grafo consiste de dos conjuntos (V, E) donde $E \subseteq V^2$. Los elementos de V se llaman *vértices*, y los de E *aristas*. Sólo vamos a considerar grafos no dirigidos (i.e. $(\forall u, v \in V)(u, v) \in E \to (v, u) \in E)$) y sin lazos (i.e. $(\forall v \in V)(v, v) \notin E$). Todos los grafos que mencionaremos son numerables infinitos, y como son numerables podemos suponer que $V \subseteq \mathbb{N}$. Decimos que un grafo es *computable* si los conjuntos $V \subseteq \mathbb{N}$ y $E \subseteq \mathbb{N}^2$ son computables.

El primer problema que estudiaremos es qué tan complicado es calcular la componente conexa de un vértice en un grafo infinito. Dado un vértice $v \in V$, la *componente conexa de v* es

$$C(v) = \{w \in V : \exists x_1, ..., x_k \in V \\ (v, x_0) \in E \ \& \ (x_0, x_1) \in E \ \& \ ... \ \& \ (x_{k-1}, x_k) \in E \ \& \ (x_k, w) \in E\}.$$

Supongamos que G es computable. ¿Es $C(v)$ computable? ¿Hay algún oráculo que calcule $C(v)$ para todo G computable?

Lema 2.2. *Para todo G computable y $v \in V$, $C(v) \leq_T 0'$.*

Demostración. Dado v, w y G, construiremos un programa φ, tal que, con entrada 0, el programa $\varphi(w)$ se detiene si y sólo si $w \in C(v)$. Si e es el índice de este programa (i.e. $\varphi = \varphi_e$), tendríamos que $w \in C(v) \iff e \in 0'$. Por lo que $C(v)$ seria computable en $0'$.

El programa $\varphi(0)$ hace lo siguiente: Una por una, enumera todas las tuplas $(x_1, ..., x_k)$ de vértices y chequea si forman un camino de v a w. Si sí, el programa para y no sigue enumerando más tuplas. Si no, el programa continua chequeando las siguientes tuplas indefinidamente. □

Lema 2.3. *Existe un grafo computable G y $v \in V$, tal que $0' \leq_T C(v)$.*

Antes de probar este lema, precisamos definir la siguiente notación: $\varphi_{e,s}(i) \downarrow$ significa que el programa φ_e con entrada i se detiene en menos de s pasos. Nótese que dados e, i, s podemos decidir si $\varphi_{e,s}(i) \downarrow$ automáticamente, ya que sólo necesitamos buscar el e-ésimo programa de la lista, correr φ_e por s pasos y ver si se detiene.

Demostración. Consideremos el siguiente grafo: $G = (V, E)$. Sea $V = \mathbb{N}$. Definimos E de la siguiente manera. Los números impares están todos por aristas: o sea $\forall n, m(2n + 1, 2m + 1) \in E$. No hay ninguna arista entre dos número pares: o sea $\forall n, m(2n, 2m) \notin E$. Entre los números pares y los impares tenemos las siguientes aristas:

$$(2n, 2m + 1) \in E \iff \varphi_{n,m}(0) \downarrow,$$

o sea si $\varphi_n(0)$ se detiene en menos de m pasos. Este grafo es claramente computable, es decir, dado cualquier par de vértices podemos decidir automáticamente si están conectados por una arista o no.

Ahora probaremos que $C(1)$ es Turing-equivalente a $0'$. Sabemos que $C(1)$ contiene a todos los números impares, y probaremos que $2n \in C(1) \iff n \in 0'$. La única forma de que $2n$ se conecte con un número impar es si $\varphi_{n,m}(0) \downarrow$ para algún $m \in \mathbb{N}$. Esto sólo ocurre si y sólo si, $\varphi_n(0) \downarrow$, o, equivalentemente, si $n \in 0'$. □

Juntando los dos lemas anteriores obtenemos el siguiente teorema.

Teorema 2.4. *$0'$ es necesario y suficiente para calcular $C(v)$ para todo grafo G computable y todo $v \in V$.*

Los resultados de esta sección son conocidos entre los investigadores de la materia, aunque puede que no sean parte de la literatura en el tema.

2.2. Ideales maximales. Sea $(R; 0, 1, +_R, \times_R)$ un anillo conmutativo infinito numerable. Podemos suponer $R \subseteq \mathbb{N}$, y por lo tanto $+_R \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ y $\times_R \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, aunque estas operaciones no tiene nada que ver con la suma y el producto de números naturales. Todos los anillos que mencionaremos son conmutativos.

Definición 2.5. R es *computable* si el conjunto $R \subseteq \mathbb{N}$ y las funciones $+_R \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ y $\times_R \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ son computables.

Definición 2.6. Un *ideal* en R es un subconjunto $I \subseteq R$ tal que

- para todos $x, y \in I$, $x +_R y \in I$,
- para todo $x \in I$ y para todo $y \in R$, $x \times_R y \in I$.

Definición 2.7. $I \subsetneq R$ es un *ideal maximal* si no existe ningún ideal J tal que $I \subsetneq J \subsetneq R$. $I \subsetneq R$ es un *ideal primo* si $x \times_R y \in I$ implica que $(x \in I)$, o $(y \in I)$.

Estudiaremos la siguiente pregunta. ¿Cual es la dificultad de es encontrar un ideal maximal o primo en un anillo computable? En esta sección nos concentraremos ideales maximales, y estudiaremos ideales primos en 3.2. Los resultados de esta sección fueron obtenidos por a Friedman, Simpson y Smith.

Lema 2.8. *Todo anillo conmutativo computable tiene un ideal maximal computable en $0'$.*

Demostración. Sea R un anillo computable. Construiremos un ideal maximal $I \subseteq R$ por pasos usando $0'$ como oráculo. En el paso s, decidiremos si $s \in I$ o no (recordemos que $R \subseteq \mathbb{N}$). Si $s \notin R$, entonces $s \notin I$. Supongamos ahora que $s \in R$ y supongamos también que para todo $t < s$ ya decidimos si $t \in I$ o no. Sea I_s el conjunto de todos estos $t < s$ que ya enumeramos en I. Para saber si agregar s a I o no, debemos saber si $\langle I_s \cup \{s\}\rangle$, el ideal generado por $I_s \cup \{s\}$, contiene a 1_R o no. ¿Que tan difícil es saber si 1_R esta en $\langle I_s \cup \{s\}\rangle$? Escribimos un programa que busca por todas las combinaciones lineales de los elementos de $I_s \cup \{s\}$ con coeficientes en R, y se detiene si encuentra una tal combinación que es igual a 1_R. Si nunca la encuentra es porque 1_R no pertenece a $\langle I_s \cup \{s\}\rangle$. El oráculo $0'$ puede responder si este programa se detiene o no, por lo tanto sabe si $1_R \in \langle I_s \cup \{s\}\rangle$. En caso de respuesta afirmativa, dejamos a s afuera de I. En caso de respuesta negativa, agregamos s a I.

Dejamos al los lectores más entendidos en el área verificar que el conjunto I construido de esta manera es un ideal propio, y que es maximal. □

Ahora que sabemos que si conocemos $0'$ podemos encontrar ideales maximales en cualquier anillo computable, nos preguntamos si $0'$ es necesario, o si hay alguna forma más fácil de construir ideales maximales. La respuesta es que sí, que $0'$ es necesario, y esto es lo que dice el próximo lema.

Lema 2.9. *Existe un anillo computable R tal que $0'$ es computable en cualquier ideal maximal de R.*

Demostración. Consideremos el anillo computable $\mathbb{Q}[X_1, X_2, ...]$ de polinomios en $\mathbb{Q}$ sobre las indeterminadas $X_1, X_2, ...$ Este anillo es computable, ya que sumar y multiplicar polinomios es claramente computable. Recordemos que $0' = \{e \in \mathbb{N} : \varphi_e(0)\downarrow\}$. Sea

$$P = \langle \{X_i : i \notin 0'\}\rangle,$$

el ideal de todos los polinomios cuyos monomios tienen al menos una variable X_i con $i \notin 0'$. Observemos que P es un ideal primo. Este ideal no es computable, pero su complemento $M = \mathbb{Q}[X_1, X_2, ...] \setminus P$ es computablemente enumerable, es decir que hay un programa que enumera todos sus miembros (ya que $0'$ es computablemente enumerable). Como P es primo, M es un conjunto multiplicativo (es decir que el producto de sus elementos se mantiene en M) . Por lo tanto podemos localizar con respecto a M. Sea

$$R = \{\frac{p}{q} : p \in \mathbb{Q}[X_1, X_2, ...], q \in M\} \subseteq \mathbb{Q}(X_1, X_2, ...).$$

Sea

$$P_R = \{\frac{p}{q} : p \in P, q \in M\}.$$

No es difícil ver que P_R es un ideal de R. Más aún, todo elemento de $R \setminus P_R$ es invertible en R, y, por lo tanto, no sólo P_R es un ideal maximal, si no que es el único

ideal maximal de R. Obsérvese que $P_R \geq_T 0'$, ya que $n \in 0'$ si y sólo si $X_n \notin P_R$. Por lo tanto, $0'$ es computable en todo ideal maximal de R (el cual sólo puede ser P_R).

La prueba no termina aquí, ya que R no es un anillo computable–pero casi. Dijimos que M es c.e., y por lo tanto también lo es R. Sea $\{r_0, r_1, ...\}$ una enumeración computable de los elementos de R. Esta secuencia nos da una biyección $r\colon \mathbb{N} \to R$. A través de esta biyección podemos definir un anillo $A = (\mathbb{N}, +_A, \times_A)$ haciendo el pull-back de las operaciones de R. O sea $x +_A y = f^{-1}(f(x) +_R f(y))$ y $x \times_A y = f^{-1}(f(x) \times_R f(y))$. Como f es computable, el anillo A es computable. Como A y R son isomorfos, $f^{-1}(P)$ es el único ideal maximal de A, y también tenemos que $f^{-1}(P) \equiv_T 0'$ ya que $n \in 0'$ si y sólo si para el único i tal que $f(i) = (X_n)$ tenemos $i \notin f^{-1}(P)$. □

Juntando estos dos lemas obtenemos el siguiente teorema.

Teorema 2.10. $0'$ *es necesario y suficiente para calcular ideales maximales en anillos conmutativos computables.*

Los resultados de esta sección se deben a Friedman, Simpson y Smith [2].

3. El Lema de König

En esta sección estudiaremos una serie de problemas cuya complejidad es menor a la del problema de la parada. El siguiente teorema es conocido. La segunda parte se debe a a Friedman, Simpson y Smith [2].

Teorema 3.1. *Sea $A \subseteq \mathbb{N}$. Los siguientes son equivalentes.*

1. *Todo árbol binario infinito computable tiene un camino computable en A;*
2. *Todo anillo computable tiene un ideal primo computable en A;*
3. *(Compacidad de $[0,1]$) Si $\{(a_i, b_i) : i \in \mathbb{N}\}$ es una familia de intervalos en $[0,1]$ con $a_i, b_i \in \mathbb{Q}$ tal que $\forall n, [0,1] \not\subseteq \bigcup_{i<n}(a_i, b_i)$, existe un número real $r \in [0,1], r \notin \bigcup_{i\in\mathbb{N}}(a_i, b_i)$ cuya representación decimal es computable en A.*

En el resto de esta sección demostraremos la equivalencia entre (1) y (2), y demostraremos que estos problemas son menos complejos que el problema de la parada, pero que tampoco son computables.

3.1. Caminos en árboles binarios. Un string binario es un secuencia finita de ceros y unos. Sea $2^{<\omega}$ el conjunto de los strings binarios finitos. Dado un string binario σ, sea $\sigma(i)$ la i-ésimo término de la secuencia, empezando por 0, y sea $|\sigma|$ el largo de la secuencia. O sea que $\sigma = (\sigma(0), \sigma(1), ..., \sigma(|\sigma| - 1))$. Dado un string binario finito σ, y dado $n \leq |\sigma|$, sea $\sigma \upharpoonright n = (\sigma(0), \sigma(1), ..., \sigma(n-1))$, el segmento inicial de σ de largo n. Dados dos strings σ y τ, decimos que $\sigma \subset \tau$ si $\sigma = \tau \upharpoonright n$ para algún n. Dados dos strings σ y τ, sea $\sigma^\frown\tau$ la concatenación de σ seguido por τ. Dada un función $f\colon \mathbb{N} \to \{0,1\}$ y $n \in \mathbb{N}$, sea $f \upharpoonright n = (f(0), ..., f(n-1)) \in 2^{<\omega}$.

Definición 3.2. Un *árbol binario* es un subconjunto $T \subseteq 2^{<\omega}$ tal que si $\tau \in T$, y $\sigma \subseteq \tau$ entonces $\sigma \in T$. Una función $f\colon \mathbb{N} \to \{0,1\}$ es un *camino* de T si $(\forall n)\ f \upharpoonright n \in T$.

Teorema 3.3 (König)**.** *Todo árbol binario infinito tiene un camino.*

Demostración. Sea T un árbol infinito. Definimos un camino f por recursión. Dado $\sigma \in T$, sea

$$T_\sigma = \{\tau \in 2^{<\omega} : \sigma^\frown \tau \in T\}.$$

Como T es infinito, sabemos que o $T_{(0)}$ es infinito, o $T_{(1)}$ es infinito, o ambos. Elijamos $f(0)$ tal que $T_{(f(0))}$ es infinito. Luego, de la misma manera, podemos definir $f(1)$ de forma que $T_{(f(0),f(1))}$ es infinito. Por recursión, siempre podemos elegir $f(n)$ de forma que $T_{f\restriction n+1}$ sea infinito. □

La prueba de este lema no es efectiva, ya que no podemos decidir mecánicamente en cada paso cual de las dos ramas del árbol es infinita.

Un árbol $T \subset 2^{<\omega}$ es *computable* si es computable como conjunto. (Usando una biyección efectiva entre $\mathbb{N}$ y $2^{<\omega}$ (como por ejemplo vía representaciones binarias) podemos traducir la noción de subconjunto de $\mathbb{N}$ computable a subconjunto de $2^{<\omega}$ computable.) Decimos que un árbol es b.i.c. si es binario infinito y computable.

Lema 3.4. *Todo árbol b.i.c. tiene un camino computable en* $0'$.

Demostración. Solamente tenemos que observar que la prueba del Teorema 3.3 produce un camino $f \leq_T 0'$. Para ver que el proceso es computable en $0'$, tenemos que observar que $0'$ puede decidir si hay un árbol T_σ es infinito o no. Todo lo que tenemos que hacer es escribir un programa que, con entrada σ, busca un número $n > |\sigma|$ tal que ninguna extensión de σ de largo n pertenece a T. Si el programa encuentra un tal n, se detiene y sabemos que el árbol T_σ es finito. Si no, el el árbol es infinito, y el programa continua buscando para siempre. □

La pregunta natural luego de este lema es si $0'$ es necesario para computar caminos en árboles b.i.c. Antes de responder esta pregunta, el siguiente lema muestra que no hay ninguna forma mecánica de hallar un camino en un árbol infinito.

Lema 3.5. *Existe un árbol b.i.c. que no tiene caminos computables.*

Demostración. Recordemos que $\varphi_0, \varphi_1, \varphi_2, ...$ es una enumeración de todos las funciones parciales computables. Tenemos que construir un árbol binario infinito y computable tal que para todo e, φ_e no es un camino en T. Usaremos un método llamado *diagonalización*. Vamos a definir un árbol T tal que si f es un camino en T, entonces para todo e, $f(e) \neq \varphi_e(e)$. Con esto logramos que para todo e, $f \neq \varphi_e$, y por lo tanto f no es computable. El único detalle a tener en cuenta es que $\varphi_e(e)$ puede no estar definido debido a que el programa no se detiene, y es esto no lo podemos saber de una forma computable. Lo que haremos es que, si luego de s pasos vemos que $\varphi_e(e)$ se detiene, entonces no permitimos que ningún σ de largo s y tal que $\sigma(e) = \varphi_e(e)$ pertenezca a T. Recordemos la siguiente notación: decimos que $\varphi_{e,s}(n) \neq k$ si, o $\varphi_e(n)$ no se detiene en menos de s pasos, o sí se detiene en s pasos pero no toma el valor k. Nótese que, dados e, n, s y k, se puede decidir computablemente si $\varphi_{e,s}(n) \neq k$. Sea

$$T = \{\sigma \in 2^{<\omega} : (\forall e < |\sigma|) \ \ \varphi_{e,|\sigma|}(e) \neq \sigma(e)\}.$$

Uno luego debería verificar que T es un árbol, que es infinito, que es computable, y que si f es un camino en T, f no es computable. □

Lema 3.6 (Jockusch, Soare [3])**.** *Todo árbol binario infinito computable tiene un camino* $f <_T 0'$.

Demostración. Sea T un árbol b.i.c. Ya sabemos que $0'$ puede encontrar un camino en T, pero ahora tenemos que probar que puede encontrar un camino f tal que $f \not\geq_T 0'$. Construiremos f usando $0'$ como oráculo. Al mismo tiempo construiremos una función g computable en $0'$ y usaremos el método de diagonalización para demostrar que $f \not\geq_T g$. Como $0' \geq_T g$, esto implica que $f \not\geq_T 0'$.

Para cada e, tenemos el siguiente requerimiento:

$$(R_e) \qquad \varphi_e^f(e) \neq g(e),$$

donde φ_e^f es el e-ésimo programa que usa f como oráculo, o sea que cada vez que el programa hace una pregunta al oráculo, estas preguntas van dirigidas a f. Como en las pruebas anteriores, vamos a estar interesados en $\varphi_{e,s}^f(n)$, que devuelve el resultado de este cálculo luego de s pasos. Sin perder generalidad, podemos suponer que en menos de s pasos sólo podemos preguntarle al oráculo sobre números menores a s (por ejemplo, en una máquina de Turing toma k pasos escribir el número k en la memoria para luego poder preguntarle al oráculo sobre k). Por lo tanto, si σ es un string de largo al menos s, tiene sentido escribir $\varphi_{e,s}^\sigma(n)$, ya que σ puede responder todas las preguntas que le hagamos al oráculo. Para simplificar la notación, escribiremos $\varphi_e^\sigma(n)$ en lugar de $\varphi_{e,|\sigma|}^\sigma(n)$, o sea que corremos $\varphi_e^\sigma(n)$ usando como máximo $|\sigma|$ pasos. Nótese que si $\varphi_e^\sigma(n) \downarrow$ y $\sigma \subseteq \tau$, tenemos que $\varphi_e^\tau(n) \downarrow = \varphi_e^\sigma(n)$. Por lo tanto, si fijamos e, n, k, el conjunto de todos los $\sigma \in 2^{<\omega}$ tales que $\varphi_e^\sigma(n) \uparrow$ es un árbol. (Recordemos que $\varphi_e^\sigma(n) \uparrow$ significa que $\varphi_e^\sigma(n)$ no se detiene en menos de $|\sigma|$ pasos.)

Volvamos ahora al la construcción de f y g computables en $0'$. Para construir f, vamos a construir una secuencia de árboles binarios infinitos computables $T_0 \supseteq T_1 \supseteq T_2 \supseteq \cdots$, y definiremos f como el único camino en común de todos estos árboles.

La construcción es por etapas. En la etapa número e, construiremos T_e y definiremos el valor de $g(e)$, con el objetivo de satisfacer el requerimiento (R_e). Supongamos que ya hemos definido T_{e-1} como un árbol b.i.c. Sea

$$S = \{\sigma \in T_{e-1} : \varphi_e^\sigma(e) \uparrow\}.$$

Como ya mencionamos, S es un árbol y es computable. Preguntémosle a $0'$ si S es infinito (o sea si $\exists n(S \cap 2^n = \emptyset)$ donde $2^n = \{\tau \in 2^{<\omega} : |\tau| = n\}$). Si sí, sea $T_e = S$. Si f es un camino en S, entonces $\varphi_e^f(e) \uparrow$, por que si $\varphi_e^f(e)$ se detuviese, usaría una cantidad finita del oráculo f, y por lo tanto para algún segmento inicial σ de f tendríamos $\varphi_e^\sigma(e) \downarrow$. Por lo que no importa que valor le damos a $g(e)$ – sea $g(e) = 0$. Si no, si S es finito, sea n tal que $S \cap 2^n = \emptyset$. Por lo tanto, para todo $\sigma \in T$ de largo n, $\varphi_e^\sigma(e) \downarrow$. Recorramos uno por uno todos estos σ hasta encontrar uno tal que $(T_{e-1})_\sigma = \{\tau \in T_{e-1} : \sigma^\frown\tau \in T_{e-1}\}$ es infinito, cosa que $0'$ puede responder. Una vez que encontramos un tal σ, definamos $T_e = (T_{e-1})_\sigma$ y $g(e) = (\varphi_e^\sigma(e)) + 1$. Cualquiera sea f, sólo por ser un camino en T_e tenemos que f es una extensión de σ y $\varphi_e^f(e) = \varphi_e^\sigma(e) \neq g(e)$. Si la respuesta es "no", sea $g(e) = 0$ y

$$T_e = \{\sigma \in T_{e-1} : \varphi_e^\sigma(e) \uparrow\}.$$

Como ya mencionamos, T_e es un árbol y es computable. Lo que no es tan inmediato es que es infinito. Si no fuese infinito, habría un nivel n tal para que todo $\sigma \in T_{e-1}$ de largo n, $\varphi_e^\sigma(e) \downarrow$. Como T_{e-1} es infinito, habría un tal σ con $(T_e)_\sigma$ infinito, y por lo tanto la respuesta a nuestra pregunta sería "sí".

En cualquiera de los dos casos tenemos que $\varphi_e^f(e) \neq g(e)$.

Para el lector interesado en entender esta demostración con mas profundidad, recomendamos verificar los detalles de esta demostración. □

El teorema original de Jockusch y Soare es que se puede encontrar un camino f tal que $f' \leq_T 0'$. La demostración de esta versión es parecida a la del lema anterior.

El siguiente lema dice que podemos encontrar un oráculo A que está estrictamente debajo de $0'$ con respecto a $\leq_T$, tal que A pude encontrar caminos en todos los árboles binarios infinitos computables simultáneamente.

Lema 3.7. *Existe $A \subseteq \mathbb{N}$, tal que $0 <_T A <_T 0'$, y que puede computar caminos en cualquier árbol b.i.c.*

Demostración. La prueba consiste en construir un árbol b.i.c. cuyos caminos computan caminos en todos los otros árboles b.i.c. y luego aplicar el lema anterior.

Primero tenemos que demostrar que podemos enumerar, computablemente, todos los árboles binarios computables. Para cada e, vamos a construir un árbol binario computable S_e tal que si φ_e es una función total y define un árbol $\{\tau \in 2^{<\omega} : \varphi_e(\tau) = 1\}$, entonces S_e y el árbol definido por φ_e tienen los mismos caminos. Lo interesante de esta definición es que si φ_e no es total, cosa que no podemos saber computablemente, igual obtenemos un árbol binario computable S_e.

$$S_e = \{\sigma \in 2^{<\omega} : (\forall \tau \subseteq \sigma)\varphi_{e,|\sigma|}(\tau) \neq 0\}.$$

Dejamos al lector interesado verificar que S_e cumple las propiedades que mencionamos. Ahora, no todos los árboles S_e son infinitos, así que vamos a construir una secuencia de árboles b.i.c. $\{T_e\}_{e\in\mathbb{N}}$ tal que si S_e es infinito, es igual a T_e. Si S_e es finito, sea n el mayor largo posible de los strings de S_e, y sea $\sigma \in S_e$ el menor (con respecto al orden lexicográfico) string de S_e de largo n. Sea $T_e = S_e \cup \{\tau : \tau \supseteq \sigma\}$. Esta definición de la secuencia T_e no es computable, ya que tenemos que saber si S_e es finito o no. Aquí también uno debería verificar que el conjunto $\{(e, \sigma) : \sigma \in T_e\}$ sí es computable.

Ahora tenemos que juntar todos los árboles T_e en un solo árbol. Recodemos que existe una biyección computable $: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Supongamos que el par (n, m) representa la imagen de esta biyección. Supongamos también que la biyección es tal que si $n_0 \leq n_1$ y $m_0 \leq m_1$, $(n_0, m_0) \leq (n_1, m_1)$. Dado $\sigma \in 2^{<\omega}$ sea $\sigma^i = (\sigma((i, 0)), \sigma((i, 1)), ..., \sigma((i, k)))$ donde k es el mayor número tal que $(i, k) < |\sigma|$. De la misma forma, dada $f\colon \mathbb{N} \to \{0, 1\}$ sea $f^i\colon \mathbb{N} \to \{0, 1\}$ tal que $f^i(k) = f((i, k))$. Ahora podemos definir

$$T = \{\sigma \in 2^{<\omega} : (\forall i < |\sigma|)\sigma^i \in T_i\}.$$

No es difícil probar que T es un árbol computable, y que f es un camino en T si y sólo si, para todo i, f^i es un camino en T_i. Como todos los T_i tienen caminos, T también tiene un camino. Como f^i es computable en f, f computa caminos en todos los arboles b.i.c., y usando el lema anterior obtenemos un camino $f <_T 0'$. Sea $A = \{n : f(n) = 1\}$. □

El siguiente lema examina la relación entre buscar caminos en árboles b.i.c. y computar conjuntos computablemente enumerable. Como ya mencionamos, el problema de la parada puede computar todos los conjuntos c.e. Por otro lado, lo más que pueden hacer los caminos en árboles b.i.c. es separar dos conjuntos c.e. Demostraremos solamente una dirección.

Lema 3.8. *Para todo árbol b.i.c., existen conjuntos c.e. disjuntos $A, B \subseteq \mathbb{N}$, tales que si $S \subseteq \mathbb{N}$ es tal que*

$$A \subseteq S \subseteq \mathbb{N} \setminus B,$$

entonces S computa un camino de T.

Demostración. Sea T un árbol b.i.c. Definiremos A y B como subconjuntos de $2^{<\omega}$. (Recordemos que hay una biyección computable entre $\mathbb{N}$ y 2^ω usando la expresión binaria de los números naturales.) El objetivo es definir A y B tal que si $T_{(\sigma^\frown 0)}$ es finito, entonces $\sigma \in A$, y si $T_{(\sigma^\frown 1)}$ es finito, entonces $\sigma \in B$. Si lográramos esto, y S separara A de B, podríamos definir un camino f en T recursivamente de la siguiente forma: Dado $f \upharpoonright n$, sea

$$f(n) = \begin{cases} 0 & \text{si } (f \upharpoonright n) \notin S \\ 1 & \text{si } (f \upharpoonright n) \in S. \end{cases}$$

De esta forma, podemos demostrar por inducción que, para cada n, $T_{(f \upharpoonright n)}$ es infinito: Si suponemos que $T_{(f \upharpoonright n)}$ es infinito, luego, si $T_{(f \upharpoonright n)^\frown 0}$ es finito, entonces $(f \upharpoonright n) \in A \subseteq S$ y si $T_{(f \upharpoonright n)^\frown 1}$ es finito, entonces $(f \upharpoonright n) \in B \subseteq \mathbb{N} \setminus S$. Por lo tanto $T_{(f \upharpoonright n+1)}$ sería infinito y podemos continuar con la inducción.

El único problema es que A y B definidos de esta forma no son necesariamente disjuntos, ya que si T_σ es finito, $T_{(\sigma^\frown 0)}$ y $T_{(\sigma^\frown 1)}$ también lo son. Lo que vamos a hacer es enumerar σ en A si $T_{(\sigma^\frown 0)}$ es "más finito" que $T_{(\sigma^\frown 1)}$:

$$\begin{aligned} A &= \{\sigma \in 2^{<\omega} : (\exists n)\ T_{(\sigma^\frown 0)} \cap 2^n = \emptyset \ \&\ T_{(\sigma^\frown 1)} \cap 2^n \neq \emptyset\}, \\ B &= \{\sigma \in 2^{<\omega} : (\exists n)\ T_{(\sigma^\frown 0)} \cap 2^n \neq \emptyset \ \&\ T_{(\sigma^\frown 1)} \cap 2^n = \emptyset\}, \end{aligned}$$

donde $2^n = \{\tau \in 2^{<\omega} : |\tau| = n\}$. De esta forma podemos demostrar que A y B son c.e. y disjuntos, y que si T_σ es infinito tenemos que si $T_{(\sigma^\frown 0)}$ es finito, $\sigma \in A$, y si $T_{(\sigma^\frown 1)}$ es finito, $\sigma \in B$. □

La mayoría de los resultados de esta sección aparecen en [3].

3.2. Ideales primos. Pasamos ahora al estudio de la complejidad de los ideales primos. No es difícil probar que todo ideal maximal es primo, y en general así es que se prueba la existencia de ideales primos. Veremos que hay métodos para construir ideales primos que son esencialmente más simples que que los métodos necesarios para construir ideales maximales. Los resultados de esta sección también fueron obtenidos por Friedman, Simpson y Smith.

Lema 3.9. *Para todo anillo computable R, existe un árbol b.i.c. cuyos caminos pueden calcular ideales primos en R.*

Demostración. Sea $R = \{r_0, r_1, ...\}$ donde $r_0 = 0_R$ y $r_1 = 1_R$. Construiremos un árbol computable $T \subseteq 2^{<\omega}$ tal que, para todo camino f de T, el conjunto

$$I_f = \{r_i : i \in \mathbb{N}, f(i) = 1\} \subseteq R \quad \text{es un ideal primo propio.}$$

Sea T el conjunto de los $\sigma \in 2^{<\omega}$ tales que

- Si $|\sigma| > 0$, $\sigma(0) = 1$.
- Si $|\sigma| > 1$, $\sigma(1) = 0$.
- Para todo $i, j, k < |\sigma|$ tales que $r_i +_R r_j = r_k$, si $\sigma(i) = \sigma(j) = 1$, entonces $\sigma(k) = 1$.
- Para todo $i, j, k < |\sigma|$ tales que $r_i \times_R r_j = r_k$, si $\sigma(i) = 1$, entonces $\sigma(k) = 1$.

- Para todo $i, j, k < |\sigma|$ tales que $r_i \times_R r_j = r_k$, si $\sigma(k) = 1$, entonces o $\sigma(i) = 1$, o $\sigma(j) = 1$, o ambos.

Estas propiedades garantizan que, si $f \in [T]$, entonces I_f contiene a 0_R, no contiene a 1_R, que $I_f + I_f \subseteq I_f$, que $I_f \times R \subseteq I_f$ y que I_f es primo, respectivamente. Nótese que T es un árbol y que es computable. □

Corolario 3.10. *Existe $A <_T 0'$ que puede calcular ideales primos en todos los anillo computables.*

Por lo tanto, encontrar ideales primos es estrictamente más fácil que encontrar ideales maximales.

Lema 3.11. *Para todo árbol b.i.c. T, existe un anillo computable cuyos ideales primos pueden calcular caminos en T.*

Demostración. Usando el Lema 3.8 tenemos que existen funciones computables f y g tales que si $S \subseteq \mathbb{N}$ separa las imágenes de f y g (es decir $(\forall n) f(n) \in X \ \& \ g(n) \notin X$), entonces S computa un camino de T. Ahora construiremos un anillo computable A, cuyos ideales primos computan conjuntos que separan f y g. Consideremos de vuelta el anillo $\mathbb{Q}[X_1, X_2, ...]$. Vamos a definir un ideal computable I en $\mathbb{Q}[X_1, ...]$, y después definir A como el cociente de $\mathbb{Q}[X_1, ...]$ módulo I. Sea I el ideal de $\mathbb{Q}[X_1, ...]$ generado por $\{X^n_{f(n)} : n \in \mathbb{N}\} \cup \{X^n_{g(n)} + 1 : n \in \mathbb{N}\}$. Para probar que este ideal es computable, observamos que todo $p \in \mathbb{Q}[X_1, ...]$ es equivalente, módulo I, a un polinomio p^* tal que si X^k_m ocurre en p^*, entonces $(\forall n \leq k)\ f(n) \neq m \ \& \ g(n) \neq m$. Para construir p^* efectivamente la idea es, cada vez que vemos un término X^k_m en p, chequeamos si $(\exists n \leq k) f(n) = m$, y si sí, lo reemplazamos por (X^{k-n}_m), y si $(\exists n \leq k) g(n) = m$, lo reemplazamos por $(X^k_m - (X^n_m + 1)^{k-n})$, y continuamos con este algoritmo hasta llegar al p^* deseado. Ahora, como I es computable, no es difícil representar $A = \mathbb{Q}[X_1, ...]/I$ computablemente: alcanza con encontrar un conjunto computable de representantes para las clases de equivalencia, y podemos hacerlo tomando dentro de cada clase de equivalencia el polinomio con menor índice en $\mathbb{N}$ (recordemos que estamos usando un subconjunto de $\mathbb{N}$ para representar $\mathbb{Q}[X_1, ...]$).

Ahora supongamos que P es un ideal primo propio de A. Si $f(n) = m$, entonces como $X^n_m = 0$ módulo I, y P es primo, $X_m \in P$. Si $f(n) = m$, entonces como $X^n_m = 1$ módulo I, y P es propio, $X_m \notin P$. Por lo tanto, el conjunto $S = \{m : X_m \in P\}$ separa las imágenes de f y g como queríamos. □

Si juntamos estos dos lemas obtenemos el siguiente teorema.

Teorema 3.12. *El problema de buscar ideales primos en anillos conmutativos computables es equivalente al problema de buscar caminos en árboles binarios infinitos computables.*

Los resultados de esta sección se deben a Friedman, Simpson y Smith [2].

Referencias

[1] C.J. Ash and J. Knight. *Computable Structures and the Hyperarithmetical Hierarchy.* Elsevier Science, 2000.

[2] Harvey M. Friedman, Stephen G. Simpson, and Rick L. Smith. Countable algebra and set existence axioms. *Annals of Pure and Applied Logic*, 25(2):141–181, 1983.

[3] Carl G. Jockusch, Jr. and Robert I. Soare. Degrees of members of Π^0_1 classes. *Pacific J. Math.*, 40:605–616, 1972.

[4] Robert I. Soare. *Recursively enumerable sets and degrees*. Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1987. A study of computable functions and computably generated sets.
[5] A. M. Turing. On Computable Numbers, with an Application to the Entscheidungsproblem. *Proc. London Math. Soc.*, S2-42(1):230, 1936.

Department of Mathematics
University of California, Berkeley, USA
E-mail address: antonio@math.berkeley.edu
URL: http://www.math.berkeley.edu/~antonio/

XXIII Encuentro Rioplatense de Álgebra y Geometría Algebraica (2013)

Publicaciones Matemáticas del Uruguay
Volumen 15, Junio 2016, Páginas 19–33
S 0797-1443

GRUPOS HIPERBÓLICOS
NOTAS DEL CURSO PARA EL XXIII ERAG

JUAN ALONSO

Introducción

Estas notas acompañan el mini-curso "Grupos Hiperbólicos" del XXIII Encuentro Rioplatense de Algebra y Geometría. El curso consistirá en una rápida introducción a los aspectos básicos de los grupos hiperbólicos de Gromov.

El tema central de la *teoría geométrica de grupos* es estudiar un grupo a partir de la geometría de su grafo de Cayley, o más generalmente, de los espacios métricos en los que actúa. Una de las principales instancias donde se aplica esto son los grupos hiperbólicos de Gromov, que forman una clase amplia de grupos para los cuales hay una teoría rica, además de ser objeto de investigación actual. M. Gromov introdujo una definición de espacio métrico hiperbólico que captura las propiedades esenciales de la curvatura negativa en variedades Riemannianas. Un grupo será hiperbólico cuando su grafo de Cayley sea hiperbólico según Gromov. Lo sorprendente es que esta definición geométrica implica muchas propiedades algebraicas de estos grupos. De hecho, los grupos que cumplen alguna noción de "curvatura negativa" (hiperbolicidad de Gromov y análogas) son una de las clases de grupos más generales que tienen teoría interesante (la otra son los grupos promediables).

Comenzaremos hablando de los grafos de Cayley vistos como espacios métricos, e introduciremos las nociones fundamentales del curso: los espacios hiperbólicos de Gromov y las quasi-isometrías, que son las equivalencias naturales entre estos espacios. Luego veremos ejemplos de propiedades algebraicas que se obtienen de la geometría: la presentación finita y el problema de las palabras en grupos hiperbólicos. Para terminar hablaremos del borde al infinito de un grupo hiperbólico, que es una de las herramientas centrales para su estudio.

El objetivo del curso es de motivación. Necesariamente será muy incompleto y se omitirán la mayoría de las demostraciones. Para cubrir esto se incluyen varias referencias, que hacen un tratamiento más sistemático del tema. ([2] y [5] son las más generales acerca de espacios métricos de "curvatura negativa". [3] y [9] son notas cortas acerca de grupos hiperbólicos y [1] un survey acerca del borde al infinito).

1. Grafo de Cayley y la métrica de las palabras

Sea G un grupo finitamente generado y $S = \{s_1, \dots, s_n\}$ un generador de G. Entonces podemos escribir todo elemento de G como un producto de los elementos de S y sus inversos. Este producto lo podemos ver como una *palabra* donde las letras son los elementos s_i y s_i^{-1}, y la concatenación corresponde a la multiplicación en el grupo. Una palabra es *reducida* si no tiene una letra y su inversa en lugares consecutivos, es decir, no contiene a $s_i s_i^{-1}$ o $s_i^{-1} s_i$ como sub-palabras. Toda palabra

se puede *reducir*: hacer las cancelaciones siempre que aparezcan letras inversas consecutivas, hasta obtener una palabra reducida. Por lo tanto, todo elemento de G puede escribirse como una palabra reducida en las s_i y s_i^{-1} (en adelante: palabra reducida en S).

Un ejemplo importante de esto son los *grupos libres*. Dado $X = \{x_1, \dots, x_n\}$ un conjunto de n elementos formales, $\mathbb{F}_n = \mathbb{F}(X) = \langle x_1, \dots, x_n \rangle$ es el grupo formado por las palabras reducidas en las letras x_i y x_i^{-1}, donde la multiplicación es concatenar y reducir. Recibe el nombre de *grupo libre* en n generadores. El conjunto X se llama *base* de $\mathbb{F}_n$.

Si tengo una palabra reducida $w \in \mathbb{F}_n$, llamo $|w|$ a su largo (su cantidad de letras). Si G es un grupo con un generador $S = \{s_1, \dots, s_n\}$, llamo $w(s_1, \dots, s_n)$ al elemento de G obtenido sustituyendo a x_i por s_i en w. Esto es lo mismo que la imágen de w bajo el único morfismo $\mathbb{F}_n \to G$ que lleva cada x_i en s_i. Si $\gamma \in G$ cumple que $\gamma = w(s_1, \dots, s_n)$, se dice que la palabra reducida w representa a γ.

En general esta palabra no es única. De hecho, si vale unicidad para todo elemento entonces G es libre y S es una base (osea: $G \cong \mathbb{F}_n$ y el isomorfismo lleva S en la base X de $\mathbb{F}_n$).

Dado un grupo G con un generador $S = \{s_1, \dots, s_n\}$, defino el *largo* de $\gamma \in G$ respecto de S como

$$l_S(\gamma) = \text{mín}\{|w| : w \in \mathbb{F}_n, w(s_1, \dots, s_n) = \gamma\}$$

Es decir, el largo de la palabra más corta que expresa γ en el generador S. Esto permite definir una distancia en G como

$$d_S(\gamma_1, \gamma_2) = l_S(\gamma_1^{-1}\gamma_2)$$

Es fácil verificar que esto es efectivamente una métrica, y que es G-invariante a izquierda, es decir $d_S(\gamma\gamma_1, \gamma\gamma_2) = d_S(\gamma_1, \gamma_2)$. Se llama la *métrica de las palabras* de G respecto al generador S. Esto asocia al par (G, S) un espacio métrico (G, d_S) donde G actúa por isometrías.

Otra construcción estándar para un grupo G y un generador $S = \{s_1, \dots, s_n\}$ finito es su *grafo de Cayley* $\text{Cay}(G, S)$. Este grafo tiene como vértices a los elementos de G, y los ejes son los de la forma $(\gamma, \gamma s_i)$ para todo $\gamma \in G$ y $s_i \in S$. Observar que $\text{Cay}(G, S)$ es conexo (pues S genera a G), y cada vértice tiene valencia $2n$. Es un grafo orientado y cada arista está etiquetada por su correspondiente generador s_i. De cada vértice sale exactamente un eje para cada elemento de $S \cup S^{-1}$, donde el eje asociado a s_j^{-1} es el eje con etiqueta s_j que llega a dicho vértice.

Todo grafo tiene una métrica natural, en la cual los ejes miden 1. Esta métrica se obtiene así: cada eje será isometrico al intervalo $[0, 1]$. Se define la longitud de un camino formado por trozos de ejes sumando las longitudes de cada uno de los trozos. La distancia entre dos puntos es el ínfimo de las longitudes de los caminos que los conectan (que es en realidad un mínimo). A los efectos de la métrica, me olvido de la orientación y las etiquetas de las aristas.

Notar que G actúa por multiplicación a izquierda en $\text{Cay}(G, S)$, por automorfismos de grafo (a diferencia de la multiplicación a derecha, que puede no respetar los ejes). Por lo tanto G también actúa por isometrías de $\text{Cay}(G, S)$.

Si restrinjo la métrica de $\text{Cay}(G, S)$ a los vértices (a G) obtengo d_S, la métrica de las palabras. Esto se ve notando que cada palabra w en S especifica un camino de ejes en $\text{Cay}(G, S)$, que empieza en 1 y sigue los ejes correspondientes a las letras que aparecen en w (en orden), llegando al vértice $w(s_1, \dots, s_n)$.

La principal ventaja del grafo de Cayley sobre (G, d_S) es ser conexo por caminos, lo que va a simplificar nuestra exposición, además de proporcionar una mejor visualización.

Ejemplos:

1. $G = \mathbb{Z}$, $S = \{1\}$. Es claro que $\mathrm{Cay}(G, S)$ es isométrico a $\mathbb{R}$ y G actúa por translaciones.
2. $G = \mathbb{F}_2 = \langle a, b\rangle$, $S = \{a, b\}$. Entonces $\mathrm{Cay}(G, S)$ es un árbol, donde cada vértice tiene valencia 4. El camino (inyectivo) de la identidad a $w \in \mathbb{F}_n$ es único y corresponde a la propia palabra w. Queda $l_S(w) = |w|$.

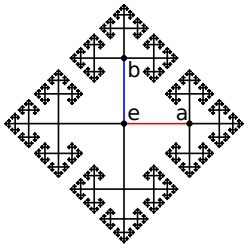


FIGURA 1. Grafo de Cayley de $\mathbb{F}_2$ respecto a una base (Imágen de Wikipedia)

3. $G = \mathbb{Z}^2$, $S = \{(1, 0), (0, 1)\}$. El grafo $\mathrm{Cay}(G, S)$ es un cuadriculado en el plano, donde la métrica corresponde a la norma de la suma en $\mathbb{R}^2$.

2. Espacios hiperbólicos de Gromov

Sea (X, d) un espacio métrico. Una *geodésica* en X es una inmersión isométrica $\alpha : [a, b] \to X$. Esto es decir que se cumple

$$d(\alpha(s), \alpha(t)) = |s - t|$$

También puedo definir geodésicas con dominio en una semirrecta (*rayo geodésico*) o la recta entera.

Digo que el espacio métrico (X, d) es *geodésico* si existen geodésicas entre cualquier par de puntos de X. O sea, dados $x, y \in X$, existe una geodésica $\alpha : [0, L] \to X$ con $L = d(x, y)$, $\alpha(0) = x$ y $\alpha(L) = y$. A una tal geodésica la anoto $[x, y]$, aunque no siempre es única.

Un *triángulo geodésico* (de vértices x, y, z) es una unión de geodésicas de la forma

$$\Delta = \Delta(x, y, z) = [x, y] \cup [y, z] \cup [z, x]$$

Para $\delta \geq 0$, decimos que Δ es δ-*flaco* si cada lado está contenido en el δ-entorno de los otros dos.

Un espacio métrico geodésico es δ-*hiperbólico* si todo triángulo geodésico en X es δ-flaco. Lo que va a importarnos es la existencia de la constante δ, más que su valor. Así, un espacio es *hiperbólico* (según Gromov) si es δ-hiperbólico para algún $\delta \geq 0$. (Existen otras definiciones de δ-hiperbólico que sirven para espacios no geodésicos, pero la definición que presentamos es más simple e intuitiva).

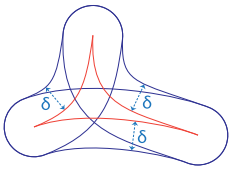


FIGURA 2. Un triángulo δ-flaco (Imágen de Wikipedia)

Ejemplos:

1. Si X es de diámetro finito, entonces es δ-hiperbólico con $\delta = \operatorname{diam}(X)$.
2. Si X es un árbol (un grafo sin circuitos), entonces es 0-hiperbólico. En este caso la geodésica $[x, y]$ entre dos puntos $x, y \in X$ es única, y todo camino inyectivo ente x e y es una reparametrización de dicha geodésica. Notar que todo triángulo es un trípode.
3. El *plano hiperbólico* (usando el modelo del semiplano superior) es
$$\mathbb{H}^2 = \{(x, y) \in \mathbb{R}^2 : y > 0\} = \{z \in \mathbb{C} : \operatorname{Im}(z) > 0\}$$
con la métrica Riemanniana $g = \frac{dx^2+dy^2}{y^2}$. Valen las siguientes propiedades:
   - Las isometrías de $\mathbb{H}$ que preservan la orientación son transformaciones de Möbius. Más aún:
$$\operatorname{Isom}^+(\mathbb{H}^2) = \left\{ \frac{az+b}{cz+d} : a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\} \cong PSL(2, \mathbb{R})$$
Este grupo actúa transitivamente en $\mathbb{H}^2$ (y en su fibrado tangente unitario $T^1\mathbb{H}^2$).
   - Las geodésicas de $(\mathbb{H}^2, g)$ son las rectas y circunferencias ortogonales a $\mathbb{R}$ (parametrizadas por longitud de arco). Estas geodésicas son bi-infinitas (por ejemplo $d_g(ia, ib) = |\log(b/a)|$ para $a, b > 0$). En particular $\mathbb{H}^2$ no es de diámetro finito.
   - La forma de área de g queda $d\text{Area}_g = \frac{dxdy}{y^2}$. El área de un disco de radio (hiperbólico) r es $\text{Area}_g(D_g(r)) = 2\pi(\cosh r - 1)$. En particular $\mathbb{H}^2$ no es de área finita.
   - Todo triángulo Δ tiene $\text{Area}_g(\Delta) \leq \pi$. Esto permite demostrar que es 2-flaco. Por lo tanto $\mathbb{H}^2$ es 2-hiperbólico. (2 no es el δ óptimo, pero esto no va a importarnos).
4. Se define el n-espacio hiperbólico como $\mathbb{H}^n = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : x_n > 0\}$, $g = \frac{dx_1^2+\cdots+dx_n^2}{x_n^2}$. Valen propiedades análogas a las de $\mathbb{H}^2$, en particular también es 2-hiperbólico.
5. Un ejemplo de un espacio que no es hiperbólico es el plano Euclídeo $\mathbb{R}^2$ (o más generalmente $\mathbb{R}^n$, con $n > 1$). Para cualquier $\delta \geq 0$ tenemos triángulos que no son δ-flacos.

Los ejemplos 3 y 4 son las geometrías hiperbólicas clásicas. Son variedades Riemannianas de curvatura constante negativa, simplemente conexas. La geometría hiperbólica de Gromov es un intento (uno de los más exitosos) por abstraer la curvatura negativa para espacios métricos generales.

El ejemplo 1 muestra que la geomertía hiperbólica de Gromov es una propiedad que sólo se ve a grán escala (mayor que δ), es decir, que no impone condiciones "locales" (a escala menor que δ). Esto contrasta bastante con la curvatura negativa en variedades Riemannianas, pero en algunas situaciones esto será ventajoso. Existen otras nociones de "curvatura negativa" para espacios métricos (como la propiedad $CAT(-1)$) que son también interesantes, pero no las trataremos aqui.

Existen también varias definiciones equivalentes de hiperbolicidad de Gromov. Hemos enunciado la más directa, a travéz de los triángulos δ-flacos, y no mencionaremos más que una alternativa. Esta es la que necesitaremos para probar la presentación finita de los grupos hiperbólicos, y es a travéz de los triángulos *δ-finos* que defino a continuación.

Sean (X, d) un espacio métrico geodésico y $\Delta = \Delta(x, y, z)$ un triángulo geodésico en X. Armo un triángulo $\bar{\Delta} = \Delta(\bar{x}, \bar{y}, \bar{z})$ en el plano Euclídeo, con los lados del mismo largo que los respectivos de Δ (esto es un *triángulo de comparación Euclídeo*). Tenemos una biyección $f : \Delta \to \bar{\Delta}$ que es isometría restricta a cada lado de Δ (recordando que $\Delta = [x, y] \cup [y, z] \cup [z, x]$). Luego tomo $\bar{p}_x$, $\bar{p}_y$, $\bar{p}_z$ los puntos de intersección de la circunferencia inscripta a $\bar{\Delta}$ con los respectivos lados $[\bar{y}, \bar{z}]$, $[\bar{x}, \bar{z}]$, $[\bar{x}, \bar{y}]$. Sean p_x, p_y, p_z sus pre-imágenes por f. Observar que $d(x, p_y) = d(x, p_z)$, $d(y, p_x) = d(y, p_z)$ y $d(z, p_x) = d(z, p_y)$.

Sea T_Δ el trípode obtenido de Δ identificando los lados $[x, p_y]$ con $[x, p_z]$, $[y, p_x]$ con $[y, p_z]$ y $[z, p_x]$ con $[z, p_y]$. Notar que p_x, p_z y p_y van a un sólo punto p. Sea $\tau_\Delta : \Delta \to T_\Delta$ el mapa cociente. (Ver figura).

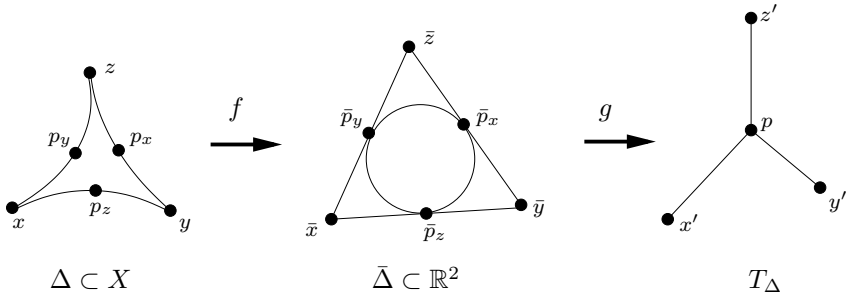


FIGURA 3. La construcción de $\tau_\Delta : \Delta \to T_\Delta$. Aquí tenemos $\tau_\Delta = g \circ f$, donde g es la misma identificación que describimos pero para $\bar{\Delta}$.

Para $\delta \geq 0$, decimos que el triángulo geodésico Δ es *δ-fino* si para todo $q \in T_\Delta$ tenemos $\operatorname{diam}(\tau^{-1}(q)) \leq \delta$.

Proposición 1. *El espacio métrico geodésico (X, d) es δ-hiperbólico si y sólo si todo triángulo geodésico en X es 6δ-fino.*

3. Quasi-Isometrías

En la sección 1 asociamos a un grupo G con un generador finito S una métrica d_S en G y un espacio métrico geodésico $\operatorname{Cay}(G, S)$, donde G actúa por isometrías. Tanto d_S como $\operatorname{Cay}(G, S)$ dependen fuertemente del generador S:

Ejemplo: $G = \mathbb{Z}$.

1. Si $S_1 = \{1\}$, entonces $\Gamma_1 = \mathrm{Cay}(\mathbb{Z}, S_1)$ es isométrico a $\mathbb{R}$.
2. Si $S_2 = \{2, 3\}$ entonces $\Gamma_2 = \mathrm{Cay}(\mathbb{Z}, S_2)$ es un grafo con circuitos, y es claro que la métrica es distinta de la anterior.

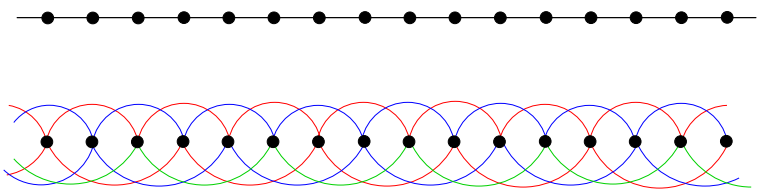


FIGURA 4. Los dos grafos de Cayley de $\mathbb{Z}$ del ejemplo.
Arriba: Para $S_1 = \{1\}$.
Abajo: Para $S_2 = \{2, 3\}$. Los ejes superiores corresponden al generador 2 y los inferiores al 3. Los colores son sólo para facilitar la visualización.

Sin embargo, los grafos Γ_1 y Γ_2 del ejemplo se parecen cuando son vistos a grán escala (ver figura 4). Hay una relación natural entre las distintas métricas de palabras y grafos de Cayley asociados a un mismo grupo (variando el generador). Esta es la *quasi-isometría*.

Definición 2. *Sean X, Y espacios métricos, $\lambda \geq 1, \epsilon \geq 0$. Una función $f : X \to Y$ es una* (λ, ϵ)–quasi-isometría *si cumple:*

1. *(f es una inmersión (λ, ϵ)–quasi-isométrica.)*
$$\frac{1}{\lambda} d_X(x, y) - \epsilon \leq d_Y(f(x), f(y)) \leq \lambda d_X(x, y) + \epsilon \,.$$
2. *(La imágen de f es ϵ–densa.) Para todo $y \in Y$ existe $x \in X$ con*
$$d_Y(y, f(x)) \leq \epsilon \,.$$

Una función es una *quasi-isometría* cuando es una (λ, ϵ)–quasi-isometría para algunos $\lambda \geq 1$, $\epsilon \geq 0$. Nuevamente, el valor de los parámetros va a tener un rol secundario, lo importante es su existencia. Dos espacios métricos X e Y son *quasi-isométricos* cuando existe $f : X \to Y$ quasi-isometría. Lo anotaremos $X \sim_{q.i.} Y$.

Valen las siguientes propiedades, de demostración simple:

- La relación de quasi-isometría entre espacios métricos es de equivalencia.
- (G, d_S) es quasi-isométrico a $\mathrm{Cay}(G, S)$: la inclusión es una $(1, 1)$–quasi-isometría.
- Si S, S' son dos generadores finitos de un grupo G, entonces $\mathrm{Id} : (G, d_S) \to (G, d_{S'})$ es una quasi–isometría con
$$\lambda = \max\{l_S(s'), l_{S'}(s) : s \in S, s' \in S'\} \qquad \epsilon = 0$$
- También $\mathrm{Cay}(G, S)$ es quasi-isométrico a $\mathrm{Cay}(G, S')$ (por transitividad).
- Un automorfismo $\varphi \in \mathrm{Aut}(G)$ es una quasi-isometría de (G, d_S).

Se dice que dos grupos finitamente generados G_1 y G_2 son *quasi-isométricos* ($G_1 \sim_{q.i.} G_2$) si sus grafos de Cayley lo son, es decir: $\mathrm{Cay}(G_1, S_1) \sim_{q.i.} \mathrm{Cay}(G_2, S_2)$ para S_1, S_2 generadores finitos de los respectivos grupos. En vista de lo anterior, esto no depende de los generadores elegidos.

La quasi-isometría entre grupos es una relación más débil que el isomorfismo, como se ve a continuación.

Ejemplo: Si X es de diámetro finito, entonces es quasi-isométrico a un punto (con $\lambda = 1$, $\epsilon = \operatorname{diam}(X)$). Entonces todo grupo finito es quasi-isométrico al grupo trivial.

Vemos entonces que la quasi-isometría no nos dice cuando dos grafos de Cayley (como espacios métricos) corresponden al mismo grupo. Sin embargo, esto puede ser ventajoso cuando nos permite estudiar propiedades de los grupos infinitos "a grán escala", con cierta independencia de la teoría (y problemas) de los grupos finitos.

Más aún, vale que si H es un subgrupo de índice finito de G entonces $H \sim_{q.i.} G$.

Ejemplo: $G = \mathbb{F}_2 = \langle a, b\rangle$, y sea $H = \langle a, b^2, bab^{-1}\rangle \leq \mathbb{F}_2$. Entonces $H \cong \mathbb{F}_3$ y de índice finito en G. Entonces $\mathbb{F}_2 \sim_{q.i.} F_3$.

En realidad es cierto que $\mathbb{F}_2 \sim_{q.i.} F_n$ para todo $n > 1$. Esto es porque todo $\mathbb{F}_n$ con $n > 1$ puede incluirse como subgrupo de índice finito en F_2.

Estos son ejemplos de *isomorfismo virtual*, que es la equivalencia entre grupos generada por el isomorfismo y tomar subgrupos de índice finito. Esta es otra relación importante entre grupos, tal vez la más natural que corresponda a "pasar al cociente" a los grupos finitos. Tenemos entonces que el isomorfismo virtual implica la quasi-isometría.

Problema 1. *Es cierto que si $G_1 \sim_{q.i.} G_2$, entonces G_1 es virtualmente isomorfo a G_2?*

En general, la respuesta es no. Pero se puede obtener una respuesta afirmativa si nos restringimos a ciertas clases de grupos. Si el problema tiene respuesta afirmativa cuando fijamos $G_1 = G$, decimos que G satisface *rigidez quasi-isométrica*. Más adelante hablaremos un poco más sobre este tema.

La herramienta fundamental para trabajar con la quasi-isometría es el *Lema de Svarc–Milnor* a continuación. Un espacio métrico es *propio* cuando toda bola cerrada es compacta (ej: grafos de valencia finita, como $\operatorname{Cay}(G, S)$ con S finito).

Teorema 3 (Svarc–Milnor)**.** *Sea (X, d) un espacio métrico geodésico y propio, G un grupo y $G \curvearrowright X$ una acción que cumple:*

1. *Es por isometrías ($d(\gamma \cdot x, \gamma \cdot y) = d(x, y)$).*
2. *Es* propiamente discontinua*, es decir, las órbitas de la acción no acumulan en X.*
3. *Es* cocompacta*, osea que X/G es compacto.*

Entonces vale lo siguiente:

a) *G es finitamente generado.*
b) *Si S es un generador finito de G y $x_0 \in X$, entonces el mapa $(G, d_S) \to (X, d)$ que manda $\gamma \mapsto \gamma \cdot x_0$ es una quasi-isometría.*

Una acción que cumple las hipótesis de este teorema se llama *geométrica*. Por transitividad, la tesis implica que también $\operatorname{Cay}(G, S) \sim_{q.i.} (X, d)$.

Este teorema permite probar que si G es finitamente generado y $H \leq G$ es un subgrupo de índice finito, entonces $H \sim_{q.i.} G$ (y es finitamente generado). Aquí $X = \operatorname{Cay}(G, S)$ para un generador finito S de G. Es claro que H actúa

en X por isometrías y es propiamente discontinuo (restringiendo la acción de G). Es cocompacto, porque H es de índice finito. (Observar que $\mathrm{Cay}(G,S)/H$ es un grafo de valencia finita cuyo conjunto de vértices es G/H).

Ejemplo: $\mathbb{Z}^2$ actúa en el plano Euclídeo R^2 por translaciones. Esta es una acción geométrica ($\mathbb{R}^2/\mathbb{Z}^2$ es un toro). Entonces $\mathrm{Cay}(\mathbb{Z}^2,S)$ (respecto a cualquier generador S) es quasi-isométrico a $\mathbb{R}^2$ con la métrica usual (Euclídea).

La geometría hiperbólica de Gromov tiene la virtud de preservarse por quasi-isometrías.

Teorema 4. *Si X es un espacio δ-hiperbólico e Y es geodésico con $X \sim_{q.i.} Y$, entonces Y es δ'-hiperbólico (para algún δ').*

4. Grupos hiperbólicos

Un grupo G finitamente generado es *hiperbólico (según Gromov)* si $\mathrm{Cay}(G,S)$ es hiperbólico para un generador finito S de G. Por el teorema 4, esto no depende del generador S elegido. También implica que es una propiedad cerrada respecto de la quasi-isometría de grupos. Veamos los ejemplos más básicos:

1. Todo grupo finito es hiperbólico. (Sin embargo, la teoría no aportará nada nuevo a este caso).
2. Los grupos libres, $\mathbb{Z}$ y $\mathbb{F}_n$ para $n > 2$, son hiperbólicos. Observar que los grafos de Cayley respecto de una base son árboles (0-hiperbólicos).
3. Por el contrario, $\mathbb{Z}^n$ para $n > 1$ no son hiperbólicos.
4. Si G_1 y G_2 son grupos hiperbólicos, entonces también lo es su producto libre $G_1 * G_2$. (Puede obtenerse directamente a partir de las definiciones).
5. Un *grupo Fuchsiano* es un subgrupo $\Gamma \leq PSL(2,\mathbb{R})$ discreto, sin torsión, y con $\mathbb{H}^2/\Gamma$ compacto. Tenemos lo siguiente:
   - $\mathbb{H}^2/\Gamma$ es homeomorfo a una superficie orientable S_g, de género $g > 1$.
   - $\Gamma \cong \langle a_1,\dots,a_g,b_1,\dots,b_g | [a_1,b_1]\cdots[a_g,b_g] = 1\rangle$. (Para ver esto es necesario conocer el *grupo fundamental* de Topología Algebraica).
   - La acción de Γ en $\mathbb{H}^2$ es geométrica, por "translaciones" del plano hiperbólico, y preserva un embaldosado de $\mathbb{H}^2$. Puede verse que:
     - Las baldosas son polígonos de $4g$ lados, y el cociente $\mathbb{H}^2/\Gamma \cong S_g$ puede obtenerse identificando lados "opuestos" en una baldosa.
     - Un grafo de Cayley de Γ (que corresponde a la presentación de arriba) es el grafo dual a este embaldosado.
   - Γ es quasi-isométrico al plano hiperbólico (Svarc–Milnor). Por lo tanto Γ es un grupo hiperbólico.

   Existen infinitos grupos en esta clase, para cada $g > 1$. Claramente son todos quasi-isométricos. También son virtualmente isomorfos (Puede verse usando *espacios de cubrimiento*).
6. También se obtienen grupos hiperbólicos como subgrupos discretos cocompactos de $\mathrm{Isom}^+(\mathbb{H}^n)$ con $n > 1$. Si $n = 3$ y no hay torsión se denominan *grupos Kleinianos.* Los grupos Kleinianos proporcionan ejemplos de grupos que son quasi-isométricos pero no virtualmente isomorfos (usando la teoría de 3-variedades hiperbólicas de Thurston).

Además de estos ejemplos, la clase de grupos hiperbólicos es abundante. Ciertas presentaciones, llamadas de *cancelación pequeña*, dan origen a grupos hiperbólicos.

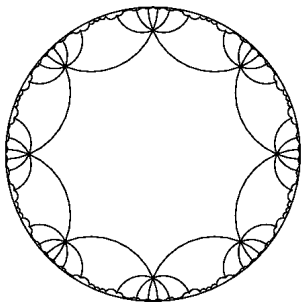


FIGURA 5. Un embaldosado del plano hiperbólico, usando el modelo del disco de Poincaré. En éste caso el cociente es el *bitoro*, la superficie orientable de género 2. (Imágen de D. Van der Werf, `http://www.geom.uiuc.edu/apps/teich-nav`)

Gromov también mostró que tomando una presentación al azar (respecto a una medida de conteo sobre las presentaciones de tamaño menor que un $N > 0$), la probabilidad de que defina un grupo hiperbólico es alta, y tiende a 1 con $N \to +\infty$.

5. Presentación finita y problema de las palabras

Recordemos que si S es un conjunto, $\mathbb{F}(S)$ es el grupo libre de base S, es decir, las palabras reducidas cuyas letras son elementos de S o sus inversos formales, con el producto de concatenación y reducción. Si $R \subset \mathbb{F}(S)$, denotamos $\langle\langle R \rangle\rangle$ al subgrupo normal de $\mathbb{F}(S)$ generado por R. Usaremos la notación

$$\langle S|R\rangle = F(S)/\langle\langle R\rangle\rangle$$

Una *presentación* de un grupo G es un isomorfismo $G \cong \langle S|R\rangle$ para algún conjunto S y $R \subset \mathbb{F}(S)$. Decimos que G es *finitamente presentado* si existe una presentación de G con S y R finitos.

Cuando G es finitamente generado, puedo elegir $S = \{s_1, \ldots, s_n\}$ finito, e identifico $\mathbb{F}(S)$ con $\mathbb{F}_n$. La siguiente es una observación básica, pero es útil enunciarla explícitamente.

Observación 1. *Sean $G = \langle s_1, \ldots, s_n|R\rangle$ y $w \in \mathbb{F}_n$. Entonces las siguientes son equivalentes:*

1. $w(s_1, \ldots, s_n) = 1$ *(w representa la identidad en G).*
2. $w \in \langle\langle R\rangle\rangle$.
3. $w = \Pi_{j=1}^{k} w_j r_j w_j^{-1}$ *con $k \geq 0$, $w_j \in \mathbb{F}_n$ y $r_j \in R$.*

Los grupos hiperbólicos son finitamente generados por definición. Mostraremos que además son finitamente presentados. Esta prueba tiene el interés de obtener una propiedad algebraica (presentación finita) a partir de una propiedad geométrica del grafo de Cayley (hiperbolicidad de Gromov). Esta situación es frecuente, y el ejemplo que mostramos es una de sus instancias más básicas, aunque sigue siendo ilustrativa.

Teorema 5. *Todo grupo hiperbólico es finitamente presentado.*

Demostración:

Sea G un grupo hiperbólico. Tomo $S = \{s_1, \dots, s_n\}$ un generador finito de G tal que $\mathrm{Cay}(G, S)$ es δ-hiperbólico. Sea

$$N = \{w \in \mathbb{F}_n : w(s_1, \dots, s_n) = 1\}$$

que es el núcleo del morfismo canónico $\mathbb{F}_n = \mathbb{F}(S) \to G$ (osea que $G \cong \mathbb{F}_n/N$). Considero

$$R = \{w \in N : |w| \leq 24\delta\}$$

Claramente R es finito. El objetivo será probar que $N = \langle\langle R \rangle\rangle$, lo que implica el teorema. Para esto supondré que $\delta > 1$ (es trivial que la δ-hiperbolicidad implica la δ'-hiperbolicidad para todo $\delta' \geq \delta$).

Como las aristas de $\mathrm{Cay}(G, S)$ están etiquetadas por los elementos de S y orientadas, resulta que un vértice de inicio y una palabra $w \in \mathbb{F}_n = \mathbb{F}(S)$ determinan un camino de ejes en $\mathrm{Cay}(G, S)$. Este camino empieza en el vértice de inicio dado, y se obtiene concatenando sucesivamente los ejes cuyas etiquetas aparecen en w. (Entendiendose que s_j^{-1} representa el eje de etiqueta s_j, recorrido en sentido inverso a su orientación). Durante esta prueba vamos a identificar palabras con caminos de ejes cuando el vértice de inicio sea evidente.

Tomo $w = a_1 \cdots a_k \in N$, donde $a_j \in S \cup S^{-1}$. Entonces w representa un circuito cerrado en $\mathrm{Cay}(G, S)$ que empieza y termina en 1. Para $j = 0, \dots, k$, considero las palabras $w_j = a_1 \cdots a_j$ y los elementos $\gamma_j = w_j(s_1, \dots, s_n) \in G$. (Observar que $\gamma_0 = \gamma_k = 1$).

Sean $\sigma_j = [1, \gamma_j]$ geodésicas en $\mathrm{Cay}(G, S)$. Claramente se puede suponer que son caminos de ejes, pues empiezan y terminan en vérices de $\mathrm{Cay}(G, S)$. Haciendo abuso de notación, también llamaré σ_j a las palabras que representan estos caminos.

Notar que $\sigma_0 = \sigma_k = 1$, y que tenemos

$$w = \prod_{j=1}^{k} \sigma_{j-1} a_j \sigma_j^{-1}$$

donde $\sigma_{j-1} a_j \sigma_j^{-1} \in N$ y define un triángulo geodésico Δ_j en $\mathrm{Cay}(G, S)$ (de vértices 1, γ_{j-1} y γ_j y lados σ_{j-1}, σ_j y el camino de γ_{j-1} a γ_j representado por a_j). Esto corresponde a subdividir el circuito $w = a_1 \cdots a_k$ en triángulos.

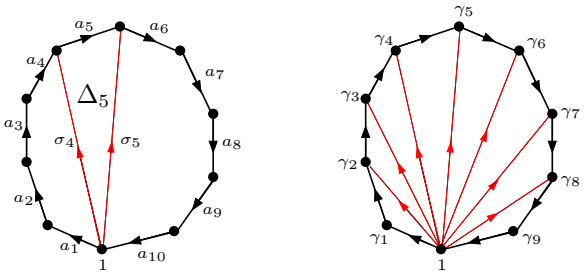


FIGURA 6. **Izquierda:** Ejemplo con $k = 10$ del circuito definido por $w = a_1 \cdots a_{10}$ en $\mathrm{Cay}(G, S)$, y de uno de los triángulos Δ_j. **Derecha:** Subdivisión de dicho circuito en triángulos, a través de los caminos σ_j.

Ahora usaremos la δ-hiperbolicidad. Por la proposición 1, cada triángulo Δ_j es 6δ-fino. Por esto puedo subdividir Δ_j en circuitos de largo a lo sumo 24δ como sigue: Tomo puntos en los lados σ_{j-1} y σ_j a partir de 1 y espaciados regularmente a 6δ. Como Δ_j es 6δ-fino, puedo conectar los puntos correspondientes por caminos de largo a lo más 6δ. (Es claro que la cota no es óptima. Tiene la ventaja, puramente visual, de que los circuitos no degeneran).

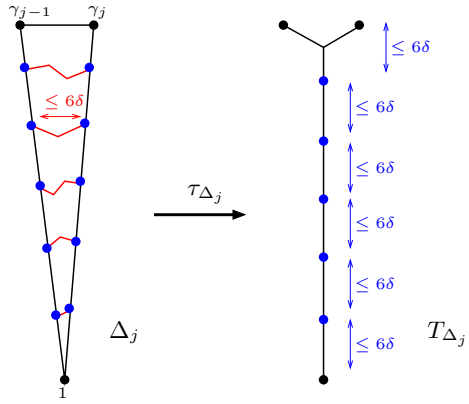


FIGURA 7. Subdivisión de Δ_j en circuitos de longitud $\leq 24\delta$.

Sean $r_{j,l}$, con $l = 1, \ldots, L_j$ palabras que representen estos circuitos. Entonces podemos escribir

$$\sigma_{j-1} a_j \sigma_j^{-1} = \prod_{l=1}^{L_j} v_{j,l} r_{j,l} v_{j,l}^{-1}$$

para elementos $v_{j,l} \in \mathbb{F}_n$ convenientemente elegidos.

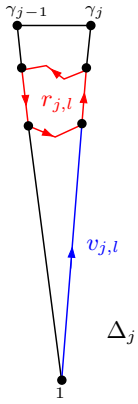


FIGURA 8. Un ejemplo genérico de los caminos en $\mathrm{Cay}(G, S)$ que definen los elementos $r_{j,l}$ y $v_{j,l}$.

Como $|r_{j,l}| \leq 24\delta$, tenemos que $\sigma_{j-1} a_j \sigma_j^{-1} \in \langle\langle R \rangle\rangle$ para cada j, y por esto $w \in \langle\langle R \rangle\rangle$.

Esto muestra que $N \subseteq \langle\langle R \rangle\rangle$, y la otra inclusión es trivial. □

Ahora hablaremos del *problema de las palabras*, que es uno de los problemas clásicos en la teoría de grupos infinitos, finitamente presentados. Sea G un grupo cualquiera (finitamente presentado) dado por la presentación $\langle s_1, \dots, s_n | r_1, \dots, r_p \rangle$. Resolver el *problema de las palabras* para G es obtener un algoritmo que pueda decidir (en tiempo finito) si una palabra $w \in \mathbb{F}_n$ representa la identidad en G. Osea, decidir si $w \in \langle\langle r_1, \dots, r_p \rangle\rangle$.

El problema de las palabras es equivalente a decidir la igualdad en G, osea, decidir si dos palabras $v, w \in \mathbb{F}_n$ representan el mismo elemento en G. Esto se reduce al problema de las palabras aplicado a wv^{-1}. No es posible resolver el problema en general. De hecho, hay ejemplos de grupos donde se puede probar que no existe un algoritmo para resolver el problema de las palabras. Sin embargo, sí se puede resolver para grupos hiperbólicos.

La prueba del teorema 5 permite construir un algoritmo para resolver el problema de las palabras en un grupo hiperbólico. Sea G es un grupo hiperbólico y $\langle s_1, \dots, s_n | r_1, \dots, r_p \rangle$ una presentación de G. Recordemos que en la prueba de 5 escribimos cualquier $w \in \langle\langle r_1, \dots, r_p \rangle\rangle$ de largo $|w| = k$ como

$$w = \prod_{j=1}^{k} \prod_{l=1}^{L_j} v_{l,j} r_{l,j} v_{l,j}^{-1} \tag{E1}$$

donde $r_{l,j} \in \{r_1, \dots, r_p\}$, $v_{j,l} \in \mathbb{F}_n$. Observar que los caminos σ_j de la prueba son geodésicas entre 1 y los vértices del circuito definido por w, por lo que deben tener largo menor a k. Repasando la prueba de 5 podemos ver que $L_j \leq |\sigma_j| \leq k$ y $|v_{j,l}| \leq |\sigma_j| \leq k$. En conclusión, el número de factores en la descomposición E1 de w está acotado por k^2 y el largo de los elementos que conjugan está acotado por k.

Si queremos saber si $w \in \mathbb{F}_n$ está en $\langle\langle r_1, \dots, r_p \rangle\rangle$, basta hacer una lista con todas las palabras de la forma

$$\prod_{i=1}^{m} v_i r_{j_i} v_i^{-1}$$

con $m \leq |w|^2$, $|v_i| \leq |w|$, y ver si w está en esta lista. Como la lista es finita (para cada $w \in \mathbb{F}_n$), esto nos dá un algoritmo que decide si w está o no en $\langle\langle r_1, \dots, r_p \rangle\rangle$.

El algoritmo que vimos no es el más eficiente. Sin embargo, ilustra la obstrucción para resolver el problema de las palabras en grupos más generales, que es acotar el número de factores en una descomposición como en E1. Existen métodos más elegantes y eficientes que son específicos a los grupos hiperbólicos (ver [2]).

6. Borde al infinito

El *borde al infinito* es una de las herramientas más útiles para trabajar con grupos y espacios hiperbólicos de Gromov. Si (X, d) es un espacio métrico δ-hiperbólico, defino

$$\partial X = \{r : [0, +\infty) \to X \text{ rayo geodésico}\} / \sim$$

donde dos rayos geodésicos son equivalentes si están a distancia de Hausdorff finita. Es decir, $r_1 \sim r_2$ si existe $K \geq 0$ tal que para todo $t \geq 0$ existe $t' \geq 0$ con $d(r_1(t), r_2(t')) \leq K$ y existe $t'' \geq 0$ con $d(r_1(t''), r_2(t)) \leq K$.

Observar que si r_1 es un rayo geodésico, y $r_2(t) = r_1(t + L)$ ($L \in \mathbb{R}$ cualquiera) entonces $r_1 \sim r_2$. Esto se llama *reparametrizar* el rayo geodésico r_1.

Ejemplos:

1. Si $\operatorname{diam}(X) < \infty$ entonces $\partial X = \emptyset$. (No hay rayos geodésicos).
2. Si X es un árbol, dos rayos geodésicos son equivalentes si y sólo si tienen reparametrizados que cooinciden eventualmente. Por ejemplo, si $X = \mathbb{R}$ es una línea, podemos identificar su borde con un par de puntos: $\partial\mathbb{R} = \{-\infty, +\infty\}$.
3. En $\mathbb{H}^2$ todo rayo geodésico converge a un punto de $\mathbb{R} \cup \{\infty\}$. Puede verse que $r_1 \sim r_2$ si y sólo si $\lim_{t\to+\infty} r_1(t) = \lim_{t\to+\infty} r_2(t)$ en $\mathbb{R}\cup\{\infty\}$. Por esto podemos identificar $\partial\mathbb{H}^2$ con $\mathbb{R} \cup \{\infty\}$.
4. Lo mismo vale para $\mathbb{H}^n$, identificando $\partial\mathbb{H}^n$ con $\mathbb{R}^{n-1} \cup \{\infty\}$.

El borde al infinito de un espacio métrico hiperbólico es un espacio topológico, con una topología natural que definiremos a continuación. En los ejemplos anteriores esta topología es la intuitiva, así que tendremos que $\partial\mathbb{R} = \{-\infty, +\infty\}$ y $\partial\mathbb{H}^n = S^{n-1} = \mathbb{R}^{n-1} \cup \{\infty\}$.

Si X es δ-hiperbólico y $x \in X$ es un punto base, podemos restringir la definición anterior para rayos geodésicos que empiezen en x. Sea

$$\partial_x X = \{r : [0, +\infty) \to X \text{ rayo geodésico con } r(0) = x\}/\sim$$

con la misma relación $\sim$ anterior. Puede probarse que el mapa natural $\partial_x X \to \partial X$ es biyectivo.

Si $y, z \in X$ su *producto de Gromov* respecto al punto base x es

$$(y|z)_x = \frac{1}{2}(d(x, y) + d(x, z) - d(y, z))$$

La idea intuitiva es que $(x|y)_x$ mide la distancia a partir de la cual dos geodésicas $[x, y]$ y $[x, z]$ comienzan a separarse a grán escala respecto de δ. Más precisamente, si $\Delta = \Delta(x, y, z)$ es un triángulo geodésico fino, y $\tau_\Delta : \Delta \to T_\Delta$ es el mapa cociente sobre el trípode correspondiente, entonces $(x|y)_x$ aproxima la distancia entre $x' = \tau_\Delta(x)$ y el centro del trípode T_Δ. Es fácil ver que cooinciden en el caso en que X es un árbol.

Observación 2. *Puede probarse que un espacio geodésico X es δ-hiperbólico si y sólo si para todo $x, y, z, w \in X$ se cumple*

$$(y|z)_x \geq \min\{(y|w)_x, (z|w)_x\} - \delta$$

Esta desigualdad permite dar una definición de δ-hiperbolicidad para espacios no necesariamente geodésicos. No tomamos este camino por ser menos intuitivo.

El producto de Gromov puede extenderse para rayos geodésicos que empiezan en x tomando límite. Puede verse que este límite sólo depende de las clases en $\partial_x X$ de los rayos geodésicos. Entonces, para $\zeta, \eta \in \partial_x X$ tomo rayos geodésicos r_1 y r_2 que los representan (respectivamente) y defino

$$(\zeta|\eta)_x = \lim_{t\to+\infty} (r_1(t)|r_2(t))_x$$

Este producto de Gromov también expresa la distancia a partir de la cual los rayos geodésicos comienzan a separarse apreciablemente. Por esto consideramos que dos rayos están cerca si su producto de Gromov es grande. Más formalmente, definimos una base de entornos de $\zeta \in \partial_x X$ como

$$V_\zeta(R) = \{\eta \in \partial_x X : e^{-(\zeta|\eta)_x} < R\}$$

para $R > 0$. Esto dá una topología en $\partial_x X$. Si X es propio (bolas cerradas compactas), puede probarse que no depende del punto base $x \in X$.

Ejemplos:

1. $\partial\mathbb{R} = \{-\infty, \infty\}$ son dos puntos discretos.
2. Sea $X = \mathrm{Cay}(\mathbb{F}_n, S)$ donde $n > 1$ y S es una base de $\mathbb{F}_n$. Entonces X es un árbol infinito, de valencia $2n$. Si $x \in X$ es un punto base y $\zeta, \eta \in \partial_x X$, entonces los rayos geodésicos empezando en x que representan a ζ y η son únicos, y $(\zeta|\eta)_x$ es la longitud del segmento común entre los dos. No es difícil ver que ∂X es un conjunto de Cantor.
3. Para $X = \mathbb{H}^n$ también se cumple que para cada $\zeta \in \partial_x X$ hay un único rayo geodésico que empieza en x y representa a ζ. Más aún, si $T^1_x\mathbb{H}^n$ son los vectores tangentes a $\mathbb{H}^n$ en x de norma 1 (en la métrica hiperbólica de $\mathbb{H}^n$), tenemos una biyección
$$\varphi : T^1_x\mathbb{H}^n \to \partial_x X$$
que a $v \in T^1_x\mathbb{H}^n$ le asocia $\lim_{t\to+\infty} r(t)$ donde r es la única geodésica con $r(0) = x$, $\dot{r}(0) = v$. Puede probarse que $(\varphi(v)|\varphi(w))_x$ tiende a $+\infty$ cuando el ángulo entre v y w tiende a 0. Por lo tanto φ es un homeomorfismo. Obtenemos $\partial\mathbb{H}^n \cong S^{n-1}$.

En general, si X es un espacio δ-hiperbólico y propio, entonces ∂X es compacto y X tiene una compactificación de la forma $\bar{X} = X \cup \partial X$.

Teorema 6. *Si X e Y son espacios hiperbólicos de Gromov propios, entonces toda quasi-isometría $f : X \to Y$ induce un homeomorfismo $f_\infty : \partial X \to \partial Y$.*

Por lo tanto puedo definir el borde al infinito para un grupo hiperbólico G, como $\partial G = \partial\mathrm{Cay}(G, S)$ para cualquier generador finito S de G. Además es un invariante de quasi-isometría.

Ejemplos:

1. $\partial\mathbb{Z} = \{-\infty, +\infty\}$.
2. $\partial\mathbb{F}_n$ es un conjunto de Cantor.
3. Los grupos Fuchsianos (grupos fundamentales de superficies de género $g > 1$) tienen borde S^1.
4. Los grupos Kleinianos (grupos fundamentales de 3-variedades hiperbólicas) tienen borde S^2.

A travéz del borde al infinito vemos que cada punto del ejemplo corresponde a clases de quasi-isometría distintas. Sin embargo, es un problema abierto decidir si la topología del borde determina la clase de quasi-isometría del grupo. En los tres primeros casos la respuesta es afirmativa:

1. Si $\partial G = \{x, y\}$ entonces G es virtualmente cíclico (virtualmente isomorfo a $\mathbb{Z}$).
2. Si ∂G es un Cantor, entonces G es virtualmente libre. (Consecuencia del Teorema de Stallings. Ver [1]).
3. Si $\partial G = S^1$, G es virtualmente Fuchsiano. (Casson, Freden, Gabai, Jungreis, Tukia. Ver, por ejemplo [4]).

Determinar que grupos hiperbólicos tienen borde S^2 es un problema abierto. La *conjetura de Cannon* afirma que estos son los grupos Kleinianos. Markovic [7] obtuvo recientemente (2013) una reducción de este problema.

El borde de un espacio métrico hiperbólico y propio tiene más estructura que la de espacio topológico. Es metrizable, con las llamadas *métricas visuales*. Si X es δ–hiperbólico y $x \in X$ es un punto base, una métrica d_x en ∂X es visual respecto de x si

$$C_1 e^{-(\zeta|\eta)_x} \leq d_x(\zeta, \eta) \leq C_2 e^{-(\zeta|\eta)_x}$$

para algunas constantes $C_1, C_2 > 0$. Puede probarse la existencia de métricas visuales, pero no son únicas y dependen del punto base. Dos métricas visuales distintas de ∂X (pueden venir del mismo o de distinto punto base) son *quasiconformemente equivalentes*. No definiremos estas nociones, pero es posible dar una *estructura quasiconforme* al borde de un espacio δ-hiperbólico. Cuando se considera esta estructura en el borde de un grupo hiperbólico, sí es posible recuperar el grupo (a menos de quasi-isometría) a partir de su borde (Paulin [8]).

Otro problema abierto es determinar que espacios topológicos pueden ser borde de un grupo hiperbólico. Ya mencionamos que deben ser compactos y metrizables. M. Kapovich y B. Kleiner [6] resolvieron este problema restricto a espacios conexos de *dimensión topológica* 1 y sin puntos de corte local (lo que saca, por ejemplo, el círculo). Obtuvieron que los únicos espacios en esta clase que son borde de un grupo hipérbolico son la *alfombra de Sierpinski* y la *curva de Menger*.

Es mucho más lo que puede decirse del borde de los grupos hiperbólicos. Para un pantallazo más amplio se recomienda [1].

Referencias

[1] N. Benakli and I. Kapovich, *Boundaries of hyperbolic groups*. Preprint (2002). Disponible en ArXiv: http://arxiv.org/abs/math/0202286

[2] M. Bridson and A. Haefliger, *Metric Spaces of non-positive curvature*. Springer, 1964.

[3] D. Calegari, *The ergodic theory of hyperbolic groups*. Geometry and topology down under. Contemporary Mathematics No. 59 (2013).

[4] A. Casson and D. Jungreis, *Convergence groups and Seifert fibered 3-manifolds*. Invent. Math. 118, No. 3 (1994). Pág. 441–456.

[5] E. Ghys and P. de la Harpe (Eds.), *Sur les groupes hyperboliques dáprès Mikhael Gromov*. Birkhäuser Boston Inc. 1990.

[6] M. Kapovich and B. Kleiner, *Hyperbolic groups with low-dimensional boundary*. Ann. Sci. Ecole Normale Sup. 33, No. 5 (2000). Pág. 647–669.

[7] V. Markovic, *A criterion for Cannon's conjecture*. GAFA Vol. 23 No. 3 (2013). Pág. 1035–1061.

[8] F. Paulin, *Un groupe hyperbolique est déterminé par son bord*. J. London Math.Soc. 54 (1996). Pág 50–74.

[9] H. Short (Ed.), *Notes on word hyperbolic groups*. Group theory from a geometrical viewpoint (Trieste, 1990). World Sci. Publishing, River Edge, NJ, 1991. Pág. 3–63.

Centro de Matemática, Facultad de Ciencias
Universidad de la República, Uruguay
E-mail address: juan@cmat.edu.uy

Publicaciones Matemáticas del Uruguay
Volumen 15, Junio 2016, Páginas 35–89
S 0797-1443

ENUMERATIVE GEOMETRY IN SPACES OF FOLIATIONS

VIVIANA FERRER

Contents

Introduction

The aim of this text is to present some applications of intersection theory to the global study of holomorphic foliations in projective spaces.

Holomorphic foliations are an offspring of the geometric theory of polynomial differential equations. Following the trend of many branches in Mathematics, interest has migrated to global aspects. Instead of focusing on just one curve, or surface, or metric, or differential equation, try and study their family in a suitable parameter space. The geometry within the parameter space of the family acquires relevance. For instance, the family of hypersurfaces of a given degree correspond to points in a suitable projective space; geometric conditions imposed on hypersurfaces, *e.g.,* requiring it to be singular, usually correspond to interesting subvarieties in the parameter space, *e.g.,* the discriminant. Hilbert schemes have their counterpart in the theory of polynomial differential equations, to wit, the spaces of foliations.

The last few years have witnessed an important development of the study of holomorphic foliations. Works of Jouanolou, [32],[33] Cerveau, [5],[6] Lins-Neto, [37],[38], Pereira [7], [9],[41], Cukierman [10],[11],[12], Calvo-Andrade [2],[3] Gómez-Mont [26], [23],[24],[25] and others have focused on global aspects, clarifying questions regarding the (non–)existence of algebraic leaves, description of components for the spaces of foliations of codimension ≥ 1, etc.

Our point of view follows the line of classical enumerative geometry, which treats questions such as: *How many plane curves pass through an appropriate number of points in general position? How many space curves varying in a given family are incident to an appropriate number of lines in general position? Find the degree of the space of planes curves having a singularity of given order; compute the degree of the variety of hypersurfaces containing linear subspaces, or conics, or twisted cubics, and so on ...*

In this work we consider similar questions for holomorphic foliations.

Holomorphic foliations of degree d on the complex projective plane $\mathbb{P}^2$ are defined by nonzero twisted 1–forms, $\omega = \sum a_i dZ_i$, with homogeneous polynomials $a_i(Z_0, Z_1, Z_2)$ of degree $d+1$, up to scalar multiples, satisfying $\sum a_i Z_i = 0$. The parameter space of foliations of degree d is a projective space $\mathbb{P}^N$ (the coordinates being the coefficients of the a_is) (cf. (2.4), (2.6), p. 48). The scheme of singularities of ω is defined by the homogeneous ideal generated by the a_i.

It is well known that a *general* foliation of degree d on $\mathbb{P}^2$ has exactly d^2+d+1 singularities, all non-degenerate. So it makes sense to try and study the geometry of the set of foliations with degenerate singularities.

We show how to find the degrees of the subvarieties of $\mathbb{P}^N$ corresponding to foliations displaying certain degenerate singularities. Given an integer $k \geq 2$ we study the locus, $\mathbb{M}_k \subset \mathbb{P}^N$, of foliations with a singularity of order $\geq k$. These are foliations defined in local coordinates by a holomorphic 1–form that can be written as $\omega = a_k dx + b_k dy +$higher order terms, with $a_k(x,y), b_k(x,y)$ homogeneous polynomials of degree k. It turns out that $\mathbb{M}_k$ is the birational image of an explicit projective bundle over $\mathbb{P}^2$. Using tools from intersection theory, we find a formula for the degree of $\mathbb{M}_k$.

Another interesting type of non-generic foliation presents a so called *dicritical* singularity of order k: require $a_k x + b_k y$ to vanish. This defines a closed subset $\mathbb{D}_k \subset \mathbb{M}_k$.

A geometric interpretation for the degree of the above subvarieties is as follow: Requiring a leaf of a foliation to be tangent to a fixed line at a given point defines a hyperplane in the parameter space $\mathbb{P}^N$. Therefore, the degree of each of the loci

$\mathbb{D}_k \subset \mathbb{M}_k \subset \mathbb{P}^N$ can be reinterpreted loosely as the number of foliations with a singularity of the specified type and further tangent to the appropriate number of flags (point, line) in $\mathbb{P}^2$. It turns out that the degrees of $\mathbb{D}_k, \mathbb{M}_k$ are expressed as explicit polynomials in k, d.

This fits nicely into the tradition of classical enumerative geometry: answers to questions such as determining the number of plane algebraic curves that have singularities of prescribed orders, besides having to pass through an appropriate number of points in general position, are often given by so called "node" polynomials. There is a wealth of results and conjectures on generating functions for counting suitably singular members of linear systems of curves on surfaces, cf. Götsche [22], Kleiman and Piene [35]. We hope similar results can be formulated in the setting of foliations.

Continuing the analogy with enumerative geometry, let us recall that, while a *general* surface of degree $d \geq 4$ in $\mathbb{P}^3$ contains no line –in fact, only complete intersection curves are allowed, those that *do contain* some line correspond to a subvariety of codimension $d-3$ and degree $\binom{d+1}{4}(3d^4+6d^3+17d^2+22d+24)/4!$ in a suitable $\mathbb{P}^N$.

Similarly, motivated by Jouanolou's celebrated theorem to the effect that a general holomorphic foliation, say in $\mathbb{P}^2$, of degree $d \geq 2$ has no algebraic leaf [32], we show that those foliations that *do have*, *e.g.,* an invariant line, correspond to a subvariety of codimension $d-1$ and degree $3\binom{d+3}{4}$ in a suitable $\mathbb{P}^N$.

The rest of these notes is dedicated to the study of the spaces of foliations having certain invariant algebraic subvarieties. First we impose linear subspaces, and then quadrics.

The general philosophy is to find a suitable complete parameter space for the families of foliations satisfying some of the above conditions: bad singularity, or invariant subvariety of a given type. Then, using techniques of intersection theory we compute their dimension and degree. In the case of foliations with a degenerate singularity (resp. with some invariant linear subspace) the construction of the parameter space is very explicit. In fact, in the case of singularities, we describe the parameter space as the image in the space of foliations of natural projective bundles over $\mathbb{P}^2$. For invariant linear subspaces, we also get a projective bundle over a Grassmannian. Actually, these bundles are projectivizations of vector bundles, the characteristic classes of which we are able to determine.

The case of foliations having an invariant quadric turns out to be subtler and hints at the difficulties to handle degrees higher than one. We make and do invoking the classical complete quadrics. In short, we blowup the projective space parametrizing the family of quadrics along the locus corresponding to singular quadrics. In this way we find a compactification of the space of foliations having an invariant quadric, with enough information to compute its degree.

Next we survey the contents of each section.

In Section 1 we give, for the reader's convenience, a brief introduction to intersection theory in projective spaces and Grassmannians. We define the Chow group of a scheme and describe it for the case of projective bundles and Grassmannians. We also review Fulton's construction of Chern and Segre classes asociated to a vector bundle. We list some of their properties that should help the reader to understand the computations developed in the rest of this text.

Section 2 contains the basic notions of holomorphic foliations of dimension one, as well as of codimension one, in projective spaces. We give references to the literature and definitions and results that will be needed in the sequel.

In Section 3 we find formulas for the dimension and degree of the space of foliations of degree d in $\mathbb{P}^2$ that have a degenerate singularity. In the first part we find parameter spaces for foliations having a singularity of given order $k \geq 2$. In the second part we study foliations with a dicritical singularity of order k.

Section 4 is dedicated to the study of foliations having some invariant algebraic subvariety. In the first part we find parameter spaces for the variety of foliations in $\mathbb{P}^n$ having an invariant linear subspace of given dimension. Using this description we obtain formulas for its dimension and degree. In the second part we find a compactification of the space of foliations having a smooth invariant conic in $\mathbb{P}^2$. In this way, we get formulas for its dimension and degree.

We include an appendix intended to be a glossary of basic concept and constructions needed in the text, such as vector bundles, Cartier divisors, Grassmannians, etc...

There are many natural generalizations of the material covered here. For instance, we could impose flags of invariant subvarieties. Indeed, the general foliation in $\mathbb{P}^3$ that leaves invariant some plane does not need to leave any invariant curve therein. So it makes sense to ask for the degree of the space of foliations that leave invariant, say a flag plane $\supset$ line, or plane $\supset$ conic, ...

Another interesting direction is to study the imposition, say of a given class of curves, to be contained in the scheme of singularities, cf. G.N. Costa, [8].

Extension to the case of higher order differential equations can be pursued following the ideas in M. Falla's thesis, [15]. In Chapter 5 of [20], we find formulas for the degree and codimension of the space of second order equations having a line as solution.

Most of the matterial covered here is taken from my thesis [16], and was published in [20], with my advisor Israel Vainsencher, cf. also [17], [18].

1. Intersection Theory in Grassmannians

In this Section we introduce briefly the Chow group of a scheme. We define Chern and Segre classes associated to a vector bundle, and discuss some of their properties. We give an explicit description of the Chow groups of the projective space $\mathbb{P}^n$ and the Grassmannian $\mathbb{G}(k, n)$, that is all we will need in the course. The reference for this material is [21], [46].

All schemes are of finite type over a field, usually the complex numbers $\mathbb{C}$. Variety means reduced and irreducible (*i.e.,* integral) scheme; likewise for subvarieties.

1.1. **Cycles.**

1.1.1. Definition. *Let X be a scheme. The* **group of cycles of dimension** k *of X is the free abelian group generated by the closed subvarieties of dimension k in X. It will be denoted by $\mathcal{C}_k X$. The* **group of cycles** *is the graded group*

$$\mathcal{C}_* = \bigoplus_k \mathcal{C}_k X.$$

By definition, each $k-$cycle $c \in \mathcal{C}_k X$ can be written in a unique way as a linear combination with coefficients in $\mathbb{Z}$,

$$c = \sum_V n_V \cdot V,$$

where V runs in the collection of closed subvarieties of X of dimension k. Here, the coefficient $n_V \in \mathbb{Z}$ is zero except for finitely many V's.

Recall that if $W \subseteq X$ is an irreducible component, then the local ring $\mathcal{O}_{X,W}$ of X along W is artinian. Therefore, its length $l(\mathcal{O}_{X,W})$ is finite. The fundamental cycle of X is defined by

$$[X] = \sum_W l(\mathcal{O}_{X,W})W, \tag{1.1}$$

where W runs over the set of irreducible components of X.

1.2. **Rational equivalence.** Let V be a variety and $W \subset V$ a subvariety of codimension one. Set $A = \mathcal{O}_{V,W}$, the stalk of the structure sheaf $\mathcal{O}_V$ at W. Thus, if $U = \mathrm{Spec}(R) \subset V$ is any affine open subset with non empty intersection with W, the ring $\mathcal{O}_{V,W}$ is just the localization $R_{\mathfrak{p}}$, where $\mathfrak{p}$ is the prime ideal corresponding to the subvariety $W \cap U$ of U.

Denote by $R(V)$ the field of rational functions on V.

1.2.1. Definition. *Let $r \in R(V)$ be a non-zero rational function.*

The **order** *of r along a subvariety $W \subset V$ of codimension one is defined by the formula*

$$\mathrm{ord}_W(r) = l(A/\langle a\rangle) - l(A/\langle b\rangle)$$

where $A = \mathcal{O}_{V,W}$, and $r = a/b$, with $a, b \in A$. Here $l(M)$ is the length of the module M over A.

It can be shown that $\mathrm{ord}_W(r)$ does not depend on the representation $r = a/b$, and that it is furthermore additive:

$$\mathrm{ord}_W(rr') = \mathrm{ord}_W(r) + \mathrm{ord}_W(r') \quad \forall r, r' \in R(V)^*.$$

1.2.2. Definition. *The* **cycle of a rational function** *$r \in R(V)^*$ is defined by*

$$[r] = \sum_W \mathrm{ord}_W(r) \cdot W$$

where the sum extends over the collection of closed subvarieties of codimension one of V.

One checks that the sum is finite, *i.e.,* $\mathrm{ord}_W(r) = 0$ except for finitely many W's.

1.2.3. Example. *An obvious example is to consider the function $f(t) = t^n$ in $k[t]$. If $p \in \mathbb{A}^1$ is a point, we have $A = k[t]_{(m_p)} = k[t]_{(t-p)}$. In these case $A/\langle t^n\rangle = 0$ if $p \neq 0$ (because t is invertible in A) and $A/\langle t^n\rangle \simeq k \oplus kt \oplus \cdots \oplus kt^{n-1}$ if $p = 0$. Therefore*

$$\mathrm{ord}_0(t^n) = l(A/\langle t^n\rangle) = n$$

as expected.

The cycle of t^n is

$$[t^n] = \sum_p \mathrm{ord}_p(t^n) \cdot p = n.0\ .$$

1.2.4. Definition. *Let X be a scheme. The* **group of k-cycles rationally equivalent to zero** *is the subgroup $\mathcal{R}_kX \subset \mathcal{C}_kX$ generated by the cycles of rational functions of closed subvarieties of X of dimension $k+1$.*

The **Chow group** *of X is the graded group,*

$$\mathcal{A}_*X = \bigoplus_k \mathcal{A}_kX = \bigoplus_k \mathcal{C}_kX/\mathcal{R}_kX$$

Two cycles are said to be **rationally equivalent** *to each other if they represent the same class modulo $\mathcal{R}_*X$.*

1.2.5. Remark.
If X is of pure dimension n, then $\mathcal{A}_iX = 0$ for $i < 0$ and for $i > n$. Moreover, $\mathcal{A}_nX = \mathcal{C}_nX$ is the free abelian group generated by the irreducible components of X. If X is a variety of dimension n, we have $\mathcal{A}_nX = \mathcal{C}_nX = \mathbb{Z}$.

1.2.6. Examples.

(1) $\mathcal{A}_{n-1}\mathbb{A}^n = 0$, because any divisor in $\mathbb{A}^n$ is the zero locus of a polynomial (*i.e.,* a function in $\mathbb{A}^n$).
(2) $\mathcal{A}_0\mathbb{A}^n = 0$ for $n > 0$. In fact, if $P \in \mathbb{A}^n$, we can choose a linear function r on a line through P that vanishes exactly at P. Therefore $[r] = [P]$, and $[P] \in \mathcal{R}_0\mathbb{A}^n$.
(3) $\mathcal{A}_k\mathbb{A}^n = 0$ for $k < n$, see Proposition (1.5.3, p. 43).
(4) $\mathcal{A}_{n-1}\mathbb{P}^n = \mathbb{Z}\cdot h$, the free abelian group generated by h, the class of a hyperplane. Indeed, let F_d be a homogeneous polynomial of degree d and let $\mathcal{Z}(F_d)$ be the corresponding hypersurface. Let $[\mathcal{Z}(F_d)]$ denote its fundamental cycle (1.1). Consider the rational function $r := F_d/F_1^d \in R(\mathbb{P}^n)$. Then $[r] = [\mathcal{Z}(F_d)] - d\cdot[\mathcal{Z}(F_1)]$, *i.e.,* $[\mathcal{Z}(F_d)] \sim d\cdot[\mathcal{Z}(F_1)]$. Since $h = [\mathcal{Z}(F_1)]$ clearly is not torsion, $\mathcal{A}_{n-1}\mathbb{P}^n$ is freely generated by h.
(5) In general, for $0 \le k \le n$, $\mathcal{A}_k\mathbb{P}^n = \mathbb{Z}\cdot[\mathbb{P}^k]$, the free abelian group generated by the class of a linear subspace of dimension k, see Proposition 1.5.3.
(6) Let X be a smooth projective curve. Then we have
$$\mathcal{C}_0X = \mathrm{Div}(X) \quad \text{and} \quad \mathcal{A}_0X = \mathrm{Pic}(X)\,.$$
(7) If X has pure dimension n, an element of $\mathcal{C}_{n-1}(X)$ is a Weil divisor, and the quotient group $\mathcal{A}_{n-1}(X)$ is the group of Weil divisor classes. In this sense the Chow groups can be viewed as a generalization of Weil divisors classes.

1.3. **Direct Image.** Given a morphism $f : X \to Y$ of schemes, we shall define a natural homomorphism of groups $f_* : \mathcal{C}_*X \to \mathcal{C}_*Y$. Moreover, if f is *proper* then $f_*(\mathcal{R}_*X) \subset \mathcal{R}_*Y$, thereby inducing a homomorphism $\mathcal{A}_*X \to \mathcal{A}_*Y$.

1.3.1. Definition. *A morphism $f : X \to Y$ is* **proper** *if it is separated and universally closed,* i.e., *for all $Z \to Y$, the morphism induced by fiber product,*

$$X \times_Y Z \to Z$$

takes closed sets to closed sets.

A scheme X is **complete** *if the structural morphism $X \to \mathrm{Spec}(\mathbb{C})$ is proper.*

Properness corresponds to compact fibers in the classical topology, while completeness is the algebraic translation of compactness in the classical topology. For another characterization and properties of proper morphism consult [31].

We will use proper morphism in order to guarantee that the image of a variety is a closed subset.

1.3.2. Definition. *Let $f : V \to W$ be a dominant morphism of varieties. We define the* **degree** *of f as*

$$\deg(f) = \begin{cases} 0 & \text{if } \dim V > \dim W \\ [R(V) : R(W)] & \text{if } \dim V = \dim W \end{cases}$$

Observe that in the case $\dim V = \dim W$, the function fields $R(V)$ and $R(W)$ are finitely generated field extensions with the same transcendence degree over $\mathbb{C}$. Hence $\deg(f)$ is finite.

We can interpret the $\deg(f)$ as the degree of the covering or as the number of points in a fiber of f.

1.3.3. Definition. *Let $p : X \to Y$ be a proper map of schemes. Let $V \subset X$ be a closed subvariety and $W := p(V)$. Let $f : V \to W$ be the map induced by p. We put*

$$p_*(V) = \deg(f) \cdot W \in \mathcal{C}_* W.$$

We extend it by linearity to a homomorphism

$$p_* : \mathcal{C}_* X \to \mathcal{C}_* Y,$$

called **direct image** *of p.*

1.3.4. Examples.

(1) If X is complete, then any morphism $f : X \to Y$ is proper. Examples of complete varieties are $\mathbb{P}^n$, $\mathbb{G}(k, n)$, and any projective bundle $\mathbb{P}(\mathcal{E})$ associated to a vector bundle $\mathcal{E}$ over a complete base. See p. 83

These are in fact the varieties which we will use in the text.

(2) $\mathbb{A}^1$ is not complete. Indeed, the map $p : \mathbb{A}^1 \to pt$ is not proper: consider $\hat{p} : \mathbb{A}^2 \to \mathbb{A}^1$, $\hat{p}(x, y) = x$. Then $\hat{p}(\{xy = 1\}) = \mathbb{A}^1 \backslash \{0\}$ that is not closed. In this case there are no direct image map, because $\mathcal{A}_0(\mathbb{A}^1) = 0 \to \mathcal{A}_0(pt) = \mathbb{Z}$, i.e. the class of a point is zero in $\mathcal{A}_0(\mathbb{A}^1)$ but non zero in $\mathcal{A}_0(pt)$.

(3) The same occurs for the inclusion $\mathbb{A}^1 \to \mathbb{P}^1$. This map is not proper, and there are no direct image, because the class of a point is zero in $\mathcal{A}_0(\mathbb{A}^1)$ but non zero in $\mathcal{A}_0(\mathbb{P}^1) = \mathbb{Z}$.

1.3.5. Theorem. *Let $p : X \to Y$ be a proper map. Then the direct image map $p_* : \mathcal{C}_* X \to \mathcal{C}_* Y$ preserves rational equivalence, i.e, we have $p_*(\mathcal{R}_* X) \subset \mathcal{R}_* Y$.*

Proof. See [21, Theorem 1.4. p. 11]. □

Using this result we can define the direct image of a morphism at the Chow group level.

1.3.6. Definition. *Let $p : X \to Y$ be a proper map. The* **direct image homomorphism** *is the induced homomorphism*

$$p_* : \mathcal{A}_* X \to \mathcal{A}_* Y.$$

1.3.7. Definition. *Let X be a complete scheme, and $f : X \to \mathrm{pt}$ be the natural proper map. For any $0-$cycle $\alpha \in \mathcal{A}_0(X)$ we define the degree of α to be $f_*(\alpha) \in \mathcal{A}_0(\mathrm{pt}) = \mathbb{Z}$. We write*

$$\deg(\alpha) = \int_X \alpha \,.$$

The degree is the number of points counted with the appropriate multiplicity.

1.3.8. Proposition. *The direct images are functorial,* i.e., *if $f : X \to Y$ and $g : Y \to Z$ are proper maps, then $(g \circ f)_* = g_* \circ f_*$. In particular, if $p : X \to Y$ is a proper map of complete schemes, we have*

$$\int_X \alpha = \int_Y p_*(\alpha), \forall \alpha \in \mathcal{A}_0(X).$$

1.4. **Inverse Image.** Let $f : X \to Y$ be a *flat* morphism (cf. [31]). We shall define a homomorphism $f^* : \mathcal{C}_*(Y) \to \mathcal{C}_*(X)$ that preserves rational equivalence, *i.e.,* $f^*(\mathcal{R}_*(Y)) \subset \mathcal{R}_*(X)$, and therefore induces a homomorphism

$$f^* : \mathcal{A}_*(Y) \to \mathcal{A}_*(X).$$

1.4.1. Definition. *Let $V \subset Y$ be a subvariety. The* **inverse image cycle** *of V under f is defined by*

$$f^*V = [f^{-1}(V)].$$

The right hand side above is the fundamental cycle ((1.1, p. 39)) of the closed subscheme $f^{-1}(V) \subseteq X$. We extend it by linearity to obtain a homomorphism

$$f^* : \mathcal{C}_*(Y) \to \mathcal{C}_*(X).$$

We say that $f : X \to Y$ is of **relative dimension** n if for each subvariety W of Y, any component V of $f^{-1}(W)$ is of dimension

$$\dim V = n + \dim W.$$

It is the case of any fibration, and these will be the morphisms that we will work with in the text.

A flat morphism will be assumed to have relative dimension n for some n. We register the following

1.4.2. Proposition. *Let $f : X \to Y$ be a flat morphism of relative dimension n. Then for each closed subscheme $Z \subseteq Y$ of pure dimension k, we have*

$$f^*[Z] = [f^{-1}Z] \quad \text{in } \mathcal{C}_{k+n}X.$$

We list out the principal examples of flat morphisms that occur in this text.

1.4.3. Examples.

(1) Any open imbedding.
(2) The structure map of a vector bundle, or a projective bundle to its base.
(3) The projection $X \times Y \to X$ where Y is a pure dimensional scheme.

Flat families (fibers of flat morphisms) are the adequate notion to work with families of schemes, for example, for flat families of subschemes in $\mathbb{P}^n$ the fibers have constant Hilbert polynomial (this mean that numerical invariants as dimension, degree etc, are preserved)

1.4.4. Proposition. *Let $f : X \to Y$ be a flat morphism of relative dimension n. Then $f^* : \mathcal{C}_kY \to \mathcal{C}_{k+n}X$ and $f^*(\mathcal{R}_kY) \subset \mathcal{R}_{k+n}X$. Therefore we obtain a homomorphism*

$$f^* : \mathcal{A}_kY \to \mathcal{A}_{k+n}X.$$

The inverse image is functorial. By this we mean that, if $f : X \to Y$, and $g : Y \to Z$ are flat morphisms of schemes, then

$$(g \circ f)^* = f^* \circ g^*.$$

Proof. See [21, Theorem 1.7, p. 19]. □

The inverse image is compatible with proper direct images:

1.4.5. Proposition. *Let be given a Cartesian diagram,*

$$\begin{array}{ccc} X \times_Y Y' = : X' & \xrightarrow{f'} & Y' \\ {\scriptstyle g'}\downarrow & & \downarrow{\scriptstyle g} \\ X & \xrightarrow{f} & Y \end{array}$$

where f is flat of relative dimension n and g is proper. Then f' (resp. *g') is flat of relative dimension n* (resp. proper) *and we have*

$$g'_* f'^* = f^* g_* : \mathcal{C}_k Y' \longrightarrow \mathcal{C}_{k+n} X.$$

1.5. **Excision.** The following proposition is a very useful tool that allows us to compute the Chow groups of $\mathbb{A}^n$ and $\mathbb{P}^n$.

1.5.1. Proposition. *Let $i : Z \hookrightarrow X$, $j : U \hookrightarrow X$ the inclusion maps of a closed subscheme Z and its complement U. Then we have the following exact sequence:*

$$\mathcal{A}_* Z \xrightarrow{i_*} \mathcal{A}_* X \xrightarrow{j^*} \mathcal{A}_* U \to 0.$$

Proof. □

1.5.2. Lemma. *Let X be a scheme and let $p : X \times \mathbb{A}^n \to X$ be the projection. Then*

$$p^* : \mathcal{A}_* X \longrightarrow \mathcal{A}_*(X \times \mathbb{A}^n)$$

is surjective.

Proof. See [21, Proposition 1.9, p. 22]. □

Using these two results we can compute the Chow groups of $\mathbb{A}^n$ and $\mathbb{P}^n$.

1.5.3. Proposition.

(1) *$\mathcal{A}_i \mathbb{A}^n = 0$ for all $i \neq n$, and $\mathcal{A}_n \mathbb{A}^n = \mathbb{Z}$.*
(2) *$\mathcal{A}_i \mathbb{P}^n = \mathbb{Z}[\mathbb{P}^i]$, the free group generated by the class of a dimension i subspace $\mathbb{P}^i \subset \mathbb{P}^n$ for all $0 \leq i \leq n$.*

Proof. We already know (1.2.6, p. 40) that $\mathcal{A}_n \mathbb{A}^n = \mathbb{Z}$ and $\mathcal{A}_{n-1} \mathbb{A}^n = 0$. If $i < n-1$, by the lemma above we have a surjective map $\mathcal{A}_{i-n+1} \mathbb{A}^1 \twoheadrightarrow \mathcal{A}_i(\mathbb{A}^1 \times \mathbb{A}^{n-1})$. But $\mathcal{A}_{i-n+1} \mathbb{A}^1 = 0$ for $i < n-1$. This proves (1).

We prove (2) using induction and the excision sequence

$$\mathcal{A}_i \mathbb{P}^{n-1} \longrightarrow \mathcal{A}_i \mathbb{P}^n \longrightarrow \mathcal{A}_i \mathbb{A}^n = 0.$$

By induction $\mathcal{A}_i \mathbb{P}^{n-1} = \mathbb{Z}[\mathbb{P}^i]$. Hence $\mathcal{A}_i \mathbb{P}^n$ is generated by $[\mathbb{P}^i]$. It remains to prove that $m[\mathbb{P}^i] = 0$ in $\mathcal{A}_i \mathbb{P}^n$ implies $m = 0$. Suppose

$$m[\mathbb{P}^i] = \sum m_k [r_k]$$

for some integers m_k and some rational functions $r_k \in R(V_k)$, where V_k's are subvarieties of $\mathbb{P}^n$ of dimension $i+1$. Set $Z := \bigcup V_k$, then $m[\mathbb{P}^i] = 0$ in $\mathcal{A}_i Z$. There exists a finite map $p : Z \to \mathbb{P}^{i+1}$ (e.g., induced by a linear projection). We find

$$m p_* [\mathbb{P}^i] = 0 \text{ in } \mathcal{A}_i \mathbb{P}^{i+1}$$

which is torsion free. Hence $m = 0$ as desired. □

1.5.4. Definition. *Let $\alpha = \sum_{i=0}^{k} m_i \cdot [\mathbb{P}^i]$ be a cycle in $\mathbb{P}^n$. If $m_k \neq 0$ we define the* **degree** *of α by the formula*

$$\deg(\alpha) = m_k.$$

1.6. **Chern classes.** In this section we define Chern classes associated to a vector bundle $\mathcal{E}$ over a scheme X (cf. Appendix A.1). These classes are constructed as operators on the Chow groups $\mathcal{A}_* X$. See [21, Chapter 3].

1.6.1. Definition. *Let X be a scheme, and $\mathcal{E}$ a vector bundle over X of rank e. The $i-$th Chern class of $\mathcal{E}$ is a homomorphism*

$$c_i(\mathcal{E}) \cap \_ : \mathcal{A}_k X \to \mathcal{A}_{k-i} X$$

characterized by the following five properties:

(1) $c_0(\mathcal{E}) = 1$ (= identity operator).

(2) (Naturality) *If $f : Y \to X$ is a flat morphism, then*

$$f^*(c_i(\mathcal{E}) \cap \alpha) = c_i(f^*\mathcal{E}) \cap f^*\alpha$$

for all cycle $\alpha \in \mathcal{A}_* X$ and all i. Here $f^*\mathcal{E}$ is the pull-back of $\mathcal{E}$ by f (cf. Appendix A.1.3).

(3) (Whitney sum) *If*

$$0 \to \mathcal{E}' \longrightarrow \mathcal{E} \longrightarrow \mathcal{E}'' \to 0$$

is an exact sequence of vector bundles, then

$$c_i(\mathcal{E}) = \sum_{r+s=i} c_r(\mathcal{E}') c_s(\mathcal{E}'').$$

(4) (Normalization) *If $\mathcal{E}$ is a line bundle, and D is a Cartier divisor on X such that $\mathcal{O}_X(D) \simeq \mathcal{E}$ (see Appendix A.2), then*

$$c_1(\mathcal{E}) \cap [X] = [D].$$

(5) (Projection formula) *If $f : Y \to X$ is a proper morphism, then*

$$f_*(c_i(f^*\mathcal{E}) \cap \alpha) = c_i(\mathcal{E}) \cap f_*\alpha$$

for all $\alpha \in \mathcal{A}_* Y$.

1.6.2. Remarks. (1) Since $\mathcal{A}_i(X) = 0$ for $i < 0$, we see that $c_i(\mathcal{E})$ is nilpotent.
(2) It is a fundamental (and nontrivial) fact that if $\mathcal{E}, \mathcal{E}'$ are vector bundles, then the operators $c_i(\mathcal{E})$ and $c_j(\mathcal{E}')$ commute.
(3) We will also see that $c_i(\mathcal{E}) = 0$ if $i > e = \mathrm{rk}(\mathcal{E})$.

1.6.3. Definition. *Let $\mathcal{E}$ be a vector bundle over a scheme X.*
The **total Chern class** *of $\mathcal{E}$ is*

$$c(\mathcal{E}) = c_0(\mathcal{E}) + c_1(\mathcal{E}) + \cdots$$

By the above remark, we see that this sum is finite and $c(\mathcal{E}) = 1 + c_1(\mathcal{E}) + \cdots$ is an invertible element of the endomorphism ring of $\mathcal{A}_* X$.

We define the **total Segre class** of $\mathcal{E}$ as the formal inverse of $c(\mathcal{E})$,

$$s(\mathcal{E}) = c(\mathcal{E})^{-1} = 1 + s_1(\mathcal{E}) + \cdots .$$

1.6.4. Remark. Expanding $s = 1 + s_1 + \cdots = 1/(1 + c_1 + \cdots)$ we find $s_1 = -c_1, s_2 = c_1^2 - c_2$, etc. Each $s_i(\mathcal{E})$ defines a homomorphism $\mathcal{A}_k X \to \mathcal{A}_{k-i} X$. It can be proved that

$$s_i(\mathcal{E}) \cap \alpha = p_*(c_1(\mathcal{O}_{\mathcal{E}}(1))^{e-1+i} \cap p^*\alpha)$$

for $\alpha \in \mathcal{A}_k X$, where $e = \mathrm{rk}(\mathcal{E})$ and $p : \mathbb{P}(\mathcal{E}) \to X$ is the projection (see Appendix A.3).

In fact the formula can be taken as the definition of Segre class.(cf. [21])

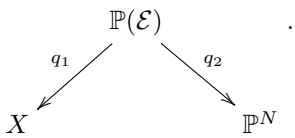
Recall the definition of degree of a cycle (Definition 1.5.4). We have that if $X \subset \mathbb{P}^n$ is a subscheme of pure dimension k and degree d then

$$d = \deg(h^k \cap [X])$$

where $h = c_1(\mathcal{O}_{\mathbb{P}^n}(1))$.

As an application of the definition and properties of Chern and Segre classes, we shall prove a lemma that will be a very usefull tool in the sequel.

1.6.5. Lemma. *Let V be a vector space of dimension $N+1$. Let $\mathcal{E}$ be a subbundle of the trivial bundle $X \times V$ over a variety X of dimension n. Consider $\mathbb{P}(\mathcal{E})$ the projective bundle associated to $\mathcal{E}$, and $\mathbb{P}^N = \mathbb{P}(V)$. Consider the following diagram:*



Let $M \subseteq \mathbb{P}^N$ denote the image of q_2. Suppose that q_2 is generically finite. Then

$$\deg(q_2) \deg M = \int s_n(\mathcal{E}) \cap [X].$$

Proof. Set for short $\delta = \deg(q_2)$. Hence $q_{2*}[\mathbb{P}(\mathcal{E})] = \delta[M]$. Now we have

$$\begin{aligned} \deg M = \int H^\nu \cap [M] &= \frac{1}{\delta} \int H^\nu \cap q_{2*}[\mathbb{P}(\mathcal{E})] \\ &= \frac{1}{\delta} \int q_2^* H^\nu \cap [\mathbb{P}(\mathcal{E})] = \frac{1}{\delta} \int \widetilde{H}^\nu \cap [\mathbb{P}(\mathcal{E})] \end{aligned}$$

where $\nu = \dim(\mathbb{P}(\mathcal{E})) = \dim M$, $H = c_1(\mathcal{O}_{\mathbb{P}^N}(1))$, $\widetilde{H} = c_1(\mathcal{O}_{\mathcal{E}}(1))$.

Set $e = \mathrm{rk}(\mathcal{E})$. Thus $\nu = e - 1 + n$. Hence

$$\int \widetilde{H}^\nu \cap [\mathbb{P}(\mathcal{E})] = \int q_{1*}(\widetilde{H}^\nu \cap q_1^*[X]) = \int s_n(\mathcal{E}) \cap [X]$$

by Remark 1.6.4. The proof is complete. □

The following Lemma will be used repeatedly in order to prove the generic injectivity of certain maps.

1.6.6. Lemma. *In the situation of the previous lemma, in order to prove that q_2 is generically one to one, it suffices to find a point $[v] \in M$ such that the fiber $q_2^{-1}([v])$ consists of one reduced point.*

Proof. If we prove the existence of such point $[v]$, by the theorem on the dimension of fibers (see [43, Chapter I §6.3]) there exists an open set U in M such that the fiber over each point in U has dimension zero, ($U \neq \emptyset$ because $[v] \in U$). Therefore q_2 is generically finite. Shrinking U we may assume (i) U is affine, say with coordinate

ring A and (ii) the restriction of q_2 over ${q_2}^{-1}U$ is finite (cf. [31, ex.11.2, p. 280]). It follows that ${q_2}^{-1}U$ is affine, with coordinate ring B which is an A-module of finite type. Now for each point $u \in U$ with corresponding maximal ideal $m_u \subset A$, the fiber ${q_2}^{-1}u = \operatorname{Spec}(B/m_uB)$ is finite and consists of $\dim_{\mathbb{C}}(B/m_uB)$ points counted with multiplicity. By semicontinuity, this vector space dimension attains a minimum over an open subset. Since the fiber over $y = [v]$ consists of one reduced point, that mininum is precisely one and we are done. □

Notice that reducedness of ${q_2}^{-1}([v])$ required above means that the tangent map of q_2 is injective.

Chern classes and Segre classes of vector bundles can be effectively computed with appropriate tools. The principal one is the splitting principle that we state in the following proposition. This, together with the next lemma give us a handy way to compute Chern classes.

1.6.7. Proposition. (The splitting principle) *Let $\mathcal{E}$ be a vector bundle over a scheme X. Then there exists a flat map $f : X' \to X$ such that*

(1) *the induced homomorphism $f^* : \mathcal{A}_*X \to \mathcal{A}_*X'$ is injective.*
(2) *$f^*\mathcal{E}$ admits a filtration by vector subbundles*

$$\mathcal{E}_e = 0 \subset \cdots \subset \mathcal{E}_1 \subset \mathcal{E}_0 = f^*\mathcal{E}$$

whose successive quotients are line bundles, $L_i = \mathcal{E}_{i-1}/\mathcal{E}_i$.

Proof. See [21, § 3.2.]. □

1.6.8. Lemma. *Let $\mathcal{E}$ be a vector bundle endowed with a filtration as in the proposition above. Put $\lambda_i = c_1(L_i)$ and define*

$$\begin{cases} \sigma_1 = \sum_i \lambda_i, \\ \sigma_2 = \sum_{i<j} \lambda_i\lambda_j, \\ \quad \vdots \\ \sigma_e = \lambda_1 \cdots \lambda_e, \end{cases}$$

the elementary symmetric functions. Then we have

$$c(\mathcal{E}) = \Pi_1^e(1 + \lambda_i), \quad \textit{that is,}$$

$$c_i(\mathcal{E}) = \begin{cases} \sigma_i & \textit{for } 1 \le i \le e; \\ 0 & \textit{for } i > e. \end{cases}$$

Proof. See [21, Remark 3.2.3. p. 54.]. □

Using the splitting principle, we see that in order to show formulas involving Chern classes we can suppose that the vector bundle $\mathcal{E}$ has a filtration with line bundle quotients. In fact, the Chern classes of $\mathcal{E}$ are the same as of $\bigoplus L_i$. The classes $\lambda_i = c_1(L_i)$ are the **Chern roots** of $\mathcal{E}$. The Chern classes are the symmetric elementary functions of the chern roots $\{\lambda_i\}$.

1.6.9. Proposition.

(1) Dual bundles. *The Chern classes of the dual bundle $\mathcal{E}^\vee$ are given by the formula*

$$c_i(\mathcal{E}^\vee) = (-1)^i c_i(\mathcal{E}).$$

(2) Twisted bundles. *Suppose that L is a line bundle, and* $\mathrm{rk}(\mathcal{E}) = e$, *then*

$$c_e(\mathcal{E} \otimes L) = \sum_{i=0}^{e} c_1(L)^i c_{e-i}(\mathcal{E}).$$

□

The following proposition is the key to many interesting geometric applications of Chern classes.

Let $\mathcal{E}$ be a vector bundle of rank e over a scheme X. We say a section s of $\mathcal{E} \to X$ is *regular* at a point $x \in X$ if there is a local trivialization of $\mathcal{E}$ around x such that s is given by $(s_1, \ldots, s_e)$ where either some s_i is a unit or the $s_i \in \mathcal{O}_{X,x}$ form a regular sequence. This means that s_1 is a nonzero divisor at the stalk $\mathcal{O}_{X,x}$ and each s_i is a nonzero divisor in $\mathcal{O}_{X,x}/\langle s_1, \ldots, s_{i-1}\rangle$. We say s is regular if it is so at each point. If X is a smooth variety, regularity of s is tantamount to requiring the scheme of zeros $\mathcal{Z}(s)$ to be either empty or of the correct codimension $e = \mathrm{rk}\,\mathcal{E}$.

1.6.10. Proposition. *Let $\mathcal{E}$ be a vector bundle of rank e over a scheme X of pure dimension n. Let s be a regular section of $\mathcal{E}$. Then*

$$c_e(\mathcal{E}) \cap [X] = [\mathcal{Z}(s)] \text{ in } \mathcal{A}_{n-e}X.$$

1.6.11. Example Let $\mathcal{X}$ be a vector field in $\mathbb{P}^n$ that defines a regular section of $\mathcal{T}\mathbb{P}^n$. Then $\mathcal{Z}(\mathcal{X})$ = scheme of singularities of $\mathcal{X}$, is a finite set. To compute the number of singularities we can use the proposition to obtain

$$\int c_n(\mathcal{T}\mathbb{P}^n) \cap [\mathbb{P}^n] = \int [\mathcal{Z}(\mathcal{X})].$$

We shall return to this in the next Section.

1.7. **Some Chow groups.** In this section we give explicit description of the Chow groups of projective vector bundles (in particular for $\mathbb{P}^n$) and Grassmannians.

1.7.1. Proposition. *Let $\mathcal{E}$ be a vector bundle of rank e over a scheme X. Then*

$$\mathcal{A}_*\mathbb{P}(\mathcal{E}) \simeq \frac{\mathcal{A}_*(X)[H]}{\langle H^e + c_1(\mathcal{E})H^{e-1} + \cdots + c_{e-1}(\mathcal{E})H + c_e(\mathcal{E})\rangle}$$

where $H = c_1(\mathcal{O}_{\mathcal{E}}(1))$, see Appendix A.3.

In particular we have, for $\mathbb{P}^n = \mathbb{P}(\mathbb{C}^{n+1})$

$$\mathcal{A}_*\mathbb{P}^n \simeq \mathbb{Z}[h]/\langle h^{n+1}\rangle$$

where $h = c_1(\mathcal{O}_{\mathbb{P}^n}(1))$.

Proof. See [21, Ex. 8.3.4, p. 141], [46, Ch. 10].. □

1.7.2. Proposition. *Let $\mathbb{G}(k, n)$ the Grassmannian of k-planes of $\mathbb{P}^n$. We have*

$$\mathcal{A}_*\mathbb{G}(k, n) \simeq \mathbb{Z}[a, b]/\langle a_* b_* - 1\rangle$$

where $a = (a_1, \ldots, a_k)$, $b = (b_1, \ldots, b_{n-k})$ are indeterminates, $a_* = 1 + a_1 + \cdots + a_k$, $b_* = 1 + b_1 + \cdots + b_{n-k}$.

Proof. See [46, Ch. 10]. □

Exercise 1. Write explicitly the above relations for $\mathbb{G}(1, 3)$.

2. Holomorphic Foliations in Projective Spaces

In this Section we introduce the basic notions of foliations of dimension one (respectively, codimension one) in $\mathbb{P}^n$. We review the definitions of degree, singularity, order of a singularity and invariant subvarieties, in the way that will be used in the text.

Throughout this work S_d will denote the vector space of homogeneous polynomials of degree d in the $(n+1)$ homogeneous coordinates $Z_0, \ldots, Z_n$. We have

$$S_d = \mathrm{Sym}_d \check{\mathbb{C}}^{n+1}\,; \quad \dim S_d = \binom{d+n}{n}.$$

We will identify

$$S_1 = \check{\mathbb{C}}^{n+1} \simeq \Omega_0 \mathbb{C}^{n+1}$$

the vector space with basis

$$\{dZ_0, \ldots, dZ_n\}.$$

Similarly, we will identify

$$S_1^\vee = \mathbb{C}^{n+1} \simeq \mathcal{T}_0 \mathbb{C}^{n+1} \tag{2.1}$$

the vector space with basis

$$\left\{\frac{\partial}{\partial Z_0}, \ldots, \frac{\partial}{\partial Z_n}\right\}.$$

2.1. **Tangent and cotangent bundles of $\mathbb{P}^n$.** The tangent bundle of $\mathbb{P}^n$ is determined by the Euler exact sequence,

$$0 \to \mathcal{O}_{\mathbb{P}^n} \longrightarrow \mathcal{O}_{\mathbb{P}^n}(1) \otimes \mathbb{C}^{n+1} \longrightarrow \mathcal{T}\mathbb{P}^n \to 0. \tag{2.2}$$

The first map is

$$1 \mapsto (Z_0, \ldots, Z_n),$$

The second map is defined by

$$F = (F_0, \ldots, F_n) \mapsto \delta_F,$$

where δ_F is the derivation $\delta_F(f/g) = \frac{f\nabla g - g\nabla f}{g^2} \cdot (F_0, \ldots, F_n)$.

Dualizing the Euler sequence we have

$$0 \to \Omega_{\mathbb{P}^n} \longrightarrow \mathcal{O}_{\mathbb{P}^n}(-1) \otimes \check{\mathbb{C}}^{n+1} \longrightarrow \mathcal{O}_{\mathbb{P}^n} \to 0. \tag{2.3}$$

The rightmost map is given by $(f_0, \ldots, f_n) = \sum f_i dZ_i \mapsto \sum_{i=0}^n f_i Z_i$. Recall that the sections of $\mathcal{O}_{\mathbb{P}^n}(-1)$ over an open subset $U \subset \mathbb{P}^n$ are given by fractions F/G such that F, G are homogeneous polynomials of degrees $\deg F = \deg G - 1$ and G has no zeros over U. Thus each $f_i Z_i$ in the sum is of degree zero, *i.e.,* a function.

2.2. **Dimension one foliations.**

2.2.1. Definition. *A* **dimension one foliation** *in $\mathbb{P}^n$ is a nonzero global section of $\mathcal{T}\mathbb{P}^n \otimes \mathcal{O}_{\mathbb{P}^n}(d-1)$ for some $d \geq 0$ modulo non-zero complex multiples.*

Let us denote

$$V_{1,n,d} = H^0(\mathbb{P}^n, \mathcal{T}\mathbb{P}^n \otimes \mathcal{O}_{\mathbb{P}^n}(d-1)) \tag{2.4}$$

and

$$\mathbb{F}(1, n, d) = \mathbb{P}(V_{1,n,d}).$$

Then a dimension one foliation is an element $\mathcal{X} \in \mathbb{F}(1, n, d)$.

Tensoring the Euler sequence by $\mathcal{O}_{\mathbb{P}^n}(d-1)$ we obtain

$$0 \to \mathcal{O}_{\mathbb{P}^n}(d-1) \to \mathcal{O}_{\mathbb{P}^n}(d) \otimes \mathbb{C}^{n+1} \to \mathcal{T}\mathbb{P}^n(d-1) \to 0. \tag{2.5}$$

Taking global sections in the last sequence and using that $H^1(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(d-1)) = 0$ ([31, Chapter III, Theorem 5.1]) we obtain the following exact sequence:

$$0 \to S_{d-1} \to S_d \otimes S_1^\vee \to H^0(\mathbb{P}^n, \mathcal{T}\mathbb{P}^n(d-1)) \to 0.$$

From this we deduce that a foliation is given in homogeneous coordinates by a vector field

$$X = F_0 \frac{\partial}{\partial Z_0} + \cdots + F_n \frac{\partial}{\partial Z_n},$$

where F_i are homogeneous polynomials of degree d, modulo multiples of the radial vector field

$$R := Z_0 \frac{\partial}{\partial Z_0} + \cdots + Z_n \frac{\partial}{\partial Z_n}.$$

We will denote by X an element in $S_d \otimes S_1^\vee$, and $\mathcal{X} := X$ modulo $S_{d-1} \cdot R$.

The Euler sequence gives us:

$$V_{1,n,d} \simeq \frac{S_d \otimes S_1^\vee}{S_{d-1} \cdot R} \tag{2.6}$$

From this it is clear that

$$N_{1,n,d} := \dim V_{1,n,d} - 1 = (n+1)\binom{d+n}{n} - \binom{d-1+n}{n} - 1 \tag{2.7}$$

and

$$\mathbb{F}(1,n,d) = \mathbb{P}^{N_{1,n,d}}.$$

2.2.2. Definition. The **degree of a foliation** $\mathcal{X} \in \mathbb{F}(1,n,d)$ is d.

For a geometric interpretation of the degree, take a hyperplane H in $\mathbb{P}^n$. Define

$$\mathcal{T}(\mathcal{X}, H) = \{p \in H \mid \mathcal{X}(H)(p) = 0\},$$

the **set of tangencies** of $\mathcal{X}$ with H. For a generic H, it can be seen that $\mathcal{T}(\mathcal{X}, H)$ has codimension one in H and the degree of $\mathcal{X}$ is the degree of $\mathcal{T}(\mathcal{X}, H)$ ([39, Chapter II §3]).

In fact, if we take a hyperplane defined by the equation

$$H := a_0 Z_0 + \cdots + a_n Z_n = 0$$

then $\mathcal{T}(\mathcal{X}, H)$ is given in H by

$$\mathcal{X}(H) := a_0 F_0 + \cdots + a_n F_n = 0.$$

For H generic, the polynomial $\mathcal{X}(H)$ is not identically zero and has degree d.

Observe that in $\mathbb{P}^2$ the set of tangencies of a degree d vector field $\mathcal{X}$ with a generic line is finite and consists of d points.

Exercise 2. The goal is to deduce the local expression of a vector field, using the Euler sequence. Let

$$\mathcal{X} = F_0 \frac{\partial}{\partial Z_0} + \cdots + F_n \frac{\partial}{\partial Z_n}$$

be a degree d vector field. Set

$$U_j := \{[Z_0 : \cdots : Z_n] \mid Z_j \neq 0\} = \{(z_0, \ldots, \hat{z_j}, \ldots, z_n) \in \mathbb{C}^n\}.$$

Prove that we have the following local expression for $\mathcal{X}$ on U_j:

$$\mathcal{X}_{U_j} = \sum_{i\neq j} a_i \frac{\partial}{\partial z_i} = \sum_{i\neq j} (f_i - z_i f_j)\frac{\partial}{\partial z_i} = \sum_{i\neq j} f_i \frac{\partial}{\partial z_i} - f_j \sum_{i=1} z_i \frac{\partial}{\partial z_i} \tag{2.8}$$

where f_i is the dehomogenization of F_i with respect to Z_j.

The notation U_j for the canonical open set $Z_j \neq 0$ will be used in all the text.

2.2.3. Definition. *We say that $p \in \mathbb{P}^n$ is a* **singularity** *of $\mathcal{X}$ if p is a zero of the section*

$$\mathcal{X} : \mathcal{O}_{\mathbb{P}^n} \to \mathcal{T}\mathbb{P}^n(d-1).$$

Explicitly, using the local expression in (2.8), the singularities of $\mathcal{X}$ in U_j are the common zeros of $\{a_i \mid i \neq j\}$. Alternatively, using homogeneous coordinates, the singularities of $\mathcal{X}$ are given by the ideal of $2\times 2-$minors, $Z_iF_j - Z_jF_i$ of the matrix $\left(\begin{smallmatrix} Z_0 & \cdots & Z_n \\ F_0 & \cdots & F_n \end{smallmatrix}\right)$, cf. [14], i.e. the singularities are the points p where $\mathcal{X}(p)$ has the same direction that $R(p)$.

Exercise 3. Using the Euler sequence we can compute the number of singularities of a generic vector field of degree d. The fact that $\mathcal{X}$ is generic implies that it has isolated singularities (see [32]). By Proposition (1.6.10, p. 47) we have:

$$\#\mathcal{Z}(\mathcal{X}) = c_n(\mathcal{T}\mathbb{P}^n(d-1)).$$

Prove that a dimension one foliation of degree d in $\mathbb{P}^n$ has

$$d^n + d^{n-1} + \cdots + d + 1$$

singularities (counting multiplicities). (Hint: use sequence (2.5, p. 49) and the properties of Chern classes.)

2.2.4. Definition. Order of a singularity.

Let p be a singularity of a vector field $\mathcal{X}$. Suppose that $p \in U_j$ and

$$\mathcal{X}_{U_j} = \sum_{i=1}^{n} a_i \frac{\partial}{\partial z_i}$$

is the local expression of $\mathcal{X}$ in U_j. Then the **order** (sometimes named **algebraic multiplicity**) of the singularity p is

$$\nu_p(\mathcal{X}) = \min\{order_p(a_i) \mid i = 1, \ldots, n\}.$$

As usual, the order $order_p(a)$ of a polynomial a at a point p means the order of vanishing: $\min\{s \mid \partial^s a/\partial z_I(p) \neq 0, |I| = s\}$.

Exercise 4. Check that the order of a singularity is independent of the choice of the open set U_j such that $p \in U_j$.

2.2.5. Definition. Invariant hypersurface.

Let $Z \subset \mathbb{P}^n$ be an irreducible hypersurface defined by a homogeneous polynomial G of degree k, and $\mathcal{X}$ be a vector field of degree d. We say that Z **is invariant by** $\mathcal{X}$ if

$$\mathcal{X}(p) \in \mathcal{T}_p Z$$

for all $p \in Z \setminus (Sing(Z) \cup Sing(\mathcal{X}))$.

If Z is reducible, we say that it is invariant by $\mathcal{X}$ if and only if each irreducible component of Z is invariant by $\mathcal{X}$.

Exercise 5.

(1) Prove that if G is irreducible, the above condition is equivalent to the existence of a degree $d-1$ homogeneuos polynomial H such that

$$dG(\mathcal{X}) = \mathcal{X}(G) = GH.$$

Hint: Use the Hilbert's Nullstellensatz.

(2) Prove that this condition does not depend on the representative of $\mathcal{X}$ in $S_d \otimes S_1^\vee$.

Hint: By the Euler relation we have that $R(G) = k \cdot G$.

(3) If G is reducible, and

$$G = G_1^{r_1} \cdots G_n^{r_n}$$

is a decomposition of G into irreducible factors, prove that $\mathcal{X}(G) = HG$ for some H if and only if for all $i = 1, \ldots, n$ we have $\mathcal{X}(G_i) = H_i G_i$ for some H_i's.

2.2.6. Definition. Invariant algebraic subvariety.

If $Z \subset \mathbb{P}^n$ is an algebraic subvariety defined by the ideal $I_Z := \langle G_1, \ldots, G_r \rangle$ and $\mathcal{X}$ is a vector field, we say that Z **is invariant by** $\mathcal{X}$ if

$$\mathcal{X}(p) \in \mathcal{T}_p Z$$

for all $p \in Z \setminus (Sing(Z) \cup Sing(\mathcal{X}))$.

Exercise 6. If I_Z is saturated, this condition is equivalent to

$$dG_i(\mathcal{X}) = \mathcal{X}(G_i) \in I_Z \qquad \text{for all } i = 1, \ldots, r.$$

The hypothesis of the ideal to be saturated is necessary. For example $\mathcal{Z}(Z_0)$ is invariant by $\frac{\partial}{\partial Z_1}$, but $\frac{\partial}{\partial Z_1}(Z_0 Z_1)$ is not in the ideal $\langle Z_0^2, Z_0 Z_1, \ldots, Z_0 Z_n \rangle$.

2.3. **Codimension one foliations.** In this section we define codimension one foliations in $\mathbb{P}^n$ (*i.e.,* foliations defined by integrable one forms in $\mathbb{P}^n$). However, in the text we only deal with codimension one foliations in $\mathbb{P}^2$, so we discuss this case and the correspondence between vector fields and forms in $\mathbb{P}^2$. For further reading see [38].

2.3.1. Definition. A **projective one form** of degree d in $\mathbb{P}^n$ is given by a global section of $\Omega_{\mathbb{P}^n} \otimes \mathcal{O}_{\mathbb{P}^n}(d+2)$, for some $d \geq 0$.

As in the case of vector fields in $\mathbb{P}^n$ we will deduce an expression in homogeneous coordinates for a form in $H^0(\mathbb{P}^n, \Omega_{\mathbb{P}^n} \otimes \mathcal{O}_{\mathbb{P}^n}(d+2))$.

Tensoring the (dual of the) Euler sequence (2.2) by $\mathcal{O}_{\mathbb{P}^n}(d+2)$ we obtain

$$0 \to \Omega_{\mathbb{P}^n}(d+2) \to \mathcal{O}_{\mathbb{P}^n}(d+1) \otimes S_1 \to \mathcal{O}_{\mathbb{P}^n}(d+2) \to 0 \tag{2.9}$$

Taking global sections, and using that $H^1(\mathbb{P}^n, \Omega_{\mathbb{P}^n}(d+2)) = 0$ we obtain the following exact sequence:

$$0 \to H^0(\mathbb{P}^n, \Omega_{\mathbb{P}^n}(d+2)) \longrightarrow S_{d+1} \otimes S_1 \xrightarrow{\iota_R} S_{d+2} \to 0$$

where

$$\iota_R(\sum A_i dZ_i) = \sum A_i Z_i$$

is the contraction by the radial vector field. Hence $H^0(\mathbb{P}^n, \Omega_{\mathbb{P}^n}(d+2))$ is the kernel of ι_R. It follows that a one form $\omega \in H^0(\mathbb{P}^n, \Omega_{\mathbb{P}^n}(d+2))$ can be written in homogeneous coordinates as

$$\omega = A_0 dZ_0 + \cdots + A_n dZ_n$$

where the A_i's are homogeneous polynomials of degree $d+1$ satisfying

$$A_0 Z_0 + \cdots + A_n Z_n = 0.$$

Notice that a one form induces a distribution of codimension one subspaces of $\mathcal{T}\mathbb{P}^n$ given by $p \mapsto \mathrm{Ker}\omega_p$. However, this distribution is not necessarily integrable. (A distribution is called **integrable** if there exists a smooth germ of hypersurface U at p such that $\mathcal{T}_q U = \mathrm{Ker}\omega_q$, $\forall\, q \in U$ near p).

The condition to be integrable is expressed by Frobenius equation,

$$\omega \wedge d\omega = 0.$$

For a geometric interpretation see [38] or [4].

2.3.2. Definition. A **codimension one foliation** is an integrable projective one form modulo non zero complex multiples.

Denote

$$V_{n-1,n,d} = H^0(\mathbb{P}^n, \Omega_{\mathbb{P}^n}(d+2)).$$

A codimension one foliation is given by an element ω of

$$\mathbb{F}(n-1, n, d) := \mathbb{P}(V_{n-1,n,d})$$

such that $\omega \wedge d\omega = 0$.

2.3.3. Remark. The condition $\omega \wedge d\omega = 0$ translates into a system of quadratic equations in $\mathbb{P}(V_{n-1,n,d})$. They define the scheme of codimension one foliations of degree d in $\mathbb{P}^n$. Very little is known about it. The problem of determining their irreducible components remains a rather challenging field of research, cf. [38].

Next we explain the local expression of a projective one form.

Let U_j denote the affine open set $Z_j \neq 0$, with coordinates $(z_0, \ldots, \hat{z_j}, \ldots, z_n)$. The local expression of a one form

$$\omega = A_0 dZ_0 + A_1 dZ_1 + \cdots + A_n dZ_n$$

on U_j is

$$\omega_{U_j} = a_0 dz_0 + \cdots + \widehat{a_j dz_j} + \cdots + a_n dz_n$$

where a_i is the dehomogenization of A_i with respect to Z_j.

2.3.4. Definition. The **degree of a codimension one foliation** is d if it is given by a one form in $\mathbb{F}(n-1, n, d)$.

Geometrically, if $\omega \in \mathbb{F}(n-1, n, d)$, the degree is the number of tangencies of the distribution induced by ω with a generic line in $\mathbb{P}^n$. For example, suppose that ω is given in U_0 by

$$a_1 dz_1 + \cdots + a_n dz_n$$

and take the parametrized line $\ell = (t, 0, \ldots, 0)$. Then the tangencies of ω with ℓ are given by the zeros of $\omega_{|\ell} = a_1(t, 0, \ldots, 0)dt$. In principle, a_1 has degree $\leq d+1$, but the condition of contraction by the radial vector field gives us $a_0(t, 0, \ldots, 0) = -t a_1(t, 0, \ldots, 0)$, so $a_1(t, 0, \ldots, 0)$ has degree $\leq d$, and the number of points of tangencies is d. For more detailed discussion see [38, Proposition 1.2.1 p. 21].

2.3.5. Definition. The **singularities** of a projective one form ω are the zeros of the section

$$\omega : \mathcal{O}_{\mathbb{P}^n} \to \Omega_{\mathbb{P}^n}(d+2).$$

Locally, if we write $\omega = a_1 dz_1 + \cdots + a_n dz_n$, the scheme of singularities of ω is defined by the ideal generated by $a_1, \ldots, a_n$. As a set, it consists of the common zeros of the a_i.

Exercise 7. As in the case of vector fields, show that a generic one form has isolated singularities. Using the sequence (2.9) and Proposition 1.6.10 show that the the number of singularities of a generic one form is the degree of the zero-cycle $c_n(\Omega_{\mathbb{P}^n}(d+2))$. Prove that this number is given by

$$(d+1)^n - (d+1)^{n-1} + \cdots + (-1)^{n-i}(d+1)^i + \cdots + (-1)^n.$$

2.3.6. Remark. In the case of integrable one forms, if $n \geq 3$ the set of singularities is not a finite set. In fact [32, p. 95] shows that there always exists a component of the singular set that has codimension two.

2.3.7. Definition. (Order of a singularity.)
Let p be a singularity of ω. Suppose that $p \in U_0$ and write

$$\omega = a_1 dz_1 + \cdots + a_n dz_n$$

for the local expression of ω in U_0. Then the **order of the singularity** p is

$$\nu_p(\omega) = \min\{\mathrm{ord}_p(a_i) \mid i = 1, \ldots, n\}.$$

It can be easily checked that this is independent of the choice of the open set U_j.

Some authors use *multiplicity* of the singularity instead of order.
In what follows we restrict ourselves to the case $n = 2$.

2.3.8. Definition. (Dicritical singularity) Let $\omega \in H^0(\mathbb{P}^2, \Omega_{\mathbb{P}^2}(d+2))$ and suppose that $p \in \mathbb{P}^2$ is a singularity of ω of order k. Let

$$\omega_p = a_k dx + b_k dy + h.o.t.$$

be a local expression of ω around $p = (0,0)$. We say p is **dicritical of order** k if

$$a_k x + b_k y \equiv 0$$

(see [39, p. 47]). In the case $k = 1$, we say that p is a **radial singularity**.

Exercise 8. Prove that the dicriticity condition is equivalent to

$$\omega_p = f(x,y)(ydx - xdy) + h.o.t$$

for some homogeneous polynomial f of degree $k-1$.

2.3.9. Definition. (Invariant hypersurface.)
Let $W \subset \mathbb{P}^2$ be an irreducible hypersurface defined by a homogeneous polynomial G of degree k, and $\mathcal{F}$ a foliation defined by a one form ω. We say that W **is invariant by** $\mathcal{F}$ if

$$\mathcal{T}_p W \subset \ker \omega_p$$

for all $p \in W \setminus (Sing(W) \cup Sing(\omega))$.

If W is reducible, we say that it is invariant by $\mathcal{F}$ if and only if each irreducible component of W is invariant by $\mathcal{F}$.

If G is irreducible, the above condition is equivalent to the existence of a two-form θ of degree d such that

$$dG \wedge \omega = G\theta.$$

See [32, p. 99].

2.3.10. Definition. (Points of tangency with a hypersurface.)

In the definition above, if W is not invariant, the two-form $dG \wedge \omega$ is not identically zero in W. The zeros of this form in $W \setminus (Sing(W))$ are the **tangencies of $\mathcal{F}$ with W.**

2.4. **Vector fields versus forms in $\mathbb{P}^2$.** In $\mathbb{P}^2$, a foliation can be defined by a vector field or by a one form.

In what follows we study one forms in $\mathbb{P}^2$ and their relation with vector fields.

Exercise 9. Prove that all one forms in $\mathbb{P}^2$ are automatically integrable *i.e.,* if

$$\omega = A_0 dZ_0 + A_1 dZ_1 + A_2 dZ_2$$

with homogeneous A_i of same degree, then

$$\iota_R(\omega) = 0 \implies \omega \wedge d\omega = 0.$$

Hence a foliation of degree d in $\mathbb{P}^2$ can be given by a vector field

$$\mathcal{X} \in H^0(\mathbb{P}^2, \mathcal{T}\mathbb{P}^2(d-1))$$

or by a one form

$$\omega \in H^0(\mathbb{P}^2, \Omega_{\mathbb{P}^2}(d+2)).$$

2.4.1. Remark. The reason behind this correspondence is the following. Recall that if $\mathcal{E}$ is a locally free sheaf of rank 2 we have a natural isomorphism

$$\mathcal{E} \simeq \mathcal{E}^\vee \otimes \overset{2}{\wedge} \mathcal{E}.$$

See [31, exercise 5.16 p. 127]. Taking $\mathcal{E} = \Omega_{\mathbb{P}^2}$ we obtain

$$\Omega_{\mathbb{P}^2} \simeq \mathcal{T}\mathbb{P}^2(-3).$$

Thus $\Omega_{\mathbb{P}^2}(d+2) \simeq \mathcal{T}\mathbb{P}^2(d-1)$.

If a foliation in $\mathbb{P}^2$ is given by a vector field

$$\mathcal{X} = F_0 \frac{\partial}{\partial Z_0} + F_1 \frac{\partial}{\partial Z_1} + F_2 \frac{\partial}{\partial Z_2}$$

and by a one form

$$\omega = A_0 dZ_0 + A_1 dZ_1 + A_2 dZ_2,$$

we may express the $F_i's$ in terms of the $A_i's$ and vice versa as follows.

Given $\mathcal{X}$ as above, the coefficients of ω are expressed by

$$\begin{cases} A_0 = Z_2F_1 - Z_1F_2, \\ A_1 = Z_0F_2 - Z_2F_0, \\ A_2 = Z_1F_0 - Z_0F_1. \end{cases}$$

Given ω, the coefficients of the vector field $\mathcal{X}$ can be obtained from

$$d\omega = (d+2)(F_0 dZ_1 \wedge dZ_2 + F_1 dZ_2 \wedge dZ_0 + F_2 dZ_0 \wedge dZ_1)$$

This is a consequence of the acyclicity of the Koszul complex associated to the regular sequence $\{Z_0, Z_1, Z_2\}$. See [32, §1.5].

Exercise 10. Prove that if ω and $\mathcal{X}$ define the same foliation in $\mathbb{P}^2$, then in U_0 we have

$$\omega_{U_0} = a_1 dz_1 + a_2 dz_2$$

and

$$\mathcal{X}_{U_0} = -a_2 \frac{\partial}{\partial z_1} + a_1 \frac{\partial}{\partial z_2}.$$

This corresponds to the intuitive idea that the vector field and the form defining a foliation are orthogonal to each other.

3. Foliations with degenerate singularities

If $\omega \in \mathbb{P}^N$, $(N = N_{1,2,d})$ defines a generic foliation of degree d in $\mathbb{P}^2$, its singularities are all nondegenerate (see [32]); in particular, they have all order one. In this Section we study foliations in $\mathbb{P}^2$ that have a degenerate singularity.

The first type of degeneration we will consider is to ask the order of the singularity to be some $k \geq 2$. The reader can easily check that, if ω_1, ω_2 are one forms that have order $\geq k$ at a point $p \in \mathbb{P}^2$, the same holds true for any linear combination $a_1\omega_1 + a_2\omega_2, a_i \in \mathbb{C}$. Thus, for fixed p, the condition is linear on the space of one forms.

This leads us to the correspondence $\mathbb{W}_k \subseteq \mathbb{P}^2 \times \mathbb{P}^N$ defined by the pairs (p, ω) such that the order of ω at p is $\geq k$. We define the locus $\mathbb{M}_k \subset \mathbb{P}^N$ of foliations with a singularity of order at least k as the image $p_2(\mathbb{W}_k) \subset \mathbb{P}^N$ by the second projection.

As expected from the previous discussion, $\mathbb{W}_k$ is actually a projective subbundle of $\mathbb{P}^2 \times \mathbb{P}^N$ over $\mathbb{P}^2$. More precisely, we have that $\mathbb{W}_k = \mathbb{P}(\mathcal{M}_k)$, the projectivization of a vector bundle $\mathcal{M}_k$ over $\mathbb{P}^2$. We are able to determine its characteristic classes, used to find the degree of $\mathbb{M}_k$.

In Section 3.2 we study the space $\mathbb{D}_k \subset \mathbb{M}_k$ of foliations that has a dicritical singularity of order k. Again, this is a closed condition, and we construct a parametrization of that space. We find a vector subbundle $\mathcal{D}_k \subset \mathcal{M}_k$ over $\mathbb{P}^2$, such that the image by the second projection of $\mathbb{P}(\mathcal{D}_k)$ is $\mathbb{D}_k$. We determine the characteristic classes of $\mathcal{D}_k$, and with this at hand we can compute the degree of $\mathbb{D}_k$.

Requiring a leaf of a foliation to be tangent to a line at a given point defines a hyperplane in $\mathbb{P}^N$. Thus, finding the degree of the loci $\mathbb{D}_k \subset \mathbb{M}_k$ can be rephrased loosely as calculating the number of foliations with a singularity of the chosen type and further tangent to the appropriate number of flags (point, line) in $\mathbb{P}^2$. It turns out that the degrees of $\mathbb{D}_k$ and $\mathbb{M}_k$ are expressed as explicit polynomials in k, d.

3.1. Singularities of prescribed order.

In order to simplify the notation we set

$$V := V_{1,2,d} = H^0(\mathbb{P}^2, \Omega_{\mathbb{P}^2}(d+2)) \quad \text{and} \quad N := N_{1,2,d} = \dim V - 1\,.$$

Fix $k \leq d+1$. In this section we describe a parameter space $\mathbb{M}_k \subset \mathbb{P}^N$ for the locus of foliations of given degree d that have some singularity of order $\geq k$. In fact we obtain a filtration of $\mathbb{P}^N$,

$$\mathbb{M}_{d+1} \subset \cdots \subset \mathbb{M}_3 \subset \mathbb{M}_2 \subset \mathbb{M}_1 = \mathbb{P}^N.$$

In Proposition (3.1.3, p. 57) we show that the codimension of $\mathbb{M}_k$ in $\mathbb{P}^N$ is

$$\mathrm{cod}\mathbb{M}_k = k(k+1) - 2$$

and

$$\deg(\mathbb{M}_k) = \int c_2(\mathcal{P}^{k-1}(\Omega_{\mathbb{P}^2}(d+2))) \cap [\mathbb{P}^2]$$

where $\mathcal{P}^{k-1}(\Omega_{\mathbb{P}^2}(d+2))$ is the $(k-1)-$jet bundle associated to $\Omega_{\mathbb{P}^2}(d+2)$, (cf. Appendix (A.1.4, p. 81)).

Recall (Definition 2.3.7, p. 53) that if $\omega \in H^0(\mathbb{P}^2, \Omega_{\mathbb{P}^2}(d+2))$, the order of a singularity $p \in \mathbb{P}^2$ is

$$\nu_p(\omega) := \min\{order_p(a), order_p(b)\},$$

where $\omega_p = adx + bdy$ is a local expression of ω in a neighborhood of p with $x(p) = y(p) = 0$.

Order one. Consider the map of fiber bundles over $\mathbb{P}^2$,

$$ev : \mathbb{P}^2 \times V \to \Omega_{\mathbb{P}^2}(d+2)$$

given by evaluation, $ev(p, \omega) = (p, \omega(p))$.

We claim that ev is surjective. In fact, it is sufficient to prove the surjectivity in the fibers. For this suppose $p = [0:0:1]$ and let $\lambda dx + \mu dy \in \Omega_p(d+2)$. Then

$$\omega := Z_2^d(Z_2\lambda dZ_0 + Z_2\mu dZ_1 - (Z_0\lambda + Z_1\mu)dZ_2) \in H^0(\mathbb{P}^2, \Omega_{\mathbb{P}^2}(d+2))$$

satisfies $\omega(p) = \lambda dx + \mu dy$.

3.1.1. Remark. The fact that $\Omega_{\mathbb{P}^2}(d+2)$ is generated by global sections can also be proven with cohomological tools, cf. [32, Lemme 2.3.6, p. 90].

Set $\mathcal{M} := \mathrm{Ker}(ev)$. Since ev is surjective, $\mathcal{M}$ is a subbundle of V of rank

$$\mathrm{rk}\,\mathcal{M} = \dim V - 2 = N - 1\,.$$

It fits into the following exact sequence

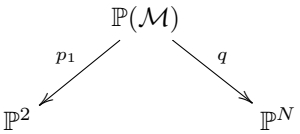
$$0 \to \mathcal{M} \longrightarrow \mathbb{P}^2 \times V \longrightarrow \Omega_{\mathbb{P}^2}(d+2) \to 0. \tag{3.1}$$

3.1.2. Definition. The **universal singular set** is the projective bundle associated to $\mathcal{M}$, *i.e.,* the incidence variety:

$$\mathbb{P}(\mathcal{M}) = \{(p, [\omega]) \mid p \text{ is singularity of } [\omega]\} \subset \mathbb{P}^2 \times \mathbb{P}^N.$$

Let us denote by p_1, q the projections of $\mathbb{P}(\mathcal{M})$ in the first and second factor respectively.

We have the diagram



where q is surjective (all foliations have singularities) and generically finite (a generic foliation has isolated singularities) cf.[32].

We may compute the cardinality of a generic fiber of q (*i.e.,* $\deg(q)$) as follows. Observe that $q_*[\mathbb{P}(\mathcal{M})] = \deg(q)[\mathbb{P}^N]$. Write $H := c_1(\mathcal{O}_{\mathbb{P}^N}(1))$. Using properties of Chern classes and degree we have

$$\deg(q) = \int s_2(\mathcal{M}) \cap [\mathbb{P}^2].$$

The equality follows by Lemma (1.6.5, p. 45), recalling that $\mathrm{rk}(\mathcal{M}) = N-1$. In this way we retrieve the number of singularities of a general degree d foliation. Indeed, by sequence (3.1) we have $s_2(\mathcal{M}) = c_2(\Omega_{\mathbb{P}^2}(d+2))$. From the Euler sequence we find

$$c_2(\Omega_{\mathbb{P}^2}(d+2)) = d^2 + d + 1.$$

Order $k > 1$. Recall the exact sequence (see Appendix (A.1.4, p. 81)) for the jet bundles of $\Omega_{\mathbb{P}^2}(d+2)$,

$$0 \to \mathrm{Sym}_n \Omega_{\mathbb{P}^2} \otimes \Omega_{\mathbb{P}^2}(d+2) \to \mathcal{P}^n(\Omega_{\mathbb{P}^2}(d+2)) \to \mathcal{P}^{n-1}(\Omega_{\mathbb{P}^2}(d+2)) \to 0 \tag{3.2}$$

and the maps $ev_n : \mathbb{P}^2 \times V \to \mathcal{P}^n(\Omega_{\mathbb{P}^2}(d+2))$.

Exercise 11.

(1) Prove that ev_n is surjective for all $n \leq d+1$.
(2) Prove that $ev_n(\mathrm{Ker}(ev_{n-1})) = \mathrm{Sym}_n \Omega_{\mathbb{P}^2} \otimes \Omega_{\mathbb{P}^2}(d+2)$.

3.1.3. Proposition. *For $1 \leq k \leq d+1$, denote by*

$$\mathbb{M}_k = \{[\omega] \in \mathbb{P}^N \mid [\omega] \text{ has a singularity of order at least } k\}.$$

Then we have

$$\mathrm{cod}_{\mathbb{P}^N}(\mathbb{M}_k) = k(k+1) - 2$$

and

$$\deg(\mathbb{M}_k) = \int_{\mathbb{P}^2} c_2(\mathcal{P}^{k-1}(\Omega_{\mathbb{P}^2}(d+2)))\,.$$

Proof. Define

$$\mathcal{M}_k = \mathrm{Ker}\left(ev_{k-1} : \mathbb{P}^2 \times V \to \mathcal{P}^{k-1}(\Omega_{\mathbb{P}^2}(d+2))\right)\,.$$

In view of the previous exercise, we see that $\mathcal{M}_k$ is a vector subbundle of V of corank equal to $\mathrm{rk}\,\mathcal{P}^{k-1}(\Omega_{\mathbb{P}^2}(d+2))$. By construction, the projective bundle associated to $\mathcal{M}_k$ is the incidence variety,

$$\mathbb{P}(\mathcal{M}_k) = \{(p, [\omega]) \in \mathbb{P}^2 \times \mathbb{P}^N \mid p \text{ is a singularity of } [\omega] \text{ and } \nu_p(\omega) \geq k\}.$$

Let $q : \mathbb{P}(\mathcal{M}_k) \to \mathbb{P}^N$ denote the projection in the second factor. We have $\mathbb{M}_k = q(\mathbb{P}(\mathcal{M}_k))$.

It is easy to check that q is generically injective (for $k > 1$) (cf. Lemma 3.1.4 below). It follows from Lemma 1.6.5, p. 45 that

$$\deg(\mathbb{M}_k) = \int s_2(\mathcal{M}_k) \cap [\mathbb{P}^2].$$

Since by definition of $\mathcal{M}_k$, $s_2(\mathcal{M}_k) = c_2(\mathcal{P}^{k-1}(\Omega_{\mathbb{P}^2}(d+2)))$, the second assertion follows. The first assertion follows from the exact sequence (A.1), p. 81, and a simple inductive argument. □

3.1.4. Lemma. *For all $2 \leq k \leq d+1$ the projection $q : \mathbb{P}(\mathcal{M}_k) \to \mathbb{P}^N$ is generically injective.*

Proof. By Lemma 1.6.6, p. 45, we shall find a form ω of degree $d+1$ such that

(i): it has a unique singularity p of order k and
(ii): $d_{(p,[\omega])}q$ is injective.

Suppose that $k > 2$. We claim that the following form fulfills (i) and (ii):

$$\omega = (Z_2^{d-(k-1)} Z_0^{k-1} + Z_2^{d-(k-1)} Z_1^{k-1} + Z_0^d + Z_1^d)(-Z_1 dZ_0 + Z_0 dZ_1).$$

Indeed, write $F := Z_2^{d-(k-1)} Z_0^{k-1} + Z_2^{d-(k-1)} Z_1^{k-1} + Z_0^d + Z_1^d$. In the chart U_2 we have

$$\omega = (x^{k-1} + y^{k-1} + x^d + y^d)(-ydx + xdy) := f \cdot (-ydx + xdy) := adx + bdy.$$

Is clear that $(0,0)$ is a singularity of order k. Suppose that $(\alpha, \beta) \in U_2 = \mathbb{C}^2$ is another singularity. Then we have

$$f(\alpha, \beta) = \alpha^{k-1} + \beta^{k-1} + \alpha^d + \beta^d = 0.$$

On the other hand, if the first jet of ω at that point is zero we have

$$\begin{cases} \frac{\partial a}{\partial x}(\alpha,\beta) &= -\beta \frac{\partial f}{\partial x}(\alpha,\beta) = -\beta\alpha^{k-2}(k-1+d\alpha^{d-k+1}) = 0 \\ \frac{\partial a}{\partial y}(\alpha,\beta) &= -\beta \frac{\partial f}{\partial y}(\alpha,\beta) = -\beta^{k-1}(k-1+d\beta^{d-k+1}) = 0 \\ \frac{\partial b}{\partial x}(\alpha,\beta) &= \alpha \frac{\partial f}{\partial x}(\alpha,\beta) = \alpha^{k-1}(k-1+d\alpha^{d-k+1}) = 0 \\ \frac{\partial b}{\partial y}(\alpha,\beta) &= \alpha \frac{\partial f}{\partial y}(\alpha,\beta) = \alpha\beta^{k-2}(k-1+d\beta^{d-k+1}) = 0. \end{cases}$$

Suppose that $\alpha \neq 0$. Then $\frac{\partial f}{\partial x}(\alpha,\beta) = 0$. If (α,β) is a singularity of order greater than two, then

$$\frac{\partial^2 b}{\partial^2 x}(\alpha,\beta) = \alpha \frac{\partial^2 f}{\partial^2 x}(\alpha,\beta) = \alpha^{k-2}((k-1)(k-2) + d(d-1)\alpha^{d-k+1}) = 0$$

i.e.,

$$((k-1)(k-2) + d(d-1)\alpha^{d-k+1}) = 0.$$

This, together with $d\alpha^{d-k+1} = -(k-1)$ implies $k-2-(d-1) = k-1-d = 0$ *i.e.,* $k = d+1$. It is easy to see that if $k = d+1$ the unique singularity of order ≥ 1 is $(0,0)$. Therefore $\alpha = 0$, and similarly $\beta = 0$.

On the other charts, for example in U_0 the expression of the form is

$$(z^{d-k+1}(1 + y^{k-1}) + 1 + y^d)dy.$$

It is easy to see that the singularities are of order less than two.

It remains to show that $d_{(p,[\omega])}q$ is injective. For this, we consider a vector $((p_1,p_2),\theta)) \in \mathcal{T}_{(p,[\omega])}\mathbb{P}(\mathcal{M}_k)$, and we have to prove that $\theta = 0$ implies $p_1 = p_2 = 0$.

The vector above is the tangent vector to a curve $([\varepsilon p_1 : \varepsilon p_2 : 1], \omega + \varepsilon\theta)$ in $\mathbb{P}(\mathcal{M}_k)$ if and only if the point is a singularity of order $\geq k$ (working in $\mathbb{C}[\varepsilon]/\langle\varepsilon^2\rangle$).

Suppose that $J_i(\omega + \varepsilon\theta)(\varepsilon p_1, \varepsilon p_2) = 0$ for all $i \leq k-1$ (here $J_i(\omega)$ stands for the part of order i of ω). It is easy to see that in this case, if $\theta = 0$, $J_{k-1}(\omega + \varepsilon\theta)(\varepsilon p_1, \varepsilon p_2) = 0$ implies

$$\begin{cases} -\varepsilon p_2 \frac{\partial^{k-1} f}{\partial^{k-1} x}(\varepsilon p_1, \varepsilon p_2) = 0 \\ -\varepsilon p_1 \frac{\partial^{k-1} f}{\partial^{k-1} x}(\varepsilon p_1, \varepsilon p_2) = 0. \end{cases}$$

But $\frac{\partial^{k-1} f}{\partial^{k-1} x} = ((k-1)! + d(d-1)\cdots(d-k+2)x^{d-k+1})$. Hence the above equations imply

$$\begin{cases} \varepsilon p_2 (k-1)! = 0 \\ \varepsilon p_1 (k-1)! = 0 \end{cases}$$

i.e., $p_1 = p_2 = 0$.

For $k = 2$, the form

$$\omega := (Z_0 Z_2^{d-1} + Z_1 Z_2^{d-1} + Z_0^d + (-Z_1)^d)(-Z_1 dZ_0 + Z_0 dZ_1)$$

has the required properties.

□

Employing the proposition above, we may now derive an explicit formula for the degree of $\mathbb{M}_k \subset \mathbb{P}^N$. We use SCHUBERT, [34] to do the computations, see the script in [16]. We find

3.1.5. Corollary. *The degree of* $\mathbb{M}_k$ *is*

$$\frac{1}{2}k(k+1)\left[(k^2+k-1)\left(d^2-(2k-3)d\right) + \frac{1}{4}(4k^4 - 8k^3 - 7k^2 + 21k - 6)\right].$$

□

3.2. **Dicritical singularities.** Recall that if $\omega \in H^0(\mathbb{P}^2, \Omega_{\mathbb{P}^2}(d+2))$ and p is a singularity of ω, we say that p is dicritical if the local expression of ω around p is

$$\omega_p = a_k dx + b_k dy + h.o.t$$

with $a_k x + b_k y = 0$ (Definition 2.3.8, p. 53). To have a dicritical singularity will be shown to be a closed condition in $\mathbb{P}^N$. This will be rephrased shortly in a coordinate-free manner.

In this section we describe the locus $\mathbb{D}_k$ of forms of given degree that have a dicritical singularity of order k.

In Proposition (3.2.3, p. 60) we obtain that the codimension of $\mathbb{D}_k$ is

$$k(k+2)$$

and the degree of $\mathbb{D}_k$ is given by the coefficient of the degree two part of

$$c(\mathcal{P}^{k-1}(\Omega_{\mathbb{P}^2}(d+2)))c(\mathrm{Sym}_{k+1}\,\Omega_{\mathbb{P}^2} \otimes \mathcal{O}_{\mathbb{P}^2}(d+2)).$$

3.2.1. Remark. Next we explain an invariant way to express the condition that a singularity is dicritical.

Suppose that $\mathcal{E}$ is a vector bundle of rank 2. Then for all $k \geq 1$ we have the following exact sequence (*e.g.,* see [13, Appendix 2 A2.6.1.]):

$$0 \to \overset{2}{\wedge}\mathcal{E} \otimes \mathrm{Sym}_{k-1}\mathcal{E} \to \mathrm{Sym}_k \mathcal{E} \otimes \mathcal{E} \xrightarrow{P_k} \mathrm{Sym}_{k+1}\mathcal{E} \to 0,$$

where the first map is given by

$$(a \wedge b \otimes c) \mapsto (ac \otimes b) - (bc \otimes a)$$

and the second by

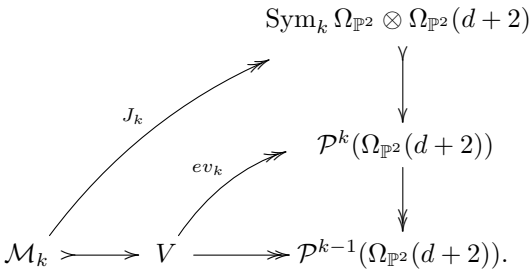
$$a \otimes b \mapsto ab.$$

Say x, y form a local basis for $\mathcal{E}$. Then for $a_k, b_k \in \mathrm{Sym}_k \mathcal{E}$, we have that $a_k x + b_k y = 0$ in $\mathrm{Sym}_{k+1}\mathcal{E}$ if and only if there is some $c \in \mathrm{Sym}_{k-1}\mathcal{E}$ such that $a_k \otimes x + b_k \otimes y$ is equal to the image of $x \wedge y \otimes c$, to wit, $xc \otimes y - yc \otimes x$. cf. Exercise (8, p. 53).

3.2.2. Lemma. *For all $1 \leq k \leq d$ there exists a subbundle $\mathcal{D}_k$ of the trivial bundle $\mathbb{P}^2 \times V$ such that*

$$\mathbb{P}(\mathcal{D}_k) = \{(p, [\omega]) \mid p \text{ is a dicritical singularity of } [\omega] \text{ with } \nu_p(\omega) \geq k\} \subset \mathbb{P}^2 \times \mathbb{P}^N.$$

Proof. From the previous section we have the following diagram,



where the map J_k is surjective in view of Exercise 11.

We obtain the surjective map

$$\mathcal{M}_k \xrightarrow{J_k} \mathrm{Sym}_k \Omega_{\mathbb{P}^2} \otimes \Omega_{\mathbb{P}^2}(d+2) \xrightarrow{P_k} \mathrm{Sym}_{k+1} \Omega_{\mathbb{P}^2}(d+2).$$
$$\mathcal{M}_k \xrightarrow{T_k} \mathrm{Sym}_{k+1} \Omega_{\mathbb{P}^2}(d+2).$$

Explicitly, on the fiber over $p \in \mathbb{P}^2$ the map is as follows:

$$T_k(p, \omega) = (p, a_k x + b_k y)$$

where

$$\omega_p = a_k dx + b_k dy + h.o.t.$$

is the local expression of ω in a neighborhood of p with $x(p) = y(p) = 0$. Set

$$\mathcal{D}_k := \ker\left(\mathcal{M}_k \xrightarrow{T_k} \mathrm{Sym}_{k+1} \Omega_{\mathbb{P}^2}(d+2)\right) \tag{3.3}$$

Thus $\mathcal{D}_k$ is a vector bundle of rank $= \mathrm{rk}(\mathcal{M}_k) - (k+2)$. Recalling (3.2.1, p. 59), we see that the projective bundle associated to $\mathcal{D}_k$ is the incidence variety,

$$\mathbb{P}(\mathcal{D}_k) = \{(p, [\omega]) \in \mathbb{P}^2 \times \mathbb{P}^N \mid p \text{ is a dicritical singularity of } [\omega] \text{ with } \nu_p(\omega) \geq k\}.$$

□

For $1 \leq k \leq d+1$, denote by

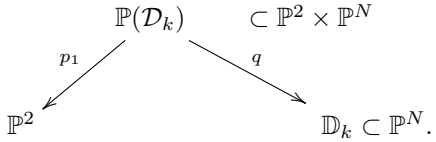
$$\mathbb{D}_k = \{[\omega] \in \mathbb{P}^N \mid [\omega] \text{ has a dicritical singularity of order at least } k\}.$$

3.2.3. Proposition. *The degree of $\mathbb{D}_k$ is the coefficient of the degree two part of*

$$c(\mathcal{P}^{k-1}(\Omega_{\mathbb{P}^2}(d+2)))c(\mathrm{Sym}_{k+1} \Omega_{\mathbb{P}^2} \otimes \mathcal{O}_{\mathbb{P}^2}(d+2)).$$

The codimension of $\mathbb{D}_k$ is $k(k+2)$.

Proof. From the above construction we have the maps



If q is generically injective the degree of $\mathbb{D}_k$ is computed as

$$\int s_2(\mathcal{D}_k) \cap [\mathbb{P}^2]$$

(see Lemma (1.6.5, p. 45)). By construction $\mathcal{D}_k$ fits into the following exact sequence,

$$0 \to \mathcal{D}_k \to \mathcal{M}_k \to \mathrm{Sym}_{k+1}\, \Omega_{\mathbb{P}^2} \otimes \mathcal{O}_{\mathbb{P}^2}(d+2) \to 0.$$

Hence

$$s(\mathcal{D}_k) = s(\mathcal{M}_k) c(\mathrm{Sym}_{k+1}\, \Omega_{\mathbb{P}^2} \otimes \mathcal{O}_{\mathbb{P}^2}(d+2))\,,$$

and from the proof of Proposition 3.1.3 we have $s(\mathcal{M}_k) = c(\mathcal{P}^{k-1}(\Omega_{\mathbb{P}^2}(d+2)))$.

On the other hand, $\mathrm{rk}(\mathcal{D}_k) = \mathrm{rk}(\mathcal{M}_k) - (k+2)$. Thus

$$\mathrm{cod}_{\mathbb{P}^N} \mathbb{D}_k = \mathrm{cod}\mathbb{M}_k + (k+2) = k(k+1) - 2 + (k+2) = k(k+2)\,.$$

It remains to prove that q is generically injective, but this follows from the generic injectivity of the projection $\mathbb{P}(\mathcal{M}_k) \to \mathbb{M}_k$. Indeed, let $U \subset \mathbb{M}_k$ denote the open set where the fiber of $\mathbb{P}(\mathcal{M}_k) \to \mathbb{M}_k$ consists of just one reduced point. Now observe that the examples constructed in Lemma (3.1.4, p. 57) are in $U \cap \mathbb{D}_k$. Hence $U \cap \mathbb{D}_k$ is a non empty open set over which the fibers of $q : \mathbb{P}(\mathcal{D}_k) \to \mathbb{D}_k$ consist of one reduced point. □

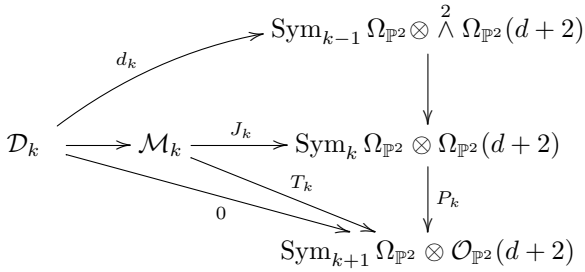
We may now compute an explicit formula for the degree of $\mathbb{D}_k \subset \mathbb{P}^N$ using Schubert, [34]. See the script in [16]. We find

3.2.4. Corollary. *The degree of $\mathbb{D}_k$ is given by*

$$(k+1)^2 \left[\frac{1}{2}(k^4+k^2-2k+2) - (k^3+k^2+k-1)d + \frac{1}{2}(k^2+2k+2)d^2\right].$$

□

3.2.5. Remarks. (i) We have by construction the following diagram:



By definition of $\mathcal{D}_k$ we get a map

$$d_k : \mathcal{D}_k \to \mathrm{Sym}_{k-1}\, \Omega_{\mathbb{P}^2} \otimes \overset{2}{\wedge} \Omega_{\mathbb{P}^2} \otimes \mathcal{O}_{\mathbb{P}^2}(d+2)$$

given in the fibers by $d_k(p, \omega) = f(x,y)dx \wedge dy$ where f is a polynomial of degree $k-1$.

(ii) In the case $k = 1$ we have

$$\omega = \lambda(ydx - xdy) + h.o.t.$$

with $\lambda \in \mathbb{C}$, *i.e.,* a radial singularity (see Definition (2.3.8, p. 53)). Thus Corollary 3.2.4 and Proposition 3.2.3 give formulas for the codimension and degree of the space of foliations with a radial singularity:

$$\begin{cases} \operatorname{cod}_{\mathbb{P}^N} \mathbb{D}_1 = 3 \\ \deg \mathbb{D}_1 = 10d^2 - 8d + 4. \end{cases}$$

(iii) In the case $k = d+1$ the map

$$J_{d+1} : \mathcal{M}_{d+1} \to \operatorname{Sym}_{d+1} \Omega^1_{\mathbb{P}^2} \otimes \Omega_{\mathbb{P}^2}(d+2)$$

is no longer surjective: its image is $\operatorname{Sym}_d \Omega_{\mathbb{P}^2} \otimes \overset{2}{\wedge} \Omega^1_{\mathbb{P}^2} \otimes \mathcal{O}_{\mathbb{P}^2}(d+2)$. Indeed, suppose that ω is a form of degree $d+1$ which has p as singularity of order $d+1$. Then a local expression of ω is

$$\omega_p = a_{d+1}dx + b_{d+1}dy\,,$$

but this form defines a projective form of degree $d+1$ in $\mathbb{P}^2$ if and only if

$$a_{d+1}x + b_{d+1}y = 0$$

i.e., if p is a dicritical singularity. Therefore we can write

$$\omega_p = f(x,y)(ydx - xdy)$$

for some homogeneous polynomial f of degree d, *i.e.,* $\omega_p \in \operatorname{Sym}_d \Omega^1_p \otimes \overset{2}{\wedge} \Omega^1_p$. Hence

$$T_{d+1} : \mathcal{M}_{d+1} \xrightarrow{J_{d+1}} \operatorname{Sym}_{d+1} \Omega_{\mathbb{P}^2} \otimes \Omega_{\mathbb{P}^2}(d+2) \xrightarrow{P_{d+1}} \operatorname{Sym}_{d+2} \Omega_{\mathbb{P}^2} \otimes \mathcal{O}_{\mathbb{P}^2}(d+2)$$

is the zero map. This shows that $\mathcal{M}_{d+1} = \mathcal{D}_{d+1}$, *i.e.,* for a foliation of degree d a singularity of order $d+1$ is automatically dicritical.

4. Foliations with invariant algebraic subvarieties

Jouanoulou shows in [32] that the set of foliations that do not have any invariant algebraic curve is dense in the ordinary topology in the variety that parametrizes foliations of degree $d \geq 2$ in $\mathbb{P}^2$. In [37] Lins-Neto proves that this set contains an open and dense subset. Finally, in [9] Coutinho and Pereira show that in a smooth complex projective variety of dimension grater or equal to two, a generic foliation of dimension one and sufficiently ample cotangent bundle (in the case of $\mathbb{P}^n$ this means degree big enough) has no invariant algebraic subvarieties of positive dimension. In fact the result of Jouanoulou (Coutinho and Pereira respectively) states that the set U_k of dimension one foliations in $\mathbb{P}^2$ ($\mathbb{P}^n$ respectively) without algebraic solution of degree k is an open set in the Zariski topology. We then ask for the complementary of the open set U_k. *i.e.,* we want to study the subset of the space of foliations of dimension one and degree $d \geq 2$ in $\mathbb{P}^n$ that has an algebraic solution of fixed degree and dimension.

To be more precise, we fix some type of positive dimensional subvarieties in $\mathbb{P}^n$. By this we mean an irreducible family of subvarieties, say hypersurfaces in $\mathbb{P}^n$ of given degree. It turns out that the subset of the space of one dimensional foliations of sufficiently high fixed degree that do have an invariant subvariety of a given "type" is irreducible. We would like to determine its codimension and degree. For this, we try to find an adequate description of these subvarieties in the spirit of the previous Section, namely, as the birrational image of projective bundles associated to vector bundles over the variety that parameterizes the desired

invariant subvarieties, e.g. Grassmannians for linear spaces, "complete conics" for conics.

Heuristically, requiring a fixed subvariety to be invariant by a foliation amounts to imposing linear conditions on the coefficients of a vector field defining the foliation. It is reasonable to expect that the number of independent conditions remains fixed as the subvariety varies in a suitable open subset of its parameter space. This is clearly the case if the type of subvariety we wish to be invariant consists of a single orbit under the group of automorphism of $\mathbb{P}^n$. For instance, imposing a linear subspace of fixed dimension does produce a nice projective bundle over the corresponding Grassmannian. However, already for hypersurfaces of any degree ≥ 2, the number of independent conditions jumps in the presence of singularities of the variety.

This question, in full generality, seems to be complicated. In this Section we solve the problem of describing foliations that have invariant subsets of degree 1 in $\mathbb{P}^n$ and of degree 2 in $\mathbb{P}^2$.

In the first Subsection we find a parameter space for foliations with linear invariant subset of any fixed dimension in $\mathbb{P}^n$.

In Subsection two, we deal with the problem of foliations in $\mathbb{P}^2$ with an invariant conic. With the same techniques it is possible to describe the space of foliations with invariant quadrics in $\mathbb{P}^n$. We will give the formulas for the degree and codimension of the space of foliations with invariant conic (respectively, quadric) in $\mathbb{P}^3$ in the last part of this Subsection.

4.1. **Foliations with invariant linear subspaces.** Fix $1 \leq r < n$. Set for short

$$\text{(4.1)} \qquad \begin{cases} N := N_{1,n,d},\ V := V_{1,n,d} \text{ cf. } (2.7, 2.4, \text{p. } 48) \\ \mathbb{G} := \mathbb{G}(r,n),\ \text{the Grassmannian of } r\text{-dimensional subspaces of } \mathbb{P}^n. \end{cases}$$

Assume $d \geq 2$; for the cases $d = 0, 1$ see Exercise $(13, \text{p. } 67)$. We define

$$\widehat{\mathbb{W}} := \{(W, [\mathcal{X}]) \in \mathbb{G} \times \mathbb{P}^N \mid W \text{ is invariant by } \mathcal{X}\}.$$

The goal of this subsection is to prove the following

4.1.1. Proposition. *Notation as above, there exists a vector subbundle*

$$\mathcal{E} \subset \mathbb{G} \times V$$

such that

(i) $\mathbb{P}(\mathcal{E}) = \widehat{\mathbb{W}} \subset \mathbb{G} \times \mathbb{P}^N$;

(ii) *if we set* $\mathbb{W} := q(\mathbb{P}(\mathcal{E}))$, *where* $q : \mathbb{P}(\mathcal{E}) \to \mathbb{P}^N$ *is the projection, then the codimension of* $\mathbb{W}$ *in* $\mathbb{P}^N$ *is*

$$\operatorname{cod}_{\mathbb{P}^N} \mathbb{W} = (n-r)\left(\binom{r+d}{d} - (r+1)\right);$$

(iii) *and the degree of* $\mathbb{W}$ *is given by the top-dimensional Chern class,*

$$\deg \mathbb{W} = \int c_g(\mathcal{Q} \otimes \operatorname{Sym}_d(\mathcal{S}^\vee)) \cap [\mathbb{G}],$$

where $g := \dim \mathbb{G}$.

The image $\mathbb{W}$ of $\widehat{\mathbb{W}}$ in $\mathbb{P}^N$ via projection is the set of dimension one degree d foliations in $\mathbb{P}^n$ that have an invariant r-plane.

Proof. Consider the tautological sequence over $\mathbb{G}$ (A.7, p. 84) and take its dual sequence

$$0 \to \mathcal{Q}^\vee \to \mathbb{G} \times S_1 \to \mathcal{S}^\vee \to 0. \tag{4.2}$$

The fiber of $\mathcal{Q}^\vee$ over $W \in \mathbb{G}$ is the space of equations that define W. The map $\mathbb{G} \times S_1 \twoheadrightarrow \mathcal{S}^\vee$ induces a surjective map

$$\mathbb{G} \times S_d \twoheadrightarrow \mathrm{Sym}_d(\mathcal{S}^\vee).$$

On the fiber over $W \in \mathbb{G}$ it is the map of restriction of degree d polynomials to W. On the other hand, from the tautological sequence,

$$0 \to \mathcal{S} \to \mathbb{G} \times S_1^\vee \to \mathcal{Q} \to 0,$$

setting $\Lambda = \mathcal{S}_W$, using (2.1), p. 48, we can interpret the surjective map

$$S_1^\vee \twoheadrightarrow \mathcal{Q}_W$$

as the quotient of $\mathcal{T}\mathbb{C}^{n+1}$ by $\mathcal{T}\Lambda$. Tensoring these two maps we obtain a surjective map of vector bundles over $\mathbb{G}$, $\varphi : S_d \otimes S_1^\vee \twoheadrightarrow \mathrm{Sym}_d(\mathcal{S}^\vee) \otimes \mathcal{Q}$, which in the fiber over W is given by $\varphi_W(F \otimes X) = F_{|W} \otimes \overline{X}$. It is easy to see that $\varphi(S_{d-1} \cdot R) \equiv 0$ (the radial field restricted to Λ is the radial field in Λ). Hence we obtain a surjective map of vector bundles, $\psi : \mathbb{G} \times V \twoheadrightarrow \mathrm{Sym}_d(\mathcal{S}^\vee) \otimes \mathcal{Q}$. It's not hard to check that the following are equivalent:

- $\psi_W(\mathcal{X}) = 0$
- $X_{|\Lambda} \in T\Lambda$
- Λ is invariant by X
- $W = \mathbb{P}(\Lambda)$ is invariant by $\mathcal{X}$.

Therefore $\mathcal{E} := \mathrm{Ker}(\psi)$ is a subbundle of V with $\mathbb{P}(\mathcal{E}) = \widehat{\mathbb{W}}$. This proves (i). We also get the rank of $\mathcal{E}$ is $\dim V - (n-r)\binom{d+r}{d}$. Assertions (ii) and (iii) will be dealt with below. □

4.1.2. The degree of $\mathbb{W}$. In order to compute the degree of $\mathbb{W}$ it remains to prove that q is generically injective, and then apply Lemma (1.6.5, p. 45).

4.1.3. Lemma. *Notation as in* Prop. (4.1.1, p. 63)*, for $d > 1$, the projection $q : \widehat{\mathbb{W}} \to \mathbb{P}^N$ is generically injective.*

Proof. Recall that $\mathbb{W} = q(\widehat{\mathbb{W}})$. It's sufficient to prove that there exists an open set $U_1 \subset \mathbb{W}$ such that for each point $y \in U_1$, $q^{-1}(y)$ consists of just one point. Indeed, in this case we deduce that $\dim \widehat{\mathbb{W}} = \dim \mathbb{W}$. Since $\widehat{\mathbb{W}}$ (resp. $\mathbb{W}$) are smooth (resp. generically smooth) varieties we have that

$$dq : \mathcal{T}\widehat{\mathbb{W}} \longrightarrow \mathcal{T}\mathbb{W}$$

is generically of maximal rank, *i.e.,* there exists an open set $U_2 \subset \mathbb{W}$ such that if $y \in U_2$, and $x \in q^{-1}(y)$, then $d_x q$ is surjective, equivalently $d_x q$ is injective. Summarizing we find an open set $U := U_1 \cap U_2$ such that if $y \in U$ then $q^{-1}(y) = \{x\}$, and x is a reduced point in the fiber. It follows that q is generically injective cf. (1.6.6, p. 45).

Let's prove the existence of U_1 above. For $W \in \mathbb{G}$, set $\mathbb{W}_W \subset \mathbb{W}$ the set of foliations which leave W invariant. For each $W' \neq W$ define $\mathbb{W}_{WW'} := \mathbb{W}_W \cap \mathbb{W}_{W'}$ and

$$\mathbb{W}_2 := \{\mathcal{X} \in \mathbb{W} \mid \mathcal{X} \in \mathbb{W}_{WW'} \text{ for some } W \neq W'\}.$$

We claim that $\dim \mathbb{W}_2 < \dim \mathbb{W}$. Indeed, define

$$G_2 := \{(W, W') \in \mathbb{G} \times \mathbb{G} \mid W \neq W'\},$$

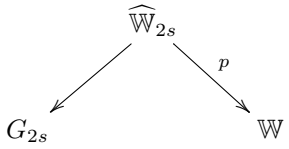
$$\widehat{\mathbb{W}}_2 = \{(\mathcal{X}, (W, W')) \mid \mathcal{X} \in \mathbb{W}_{WW'}; (W, W') \in G_2\}.$$

For each $1 \leq s \leq \min\{r, n-r\}$ set

$$G_{2s} := \{(W, W') \in \mathbb{G} \times \mathbb{G} \mid \operatorname{cod}(W \cap W') = n - r + s\},$$

$$\widehat{\mathbb{W}}_{2s} = \{(\mathcal{X}, (W, W')) \mid \mathcal{X} \in \mathbb{W}_{WW'}; (W, W') \in G_{2s}\}.$$

Let $p : \widehat{\mathbb{W}}_{2s} \to \mathbb{W} \subset \mathbb{P}^N$ denote the projection. Then we have, for each s



It is easy to see that $\dim G_{2s} = r(n-r) + s(r-s) = m + s(r-s)$. Furthermore each $\widehat{\mathbb{W}}_{2s} \to G_{2s}$ is a fibration with fiber dimension equal to $\dim \mathbb{W}_{WW'}$. We claim that

$$\dim \mathbb{W}_{WW'} \leq \dim \mathbb{W}_W - s\binom{r+d}{d}.$$

In fact, suppose that $W = \mathcal{Z}(Z_0, \ldots, Z_{n-r-1})$. Then W is invariant by a field of degree d,

$$\mathcal{X} = F_0 \frac{\partial}{\partial Z_0} + \cdots + F_n \frac{\partial}{\partial Z_n}$$

if and only if

$$F_0, \ldots, F_{n-r-1} \in \langle Z_0, \ldots, Z_{n-r-1} \rangle. \tag{4.3}$$

Take W' such that $\operatorname{cod}(W \cap W') = n - r + s$. Acting with the stabilizer of W in PGL_{n+1} we can suppose that $W = \mathcal{Z}(Z_{i_1}, \ldots, Z_{i_{n-r}})$, with $W' \cap W = \mathcal{Z}(Z_{i_1}, \ldots, Z_{i_s})$ where $i_1, \ldots, i_s \notin \{0, \ldots, n-r-1\}$. Now the condition of W' to be invariant by $\mathcal{X}$ implies that, for each $j = 1, \ldots, s$ we have

$$F_{i_j} \in \langle Z_{i_1}, \ldots, Z_{i_{n-r}} \rangle.$$

These conditions are independent of the others in (4.3). On the other hand it is easy to count the new conditions imposed by $F_{i_j} \in \langle Z_{i_1}, \ldots, Z_{i_{n-r}} \rangle$: this number is $\binom{r+d}{d}$. So we have that $\operatorname{cod}_{\mathbb{W}_W} \mathbb{W}_{WW'} \geq s\binom{r+d}{d}$. This proves the claim.

Next, let ϵ denote the dimension of the generic fiber of q and ϵ_2 the dimension of the generic fiber of p. It is clear that $\epsilon_2 \geq \epsilon$. Hence

$$\begin{aligned} \dim \mathbb{W}_{2s} &= \dim \widehat{\mathbb{W}}_{2,s} - \epsilon_2 \\ &\leq m + s(r-s) + \dim \mathbb{W}_W - s\tbinom{r+d}{d} - \epsilon \\ &= \dim \mathbb{W} + s(r-s) - s\tbinom{r+d}{d}. \end{aligned}$$

Therefore, in order to prove that $\dim \mathbb{W}_2 < \dim \mathbb{W}$ it is enough to prove that

$$s(r-s) - s\binom{r+d}{d} < 0. \tag{4.4}$$

As $s \geq 1$ we have $(r-s) \leq (r-1) < (r+1)$. On the other hand, we have

$$\begin{aligned} (r+d)\cdots(r+2)(r+1) &\geq (d+1)\cdots 3\,(r+1) \\ &\geq d!\,(r+1) > d!\,(r-s). \end{aligned}$$

This proves (4.4). Now, define $U_1 := \mathbb{W} \setminus \mathbb{W}_2$. Clearly U_1 is an open dense subset of $\mathbb{W}$ such that if $\mathcal{X} \in U_1$ then $\#q^{-1}(\mathcal{X}) = 1$. □

We can now complete the proof of (ii) and (iii) of the Prop. (4.1.1, p. 63). By construction of $\mathcal{E}$ (cf. p. 63) we have the following diagram:

$$\begin{array}{ccccc} & & \mathbb{P}(\mathcal{E}) & = & \widehat{\mathbb{W}} \\ & \swarrow^{p_1} & & \searrow_{q} & \\ \mathbb{G} & & & & \mathbb{W} \end{array}$$

and we have proved that q is generically injective. Therefore

$$\operatorname{cod}_{\mathbb{P}^N} \mathbb{W} = N - \dim(\mathbb{P}(\mathcal{E})) = N - (g + \operatorname{rk}(\mathcal{E}) - 1) =$$
$$N - \left(g + (N - (n-r)\binom{r+d}{d})\right) = (n-r)\binom{r+d}{d} - g$$

where $g = \dim \mathbb{G} = (n-r)(r+1)$.

By Lemma (1.6.5, p. 45) the degree of $\mathbb{W}$ is equal to

$$\int s_g(\mathcal{E}) \cap [\mathbb{G}].$$

From the exact sequence that defines $\mathcal{E}$,

$$0 \to \mathcal{E} \to V \to \mathcal{Q} \otimes \operatorname{Sym}_d(\mathcal{S}^\vee) \to 0$$

we get

$$\int s_g(\mathcal{E}) \cap [\mathbb{G}] = \int c_g(\mathcal{Q} \otimes \operatorname{Sym}_d(\mathcal{S}^\vee)) \cap [\mathbb{G}]\,.$$

□

4.1.4. Examples Next we give explicitly some codimensions and degrees. We use a script for SCHUBERT, [34] (see [16]) for the computations.

($\mathbb{P}^2$, $r = 1$)

$$\operatorname{cod}_{\mathbb{P}^N} \mathbb{W} = d - 1$$
$$\deg \mathbb{W} = \frac{1}{8} d(d+1)(d+2)(d+3)$$

($\mathbb{P}^3$, $r = 1$)

$$\operatorname{cod}_{\mathbb{P}^N} \mathbb{W} = 2(d-1)$$
$$\deg \mathbb{W} = \frac{1}{36} d(d+2)(d+1)(3d^5 + 9d^4 + 11d^3 + 9d^2 - 11d + 15)$$

($\mathbb{P}^3$, $r = 2$)

$$\operatorname{cod}_{\mathbb{P}^N} \mathbb{W} = \frac{1}{2}(d+4)(d-1)$$
$$\deg \mathbb{W} = \frac{1}{6^4} d(d+3)(d+2)(d+1)(d^2 + 6d + 11)(d^3 + 6d^2 + 11d - 6)$$

($\mathbb{P}^4$, $r = 1$)

$$\operatorname{cod}_{\mathbb{P}^N} \mathbb{W} = 3(d-1)$$
$$\deg \mathbb{W} = \tfrac{1}{2^{10} \cdot 3^2} d(d+2)(d+1)\left[729d^9 + 2187d^8 + 3402d^7 + 3750d^6 - 279d^5 + 651d^4 - 2668d^3 + 9732d^2 - 8864d + 6720\right].$$

Exercise 12. In the case of a hyperplane in $\mathbb{P}^n$, $\mathrm{rk}(\mathcal{Q}) = 1$,$(\mathcal{Q} = \mathcal{O}_{\mathbb{P}^n}(1))$ we have the following exact sequence:

$$0 \to S_{d-1} \otimes \mathcal{Q}^\vee \to S_d \to \mathrm{Sym}_d(\mathcal{S}^\vee) \to 0.$$

Twisting by $\mathcal{Q}$ we obtain:

$$0 \to S_{d-1} \to S_d \otimes \mathcal{Q} \to \mathrm{Sym}_d(\mathcal{S}^\vee) \otimes \mathcal{Q} \to 0.$$

Use this to prove that $c_n(\mathrm{Sym}_d(\mathcal{S}^\vee) \otimes \mathcal{Q}) = c_n(S_d \otimes \mathcal{Q}) = \binom{d+n}{n}$.

Exercise 13. In this exercise we review the case of foliations of degree 0.

Prove that a degree 0 foliation given by a field

$$\mathcal{X} = \lambda_0 \frac{\partial}{\partial Z_0} + \lambda_1 \frac{\partial}{\partial Z_1} + \cdots + \lambda_n \frac{\partial}{\partial Z_n}$$

with $\lambda_i \in \mathbb{C}$, is radial with center $p := [\lambda_0 : \lambda_1 : \cdots : \lambda_n]$.

It follows that any line trough p is invariant. Therefore in this case the map q is infinity to one.

In the case of foliations of degree 1 the well known correspondence between the set of such foliations, and the space of $(n+1)\times(n+1)$ matrices of trace zero (see [32, p. 9]), shows that a generic foliation of degree 1 has $\binom{n+1}{r+1}$ invariant subspaces of dimension r.

A degree one foliation is given by a field

$$\mathcal{X} = F_0 \frac{\partial}{\partial Z_0} + F_1 \frac{\partial}{\partial Z_1} + \cdots + F_n \frac{\partial}{\partial Z_n}$$

where F_i is a homogeneous polynomial of degree 1 for all $i = 0, \ldots, n$.

Let us write $F_i = \sum_j a_{ij} Z_j$. Then we associate to $\mathcal{X}$ the matrix of coefficients $B := ((a_{ij}))_{i,j}$ (this matrix will have trace zero because we are taking $\mathcal{X}$ of divergence zero, to ensure uniqueness).

Exercise 14. Prove that the invariant subspaces of dimension r are in correspondence with the dimension $n-r$ invariant subspaces of the transpose B^t.

Since a generic matrix is diagonalizable, the invariant subspaces of dimension $n-r$ are generated by $n-r$ eigenvectors. Therefore, a generic matrix has $\binom{n+1}{n-r}$ invariant subspaces.

Obtain this result from the previous analysis, as follows. In this case the map q from (4.1.3, p. 64) is not generically injective but only finite. It follows from (1.6.5, p. 45), that the degree of q is $c_g(\mathcal{Q} \otimes \mathcal{S}^\vee)$. Now $\mathcal{Q} \otimes \mathcal{S}^\vee = \mathcal{T}\mathbb{G}$, the tangent bundle to the Grassmannian, (see [21, B.5.8. p. 435]). Thus $c_g(\mathcal{T}\mathbb{G})$ can be computed with Bott's formula cf. Theorem (A.7.1, p. 87). We just have to find the number of fixed points for a convenient action of $\mathbb{C}^*$ on $\mathbb{G}$. For a suitable choice of the weights of the action we will find that there is one fixed point in each of the $\binom{n+1}{n-r}$ canonical open sets of $\mathbb{G}$. Alternatively, we could argue invoking Plücker embedding.

4.2. **Foliations with invariant conic.** We set throughout this section $N = N_{1,2,d}$, $V = V_{1,2,d}$ (cf. (2.7, 2.4, p. 48).)

4.2.1. Foliations in $\mathbb{P}^2$ with invariant conic. In this section we find a compactification $\mathbb{Y}_d \subset \mathbb{P}^N$ of the space of foliations of degree $d \geq 2$ in $\mathbb{P}^2$ that have an invariant smooth conic.

Let Y be a parameter space for the family of smooth conics. As we did in the previous sections, we want to describe the incidence variety

$$\widehat{\mathbb{Y}} := \{(\mathcal{C}, \mathcal{X}) \mid \mathcal{C} \text{ is invariant by } \mathcal{X}\} \subset Y \times \mathbb{P}^N$$

as the projective bundle associated to a subbundle $\mathcal{E}$ of the trivial bundle $Y \times V$. If we obtain such description the image of the projection $q_2 : \mathbb{P}(\mathcal{E}) \to \mathbb{P}^N$ will be the parameter space for foliations with an invariant conic. But this construction has the drawback that the space of smooth conics is not complete, whereas in order to compute degrees we need vector bundles over complete basis.

Thus we have to compactify the space of smooth conics, for example, allowing singular conics too. The most natural parameter space for conics is $\mathbb{P}^5$ cf. (A.6, p. 86), so we try and use it. But as we will see, when we go on to examine the fibers of $\widehat{\mathbb{Y}}$ over $\mathbb{P}^5$, the singular conics cause problems: the dimensions jump.

What we are going to do to solve this problem is to blowup $\mathbb{P}^5$ along an appropriate subvariety. We will obtain a variety $\mathbb{B}$, a birrational map $\pi : \mathbb{B} \to \mathbb{P}^5$ and a projective bundle $\mathbb{P}(\mathcal{E})$ *over* $\mathbb{B}$ such that it coincides with $\widehat{\mathbb{Y}}$ over the open set of smooth conics. Fortunately $\mathbb{B}$ is a well known variety, the variety of "complete conics" [47].

The construction of $\mathcal{E}$ will not be explicit, so in order to compute the degree of $\mathbb{Y}_d$ we will use Bott's formula (cf. Appendix (A.7, p. 87)). The point is that we only have to know the weights appearing in a decomposition of the fibers of $\mathcal{E}$ over fixed points of an adequate action of $\mathbb{C}^*$ on $\mathbb{B}$, and we will be able to describe these fibers as limits of the fibers over smooth conics.

Finally we present a script for SINGULAR, [27] that implements the calculation of the degree of $\mathbb{Y}_d$.

In Proposition 4.2.13 we find the codimension

$$\operatorname{cod}_{\mathbb{P}^N} \mathbb{Y}_d = 2(d-1)$$

and its degree,

$$\deg \mathbb{Y}_d = \frac{1}{2^5\,5!}(d-1)\,d\,(d+1)\,(d^7+25d^6+231d^5+795d^4 + 1856d^3+2468d^2+2256d+768).$$

4.2.2. The invariance condition for one conic. Fix a generic conic $\mathcal{C} = \mathcal{Z}(P)$ and let $\mathcal{X} \in V$ be a field given by

$$\mathcal{X} = F_0\frac{\partial}{\partial Z_0} + F_1\frac{\partial}{\partial Z_1} + F_2\frac{\partial}{\partial Z_2}.$$

Recalling (2.2.5, p. 50), $\mathcal{C}$ is invariant by $\mathcal{X}$ if and only if there exists a homogeneous polynomial $G \in S_{d-1}$ such that

$$\mathcal{X}(P) := F_0\frac{\partial P}{\partial Z_0} + F_1\frac{\partial P}{\partial Z_1} + F_2\frac{\partial P}{\partial Z_2} = GP.$$

Exercise 15. Prove that $\mathcal{C} = \mathcal{Z}(P)$ is invariant by $\mathcal{X}$ if and only if there exists a unique representative $Y \in S_d \otimes S_1^\vee$ of $\mathcal{X}$ with $Y(P) = 0$.

Therefore, for a fixed conic $\mathcal{C} = \mathcal{Z}(P)$ we may define the linear map

$$\begin{array}{rcl} \varphi_P : S_d \otimes S_1^\vee & \longrightarrow & S_{d+1} \\ X & \mapsto & X(P). \end{array}$$

Observe that $\varphi_P(GR) = 2GP$ for all $G \in S_{d-1}$. Thus φ_P induces a linear map

$$\psi_P : V \to \frac{S_{d+1}}{P \cdot S_{d-1}}.$$

Moreover, $\mathcal{X} \in \operatorname{Ker}\psi_P$ if and only if $\mathcal{C}$ is invariant by $\mathcal{X}$.

These two maps maps fit into the following commutative diagram:

$$\begin{array}{ccccc}
 & & \mathrm{Ker}\varphi_P & \longrightarrow & \mathrm{Ker}\psi_P \\
 & & \downarrow & & \downarrow \\
S_{d-1}R & \longrightarrow & S_d \otimes S_1^\vee & \longrightarrow & V \\
\downarrow \simeq & & \downarrow \varphi_P & & \downarrow \psi_P \\
P \cdot S_{d-1} & \longrightarrow & S_{d+1} & \longrightarrow & \frac{S_{d+1}}{P \cdot S_{d-1}}.
\end{array}$$

Hence, by the snake lemma we have an isomorphism

$$\mathrm{Ker}\varphi_P \simeq \mathrm{Ker}\psi_P.$$

4.2.3. The incidence variety. Now, let $\mathcal{C}$ vary in the parameter space of conics, $\mathbb{P}^5$. Consider the map of vector bundles over $\mathbb{P}^5$:

$$\varphi : \mathcal{O}_{\mathbb{P}^5}(-1) \otimes S_d \otimes S_1^\vee \longrightarrow S_{d+1} \tag{4.5}$$

given by $\varphi(\mathcal{C}, (P, X)) = (\mathcal{C}, X(P))$. As observed above, φ induces a map

$$\psi : \mathcal{O}_{\mathbb{P}^5}(-1) \otimes V \longrightarrow \frac{S_{d+1}}{S_{d-1} \otimes \mathcal{O}_{\mathbb{P}^5}(-1)}.$$

Again this map fits into the following commutative diagram:

$$\begin{array}{ccccc}
 & & \mathrm{Ker}\varphi & \xrightarrow{\simeq} & \mathrm{Ker}\psi \\
 & & \downarrow & & \downarrow \\
\mathcal{O}_{\mathbb{P}^5}(-1) \otimes S_{d-1}R & \longrightarrow & \mathcal{O}_{\mathbb{P}^5}(-1) \otimes S_d \otimes S_1^\vee & \longrightarrow & \mathcal{O}_{\mathbb{P}^5}(-1) \otimes V \\
\downarrow \simeq & & \downarrow \varphi & & \downarrow \psi \\
\mathcal{O}_{\mathbb{P}^5}(-1) \otimes S_{d-1} & \longrightarrow & S_{d+1} & \longrightarrow & \frac{S_{d+1}}{\mathcal{O}_{\mathbb{P}^5}(-1) \otimes S_{d-1}}.
\end{array}$$

Twisting by $\mathcal{O}_{\mathbb{P}^5}(1)$ we obtain:

$$\begin{array}{ccccc}
 & & \Theta & \xrightarrow{\simeq} & \bar{\Theta} \\
 & & \downarrow & & \downarrow \\
S_{d-1} \cdot R & \longrightarrow & S_d \otimes S_1^\vee & \longrightarrow & V \\
\downarrow \simeq & & \downarrow & & \downarrow \\
S_{d-1} & \longrightarrow & \mathcal{O}_{\mathbb{P}^5}(1) \otimes S_{d+1} & \longrightarrow & \frac{\mathcal{O}_{\mathbb{P}^5}(1) \otimes S_{d+1}}{S_{d-1}}
\end{array} \tag{4.6}$$

where

$$\Theta := \mathcal{O}_{\mathbb{P}^5}(1) \otimes \mathrm{Ker}\varphi \simeq \bar{\Theta} := \mathcal{O}_{\mathbb{P}^5}(1) \otimes \mathrm{Ker}\psi.$$

Restricting over the open subset $U \subset \mathbb{P}^5$ of smooth conics, we see that

$$\mathbb{P}(\bar{\Theta}_{|U}) \subset \mathbb{P}^5 \times \mathbb{P}^N$$

is the incidence variety

$$\{(\mathcal{C}, \mathcal{X}) \mid \mathcal{C} \text{ is invariant by } \mathcal{X}\} \subset U \times \mathbb{P}^N.$$

But as we will see soon, $\bar{\Theta}$ is not a vector bundle. In fact its fibers have different dimensions depending on the singularities of the conic.

The isomorphism $\bar{\Theta} \simeq \Theta$ is very usefull, because to describe the jumps in the dimension of the fibers of Θ will be easier.

4.2.4. Θ is not a vector bundle. Let us see why $\mathrm{Im}\varphi$ (and consequently Θ) is not a vector bundle.

Exercise 16. Recall that if

$$X = F_0\frac{\partial}{\partial Z_0} + F_1\frac{\partial}{\partial Z_1} + F_2\frac{\partial}{\partial Z_2} \in S_d \otimes S_1^\vee$$

and $\mathcal{C} = \mathcal{Z}(P)$ then

$$\varphi(\mathcal{C}, (P, X)) = X(P) = F_0\frac{\partial P}{\partial Z_0} + F_1\frac{\partial P}{\partial Z_1} + F_2\frac{\partial P}{\partial Z_2}.$$

Show that $X(P)$ vanishes at the singularities of $\mathcal{C}$, and the dimension of the fibers of $\mathrm{Im}\varphi$ depends on the rank of the conic:

(1) If $\mathcal{C}$ is smooth ($\mathrm{rk}\,\mathcal{C} = 3$) then $\mathrm{rk}\,\varphi_P = \dim S_{d+1} = \binom{d+3}{2}$.
Use that in this case $\mathcal{C}$ is projectively equivalent to $\mathcal{Z}(P)$ with
$$P = Z_0^2 + Z_1^2 + Z_2^2.$$
(2) If $\mathcal{C}$ is the union of two lines ($\mathrm{rk}\,\mathcal{C} = 2$), then $\mathrm{rk}\,\varphi_P = \dim S_{d+1} - 1$. In this case $\mathcal{C}$ is projectively equivalent to $\mathcal{Z}(P)$ with $P = Z_0Z_1$.
(3) If $\mathcal{C}$ is a double line ($\mathrm{rk}\,\mathcal{C} = 1$) then $\mathrm{rk}\,\varphi_P = \dim S_d = \binom{d+2}{2}$. Now $\mathcal{C}$ is projectively equivalent to $\mathcal{Z}(P)$ with $P = Z_0^2$.

4.2.5. The blow-up. Let $r = \binom{d+2}{2}$ denote the minimal rank of φ, and denote by Y_r the scheme defined by the Fitting ideal of φ, generated by the $(r+1)\times(r+1)$-minors of a local representation of φ, cf. (4.5).

The analysis of the dimensions of the fibers above shows that Y_r coincides with the Veronese variety $\mathbb{V}$ of double lines (cf. Appendix (A.6, p. 86)), at least as sets. We are going to blowup $\mathbb{P}^5$ along $\mathbb{V}$ and prove in Lemma 4.2.6 below that this solves our problem.

Let $\mathbb{B}$ denote the blowup of $\mathbb{P}^5$ along $\mathbb{V}$, and $\pi : \mathbb{B} \to \mathbb{P}^5$ the map of blowup (see Appendix A.5, p. 84 and A.6).

Consider the pullback by π of the maps φ and ψ

$$\varphi_{\mathbb{B}} : \pi^*(\mathcal{O}_{\mathbb{P}^5}(-1) \otimes S_d \otimes S_1^\vee) \longrightarrow \pi^* S_{d+1}$$

$$\psi_{\mathbb{B}} : \pi^*(\mathcal{O}_{\mathbb{P}^5}(-1) \otimes V) \longrightarrow \pi^*\left(\frac{S_{d+1}}{S_{d-1} \otimes \mathcal{O}_{\mathbb{P}^5}(-1)}\right).$$

The following lemma describes the effect of the blowup in the minors of $\varphi_{\mathbb{B}}$. This result together with Lemma 4.2.8 will be used to prove that blowing up $\mathbb{P}^5$ along $\mathbb{V}$ we obtain a vector bundle.

4.2.6. Lemma. *The $k \times k$ minors of $\varphi_{\mathbb{B}}$ are locally principal for all $k \geq 1$.*

Proof. Let $\varphi_0 : \mathcal{O}_{\mathbb{P}^5}(-1) \otimes S_1^\vee \to S_1$ be the universal symmetric map that gives the matrix of the conic. We are blowing-up the ideal of 2×2-minors of φ_0, so we have that the minors of $\varphi_{0\mathbb{B}}$ are locally principal, say generated by t. Thus we can assume that the matrix is locally of the form

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & t & a_4 \\ 0 & a_4 & a_5 \end{pmatrix}$$

with ideal of 2×2-minors $\langle t, a_4, a_5 \rangle$. So t divides a_4, a_5. Performing elementary operations we can assume that the matrix assumes the form

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & t & 0 \\ 0 & 0 & ts \end{pmatrix}.$$

Let us analyze the map $\varphi_{\mathbb{B}}$ at the conic corresponding to A, *i.e.,*

$$\varphi_{\mathcal{C}} : S_d \otimes S_1^\vee \longrightarrow S_{d+1}$$

where $\mathcal{C} = \mathcal{Z}(Z_0^2 + tZ_1^2 + tsZ_2^2)$.

Set $\nu_m := \dim S_m = \binom{m+2}{2}$. Choose a basis for $S_d \otimes S_1^\vee$ as follows: take the first ν_{d+1} vectors as

(ν_d vectors) a basis of $S_d \otimes \dfrac{\partial}{\partial Z_0}$;

($d+1$ vectors) a basis of $\operatorname{Sym}_d(Z_1, Z_2) \otimes \dfrac{\partial}{\partial Z_1}$;

(1 vector) $Z_2^d \dfrac{\partial}{\partial Z_2}$.

Next take

(ν_{d-1} vectors) a basis of $Z_0 S_{d-1} \otimes \dfrac{\partial}{\partial Z_1}$;

($\nu_d - 1$ vectors) a basis of $\dfrac{S_d}{\mathbb{C} \cdot Z_2^d} \otimes \dfrac{\partial}{\partial Z_2}$.

Now we pick the following basis for S_{d+1}:

(ν_d vectors) a basis of $Z_0 S_d$;

($d+1$ vectors) a basis of $Z_1 \operatorname{Sym}_d(Z_1, Z_2)$;

(1 vector) Z_2^{d+1}.

Then the matrix of $\varphi_{\mathcal{C}}$ in this basis looks like

$$A_d = \begin{pmatrix} 2I_{\nu_d} & 0 & 0 & B_1 & B_3 \\ 0 & 2tI_{d+1} & 0 & 0 & B_4 \\ 0 & 0 & 2ts & 0 & 0 \end{pmatrix},$$

where the entries of B_1 are multiples of t, and the entries of B_3, B_4 are multiples of ts. Here I_m stands for the identity matrix of size m.

From this we conclude that the ideals J_i of $i \times i$-minors of A_d are:

$$\begin{cases} J_i = \langle 1 \rangle & \text{for } i = 1, \dots, \nu_d \\ J_{\nu_d + j} = \langle t^j \rangle & \text{for } j = 1, \dots, d+1 \\ J_{\nu_{d+1}} = \langle t^{d+2} s \rangle. \end{cases}$$

In particular these minors are principal as we claimed. □

4.2.7. Construction of $\mathcal{E}$. Next, we are going to construct a vector subbundle $\mathcal{E} \subset \mathbb{B} \times V$ over $\mathbb{B}$ which coincides with $\pi^* \bar{\Theta}$ over the open set of smooth conics.

First we prove a technical lemma.

4.2.8. Lemma. *Let R be a local Noetherian domain, and $\varphi : R^n \to R^m$ a homomorphism of free, finitely generated R-modules. Suppose that the ideals $\langle k \times k$ minors of $\varphi \rangle$ are principal for all k. Then $\mathcal{M} := \operatorname{Im}\varphi$ is free.*

Proof. Let

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

be the $m \times n$ matrix associated to φ with respect to some basis. Thus, the columns of A generate $\mathcal{M}$. By hypothesis for $k = 1$, the ideal of the entries of A is principal:

$$\langle a_{11}, \ldots, a_{ij}, \ldots, a_{mn} \rangle = \langle f \rangle .$$

We may assume $f \neq 0$. Let $b_{ij} := \frac{a_{ij}}{f}$. We may suppose $a_{11} = f$. Let $\mathcal{M}'$ be the module generated by the columns of

$$B = \begin{pmatrix} 1 & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix} .$$

Equivalently (by elementary operations) $\mathcal{M}'$ is generated by the columns of $\left(\begin{smallmatrix} 1 & 0 \\ 0 & B' \end{smallmatrix}\right)$, where

$$B' = \begin{pmatrix} b_{22} & \cdots & b_{2m} \\ \vdots & \ddots & \vdots \\ b_{m2} & \cdots & b_{mn} \end{pmatrix} .$$

Applying induction, we have that $\mathrm{Im}B'$ is free. Thus $\mathcal{M}'$ is free. Since R is a domain we have $\mathcal{M} = f \cdot \mathcal{M}' \simeq \mathcal{M}'$. Hence $\mathcal{M}$ is free. □

4.2.9. Proposition. *There exists a vector bundle $\mathcal{E}$ over $\mathbb{B}$ such that:*

(1) *$\mathcal{E}$ is a subbundle of the trivial bundle π^*V.*
(2) *$\mathcal{E}$ coincides generically with $\pi^*\bar{\Theta} \simeq \pi^*\Theta$* (cf. 4.6, p. 69).

Proof. By Lemma 4.2.6 and the above Lemma we deduce that $\mathcal{M} := \mathrm{Im}\varphi_{\mathbb{B}}$ is locally free. Therefore we obtain a factorization of $\varphi_{\mathbb{B}} = \iota \circ \widetilde{\varphi}$,

$$\begin{array}{ccc} \pi^*(\mathcal{O}_{\mathbb{P}^5}(-1) \otimes S_d \otimes S_1^\vee) & \xrightarrow{\varphi_{\mathbb{B}}} & \pi^*S_{d+1} \\ & \searrow^{\widetilde{\varphi}} & \uparrow{\scriptstyle \iota} \\ & & \mathcal{M}, \end{array} \tag{4.7}$$

where $\mathcal{M}$ is a vector bundle.
Observe that $\pi^*(\mathcal{O}_{\mathbb{P}^5}(-1) \otimes S_{d-1}) = \varphi_{\mathbb{B}}(\pi^*(\mathcal{O}_{\mathbb{P}^5}(-1) \otimes S_{d-1}R)) \subset \mathcal{M}$. Therefore this factorization induces a factorization of $\psi_{\mathbb{B}} = \bar{\iota} \circ \widetilde{\psi}$,

$$\begin{array}{ccc} \pi^*(\mathcal{O}_{\mathbb{P}^5}(-1) \otimes V) & \xrightarrow{\psi_{\mathbb{B}}} & \pi^*\left(\dfrac{S_{d+1}}{\mathcal{O}_{\mathbb{P}^5}(-1) \otimes S_{d-1}}\right) \\ & \searrow^{\widetilde{\psi}} & \uparrow{\scriptstyle \bar{\iota}} \\ & & \overline{\mathcal{M}}, \end{array}$$

where $\overline{\mathcal{M}} := \dfrac{\mathcal{M}}{\pi^*(\mathcal{O}_{\mathbb{P}^5}(-1) \otimes S_{d-1})}$ is a vector bundle. Define

$$\mathcal{E} := \pi^*\mathcal{O}_{\mathbb{P}^5}(1) \otimes \mathrm{Ker}\widetilde{\psi}.$$

It follows that $\mathcal{E}$ is a subbundle of $\mathbb{B} \times V$ that coincides with $\pi^*\bar{\Theta}$ over $\pi^{-1}(U)$, where $U \subset \mathbb{P}^5$ is the open set of smooth conics. Indeed, over $\pi^{-1}(U)$ the map

$\iota : \mathcal{M} \to \pi^* S_{d+1}$ as in (4.7) is an isomorphism. Therefore

$$\overline{\mathcal{M}} \simeq \pi^*\left(\frac{S_{d+1}}{\mathcal{O}_{\mathbb{P}^5}(-1) \otimes S_{d-1}}\right)$$

and $\mathrm{Ker}\widetilde{\psi} = \mathrm{Ker}\psi_{\mathbb{B}}$ and likewise $\mathcal{E} \simeq \pi^*(\mathcal{O}_{\mathbb{P}^5}(1)) \otimes \mathrm{Ker}\psi_{\mathbb{B}} = \pi^*(\bar{\Theta})$, all over $\pi^{-1}(U)$. □

4.2.10. A parameter space for foliations with invariant conic. Since $\mathcal{E} \subset \mathbb{B} \times V$ is locally split, taking the projectivization yields the following diagram:

$$\begin{array}{ccc} & \mathbb{P}(\mathcal{E}) \subset \mathbb{B} \times \mathbb{P}^N & \\ {\scriptstyle q_1}\swarrow & & \searrow{\scriptstyle q} \\ \mathbb{B} & & \mathbb{P}^N \end{array}$$

Define $\mathbb{Y}_d := q(\mathbb{P}(\mathcal{E})) \subset \mathbb{P}^N$. We have that $\mathbb{Y}_d$ is the closure of the variety of foliations with an invariant smooth conic.

In Lemma 4.2.12 below we prove that q is generically injective. Therefore in order to compute $\deg \mathbb{Y}_d$ it is sufficient to calculate $s_5(\mathcal{E})$ (see Lemmas 1.6.5 and 1.6.6, p. 45).

4.2.11. The degree of $\mathbb{Y}_d$.

4.2.12. Lemma. *The projection $q : \mathbb{P}(\mathcal{E}) \to \mathbb{P}^N$ is generically injective.*

Proof. By Lemma (1.6.6, p. 45) it is sufficient to find, for $d \geq 2$, a degree d vector field $\mathcal{X}$ with a single invariant conic $\mathcal{C}$ and such that $\mathcal{C}$ is a reduced point in the fiber $q^{-1}(\mathcal{X})$ (equivalently, such that $d_{(\mathcal{C},\mathcal{X})}q$ is injective).

For $d = 2$ we claim that

$$\mathcal{X} = (Z_2Z_0 - Z_1^2)\partial Z_0 - (Z_0Z_1 - Z_2^2)\partial Z_1 + (Z_1Z_2 - Z_0^2)\partial Z_2$$

and $\mathcal{C} = \mathcal{Z}(P)$ with $P = Z_0^2 - Z_1^2 + Z_2^2 = 0$ do the job.

In fact, $\mathcal{X}(P) = 0$. Now, if $\mathcal{C}'$ is another conic invariant by $\mathcal{X}$, say $\mathcal{C}' = \mathcal{Z}(Q)$ with $Q = a_0Z_0^2 + a_1Z_0Z_1 + \cdots + a_5Z_2^2$ then there exists $H = b_0Z_0 + b_1Z_1 + b_2Z_2$ such that $\mathcal{X}(Q) = HQ$. This equality provides a system of linear equations from which we can eliminate b_0, b_1, b_2 (we use Singular, [27], see [16]) to find that $a_0 - a_5 = a_1 = a_2 = a_3 + a_5 = a_4 = 0$. Thus $Q = P$.

To prove that $d_{(\mathcal{C},\mathcal{X})}q$ is injective take for example a tangent vector

$$(a_1Z_0Z_1 + a_2Z_0Z_2 + a_3Z_1^2 + a_4Z_1Z_2 + a_5Z_2^2, v) = (m, v) \in \mathcal{T}_{(P,\mathcal{X})}\mathbb{P}(\mathcal{E}).$$

We have to prove that $v = 0$ implies $a_i = 0$, $\forall\, i = 1, \ldots, 5$. Now

$$(m, v) \in \mathcal{T}_{(P,\mathcal{X})}\mathbb{P}(\mathcal{E}) \Leftrightarrow (P + \varepsilon m, \mathcal{X} + \varepsilon v) \in \mathbb{P}(\mathcal{E})(\mathbb{C}[\varepsilon]).$$

This means that modulo ε^2 we have

$$(\mathcal{X} + \varepsilon v)(P + \varepsilon m) = (P + \varepsilon m)h$$

for some $h = h_1 + \varepsilon h_2$, where h_1, h_2 are polynomials of degree one. Thus,

$$\mathcal{X}(P) + \varepsilon(\mathcal{X}(m) + v(P)) = (P + \varepsilon m)h$$

but $\mathcal{X}(P) = 0$ so we have

$$\varepsilon(\mathcal{X}(m) + v(P)) = h_1P + \varepsilon(h_1m + h_2P).$$

Therefore $h_1 = 0$ and the condition now reads

$$\mathcal{X}(m) + v(P) = h_2 P.$$

So if $v = 0$ this implies $\mathcal{X}(m) = h_2 P$. Performing a simple elimination (*e.g.,* using SINGULAR, [27], see [16]) of coefficients of h_2 we obtain all $a_i = 0$.

For $d = 3$ take

$$\mathcal{X} = (Z_2^2 Z_0 - Z_1^3)\partial Z_0 + (Z_0 Z_1^2 - Z_2^3)\partial Z_1 + (Z_1 Z_2^2 - Z_0^2 Z_2)\partial Z_2$$

As above we can prove that $\mathcal{X}$ has $\mathcal{C} = \mathcal{Z}(Z_0^2 + Z_1^2 + Z_1^2)$ as unique invariant conic and check that $\mathcal{C}$ is a reduced point in $q^{-1}(\mathcal{X})$ (see [16]).

For $d \geq 4$ we will construct, using the example of Jouanolou, a field of degree d with a unique invariant conic.

Recall Jouanolou proves in [32, p. 157] that the field

$$\mathcal{Y} := Z_2^e \partial Z_0 + Z_0^e \partial Z_1 + Z_1^e \partial Z_2$$

has no invariant algebraic subset if $e \geq 2$.

Let P be an irreducible polynomial of degree 2. We claim that $\mathcal{X} := P \cdot \mathcal{Y}$ is a field of degree $d \geq 4$ that has $\mathcal{C} = \mathcal{Z}(P)$ as unique invariant conic (in fact $\mathcal{C}$ is in the singular set of $\mathcal{X}$, but this is sufficient for us). Indeed, $\mathcal{X}(P) = P \cdot \mathcal{Y}(P)$. Now if $\mathcal{C}' = \mathcal{Z}(Q)$ is another conic invariant by $\mathcal{X}$ we have that Q divides $P \cdot \mathcal{Y}(Q)$. If Q is irreducible, this implies that Q divides $\mathcal{Y}(Q)$ *i.e.,* $\mathcal{Z}(Q)$ would be invariant by $\mathcal{Y}$.

If $Q = l_1 l_2$, then l_i divides $P \cdot \mathcal{Y}(l_i)$ (see Definition 2.2.5). Hence $\mathcal{Z}(l_i)$ would be invariant by $\mathcal{Y}$.

To prove that $d_{(P,\mathcal{X})}q$ is injective we argue as in the case $d = 2$. Let

$$(m, v) \in \mathcal{T}_{(P,\mathcal{X})}\mathbb{P}(\mathcal{E}) \Leftrightarrow (P + \varepsilon m, \mathcal{X} + \varepsilon v) \in \mathbb{P}(\mathcal{E})(\mathbb{C}[\varepsilon]),$$

where m is a polynomial of degree two linearly independent of P. Then modulo ε^2 we have:

$$(\mathcal{X} + \varepsilon v)(P + \varepsilon m) = (P + \varepsilon m)h$$

for some $h = h_1 + \varepsilon h_2$, where h_1, h_2 are polynomials of degree $d - 1$. Expanding we obtain

$$\mathcal{X}(P) + \varepsilon(\mathcal{X}(m) + v(P)) = (h_1 + \varepsilon h_2)(P + \varepsilon m).$$

Recalling $\mathcal{X}(P) = P \cdot \mathcal{Y}(P)$, we have

$$P \cdot \mathcal{Y}(P) + \varepsilon(P \cdot \mathcal{Y}(m) + v(P)) = h_1 P + \varepsilon(h_1 m + h_2 P).$$

Therefore $h_1 = \mathcal{Y}(P)$ and the condition reads

$$P \cdot \mathcal{Y}(m) + v(P) = h_2 P + \mathcal{Y}(P)m.$$

Thus, if $v = 0$ we get

$$P\mathcal{Y}(m) = h_2 P + \mathcal{Y}(P)m$$

whence P must divide m (cf. [19]) and this implies $m = 0$.

□

4.2.13. Proposition. *Notation as above, let $\mathbb{Y}_d$ be the compactification for the parameter space of 1-dimensional foliations of degree d on $\mathbb{P}^2$ with an invariant smooth conic. Then the degree of $\mathbb{Y}_d$ is given by*

$$\frac{1}{2^5\,5!}\,(d-1)\,d\,(d+1)\,(d^7 + 25d^6 + 231d^5 + 795d^4 + 1856d^3 + 2468d^2 + 2256d + 768).$$

and its codimension is equal to $2(d-1)$.

Proof. From Proposition 4.2.9 and definition of Θ we have $\mathrm{rk}(\mathcal{E}) = d(d+2)$. As q is finite we have $\dim \mathbb{Y}_d = \dim \mathbb{P}(\mathcal{E}) = 5 + d(d+2) - 1$. Hence

$$\mathrm{cod}\mathbb{Y}_d = N - \dim \mathbb{Y}_d = (d+1)(d+3) - 1 - (5 + d(d+2) - 1) = 2(d-1)\,.$$

To compute the degree of $\mathbb{Y}_d = \int s_5(\mathcal{E}) \cap [\mathbb{B}]$ we use Bott's formula (A.7.1, p. 87):

$$\int s_5(\mathcal{E}) \cap [\mathbb{B}] = \sum_{p \in \mathbb{B}^T} \frac{s_5^T(\mathcal{E}_p) \cap [p]}{c_5^T(\mathcal{T}_p\mathbb{B})}$$

where $T := \mathbb{C}^*$ acts on $\mathbb{B}$ with isolated fixed points.

The action of T on $\mathbb{B}$ will be induced by an action of T on $\mathbb{P}^2$. With the notation of Appendix A.6, write $\mathbb{P}^2 = \mathbb{P}(F)$, where $F = \mathbb{C}^3$ has basis $\{e_0, e_1, e_2\}$. We begin by considering an action of $T = \mathbb{C}^*$ on F:

$$T \times F \to F$$

given by

$$t \cdot e_i = t^{w_i} e_i \tag{4.8}$$

for some $w_i \in \mathbb{Z}$ to be chosen appropriately.

This action induces an action on $\mathrm{Sym}_2 F^\vee$:

$$T \times \mathrm{Sym}_2 F^\vee \to \mathrm{Sym}_2 F^\vee$$

given by

$$t \cdot Z_i Z_j = t^{-(w_i + w_j)} Z_i Z_j.$$

In this way we obtain an action of T on $\mathbb{P}^5 = \mathbb{P}(\mathrm{Sym}_2 F^\vee)$. It is easy to see that if we choose the weights in such a way that $\{w_i + w_j$, with $0 \le i \le j \le 2\}$ are pairwise distinct, we obtain precisely the following six isolated fixed points in $\mathbb{P}^5$:

$$[1:0:\cdots:0:0], [0:1:\cdots:0:0], \ldots, [0:0:\cdots:0:1].$$

These correspond to the conics defined by the monomials

$$Z_0^2, Z_0Z_1, Z_0Z_2, Z_1^2, Z_1Z_2, Z_2^2.$$

In order to induce an action on $\mathbb{B}$ consider the map (see Appendix A.6):

$$\epsilon : \mathbb{P}^5 = \mathbb{P}(\mathrm{Sym}_2 F^\vee) \dashrightarrow \check{\mathbb{P}}^5 = \mathbb{P}(\mathrm{Sym}_2 \overset{2}{\wedge} F^\vee)$$

given by $\epsilon(u) = \overset{2}{\wedge} u$.

Recall that $\mathbb{B} = \overline{\mathrm{Graph}\,\epsilon}$, the closure of the graph of ϵ, and that π denotes the map of blowup $\pi : \mathbb{B} \to \mathbb{P}^5$.

It is easy to see that ϵ is $T-$equivariant. Hence $\mathbb{B} = \overline{\mathrm{Graph}\,\epsilon}$ inherits an action of T. Moreover, if $(A, B) \in \mathbb{B}$ is a fixed point then $A \in \mathbb{P}^5$ is a fixed point, T acts on $\pi^{-1}(A)$ and B is a fixed point for this action.

Therefore, in order to obtain the fixed points in $\mathbb{B}$ we have to find the fixed points on the fiber of π over each fixed point in $\mathbb{P}^5$.

If A is a fixed point with $A \notin \mathbb{V}$ *i.e.,* $A \in \{Z_0Z_1, Z_0Z_2, Z_1Z_2\}$, then $\pi^{-1}(A)$ has just one (fixed) point. So take $A \in \mathbb{V}$ *i.e.,* $A \in \{Z_0^2, Z_1^2, Z_2^2\}$. By Appendix A.5 we have that the exceptional divisor of our blowup is

$$E = \mathbb{P}(\mathcal{N})$$

where $\mathcal{N} := N_{\mathbb{V}}\mathbb{P}^5$ stands for the normal bundle of $\mathbb{V}$ in $\mathbb{P}^5$. Then for $A = Z_0^2$ we have (see (A.18) of Appendix A.6)

$$\pi^{-1}(A) = E_A = \mathbb{P}(\mathbb{C} \cdot Z_0^{2\vee} \otimes \langle Z_1^2, Z_1Z_2, Z_2^2\rangle_{\mathbb{C}}).$$

By our choice of the weights, there are three fixed points in the fiber of each $A \in \mathbb{V}$. For $A = Z_0^2$ these point are

$$Z_0^{2\vee} \otimes Z_1^2, Z_0^{2\vee} \otimes Z_1Z_2, Z_0^{2\vee} \otimes Z_2^2.$$

Summarizing, we have twelve fixed points in $\mathbb{B}$, three of them outside E and nine in E. These fixed points are of three types:

$$Z_iZ_j \text{ with } i \neq j;$$
$$(Z_i^2, Z_i^{2\vee} \otimes Z_jZ_k) \text{ with } j, k \neq i;\ j \neq k;$$
$$(Z_i^2, Z_i^{2\vee} \otimes Z_j^2) \text{ with } i \neq j.$$

The next step is to compute the fibers of $\mathcal{E}$ (see Proposition 4.2.9) over each fixed point.

Suppose that $B \in \mathbb{B}$ is a fixed point. The strategy is to take a curve $B(t) \in \mathbb{B}$ such that

$$\lim_{t\to 0} B(t) = B$$

and such that $A(t) := \pi(B(t)) \in \mathbb{P}^5$ is a curve of smooth conics for $t \neq 0$. Therefore $\mathcal{E}_B$ will be obtained as the limit of $\mathcal{E}_{B(t)} = \pi^*\Theta_{B(t)} = \Theta_{A(t)}$ (notation as in (4.6), p. 69) :

$$\lim_{t\to 0} \Theta_{A(t)} = \mathcal{E}_B$$

This enables us to use the well known space of vector fields of degree d that leave invariant a smooth conic $\mathcal{C} = \mathcal{Z}(G)$ (see [14]), to wit,

$$(\spadesuit) \qquad \left\{F_{ij}\left(\frac{\partial G}{\partial Z_i}\frac{\partial}{\partial Z_j} - \frac{\partial G}{\partial Z_j}\frac{\partial}{\partial Z_i}\right) \mid F_{ij} \in S_{d-1}\right\}$$

modulo multiples of the radial vector field. We will adopt the following notation: for each subset $J := \{v_0, \ldots, v_k\} \subset \{Z_0, Z_1, Z_2\}$ we set

$$M_m(J) = \{v_0^m, v_0^{m-1}v_1, \ldots, v_k^m\},$$

the canonical monomial basis of $\mathrm{Sym}_m(J)$. We write M_m for $M_m(\{Z_0, Z_1, Z_2\})$.

Set $\mathcal{X}_{i,j} := Z_i\frac{\partial}{\partial Z_i} - Z_j\frac{\partial}{\partial Z_j}$. Notice this is a vector of weight 0, since $t \cdot Z_i = t^{w_i}Z_i$ whereas $t \cdot \frac{\partial}{\partial Z_i} = t^{-w_i}\frac{\partial}{\partial Z_i}$.

We now describe suitable 1-parameter families of smooth conics abutting each type of fixed point.

(1) $B_1 = Z_0Z_1$. We take $A(t) = Z_0Z_1 + tZ_2^2 \in \mathbb{P}^5$. Using the characterization ($\spadesuit$) we see that the space $\mathcal{E}_{A(t)}$ of vector fields leaving $A(t)$ invariant is given by

$$\Big\{F_{10}(Z_1\tfrac{\partial}{\partial Z_1} - Z_0\tfrac{\partial}{\partial Z_0}),\ F_{20}(Z_1\tfrac{\partial}{\partial Z_2} - 2tZ_2\tfrac{\partial}{\partial Z_0}),\ F_{21}(Z_0\tfrac{\partial}{\partial Z_2} - 2tZ_2\tfrac{\partial}{\partial Z_1}) \mid F_{ij} \in S_{d-1}\Big\}.$$

Taking limit as $t \to 0$, we find a basis for $\mathcal{E}_{B_1}$:

$$\{F_1\mathcal{X}_{0,1}, F_2\frac{\partial}{\partial Z_2} \mid F_1 \in M_{d-1}\,,\ F_2 \in M_d \setminus \{Z_2^d\}\}.$$

Clearly this basis consists of T-eigenvectors.

(2) $B_2 = (Z_0^2, Z_0^{2\vee} \otimes Z_1 Z_2)$. In this case, we take $A(t) = Z_0^2 + tZ_1Z_2$. With the same procedure as above, we obtain the following basis (of T-eigenvectors) for $\mathcal{E}_{B_2}$:

$$\{F_1 Z_0 \frac{\partial}{\partial Z_1}, F_2 Z_0 \frac{\partial}{\partial Z_2}, F_3 \mathcal{X}_{1,2} \mid F_1, F_2 \in M_{d-1}\,,\ F_3 \in M_{d-1}(\{Z_1, Z_2\})\}.$$

(3) $B_3 = (Z_0^2, Z_0^{2\vee} \otimes Z_1^2)$. In this case a curve of smooth conics that approximates B_3 is $A(t) = Z_0^2 + tZ_1^2 + t^2 Z_2^2$. As before, we obtain the following basis of T-eigenvectors for $\mathcal{E}_{B_3}$:

$$\{F_1 Z_0 \frac{\partial}{\partial Z_1}, F_2 \frac{\partial}{\partial Z_2} \mid F_1 \in M_{d-1}\,,\ F_2 \in M_d \setminus \{Z_2^d\}\}.$$

This concludes the computation of the fibers of $\mathcal{E}$.

Next we obtain, for each fixed point B, a base consisting of T-eigenvectors of $\mathcal{T}_B\mathbb{B}$.

If $B \notin E$ then $\mathcal{T}_B\mathbb{B} \simeq \mathcal{T}_{\pi(B)}\mathbb{P}(\mathrm{Sym}_2 F^\vee)$. For example, for $B_1 = Z_0Z_1$ we have

$$\mathcal{T}_{B_1}\mathbb{B} \simeq \langle Z_0Z_1\rangle^\vee \otimes \langle Z_0^2, Z_0Z_2, \ldots, Z_2^2\rangle.$$

If $B \in E$, then $B = (A, [v])$ with $A \in \mathbb{V}$ and $v \in \mathcal{N}_A$. Now

$$\mathcal{T}_B\mathbb{B} = \mathcal{T}_A\mathbb{V} \oplus \mathrm{Hom}(\mathbb{C}\cdot v, \frac{\mathcal{N}_A}{\mathbb{C}\cdot v}) \oplus \mathbb{C}\cdot v,$$

see (A.15, p. 85).

For $B_2 = (Z_0^2, Z_0^{2\vee} \otimes Z_1Z_2)$ we have:

$$\mathcal{T}_{B_2}\mathbb{B} = \mathcal{T}_{Z_0^2}\mathbb{V} \oplus \langle Z_0^{2\vee} \otimes Z_1Z_2\rangle^\vee \otimes \langle Z_0^{2\vee} \otimes Z_1^2, Z_0^{2\vee} \otimes Z_2^2\rangle \oplus \langle Z_0^{2\vee} \otimes Z_1Z_2\rangle$$

where $\mathcal{T}_{Z_0^2}\mathbb{V} = \langle Z_0^2\rangle^\vee \otimes \langle Z_0Z_1, Z_0Z_2\rangle$.

Similarly, for $B_3 = (Z_0^2, Z_0^{2\vee} \otimes Z_1^2)$ we find

$$\mathcal{T}_{B_3}\mathbb{B} = \mathcal{T}_{Z_0^2}\mathbb{V} \oplus \langle Z_0^{2\vee} \otimes Z_1^2\rangle^\vee \otimes \langle Z_0^{2\vee} \otimes Z_1Z_2, Z_0^{2\vee} \otimes Z_2^2\rangle \oplus \langle Z_0^{2\vee} \otimes Z_1^2\rangle.$$

The explicit calculation in Bott's formula is better left for a script in SINGULAR, [27] (see [19] or [16]).

Note that the above computations of the fibers are performed for fixed d. In order to obtain the polynomial formula in Proposition 4.2.13 we have to interpolate the obtained results. We use Lemma 4.2.14 below which enables us to restrict the computation just for the first sixteen values of $d = 2, \ldots, 17$ and then interpolate the answers obtained.

□

4.2.14. Lemma. *Notation as above, the sum in the right hand side of Bott's formula*

$$\int s_5(\mathcal{E}(d)) \cap [\mathbb{B}] = \sum_{B \in \mathbb{B}^T} \frac{s_5^T(\mathcal{E}(d)_B) \cap [B]}{c_5^T(\mathcal{T}_B\mathbb{B})},$$

is a combination of $w_i's$ cf. (4.8) *with polynomial coefficients in d of degree ≤ 15.*

Proof. For each fixed point B let $\{\xi_1(d), \ldots, \xi_{m(d)}(d)\}$ denote the set of weights of $\mathcal{E}(d)_B$. Since $s_5^T(\mathcal{E}(d)_B)$ is a polynomial in the $T-$equivariant Chern classes

$$\{c_k^T(\mathcal{E}(d)_B) \mid k = 1, \ldots, 5\}$$

it's enough to prove that each

$$c_k^T(\mathcal{E}(d)_B) = \sigma_k(\xi_1(d), \ldots, \xi_{m(d)}(d))$$

is a combination of $w_i's$ with polynomial coefficients in d of degree $\leq 3k$.

Recalling Newton's identities

$$k\sigma_k = \sum_{i=1}^{k} (-1)^{i+1} \sigma_{k-i} p_i$$

where

$$p_k(\xi_1(d), \ldots, \xi_{m(d)}(d)) := \sum_{i=1}^{m(d)} \xi_i(d)^k$$

we see that it suffices to prove that $p_k(\xi_1(d), \ldots, \xi_{m(d)}(d))$ is a combination of $w_i's$ with polynomial coefficients in d of degree $\leq k+2$.

On the other hand, a careful analysis of the weights appearing in the basis of $\mathcal{E}(d)_B$ at each fixed point shows that these weights can be separated into sets of the form

$$\{\text{weights of } M_e(J)\} \text{ or } \{\text{weights of } M_e(J)\} + w$$

where

$$\begin{cases} w \text{ is a (fixed) combination of } w_i's; \\ e = d, d-1 \text{ and} \\ J = \langle Z_0, Z_1, Z_2 \rangle \text{ or} \\ J = \langle Z_i, Z_j \rangle,\ i \neq j\,. \end{cases}$$

From this the reader may be convinced that it's enough to prove the following

Claim: Let $m = m(d,n) := \binom{d+n}{n}$ and $\{\xi_{n,1}(d), \ldots, \xi_{n,m}(d)\}$ be the weights associated to a basis $M_d(\{Z_0, \ldots, Z_n\})$ of $\mathrm{Sym}_d(\langle Z_0, \ldots, Z_n \rangle)$. Then

$$p_k^n(d) := \sum_{i=1}^{m} \xi_{n,i}(d)^k$$

is a combination of $w_i's$ with polynomial coefficients in d of degree $\leq k+n$.

To prove the claim we proceed by induction on $n \geq 1$ and on $k \geq 0$. For $n = 1$,

$$M_d(\{Z_0, Z_1\}) = \{Z_0^d, Z_0^{d-1} Z_1, \ldots, Z_0 Z_1^{d-1}, Z_1^d\}$$

so that $m(d,1) = d+1$. We have

$$\begin{aligned} p_k^1(d) &= \sum_{i=1}^{d+1} \xi_{1,i}(d)^k = \sum_{i=0}^{d} (iw_0 + (d-i)w_1)^k \\ &= \sum_{i=0}^{d} (i(w_0 - w_1) + dw_1)^k = \sum_{i=0}^{d} \sum_{j=1}^{k} \binom{k}{j} (i(w_0 - w_1))^j (dw_1)^{k-j} \\ &= \sum_{j=1}^{k} \binom{k}{j} (dw_1)^{k-j} (w_0 - w_1)^j \sum_{i=0}^{d} i^j. \end{aligned}$$

The sum $\sum_{i=0}^{d} i^j$ is polynomial in d of degree $j+1$, therefore $p_k^1(d)$ is a combination of $w_i's$ with polynomial coefficients in d of degree $\leq k+1$.

For $k = 0$, we have $p_0^n(d) = m(d,n)$, a polynomial in d of degree n.

For the general case, write the basis $M_d(\{Z_0, \ldots, Z_n\})$ in the following form:

$$Z_0 M_{d-1}(\{Z_0, \ldots, Z_n\}) \cup Z_1 M_{d-1}(\{Z_1, \ldots, Z_n\}) \cup Z_2 M_{d-1}(\{Z_2, \ldots, Z_n\}) \cup \cdots \cup \{Z_n^d\}.$$

Then the weights are:

$$w_0 + \{\xi_{n,i}(d-1)\} \cup w_1 + \{\xi_{n-1,i}(d-1)\} \cup w_2 + \{\xi_{n-2,i}(d-1)\} \cup \cdots \cup \{dw_n\}.$$

Hence we can write

$$p_k^n(d) = \sum_{i=1}^{m(d,n)} (\xi_{n,i}(d))^k = \sum_{i=1}^{m(d-1,n)} (w_0 + \xi_{n,i}(d-1))^k +$$

$$\sum_{i=1}^{m(d-1,n-1)} (w_1 + \xi_{n-1,i}(d-1))^k + \sum_{i=1}^{m(d-1,n-2)} (w_2 + \xi_{n-2,i}(d-1))^k + \cdots + (dw_n)^k$$

$$= \sum_{j=0}^{k} \binom{k}{j} w_0^j p_{k-j}^n(d-1) + \sum_{j=0}^{k} \binom{k}{j} w_1^j p_{k-j}^{n-1}(d-1) +$$

$$\sum_{j=0}^{k} \binom{k}{j} w_2^j p_{k-j}^{n-2}(d-1) \ + \cdots + \ (dw_n)^k.$$

By induction we conclude that $p_k^n(d) - p_k^n(d-1)$ is a combination of $w_i's$ with polynomial coefficients in d of degree $\leq k+n-1$, and this implies that $p_k^n(d)$ is a combination of $w_i's$ with polynomial coefficients in d of degree $\leq k+n$.

□

4.3. **Foliations with invariant quadrics.** The varieties of complete quadrics (cf. [47]) can also be employed to construct a compactification of the space of 1-dimensional foliations in $\mathbb{P}^n$ that leave invariant a smooth quadric of arbitrary dimension. For example, in the case of conics and quadrics in $\mathbb{P}^3$ we obtain the following.

4.3.1. Theorem. *Let $\mathbb{Y}_{1,d}$ (resp.$\mathbb{Y}_{2,d}$) denote the closure in $\mathbb{P}^N$ of the variety of 1-dimensional foliations in $\mathbb{P}^3$ that have an invariant smooth conic (resp. quadric surface). Then we have the formulas for the degrees and codimensions,*

(i) $\deg \mathbb{Y}_{1,d} = \dfrac{4}{8!\,3^2}\,(d-1)\,d\,\big(207d^{14}+2763d^{13}+15447d^{12}+54395d^{11}+114847d^{10}+207891d^9+256737d^8+225801d^7+164937d^6+182101d^5+38993d^4+316221d^3+248856d^2-118908d-332640\big)$ *and its codimension is equal to* $4(d-1)$*;*

(ii) $\deg \mathbb{Y}_{2,d} = \dfrac{1}{9!\,(3!)^9}\,(d-1)\,d\,(d+1)\,\big(d^{24}+81d^{23}+3151d^{22}+77949d^{21}+1369333d^{20}+18084843d^{19}+185031133d^{18}+1481854743d^{17}+9251138050d^{16}+44737976160d^{15}+168507293704d^{14}+503603726976d^{13}+1212870415960d^{12}+2353394912904d^{11}+3628929239056d^{10}+4249158105672d^9+3232639214668d^8+413912636928d^7-2874493287072d^6-3885321416832d^5-1115680433472d^4+4477695012864d^3+8264265366528d^2+8139069775872d+4334215495680\big)$ *and its codimension is equal to* $(d-1)(d+5)$.

Appendix A

A.1. **Vector bundles.** A basic reference for this subject is [44], Chapter VI. A vector bundle $\mathcal{E}$ of rank e over a variety X is a variety $\mathcal{E}$ equipped with a morphism

$$\pi : \mathcal{E} \to X$$

such that

(1) There exists an open covering $\{U_i\}$ of X and isomorphisms

$$\varphi_i : \pi^{-1}(U_i) \to U_i \times \mathbb{A}^e.$$

(2) Over $U_{ij} := U_i \cap U_j$, the compositions

$$\varphi_{ij} := \varphi_i \circ \varphi_j^{-1} : U_{ij} \times \mathbb{A}^e \to U_{ij} \times \mathbb{A}^e$$

are linear, in the sense that $\varphi_{ij}(x, v) = (x, g_{ij}(x)v)$ with transition functions

$$g_{ij} : U_{ij} \to GL_e(\mathbb{C}).$$

(3) These transition functions are **cocycles**: $g_{ik} = g_{ij}g_{jk}$, $g_{ij}^{-1} = g_{ji}$ and $g_{ii} = 1$.

Conversely, given cocycles $\{g_{ij}\}$ it is possible to define a rank e vector bundle $\mathcal{E}$ whose transition functions are $\{g_{ij}\}$. The morphisms $\varphi_i : \pi^{-1}(U_i) \to U_i \times \mathbb{A}^e$ are called **local trivializations**.

A **line bundle** is a vector bundle of rank one.

A.1.1. Morphism of vector bundles. A morphism of vector bundles $\pi : \mathcal{E} \to X$, $\pi' : \mathcal{E}' \to X$ is a morphism $\psi : \mathcal{E} \to \mathcal{E}'$ such that

(1) $\pi' \circ \psi = \pi$ and
(2) if $\varphi_i : \pi^{-1}(U_i) \to U_i \times \mathbb{A}^e$ and $\varphi_i' : \pi'^{-1}(U_i) \to U_i \times \mathbb{A}^{e'}$ are local trivializations of $\mathcal{E}, \mathcal{E}'$, then $\psi_i := \psi_{|\pi^{-1}(U_i)}$ fits into the commutative diagram

$$\begin{array}{ccc} \pi^{-1}(U_i) & \xrightarrow{\psi_i} & \pi'^{-1}(U_i) \\ \downarrow{\scriptstyle \varphi_i} & & \downarrow{\scriptstyle \varphi_i'} \\ U_i \times \mathbb{A}^e & \xrightarrow[\psi_i']{} & U_i \times \mathbb{A}^{e'} \end{array}$$

where $\psi_i'(x, v) = (x, \gamma_i(x)v)$ with $\gamma_i : U_i \to \mathrm{Hom}(\mathbb{A}^e, \mathbb{A}^{e'})$ a morphism from U_i to the space of linear maps. Chosing basis, we may think of γ_i as a local matrix representation for ψ.

Since over U_{ij} the diagram below commutes,

$$\begin{array}{ccc} \pi^{-1}(U_{ij}) & \xrightarrow{\psi_j} & \pi'^{-1}(U_{ij}) \\ \downarrow{\scriptstyle \varphi_j} & & \downarrow{\scriptstyle \varphi_j'} \\ U_{ij} \times \mathbb{A}^e & \xrightarrow[\psi_j']{} & U_{ij} \times \mathbb{A}^{e'} \\ \downarrow{\scriptstyle \varphi_{ij}} & & \downarrow{\scriptstyle \varphi_{ij}'} \\ U_{ij} \times \mathbb{A}^e & \xrightarrow[\psi_i']{} & U_{ij} \times \mathbb{A}^{e'} \end{array}$$

(with φ_i and φ_i' connecting the first and last rows)

we have

$$g_{ij}'(x)\gamma_j(x) = \gamma_i(x)g_{ij}(x)\,.$$

A.1.2. Sections of a vector bundle. A section of $\mathcal{E}$ is a morphism $s : X \to \mathcal{E}$ such that $\pi \circ s = \mathrm{id}_X$.

A section s is determined by a collection of functions $s_i : U_i \to \mathbb{A}^e$ such that

$$s_i = g_{ij} s_j$$

in U_{ij}. We have $\varphi_i(s(x)) = (x, s_i(x))$ for $x \in U_i$.

A section of $\mathcal{E}$ determines a morphism of vector bundles that we also denote by s,

$$s : \mathcal{O}_X \to \mathcal{E}.$$

If s is a section of $\mathcal{E}$ as above, the **zero scheme of** s, denoted $\mathcal{Z}(s)$, is defined in each open set U_i by the ideal $\langle s_{i1}, \ldots, s_{ie} \rangle$, where $s_i = (s_{i1}, \ldots, s_{ie})$ with $s_{ij} \in \mathcal{O}_X(U_i)$.

In fact $\mathcal{Z}(s)$ is the scheme defined by the ideal sheaf image of the map $s^\vee : \mathcal{E}^\vee \to \mathcal{O}_X$ dual of s.

A.1.3. Pull-back of vector bundles. Suppose that $\pi : \mathcal{E} \to X$ is a vector bundle, and let $f : Y \to X$ a morphism. We define a vector bundle over Y, denoted $f^*\mathcal{E}$ as follows.

Take the open covering $\{V_i\}$ of Y, where $V_i := f^{-1}(U_i)$, and glue the patches $\{V_i \times \mathbb{A}^e\}$ along $V_{ij} := V_i \cap V_j$ using the cocycles $h_{ij} := g_{ij} \circ f$, (*i.e.,* by the isomorphism $(y, v) \to (y, g_{ij}(f(y))v)$). The variety obtained in this way has a natural projection to Y, $\rho(y, v) = y$, and $\rho^{-1}(y) = \pi^{-1}(f(y))$, *i.e.,* in the fibers we have $(f^*\mathcal{E})_y = \mathcal{E}_{f(y)}$.

A.1.4. Jet bundles.

We recall the notion of jet bundles associated to a vector bundle. A basic reference is [28, 16.7] and [42]. Here we state without proofs the results that we need in the text.

Let $\mathcal{E}$ be a vector bundle over a smooth projective variety X. For $n \geq 0$ the n-jet bundle associated to $\mathcal{E}$, denoted $\mathcal{P}^n(\mathcal{E})$, is a vector bundle over X whose fiber over $x \in X$ is given by

$$\mathcal{P}^n(\mathcal{E})_x = (\mathcal{O}_X / m_x^{n+1}) \otimes \mathcal{E}_x$$

where m_x is the maximal ideal of the point x.

For each $n \geq 0$ there exist exact sequences:

$$0 \to \operatorname{Sym}_{n+1} \Omega_X \otimes \mathcal{E} \to \mathcal{P}^{n+1}(\mathcal{E}) \to \mathcal{P}^n(\mathcal{E}) \to 0. \tag{A.1}$$

As an example let's analyse the case $n = 0$. We have

$$0 \to \Omega_X \otimes \mathcal{E} \to \mathcal{P}^1(\mathcal{E}) \to \mathcal{E} \to 0. \tag{A.2}$$

Consider the evaluation map

$$ev : X \times H^0(X, \mathcal{E}) \to \mathcal{E}$$

given by $ev(x, s) = (x, s(x))$.

The map ev lifts to a map

$$ev_1 : X \times H^0(X, \mathcal{E}) \to \mathcal{P}^1(\mathcal{E}).$$

Suppose that we are in a neighborhood of $0 \in X$ and that $x = (x_1, \ldots, x_m)$ are local coordinates of X.

On the fiber of 0 we have $ev_1(0, s) = (0, s(0) + J_0 s \cdot x)$, where $J_0 s$ is the Jacobian of s at 0. If $s(0) = 0$ then

$$ev_1(s) = J_0 s \cdot x \in \Omega_{X,0} \otimes \mathcal{E}_0 \simeq m/m^2 \otimes \mathcal{E}_0$$

i.e., we retrieve the differential of the section.

In general ev lifts to a map $ev_n : X \times H^0(X, \mathcal{E}) \to \mathcal{P}^n(\mathcal{E})$ given by

$$ev_n(x, s) = (x, s_n(x))$$

where $s_n(x)$ is the Taylor expansion of s truncated in order $n + 1$.

We have a commutative diagram

$$\begin{array}{ccc} X \times H^0(X, \mathcal{E}) & \xrightarrow{ev_n} & \mathcal{P}^n(\mathcal{E}) \\ & \searrow^{ev_{n-1}} & \downarrow \\ & & \mathcal{P}^{n-1}(\mathcal{E}) \ . \end{array} \tag{A.3}$$

A.2. **Cartier Divisors.** General references for this subject are [43] Chapter III and [44] Chapter VI.

A.2.1. Definition. Let X be a scheme. A **Cartier divisor** D on X is given by an affine open cover $\{U_i\}$ of X together with a choice of an invertible element f_i in the total ring of fractions $R(U_i)$ of the coordinate ring $\mathcal{O}_X(U_i)$ such that $f_i {f_j}^{-1}$ is invertible in $\mathcal{O}_X(U_{ij})$, with $U_{ij} = U_i \cap U_j$, $\forall i, j$. Each f_i is said to be a **local equation of** D **in** U_i.

The data $(\{U_i\}, f_i)$ and $(\{V_\alpha\}, g_\alpha)$ determine the same Cartier divisor if there exists a refinement $\{W_\lambda\}$ of $\{U_i \cap V_\alpha\}$ such that

$$(f_{i\,|W_\lambda})(g_{\alpha\,|W_\lambda})^{-1} \quad \text{is invertible in } \mathcal{O}_X(W_\lambda) \tag{A.4}$$

for all $i = i(\lambda)$, $\alpha = \alpha(\lambda), W_\lambda \subseteq U_i \cap V_\alpha$.

For each Cartier divisor on a scheme X, we are given a collection of local equations $f_x \in R(\mathcal{O}_{X,x})$, $\forall x \in X$ with the following property. For each $x \in X$, there exists an affine neighborhood U_x together with some $\widetilde{f} \in R(U_x)$ such that f_y is the image of $\widetilde{f}$ in $R(U_y)$ for all $y \in U_x$. Two such collections $\{f_x\}, \{g_x\}$ define the same Cartier divisor if and only if for all x we have that $f_x {g_x}^{-1}$ lies in $\mathcal{O}^\star_{X,x}$, the subgroup of invertible elements. Put in other words, a Cartier divisor is an element of $H^0(X, R^\star/\mathcal{O}^\star)$.

A Cartier divisor is said to be **effective** if it admits a representation by local equations $(\{U_i\}, f_i)$ such that f_i is a regular function, *i.e.,* f_i lies in $\mathcal{O}_X(U_i)$ for all i. This is the same as a closed subscheme locally defined by a nonzero divisor.

A Cartier divisor $D = (\{U_i\}, f_i)$ is said to be **principal** if $f_i = f_j$ in U_{ij}, $\forall i, j$. In other words, the given local equations are compatible along the intersection, thereby yielding a global section f of the subsheaf $R^\star_X$ of invertible elements of the sheaf of total ring of fractions, so that we may also write $D = (\{X\}, f)$, a single equation.

A.2.2. Example. *Let $X = \mathbb{P}^n$ and let $F(Z_0, \ldots, Z_n)$ be a nonzero homogeneous polynomial of degree m. Let U_i be the standard affine open subset complementary of the hyperplane $Z_i = 0$. The coordinate ring of U_i is the polynomial ring in the indeterminates $Z_0/Z_i, \ldots, Z_n/Z_i$. Put*

$$f_i = {Z_i}^{-m} F = F(Z_0/Z_i, \ldots, Z_n/Z_i) \in \mathcal{O}_X(U_i).$$

Then (U_i, f_i), $i = 0, \ldots, n$ is an effective Cartier divisor. It is equal to the hypersurface defined by F.

A.2.3. Definition. Let $D = (\{U_i\}, f_i)$ be a Cartier divisor on X. The **cycle associated** to D is

$$[D] = \sum \mathrm{ord}_V(D) \cdot V,$$

where the sum is taken over the subvarieties of codimension one and the coefficient is defined by

$$\mathrm{ord}_V(D) = \mathrm{ord}_{V_i}(f_i) \tag{A.5}$$

with $V_i = U_i \cap V \neq \emptyset$.

A.2.4. Definition. Let $D = (\{U_i\}, f_i)$ be a Cartier divisor on X. We write $\mathcal{O}_X(D)$ for the *line bundle associated* to D, defined by the transition functions $f_{ij} = f_i f_j^{-1}$ on U_{ij} (cf.[43], p.270).

Explicitly, $\mathcal{O}_X(D)$ is the scheme over X obtained by glueing. One takes the disjoint union

$$\coprod U_i \times \mathbb{A}^1$$

and identify pairs

$$(x, v) \in U_i \times \mathbb{A}^1,\ (y, w) \in U_j \times \mathbb{A}^1$$

if and only if

$$x = y \in U_{ij} \quad \text{and} \quad v = f_{ij}(x)w.$$

In other words, we glue the open affine subsets $U_i \times \mathbb{A}^1, U_j \times \mathbb{A}^1$ identifying the open subsets $U_{ij} \times \mathbb{A}^1 \subseteq U_i \times \mathbb{A}^1,\ U_{ij} \times \mathbb{A}^1 \subseteq U_j \times \mathbb{A}^1$ via the isomorphism $A[T] \simeq A[T]$ defined by $T \mapsto f_{ij} \cdot T$, where A denotes the coordinate ring of U_{ij}.

A.2.5. Proposition. *Let $\mathcal{L} \to X$ be a line bundle over a variety. Then there exists a Cartier divisor D on X such that $\mathcal{O}_X(D)$ is isomorphic to $\mathcal{L}$.*

Proof. Let $\{U_i\}$ be an affine open cover of X and let $f_{ij} \in \mathcal{O}_X(U_{ij})^\star$ be transition functions for $\mathcal{L}$. Since X is a variety, each coordinate ring $\mathcal{O}_X(U_{ij})$ is a domain, contained in the function field $R(X) = R(U)$ for any open subset $U \neq \emptyset$. Fix an index i_0, and write it 0 for short. Set $f_i = f_{i0}$. It is clear that $(\{U_i\}, f_i)$ defines a Cartier divisor D. Furthermore, the associated line bundle $\mathcal{O}_X(D)$ is given by the transition functions $f_i f_j^{-1} = f_{i0} {f_{j0}}^{-1} = f_{ij}$, whence $\mathcal{O}_X(D)$ is isomorphic to $\mathcal{L}$. □

A.2.6. Remark. The result above does not hold for arbitrary schemes, cf. Hartshorne, [30].

A.3. **Projective bundles.** Associated to a vector bundle $\mathcal{E}$ we have a projective bundle $\mathbb{P}(\mathcal{E})$. It is obtained by replacing the vector space fibers of $\mathcal{E}$, all isomorphic to $\mathbb{A}^e$, by the projective space $\mathbb{P}(\mathbb{A}^e) \simeq \mathbb{P}^{e-1}$. See [44, Chapter VI p.73] and [21, Appendix B.5].

Explicitly, given a vector bundle defined by transition functions $\{g_{ij}\}$, we glue the patches $\{U_i \times \mathbb{P}^{e-1}\}$ along $U_{ij} \times \mathbb{P}^{e-1}$ using the linear isomorphisms g_{ij}'s. We glue $U_i \times \mathbb{P}^{e-1}$ with $U_j \times \mathbb{P}^{e-1}$ with the isomorphism $(x, [v]) \mapsto (x, [g_{ij}v])$, for $x \in U_{ij}$.

We have a projection

$$p : \mathbb{P}(\mathcal{E}) \to X \text{ such that } p(\varphi_i^{-1}(x, [v])) = x.$$

This map is proper.

Consider $p^*\mathcal{E}$, it is a vector bundle over $\mathbb{P}(\mathcal{E})$, whose fiber over $(x, [v])$ is $\mathcal{E}_x$.

In analogy with the tautological line bundle of $\mathbb{P}^n$, there exist a **tautological** vector subbundle $\mathcal{O}_{\mathcal{E}}(-1)$ of $p^*\mathcal{E}$, whose fiber over $(x,[v]) \in \mathbb{P}(\mathcal{E})$ is $\mathbb{C}v$. We have

$$\mathcal{O}_{\mathcal{E}}(-1) \longrightarrow p^*\mathcal{E}$$

which is nonzero on every fiber. The above correspond to a section

$$\mathcal{O}_{\mathbb{P}(\mathcal{E})} \longrightarrow p^*\mathcal{E} \otimes \mathcal{O}_{\mathcal{E}}(1).$$

The cokernel is the **relative tangent bundle** of $\mathbb{P}(\mathcal{E})$ over X:

$$0 \to \mathcal{O}_{\mathbb{P}(\mathcal{E})} \longrightarrow p^*\mathcal{E} \otimes \mathcal{O}_{\mathcal{E}}(1) \longrightarrow \mathcal{T}_{\mathbb{P}(\mathcal{E})/X} \to 0. \tag{A.6}$$

A.4. **Grassmannians.** For the definition and first properties of Grassmannians consult ([29] Lecture 6) or [43] and [44]). Let $\mathbb{G} = \mathbb{G}(k,n)$ denote the variety parametrizing projective k-planes of $\mathbb{P}^n$ (equivalently $\mathbb{G}$ parametrizes vector $(k+1)$-planes of $\mathbb{C}^{n+1}$.) We have

$$\dim \mathbb{G}(k,n) = (k+1)(n-k)\,.$$

There exists a tautological exact sequence of fiber bundles over $\mathbb{G}$,

$$0 \to \mathcal{S} \to \mathbb{G} \times \mathbb{C}^{n+1} \to \mathcal{Q} \to 0 \tag{A.7}$$

where $\mathcal{S}$ is of rank $k+1$ and $\mathcal{Q}$ is of rank $n-k$. Explicitly, if $W \in \mathbb{G}$ is the projectivization of a $k+1$-plane $\Lambda \subset \mathbb{C}^{n+1}$,*i.e.,* $W = \mathbb{P}(\Lambda)$, then the fiber of $\mathcal{S}$ over W is $\mathcal{S}_W = \Lambda$ (respectively, the fiber of $\mathcal{Q}$ is $\mathbb{C}^{n+1}/\Lambda$).

If we dualize the sequence (A.7), we obtain

$$0 \to \mathcal{Q}^\vee \to \mathbb{G} \times \check{\mathbb{C}}^{n+1} \to \mathcal{S}^\vee \to 0. \tag{A.8}$$

The fiber of $\mathcal{Q}^\vee$ over W is the subspace of $\check{\mathbb{C}}^{n+1}$ generated by the equations defining W.

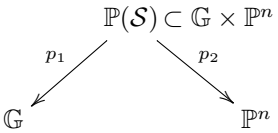
In the case $k=0$, we have $\mathbb{G}(0,n) = \mathbb{P}^n$, and the tautological bundle is $\mathcal{S} = \mathcal{O}_{\mathbb{P}^n}(-1)$.

The projective bundle $\mathbb{P}(\mathcal{S})$ is the *universal k-plane*:

$$\mathbb{P}(\mathcal{S}) = \{(W,p) \in \mathbb{G} \times \mathbb{P}^n \mid p \in W\}.$$

We have projection maps

(A.9)



Observe that $p_2^*\mathcal{O}_{\mathbb{P}^n}(-1) = \mathcal{O}_{\mathbb{P}(\mathcal{S})}(-1)$.

A.5. **Blowup.** In this section we present without proofs some basic facts about the blowup of a scheme along a subscheme. A reference for this subject is [21, Appendix B.6] or [43, Chapter II].

Let X be a closed subscheme of a scheme Y, defined by an ideal sheaf $\mathcal{J}$. Then the blowup of Y along X, denoted $\widetilde{Y}$ is defined by

$$\widetilde{Y} := \operatorname{Proj}\Big(\bigoplus_{n\geq 0} \mathcal{J}^n\Big).$$

Denote by $\pi : \widetilde{Y} \to Y$ the projection and set $E := \pi^{-1}(X)$. Then E is a Cartier divisor, called the **exceptional divisor**. Moreover, π restricted to $\widetilde{Y} \setminus E$ is an isomorphism onto $Y \setminus X$.

Suppose that the embedding of X in Y is regular of codimension d. Then we have

$$E = \mathbb{P}(\mathcal{N})$$

with projection $\eta : E \to X$, where $\mathcal{N} = \mathcal{N}_X Y$, stands for the normal bundle. Moreover,

$$\mathcal{N}_E \widetilde{Y} = \mathcal{O}_{\widetilde{Y}}(E)_{|E} = \mathcal{O}_{\mathcal{N}}(-1). \tag{A.10}$$

Next we want to compute the fiber of $T\widetilde{Y}$ over a point $y \in E$. We have the following exact sequence

$$0 \to \mathcal{T}E \to \mathcal{T}\widetilde{Y}_{|E} \to \mathcal{N}_E \widetilde{Y} \to 0.$$

Therefore

$$\mathcal{T}_y \widetilde{Y} = \mathcal{T}_y E \oplus \mathcal{O}_{\mathcal{N}}(-1)_y \tag{A.11}$$

though not canonically. However, if $y \in Y$ happens to be a fixed point of some $\mathbb{C}^*-$action on Y that leaves X invariant, the above decomposition is unique as $\mathbb{C}^*-$modules.

If $y = (x, [v])$, with $x \in X$ and $v \in \mathcal{N}_x$, then

$$\mathcal{O}_{\mathcal{N}}(-1)_y = \mathbb{C} \cdot v. \tag{A.12}$$

In order to compute $\mathcal{T}_y E$, we observe that

$$\mathcal{T}_y E = \mathcal{T}_x X \oplus \mathcal{T}_{[v]} \mathbb{P}(\mathcal{N}_x). \tag{A.13}$$

But $\mathcal{T}_{[v]} \mathbb{P}(\mathcal{N}_x)$ is the fiber over y of the relative tangent bundle of $\mathbb{P}(\mathcal{N})$ over X, which is defined by the following (Euler) exact sequence (see [21, B.5.8.]):

$$0 \to \mathcal{O}_{\mathbb{P}(\mathcal{N})} \to \eta^* \mathcal{N} \otimes \mathcal{O}_{\mathbb{P}(\mathcal{N})}(1) \to \mathcal{T}_{\mathbb{P}(\mathcal{N})/X} \to 0.$$

Moreover, from this we deduce that $\mathcal{T}_{\mathbb{P}(\mathcal{N})/X} = \mathrm{Hom}(\mathcal{O}_{\mathbb{P}(\mathcal{N})}(-1), \mathcal{Q})$ where $\mathcal{Q}$ is the universal quotient bundle of $\mathbb{P}(\mathcal{N})$. Thus

$$\mathcal{T}_{[v]} \mathbb{P}(\mathcal{N}_x) = \mathrm{Hom}(\mathbb{C} \cdot v, \frac{\mathcal{N}_x}{\mathbb{C} \cdot v}). \tag{A.14}$$

Putting together (A.11), (A.12), (A.13) and (A.14) we obtain

$$\mathcal{T}_y \widetilde{Y} = \mathcal{T}_x X \oplus \mathrm{Hom}(\mathbb{C} \cdot v, \frac{\mathcal{N}_x}{\mathbb{C} \cdot v}) \oplus \mathbb{C} \cdot v. \tag{A.15}$$

As a final remark observe that since π is an isomorphism from $\widetilde{Y} \setminus E$ onto $Y \setminus X$ we have, for a point $y \in \widetilde{Y} \setminus E$,

$$\mathcal{T}_y \widetilde{Y} = \mathcal{T}_{\pi(y)} Y.$$

A.6. **Complete conics.** In this subsection we review some results about conics and the space of complete conics. References for this topic are [29], [47].

Let F denote the vector space $\mathbb{C}^3$, $\mathbb{P}^2 = \mathbb{P}(F)$. A conic is given by a nonzero symmetric map $u : F \to F^\vee$ modulo non-zero multiples, *i.e.,* an element of $\mathbb{P}(\mathrm{Sym}_2(F^\vee)) = \mathbb{P}^5$.

The rank of a conic is by definition the rank of the map u. It defines two distinguished subvarieties in $\mathbb{P}(\mathrm{Sym}_2(F^\vee))$. The first one is the locus of double lines, corresponding to the maps with $\operatorname{rk} u = 1$. We denote it by $\mathbb{V}$. The locus of singular conics (the maps with $\operatorname{rk} u \leq 2$) is denoted by $\mathbb{V}_2$. We have that $\mathbb{V}_2$ is the (cubic) hypersurface defined by $\det(u) = 0$ and $\mathbb{V}$ is the Veronese surface, given by the image of

$$\nu_2 : \mathbb{P}(F^\vee) \to \mathbb{P}(\mathrm{Sym}_2 F^\vee)$$

where $\nu_2([a_0 : a_1 : a_2]) = [a_0^2 : 2a_0a_1 : \cdots : a_2^2]$ *i.e.,* ν_2 sends a line $L := a_0Z_0 + a_1Z_1 + a_2Z_2$ to $L^2 := a_0^2Z_0^2 + 2a_0a_1Z_0Z_1 + \cdots + a_2^2Z_2^2$.

Next we compute the tangent and normal spaces of the Veronese variety in $\mathbb{P}^5$. Suppose that the double line we are considering is Z_0^2. Then a vector $v = (a_1, a_2, \ldots, a_5)$ is in $\mathcal{T}_{Z_0^2}\mathbb{V}$ if and only if

$$Z_0^2 + \varepsilon(a_1Z_0Z_1 + a_2Z_0Z_2 + \cdots + a_5Z_2^2) \in \mathbb{V}(\mathbb{C}[\varepsilon])$$

i.e., if the matrix representing this conic has all 2×2–minors equal to zero over the ring $\mathbb{C}[\varepsilon]$, $\varepsilon^2 = 0$. This matrix reduces (after some elementary operations) to

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon a_3 & \varepsilon a_4 \\ 0 & \varepsilon a_4 & \varepsilon a_5 \end{pmatrix}.$$

So it is clear that all 2×2 minors of A vanish if and only if $a_3 = a_4 = a_5 = 0$. It follows that

$$\mathcal{T}_{Z_0^2}\mathbb{V} = \mathbb{C} \cdot Z_0^{2\vee} \otimes \langle Z_0Z_1, Z_0Z_2\rangle_{\mathbb{C}} \subset \mathcal{T}_{Z_0^2}\mathbb{P}^5 = (\mathcal{O}_{\mathbb{P}^5}(1) \otimes Q)_{Z_0^2}. \tag{A.16}$$

and

$$(\mathcal{O}_{\mathbb{P}^5}(1) \otimes Q)_{Z_0^2} = \mathbb{C} \cdot Z_0^{2\vee} \otimes \langle Z_0Z_1, Z_0Z_2, Z_1^2, Z_1Z_2, Z_2^2\rangle_{\mathbb{C}}. \tag{A.17}$$

Consequently the normal to $\mathbb{V}$ in $\mathbb{P}^5$ is:

$$\mathcal{N}_{Z_0^2} = \mathbb{C} \cdot Z_0^{2\vee} \otimes \langle Z_1^2, Z_1Z_2, Z_2^2\rangle_{\mathbb{C}}. \tag{A.18}$$

In fact, in [47, Proposition 4.4.] is proved that if we consider the Grassmannian of lines in $\mathbb{P}^2$ with tautological sequence:

$$\mathcal{S}_2 \to \mathbb{G} \times F \to \mathcal{Q}_2$$

where $\mathcal{S}_2$ has rank 2, then

$$\mathcal{N}_{\mathbb{V}}\mathbb{P}^5 = (\mathcal{O}_{\mathbb{P}^5}(1) \otimes \mathrm{Sym}_2(\mathcal{S}_2^\vee))_{|\mathbb{V}}.$$

This may clarify the description (A.18).

The Gauss map associates to each point on a conic $\mathcal{C}$ its tangent line. If a conic $\mathcal{C}$ is smooth, this map is an isomorphism and the dual $\mathcal{C}^*$ is again a smooth conic in $\check{\mathbb{P}}^2$, also referred to as the envelope of tangent lines to $\mathcal{C}$. It is the restriction to the conic of the map $\mathbb{P}(F) \to \mathbb{P}(F^\vee)$ induced by the linear map u. But there is no well defined tangent line at a singular point of the conic. In order to produce a well defined envelope for every conic, H. Schubert ([45]) introduced the variety of "complete conics". This variety is a compactification of the variety of smooth

conics, different from $\mathbb{P}^5$. Let us explain how this compactification is obtained. Consider the rational map

$$\epsilon : \mathbb{P}^5 = \mathbb{P}(\mathrm{Sym}_2 F^\vee) \dashrightarrow \check{\mathbb{P}}^5 = \mathbb{P}(\mathrm{Sym}_2 \overset{2}{\wedge} F^\vee)$$

given by $\epsilon(u) = \overset{2}{\wedge} u$. This map restricted to the open set of smooth conics is a bijection that sends a conic to its dual conic.

The variety of complete conics is the blowup $\mathbb{B}$ of $\mathbb{P}^5$ along $\mathbb{V}$. In [47, p. 210] it is proved that $\mathbb{B}$ is embedded in $\mathbb{P}^5 \times \check{\mathbb{P}}^5$ as $\mathbb{B} = \overline{\mathrm{Graph}\,\epsilon}$, closure of the graph of ϵ.

A.7. **Bott's Formula.** In this section we explain Bott's equivariant formula. A reference for this subject in the general case is [40] and the bibliography therein.

Let X be a smooth complete variety of dimension n, and let $T = \mathbb{C}^*$ act on X with isolated fixed points. Write X^T for the set of fixed points.

Let $\mathcal{E}$ be a T-equivariant vector bundle over X of rank r.

If $p(c_1, \ldots, c_r)$ is a weighted homogeneous polynomial of total degree n with rational coefficients, where $\deg c_i = i$, then

$$p(c_1(\mathcal{E}), \ldots, c_r(\mathcal{E})) \cap [X]$$

is a zero cycle in X. Bott's formula expresses the degree of this zero cycle in terms of data given by the induced action of T on the fibers of $\mathcal{E}$ and of the tangent bundle $\mathcal{T}X$ over the fixed points of the action. Below is an outline for its usage.

Let $p \in X^T$ be a fixed point. The torus T acts on the fiber $\mathcal{E}_p$ and (as T is semisimple) we have a complete decomposition of $\mathcal{E}_p$ into T-eigenspaces, with certain weights $\xi_i \in \mathbb{Z}$:

$$\mathcal{E}_p = \oplus_{i=1}^r \mathcal{E}_p^{\xi_i}$$

with

$$\mathcal{E}_p^{\xi_i} = \{v \in \mathcal{E}_p \mid t \cdot v = t^{\xi_i} v, t \in T\}\,.$$

Set

$$c_i^T(\mathcal{E}_p) := \sigma_i(\xi_1, \ldots, \xi_r)\,,$$

where σ_i denotes the i-th elementary symmetric polynomial:

$$\sigma_1 = \sum \xi_j,\ \sigma_2 = \sum_{i<j} \xi_i \xi_j,\ \ldots,\ \sigma_r = \xi_1 \cdots \xi_r\,.$$

Set $p^T(\mathcal{E}_p) = p(c_1^T(\mathcal{E}_p), \ldots, c_r^T(\mathcal{E}_p))$. Here the magic comes:

A.7.1. Theorem. (Bott's formula)

$$\int p(c_1(\mathcal{E}), \ldots, c_r(\mathcal{E})) \cap [X] = \sum_{p \in X^T} \frac{p^T(\mathcal{E}_p)}{c_n^T(\mathcal{T}_p X)}.$$

□

It is a nice fact that the integer appearing in the left hand side is obtained as a sum of *rational* numbers!

References

[1] A. Altman and S. Kleiman. *Foundations of the Theory of Fano Schemes*. Compositio Math. **34**, 3–47 1977.

[2] O. Calvo-Andrade. *Irreducible components of the space of holomorphic foliations*. Math. Ann. 299 1994, no. 4, 751–767.

[3] O. Calvo-Andrade, D. Cerveau, L. Giraldo and A. Lins Neto. *Irreducible components of the space of foliations associated to the affine Lie algebra*. Ergodic Theory Dynam. Systems 24, no. 4, 987–1014, 2004.

[4] C. Camacho and A. Lins Neto. *Teoria Geométrica das Folheações*. IMPA,1979.

[5] D. Cerveau and A. Lins Neto. *Holomorphic Foliations in $\mathbb{P}^2$ having an Invariant Algebraic Curve*. Annales de l'Institut Fourier 41 fasc. 4, 883-904, 1991.

[6] ———. *Irreducible Components of the Space of Holomorphic Foliations of degree two in $\mathbb{P}^n$, $n \geq 3$* The Annals of Mathematics, Second Series, vol. 143, No 3, pp. 577-612, 1996.

[7] C. Christopher, J. Llibre and J.V. Pereira. *Multiplicity of Invariant Algebraic Curves in Polynomial Vector Fields* Pacific Journal of Mathematics Vol. 229, No. 1, p.63-117, 2007.

[8] G. N. Costa, *Holomorphic foliations by curves on $\mathbb{P}^3$ with non-isolated singularities*, Ann. F. Sciences de Toulouse, Sér. 6, 15 no. 2, p. 297–321, 2006.

[9] S.C. Coutinho and J.V. Pereira. *On the density of algebraic foliations without algebraic invariant sets*. J. Reine Angew. Math., 594. 2006.

[10] F. Cukierman and J.V. Pereira. *Stability of Holomorphic Foliations with Split Tangen Sheaf*. American Journal of Mathematics 130.2. 413-439, 2008.

[11] F. Cukierman, J.V. Pereira and I. Vainsencher. *Stability of Foliations induced by rational maps*. Annales de la Faculté des Sciences de Toulouse. 2007.

[12] F. Cukierman, M. Soares and I. Vainsencher. *Singularities of logarithmic foliations*. Compositio Mathematica. vol. 142, p 131-142, 2006.

[13] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics, 150. New York Springer-Verlag, 1994.

[14] E. Esteves. *The Castelnuovo-Mumford regularity of an integral variety of a vector field on projective space*, Math. Res. Lett. **9**, 1-15.

[15] M. Falla Luza. *Global Geometry of Second Order Differential Equations*. Doctoral Thesis, IMPA. `http://www.impa.br/opencms/pt/ensino/downloads/teses_de_doutorado/teses_2010/Hernan_Maycol_Falla_Luza.pdf`. 2010

[16] V. Ferrer. *Aspectos enumerativos de Folheações Holomorfas*. Doctoral Thesis, UFMG. 2010. `http://www.mat.ufmg.br/intranet-atual/pgmat/TesesDissertacoes/uploaded/Tese024.pdf`.

[17] V. Ferrer and I. Vainsencher. *Polynomial vector fields with algebraic trajectories*. Commutative algebra and its connections to geometry, pp. 71-85, Contemp. Math., 555, Amer. Math. Soc., Providence, RI, 2011.

[18] ———. *Degenerate singularities of one dimensional foliations*. Commentarii Mathematici Helvetici. Vol 88. Issue 2, pp.305-321, 2013

[19] ———. *Scripts*. `http://www.mat.ufmg.br/~israel/Publicacoes/Vivis/index.html`. 2010.

[20] ———. *Enumerative Aspects of Holomorphic Foliations*. Monografas del IMCA N. 53, v. 1. 77p. Lima. 2010.

[21] W. Fulton. *Intersection Theory*. Springer-Verlag. New York. 1985.

[22] L. Göttsche, *A conjectural generating function for numbers of curves on surfaces*, Comm. Math. Phys. 196, 523–533, 1998. eprint alg-geom/9711012

[23] X. Gómez-Mont. *Holomorphic foliations in ruled surfaces*. Trans. Amer. Math. Soc., 312(1):179-201, 1989.

[24] ———. *On the spaces of polynomial vector fields modulo projectivities*, Proc. Cong. Dyn. Syst., Trieste 1988, Pitman 1990, 112-127.

[25] ———. *On foliations in $\mathbb{P}^2$ tangent to an algebraic curve*, Proc. Cong. Alg. Geom., Cimat, 1989; Aportaciones Matematicas, Investigacion 5 , 87-99, 1992.

[26] X. Gómez-Mont and L. Ortíz-Bobadilla. *Sistemas dinámicos holomorfos en superficies*. Sociedad Matemática Mexicana, México City, 1989.

[27] G.-M. Greuel, G. Pfister and H. Schönemann, SINGULAR 3-1-1, A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern, 2010. `http//www.singular.uni-kl.de`.

[28] A. Grothendieck and J. Dieudonné. *Éléments de Géométrie Algébrique IV-4*. Publ. Math. IHES, **32**, 5–361, 1967.
[29] J. Harris. *Algebraic Geometry. A First Course*. Graduate Texts in Mathematics. 133. New York - Heidelberg - Berlin: Springer-Verlag, 1992.
[30] R. Hartshorne. *Ample subvarieties of algebraic varieties*, LNM 156 Springer-Verlag, 1970.
[31] ———. *Algebraic Geometry*. Graduate Texts in Mathematics. 52. New York - Heidelberg - Berlin: Springer-Verlag, 1977.
[32] J.P. Jouanolou. *Equations de Pfaff algébriques*. Lectures Notes in Mathematics, **708**. Springer-Verlag, 1979.
[33] ———. *Hypersurfaces solutions d´une équation de Pfaff analytique*. Math. Ann. 232(3), 239-245, 1978.
[34] S. Katz and S. A. Stromme. SCHUBERT: *A Maple package for Intersection Theory*. 2001. Available at `http://stromme.uib.no/home/schubert/`.
[35] S. L. Kleiman and R. Piene. *Node polynomials for families: methods and applications*. Math. Nachr. 271, 69–90, 2004.
[36] D. Laksov. *Complete linear maps*. Ark. Mat. 26, 231-263, 1988.
[37] A. Lins Neto. *Algebraic Solutions of Polynomial Differential Equations and Foliations in Dimension 2*. Holomorphic Dynamics, Springer Lecture Notes In Mathematics, v. 1345, pp. 192-232. 1988.
[38] ———. *Componentes Irredutíveis dos Espaços de Folheações*. 26 Colóquio Brasileiro de Matemática, IMPA, 2007.
[39] A. Lins Neto. and B. Scardua. *Folheações Algébricas Complexas*. 21 Colóquio Brasileiro de Matemática, IMPA, 1997.
[40] A. Meireles Araújo and I. Vainsencher. *Equivariant intersection theory and Bott's residue formula*. 16th School of Algebra, Part I. Brasília, 2000. Mat. Contemp. 20, 2001.
[41] J. V. Pereira. *Vector Fields, Invariant Varieties and Linear Systems*, Annales de L'Institut Fourier, 51 no.5, 1385-1405, 2001.
[42] R. Piene. *Some formulas for a surface in P^3*. Algebraic geometry (Proc. Sympos., Univ. Tromsø, Tromsø, 1977), pp. 196–235, Lecture Notes in Math., 687, Springer, Berlin, 1978.
[43] I. Shafarevich. *Basic Algebraic Geometry I*. Second Edition, New York - Heidelberg - Berlin. Springer-Verlag, 1994.
[44] ———. *Basic Algebraic Geometry 2*. Second Edition, New York - Heidelberg - Berlin. Springer-Verlag, 1997.
[45] H. Schubert. *Kalkül der abzählenden Geometrie*, reprint, Springer-Verlag. 1979.
[46] I. Vainsencher. *Classes características em Geometria Algébrica*. 15 Colóquio Brasileiro de Matemática, IMPA, 1985. *Characteristic Classes in Algebraic Geometry*, available at `http://www.mat.ufmg.br/~israel/Ensino/int.pdf`.
[47] ———. *Schubert calculus for complete quadrics*. Enumerative geometry and classical algebraic geometry (Nice, 1981), 199–235, Progr. Math., 24, Birkhäuser, Boston, Mass. 1982.

GAN–Depto. Matemática, UFF
R. Mário Santos Braga, s/n, 4 andar
24020-140, Niterói, RJ - Brazil
E-mail address: `vivisferrer@gmail.com`

4to Coloquio Uruguayo de Matemática (2013)

Publicaciones Matemáticas del Uruguay
Volumen 15, Junio 2016, Páginas 93–108
S 0797-1443

CENTRAL LIMIT THEOREM FOR THE NUMBER OF CROSSING OF RANDOM PROCESSES

JEAN-MARC AZAÏS

1. Introduction

This course presents the application of the Malevich [15],Cuzick [6] Berman [4] method for establishing a central limit theorem for non linear functional of Gaussian processes (see Section 3).These methods have been introduced in the 70's for studying zero crossing of stationary processes or the sojourn time of a stochastic process. We present here mainly its application to the number of roots of random processes. The basic argument is the approximation of the original process by a m-dependent process (see Section 3). Section 2 presents a short memento of crossings of process and the calculation of their moments. Our main tools and results are presented in Section 3. Section 4 presents generalizations and applications to some particular processes, in particular random trigonometric polynomials and specular point in sea-wave modeling.

2. Basic facts on crossings of functions

This section contains preliminary results almost without proofs. They can be found for example in Azaïs and Wschebor [3].

For simplicity all the functions $f(t)$ considered are real and of class C^1. If I is a real interval we will define:

$$N_u(f,I) := \#\left\{t \in I :\ f(t) = u\right\}.$$

$N_u(f,I)$, (N_u for short in case of no ambiguity) is the number of crossings of the level u or the number of roots of the equation $f(t) = u$ in the interval I. In a similar way, we define the number of up-crossings or down crossings:

$$U_u(f,I) := \#\left\{t \in I :\ f(t) = u,\ f'(t) > 0\right\}$$

$$D_u(f,I) := \#\left\{t \in I :\ f(t) = u,\ f'(t) < 0\right\}.$$

Down-crossings will not be considered in the sequel since the results are strictly equivalent to those for the up-crossings.

We will say that the real-valued function f defined on the interval $I = [t_1, t_2]$ satisfies hypothesis $H_{1.u}$ if:

- f is a function of class C^1;
- $f(t_1) \neq u$, $f(t_2) \neq u$;
- $\{t : t \in I,\ f(t) = u,\ f'(t) = 0\} = \emptyset$.

Key words and phrases. Rice formula,Wiener Chaos, Gaussian processes.

Proposition 1 (Kac's counting formula)**.** *If f satisfies $H_{1.u}$, then*

$$N_u(f,I) = \lim_{\delta\to 0}\frac{1}{2\delta}\int_I \mathbb{1}_{\{|f(t)-u|<\delta\}}\ |f'(t)|\ dt. \tag{1}$$

The Kac counting formula has a weak version that will be useful

Proposition 2 (Banach formula)**.** *Assume that f is only absolutely continuous. Then for any bounded Borel-measurable function $g:\mathbb{R}\to\mathbb{R}$, one has:*

$$\int_{-\infty}^{+\infty} N_u(f,I)\ g(u)\ du = \int_I |f'(t)|g(f(t))\ dt. \tag{2}$$

This formula is a version of the change of variable formula for non one-to-one functions.

From these formula we deduce by passage to the limit the Rice formula that gives the factorial moments of the number of (up-) crossings. For simplicity we limit to the Gaussian case and to the first two moments.

Theorem 3 (Gaussian Rice formula)**.** *Let $\mathcal{X}=\{X(t):t\in I\}$, I a compact interval of the real line, be a Gaussian process having $\mathcal{C}^1$-paths.*

- *Suppose that for every point $t\in I$ the variance of $X(t)$ does not vanish. Then*

$$\mathrm{E}\big(N_u\big) = \int_I \mathrm{E}\big(|X'(t)|\Big|X(t)=u\big)p_{X(t)}(u)dt, \tag{3}$$

  and the expression above is finite.
- *Suppose that*

(4) *for every $s\neq t\in I$, the distribution of $\big(X(s),X(t)\big)$ does not degenerate .*

  Then

$$\mathrm{E}\big(N_u(N_u-1)\big) = \int_{I^2} \mathrm{E}\big(|X'(s)||X'(t)|\Big|X(s)=X(t)=u\big)p_{X(s),X(t)}(u,u)dt, \tag{5}$$

  and the expression above may be finite or infinite.

Remarks: We have the same kind of formulas for the up-crossings if we replace $|X'(t)|$ by the positive part $(X'(t))^+$.

In case of stationary processes, assuming that the process is centered with variance 1, (3) takes the simpler form

$$\mathrm{E}\big(N_u\big) = 2\mathrm{E}\big(U_u\big) = |I|\frac{\sqrt{2\lambda_2}}{\sqrt{\pi}}\phi(u),$$

where $\phi(.)$ is the standard normal density.

A very important issue is the finiteness of the second (factorial) moment. For stationary processes a necessary and sufficient condition (in addition to (4)) is given by the Geman condition: let $\Gamma(.)$ be the covariance of the process and define the function $\theta(.)$ by means of

$$\Gamma(\tau) := \mathrm{E}\big(X(t)X(t+\tau)\big) = 1-\frac{\lambda_2\tau^2}{2}+\theta(\tau).$$

The Geman condition [5]is

$$\int \frac{\theta'(\tau)}{\tau^2}d\tau \text{ converges at } \tau=0^+, \tag{6}$$

More precisely we have the bound

Proposition 4. *Let $X(t)$ be a stationary Gaussian process with $\mathrm{E}(X(t)) = 0$, $\mathrm{Var}(X(t)) = 1$. Let $\Gamma(.)$ be its covariance function, we assume that for every $\tau > 0$, $\Gamma(\tau) \neq \pm 1$ and the Geman condition. Let $U_u = U_u([0,T])$, then*

$$\begin{aligned}
&\mathrm{E}\big((U_u)(U_u - 1)\big) \\
&\quad = 2\int_0^T (T-\tau)\mathrm{E}\big(|X(0)||X'(\tau)|\Big|X(0) = X(\tau) = u\big) \times p_{X(0),X(\tau)}(u,u)d\tau \\
&\quad \leq 2\int_0^T (T-\tau)\frac{\theta'(\tau)}{\tau^2}d\tau.
\end{aligned}$$

Remark that because of the Rolle theorem: $N_u \leq 2U_u + 1$, thus the proposition above also gives a bound for the variance of the number of crossings.

3. Central limit theorem for non-linear functionals

Our next main tool will be chaos expansion and Hermite polynomials. These polynomials are orthogonal polynomials for the Gaussian measure $\phi(x)dx$ where ϕ is the standard normal density. The nth Hermite polynomial H_n can be defined by means of the identity:

$$\exp(tx - t^2/2) = \sum_{n=0}^{\infty} H_n(x)\frac{t^n}{n!}.$$

We have for example $H_0(x) = 1$, $H_1(x) = x$, $H_2(x) = x^2 - 1$.

For F in $L^2(\phi(x)\,dx)$, F can be written as

$$F(x) = \sum_{n=0}^{\infty} a_n H_n(x),$$

with

$$a_n = \frac{1}{n!}\int_{-\infty}^{\infty} F(x)H_n(x)\phi(x)dx,$$

and the norm of F in $L^2(\phi(x)dx)$ satisfies

$$||F||_2^2 = \sum_{n=0}^{\infty} a_n^2 n!.$$

The Hermite rank of F is defined as the smallest n such that $a_n \neq 0$. For our purpose, we can assume that this rank greater or equal than 1.

A useful standard tool to perform computations with Hermite polynomials and Gaussian variables is Mehler's formula which we state with an extension (see León and Ortega, [13]).

Lemma 5 (Generalized Mehler's formula)**.** *(a) Let (X,Y) be a centered Gaussian vector $\mathrm{E}(X^2) = \mathrm{E}(Y^2) = 1$ and $\rho = \mathrm{E}(XY)$. Then,*

$$\mathrm{E}(H_j(X)H_k(Y)) = \delta_{j,k}\rho^j.$$

(b) Let (X_1, X_2, X_3, X_4) be a centered Gaussian vector with variance matrix

$$\Sigma = \begin{pmatrix} 1 & 0 & \rho_{13} & \rho_{14} \\ 0 & 1 & \rho_{23} & \rho_{24} \\ \rho_{13} & \rho_{23} & 1 & 0 \\ \rho_{14} & \rho_{24} & 0 & 1 \end{pmatrix}$$

Then, if $r_1+r_2=r_3+r_4$,

$$\mathrm{E}\big(H_{r_1}(X_1)H_{r_2}(X_2)H_{r_3}(X_3)H_{r_4}(X_4)\big)=\sum_{(d_1,d_2,d_3,d_4)\in Z}\frac{r_1!r_2!r_3!r_4!}{d_1!d_2!d_3!d_4!}\rho_{13}^{d_1}\rho_{14}^{d_2}\rho_{23}^{d_3}\rho_{24}^{d_4},$$

where Z *is the set of* d_i*'s satisfying:* $d_i\geq 0$*;*

$$d_1+d_2=r_1\ ;\ d_3+d_4=r_2\ ;\ d_1+d_3=r_3\ ;\ d_2+d_4=r_4. \tag{7}$$

If $r_1+r_2\neq r_3+r_4$ *the expectation is equal to zero.*
Notice that the four equations in (7) are not independent, and that the set Z *is finite and contains, in general, more than one 4-tuple.*

Wiener chaos. Let $L^2(\Omega,\mathcal{A},\mathrm{P})$ be the space of square integrable variables generated by the process $X(t),t\in\mathbb{R}$. This Hilbert space is the orthogonal sum of the Wiener chaos of order p, $p=0,\dots,n,\dots:\mathcal{H}_p$. $\mathcal{H}_p$ is defined as the closed linear subspace of $L^2(\Omega,\mathcal{A},\mathrm{P})$ generated by the variables $H_p(X(t)),t\in\mathbb{R}$. In particular the space $\mathcal{H}_1$ is simply the Gaussian space associated to $X(t)$. A good reference on this subject is the Nualart book [16].

3.1. **A first central limit theorem.** Let $\mathcal{X}=\{X(t):t\in\mathbb{R}\}$ be a centered real-valued stationary Gaussian process. Without loss of generality, we assume that $\mathrm{Var}(X(t))=1\ \forall t\in\mathbb{R}$. We want to consider functionals having the form:

$$T_t:=1/t\int_0^t F(X(s))\,ds, \tag{8}$$

where F is some function in $L^2(\phi(x)dx)$.

Set $\mu:=\mathrm{E}(F(Z))$, Z being a standard normal variable. μ is well defined. The Maruyama Theorem implies that if the spectral measure of the process $X(t)$ has no atoms, it is ergodic and T_t converges almost surely to μ. Our aim is to compute the speed of convergence and establish for it a central limit theorem.

For the statement of the next result, which is not hard to prove, we need the following additional definition.

Definition 6. *Let* m *be some positive real, the Gaussian process* $\{X(t):t\in\mathbb{R}\}$ *is called "*m*-dependent" if* $\mathrm{Cov}(X(s),X(t))=0$ *whenever* $|t-s|>m$.

An example of such a 1-dependent process is the Slepian process which is stationary with covariance $\Gamma(t)=(1-t)^+$.

Theorem 7 (Hoeffeding and Robins [7])**.** *With the notations and hypotheses above, if the process* $X(t)$ *is* m *dependent, then*

$$\sqrt{t}\bigg(1/t\int_0^t F(X(s))-\mu\,ds\bigg)\to N(0,\sigma^2)\ \textit{in distribution as}\ t\to+\infty,$$

where

$$\sigma^2=\frac{1}{m}\mathrm{Var}\Big(\int_0^m F(X(s))ds\Big).$$

The proof is easy by the "shortening method": we cut $[0,T]$ into smaller intervals separated by gaps of size m giving the independence.

Our aim is to extend this result to processes which are not $m-$dependent. The proof we present follows Berman [4] with a generalization, due to Kratz and León [10] , to functions F in (8) having an Hermite rank not necessarily equal to 1.

For $\varepsilon > 0$, we will approximate the given process $X(t)$ by a new one $X_\varepsilon(t)$ which is $1/\varepsilon$-dependent and estimate the error.

As an additional hypothesis, we will assume that the process $X(t)$ has a spectral density $f(\lambda)$. It has the following spectral representation:

$$X(t) = \sqrt{2}\int_0^\infty \big[\cos(t\lambda)\sqrt{f(\lambda)}dW_1(\lambda) + \sin(t\lambda)\sqrt{f(\lambda)}dW_2(\lambda)\big], \tag{9}$$

where W_1 and W_2 are two independent Wiener processes (Brownian motions). Indeed, using isometry properties of the stochastic integral, it is easy to see that the process given by (9) is centered, Gaussian and with the good covariance:

$$\begin{aligned}\Gamma(t) &= \mathrm{E}(X(s)X(s+t)) \\ &= 2\int_0^\infty \cos(\lambda s)\cos(\lambda(t+s))f(\lambda)d\lambda + 2\int_0^\infty \sin(\lambda s)\sin(\lambda(t+s))f(\lambda)d\lambda \\ &= 2\int_0^\infty \cos(\lambda t)f(\lambda)d\lambda.\end{aligned}$$

Define now the function $\psi(.)$ as the convolution $\mathbb{1}_{[-\frac{1}{2},\frac{1}{2}]} * \mathbb{1}_{[-\frac{1}{2},\frac{1}{2}]}$. This function is even, non negative, $\psi(0) = 1$, has support included in $[-1,1]$ and a non-negative Fourier transform. Set $\psi_\varepsilon(.) := \frac{1}{\varepsilon}\psi(\varepsilon.)$ and let $\widehat{\psi_\varepsilon}$ be its Fourier transform. Define

$$X^\varepsilon(t) := \sqrt{2}\int_0^\infty \big[\cos(t\lambda)\sqrt{f * \widehat{\psi_\varepsilon}(\lambda)}dW_1(\lambda) + \sin(t\lambda)\sqrt{f * \widehat{\psi_\varepsilon}(\lambda)}dW_2(\lambda)\big], \tag{10}$$

where the convolution must be understood after prolonging f as an even function on $\mathbb{R}$. The covariance function Γ_ε of $X^\varepsilon(t)$ satisfies $\Gamma_\varepsilon(t) = \Gamma(t)\psi(\varepsilon t)$. This implies that the process $X^\varepsilon(t)$ is $\frac{1}{\varepsilon}$-dependent. We have the following proposition:

Proposition 8. *Let $\mathcal{X}$ be a centered stationary Gaussian process with spectral density $f(\lambda)$ and covariance function Γ with $\Gamma^\ell \in L^1(\mathbb{R})$, ℓ positive integer. Let $X_\varepsilon(t)$ be defined by (10). Then*

$$\lim_{\varepsilon\to 0}\lim_{t\to\infty} \mathrm{E}\left[\frac{1}{\sqrt{t}}\int_0^t \left(H_\ell(X(s)) - H_\ell(X^\varepsilon(s))\right)ds\right]^2 = 0. \tag{11}$$

Theorem 9. *Let $\mathcal{X}$ be a Gaussian process satisfying the hypotheses of Proposition 8 and F a function in $L^2(\phi(x)dx)$ with Hermite rank $\ell \geq 1$. Then, as $t \to +\infty$,*

$$\sqrt{t}T_t = \frac{1}{\sqrt{t}}\int_0^t F(X(s))ds \to N(0,\sigma^2(F)) \text{ in distribution}$$

where

$$\sigma^2(F) := 2\sum_{k=\ell}^\infty a_k^2 k! \int_0^\infty \Gamma^k(s)ds.$$

Proof:

Define $F_M := \sum_{n=\ell}^M a_n H_n(x)$ and $T_t^M := \frac{1}{t}\int_0^t F_M(X(s))ds$. Let $M = M(\delta) > \ell$ such that

$$2\sum_{k=M+1}^\infty a_k^2 < \delta.$$

Using Mehler's formula, we get

$$t\ \mathrm{Var}(T_t - T_t^M) = 2\sum_{k=M}^{\infty} c_k^2 k! \int_0^t (1-\frac{s}{t})\Gamma^k(s)ds \leq 2\sum_{k=M}^{\infty} c_k^2 k! \int_0^{\infty} |\Gamma|^k(s)ds$$
$$< \delta \int_0^{\infty} |\Gamma|^{\ell}(s)ds.$$

Since δ is arbitrary, we only need to prove the asymptotic normality for T_t^M. Let us introduce

$$T_t^{M,\varepsilon} = \frac{1}{t}\int_0^t F_M(X^{\varepsilon}(s))ds,$$

where $X_\varepsilon(t)$ has been defined in (10). By Proposition 8 recalling that for $k \geq l$, Γ^k is in $L^1(\mathbb{R})$ since Γ^ℓ is, we obtain:

$$\lim_{\varepsilon\to 0}\lim_{t\to\infty} t\ \mathrm{Var}(T_t^M - T_t^{M,\varepsilon}) = 0.$$

Now Theorem 7 for m- dependent sequences implies that $\sqrt{t}\ T_t^{M,\varepsilon}$ is asymptotically normal. Notice that

$$\sigma_{M,\varepsilon} := \lim_{t\to\infty} t\,\mathrm{Var}(T_t^{M,\varepsilon}) = 2\sum_{k=0}^{M} a_k^2 k! \int_0^{\frac{1}{\varepsilon}} \Gamma_{\varepsilon}^k(s)ds$$

and that $\sigma_{M,\varepsilon} \to \sigma^2(F)$ when $\varepsilon \to 0$ and $M \to \infty$, giving the result. ∎

3.2. **Hermite expansion for crossings of regular processes.** Our aim is to extend the result above to crossings. Let $X(t)$ be a centered stationary Gaussian process. With no loss of generality for our purposes, we assume that $\Gamma(0) = -\Gamma''(0) = 1$ and $\Gamma(t) \neq \pm 1$ for $t \neq 0$. We also assume Geman's Condition (6).

$$\Gamma(t) = 1 - t^2/2 + \theta(t) \quad \text{with } \int \frac{\theta'(t)}{t^2}dt \text{ converges at } 0^+.$$

We define the following expansions

$$x^+ = \sum_{k=0}^{\infty} a_k H_k(x), \quad x^- = \sum_{k=0}^{\infty} b_k H_k(x), \quad |x| = \sum_{k=0}^{\infty} c_k H_k(x). \tag{12}$$

We have $a_1 = 1/2,\ b_1 = -1/2,\ c_1 = 0$ and using integration by parts for $k > 2$:

$$a_k = \frac{1}{k!}\int_0^{+\infty} xH_k(x)\varphi(x)dx = \frac{1}{k!\sqrt{2\pi}}H_{k-2}(0).$$

The classical properties of Hermite polynomials easily imply that for positive k:

$$a_{2k+1} = b_{2k+1} = c_{2k+1} = 0,$$
$$a_{2k} = b_{2k} = \frac{(-1)^{k+1}}{\sqrt{2\pi}2^k k!(2k-1)},$$
$$c_{2k} = 2a_{2k}.$$

We have the following Hermite expansion for the number of up-crossings:

Theorem 10. *Under the conditions above,*

$$U_u := U_u(X,[0,T]) = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} d_j(u)a_k \int_0^T H_j(X(s))H_k(X'(s))ds \text{ a.s.}$$

where $d_j(u) = \frac{1}{j!}\phi(u)H_j(u)$ *and* a_k *is defined by (12). We have similar results, replacing* a_k *by* b_k *or* c_k*, for the number* $D_u([0,T])$ *of down-crossings and for the total number of crossings* $N_u([0,T])$*.*

Proof : Let $g(.) \in L^2(\phi(x)dx)$ and define the functional

$$T_g^+(t) = \int_0^t g(X(s))X'^+(s)ds.$$

The convergence of the Hermite expansion implies that a.s.

$$T_g^+(t) = \sum_{j=0}^{\infty}\sum_{k=0}^{\infty} g_j\, a_k \int_0^t H_j(X(s))H_k(X'(s))ds, \tag{13}$$

where the g_j's are the coefficients of the Hermite expansion of g. Using that for each s, $X(s)$ and $X'(s)$ are independent, we get:

$$\mathrm{E}\Big[\int_0^t \Big[g(X(s))(X'(s))^+ - \sum_{j,k\geq 0: k+j\leq Q} g_j a_k H_j(X(s))H_k(X'(s))\Big]ds\Big]^2 \leq (const)t^2 \sum_{j,k\geq 0: k+j\geq Q} j!g_j^2 k!a_k^2. \tag{14}$$

On the other hand, using the Geman condition

$$\nu_2(u,T) := \mathrm{E}\big(U_u([0,T])(U_u([0,T])-1)\big) < +\infty.$$

For every T, $\nu_2(u,T)$ is a bounded continuous function of u and the same holds true for $\mathrm{E}(U_u^2)$. Let us now define

$$U_u^\delta := \frac{1}{2\delta}\int_0^T \mathbb{1}_{|X(t)-u|\leq\delta} X'^+(t)dt.$$

In our case, hypotheses of Proposition 1 are a.s. satisfied. The result can be easily extended to up-crossings, showing that

$$U_u^\delta \to U_u \text{ a.s. as } \delta \to 0.$$

By Fatou's Lemma

$$\mathrm{E}\big((U_u)^2\big) \leq \liminf_{\delta\to 0} \mathrm{E}\big((U_u^\delta)^2\big).$$

To obtain an inequality in the opposite sense, we use the Banach formula (Proposition 2). To do that, notice that this formula remains valid if one replaces in the left-hand side the total number of crossings by the up-crossings and in the right-hand side $|f'(t)|$ by $f'^+(t)$. So, on applying it to the random path $X(.)$, we see that:

$$U_u^\delta = \frac{1}{2\delta}\int_{u-\delta}^{u+\delta} U_x dx.$$

Using Jensen's inequality,

$$\limsup_{\delta\to 0} \mathrm{E}\big((U_u^\delta)^2\big) \leq \limsup_{\delta\to 0} \frac{1}{2\delta}\int_{u-\delta}^{u+\delta} \mathrm{E}\big((U_x)^2\big)dx = \mathrm{E}\big((U_u)^2\big)$$

So, $\mathrm{E}\big((U_u^\delta)^2\big) \to \mathrm{E}\big((U_u)^2\big)$ and since the random variables involved are non-negative, a standard argument of passage to the limit based upon Fatou's Lemma shows that $U_u^\delta \to U_u$ in L^2.

We now apply (13) to U_u^δ.

$$U_u^\delta = \sum_{j,k=0}^{\infty} d_j^\delta(u) a_k \zeta_{jk}, \tag{15}$$

where $d_j^\delta(u)$ are the Hermite coefficients of the function $x \rightsquigarrow \frac{1}{\delta}\mathbb{1}_{\|x-u\|\leq\delta}$ and

$$\zeta_{jk} = \int_0^T H_j(X(s)) H_k(X'(s)) ds.$$

Notice that

$$d_j^\delta(u) \to \frac{1}{j!}\phi(u) H_j(u) = d_j(u). \tag{16}$$

This implies that:

$$U_u = \sum_{q=0}^{\infty} \sum_{j+k=q} d_j(u) a_k \zeta_{jk}. \tag{17}$$

∎

Theorem 11. *Let $\{X(t) : t \in \mathbb{R}\}$ be a centered stationary Gaussian process verifying the conditions at the beginning of this subsection. Furthermore, let us assume that:*

$$\int_0^{+\infty} |\Gamma(t)| dt, \int_0^{+\infty} |\Gamma'(t)| dt, \int_0^{+\infty} |\Gamma''(t)| dt < \infty. \tag{18}$$

Let $\{g_k\}_{k=0,1,2,\ldots}$ a sequence of coefficients which satisfies $\sum_0^{+\infty} g_k^2 k! < \infty$. Put:

$$F_t := \frac{1}{\sqrt{t}} \sum_{k,j\geq 0} g_j a_k \int_0^t H_j(X(s)) H_k(X'(s)) ds$$

where a_k has been defined in (12). Then

$$F_t - \mathrm{E}(F_t) \to N(0, \sigma^2) \text{ in distribution as } t \to +\infty$$

where

$$0 < \sigma^2 = \sum_{q=1}^{\infty} \sigma^2(q) < \infty,$$

and

$$\sigma^2(q) := 2 \sum_{k=0}^{q} \sum_{k'=0}^{q} a_k a_{k'} g_{q-k} g_{q-k'} \times \int_0^{+\infty} \mathrm{E}\big[H_{q-k}(X(0)) H_k(X'(0)) H_{q-k'}(X(s)) H_{k'}(X'(s))\big] ds.$$

The integrand in the right-hand side of this formula can be computed using Lemma 5. Similar results exist, mutatis mutandis, for the sequences $\{b_k\}$ and $\{c_k\}$.

A consequence is

Corollary 12. *If the process $X(t)$ satisfies the conditions of Theorem 11 then, as $T \to +\infty$*

$$\frac{1}{\sqrt{T}}\Big(U_u\big([0,T]\big) - T\frac{e^{-u^2/2}}{2\pi}\Big) \to N(0,\sigma_1^2) \text{ in distribution}$$
$$\frac{1}{\sqrt{T}}\Big(N_u\big([0,T]\big) - T\frac{e^{-u^2/2}}{\pi}\Big) \to N(0,\sigma_2^2) \text{ in distribution,}$$

where σ_1^2 and σ_2^2 are finite and positive.

Remark The result of Theorem 11 is in fact true under weaker hypotheses namely

$$\int_0^{+\infty} |\Gamma(t)|dt < \infty\,, \qquad \int_0^{+\infty} |\Gamma''^2(t)|dt < \infty\,,$$

see Theorem 1 of Kratz and León [11] or Kratz [9].See also Azaïs and Leon [1] for another generalization where the integral $\int_{\mathbb{R}} \Gamma(t)dt$ is defined only in a generalized sense. Our stronger hypotheses make it possible to make a shorter proof.

Proof of the theorem:

Since Γ is integrable, the process $\mathcal{X}$ admits a spectral density. The hypotheses and the Riemann-Lebesgue lemma imply that:

$$\Gamma^{(i)}(t) \to 0 \quad i = 0,1,2 \quad \text{as } t \to +\infty.$$

Hence, we can choose T_0 so that for $t \geq T_0$

$$\overline{\Gamma}(t) := \sup\{|\Gamma(t)|, |\Gamma'(t)|, |\Gamma''(t)|\} \leq 1/4. \tag{19}$$

Step 1. In this step we prove that one can choose Q large enough (and that doesn't depend on t) so that F_t can be replaced with an arbitrarily small error (in the L^2 sense) by its components in the first Q chaos

$$F_t^Q := \frac{1}{\sqrt{t}}\sum_{q=0}^{Q} G_t^q \quad \text{with } G_t^q := \sum_{k=0}^{q} g_{q-k}a_k \int_0^t H_{q-k}(X(s))H_k(X'(s))ds.$$

Let us consider

$$\frac{1}{t}\mathrm{E}\big((G_t^q)^2\big) = 1/t \sum_{k,k'=0}^{q} g_{q-k}a_k g_{q-k'}a_{k'} \int_0^t dt_1 \cdot \int_0^t \mathrm{E}\big(H_{q-k}(X(t_1))H_k(X'(t_1))H_{q-k'}(X(t_2))H_{k'}(X'(t_2))dt_2. \tag{20}$$

To give an upper-bound for this quantity we split it into two parts.

The part corresponding to $|t_1 - t_2| \geq T_0$ is bounded, using Lemma 5, by

$$
\begin{aligned}
(21)\quad & (const) \sum_{k,k'=0}^{q} |g_{q-k}||a_k||g_{q-k'}||a_{k'}| \\
& \times \int_{T_0}^{t} \sum_{(d_1,d_2,d_3,d_4)\in Z} \frac{k!(q-k)!k'!(q-k')!}{d_1!d_2!d_3!d_4!} |\Gamma(s)|^{d_1} |\Gamma'(s)|^{d_2+d_3} |\Gamma''(s)|^{d_4} ds \\
& \leq (const) \sum_{k,k'=0}^{q} |g_{q-k}||a_k||g_{q-k'}||a_{k'}| \\
& \times \int_{T_0}^{t} \sum_{(d_1,d_2,d_3,d_4)\in Z} \frac{k!(q-k)!k'!(q-k')!}{d_1!d_2!d_3!d_4!} (\frac{1}{4})^{(q-1)} \overline{\Gamma}(s) ds,
\end{aligned}
$$

where Z is as in Lemma 5, setting $r_1 = q-k, r_2 = k, r_3 = q-k', r_4 = k'$.

Remarking that $\sup_d \frac{1}{d!(k-d)!} \leq \frac{2^k}{k!}$ it follows that $\frac{k!(q-k)!k'!(q-k')!}{d_1!d_2!d_3!d_4!}$ in (21) is bounded above by $2^q(k')!(q-k')!$ or $2^q(k)!(q-k)!$ depending on the way we group terms. As a consequence it is also bounded above by $2^q\sqrt{(k')!(q-k')!(k)!(q-k)!}$ and the right-hand side of (21) is bounded above by

(22)

$$
\begin{aligned}
& (const) \sum_{k,k'=0}^{q} |g_{q-k}||a_k||g_{q-k'}||a_{k'}| q 2^{-q} \sqrt{(k')!(q-k')!(k)!(q-k)!} \int_0^{+\infty} \overline{\Gamma}(t) dt \\
& \qquad \leq (const) \sum_{k,k'=0}^{q} |g_{q-k}||a_k||g_{q-k'}||a_{k'}| \sqrt{(k')!(q-k')!(k)!(q-k)!}
\end{aligned}
$$

where we have used that the number of terms in Z is bounded by q.

On the other hand, the integration region in (20) corresponding to $|t_1 - t_2| \leq T_0$ can be covered by at most $[t/T_0]$ squares of size $2T_0$. Using Jensen's inequality as we did for the proof of (14) we obtain:

$$
(23)\qquad \mathrm{E}\Big(\big(G^q_{2T_0}\big)^2\Big) \leq (const) T_0^2 \sum_{k=0}^{q} (q-k)!k! g^2_{q-k} a_k^2.
$$

Finally,

$$
\frac{1}{t}\mathrm{E}\Big(\big(G^q_t\big)^2\Big) \leq (const) \sum_{k=0}^{q} (q-k)!k! g^2_{q-k} a_k^2,
$$

which is the general term of a convergent series. This proves also that σ^2 is finite.

Step 2. Let us prove that $\sigma^2 > 0$. It is sufficient to prove that $\sigma^2(2) > 0$. Recall that $a_1 = 0$ so that

$$\begin{aligned}(24)\quad \sigma^2(2) = a_0^2 g_2^2 \int_0^{+\infty} \mathrm{E}\big(H_2(X(0))H_2(X(s))ds \\ + a_2^2 g_0^2 \int_0^{+\infty} \mathrm{E}\big(H_2(X'(0))H_2(X'(s))ds \\ + 2a_0 g_2 a_2 g_0 \int_0^{+\infty} \mathrm{E}\big(H_2(X(0))H_2(X'(s))ds.\end{aligned}$$

Using the Mehler formula

$$\begin{aligned}(25)\qquad \sigma^2(2) &= 2a_0^2 g_2^2 \int_0^{+\infty} \Gamma^2(s)ds \\ &\quad + 2a_2^2 g_0^2 \int_0^{+\infty} (\Gamma''(s))^2 ds + 4a_0 g_2 a_2 g_0 \int_0^{+\infty} (\Gamma'(s))^2 ds \\ &= \int_{-\infty}^{+\infty} \big(\lambda^4 a_0^2 g_2^2 + \lambda^2 2a_0 g_2 a_2 g_0 + a_0^2 g^2\big) f^2(\lambda)d\lambda \\ &= \int_{-\infty}^{+\infty} \big(\lambda^2 a_2 g_0 + a_0 g_2\big)^2 f^2(\lambda)d\lambda > 0.\end{aligned}$$

Step 3. We define $\psi(.) = K\big(\mathbb{1}_{[1/4,1/4]}\big)^{*4}$, where the constant K is chosen such that $\psi(0) = 1$. Then we define $X^\varepsilon(t)$ using (10). The new definition of $\psi(.)$ ensures now that $X^\varepsilon(t)$ is differentiable. Define

$$F_t^{Q,\varepsilon} := \frac{1}{\sqrt{t}} \sum_{q=0}^{Q} G_t^{q,\varepsilon},$$

with

$$G_t^{q,\varepsilon} = \sum_{k=0}^{q} g_{q-k} a_k \int_0^t H_{q-k}(X^\varepsilon(s)) H_k\big((X^\varepsilon)'(s)\big)ds.$$

In this step, we prove that F_t^Q can be replaced, with an arbitrarily small error if ε is small enough, by $F_t^{Q,\varepsilon}$. Since the expression of F_t^Q involves only a finite number of terms having the form:

$$K_{q-k,k}^0 := \frac{1}{\sqrt{t}} \int_0^t H_{q-k}(X(s)) H_k\big(X'(s)\big)ds$$

if ε is small enough, one can replace with an arbitrarily small error by

$$K_{q-k,k}^\varepsilon := \frac{1}{\sqrt{t}} \int_0^t H_{q-k}(X^\varepsilon(s)) H_k\big((X^\varepsilon)'(s)\big)ds.$$

For that purpose we study

$$\begin{aligned}
&\mathrm{E}(K^0_{q-k,k} - K^\varepsilon_{q-k,k})^2 \\
&= 2\int_0^t \frac{t-s}{t}\mathrm{E}\Big[H_{q-k}(X(0))H_k\big(X'(0)\big)H_{q-k}(X(s))H_k\big(X'(s)\big)\Big] \\
&\quad + \mathrm{E}\Big[H_{q-k}(X^\varepsilon(0))H_k\big((X^\varepsilon)'(0)\big)H_{q-k}(X^\varepsilon(s))H_k\big((X^\varepsilon)'(s)\big)\Big] \\
&\quad - 2\mathrm{E}\Big[H_{q-k}(X(0))H_k\big(X'(0)\big)H_{q-k}(X^\varepsilon(s))H_k\big((X^\varepsilon)'(s)\big)\Big]ds.
\end{aligned}$$

Consider the computation of terms of the kind

$$\int_0^t \frac{t-s}{t}\mathrm{E}\Big[H_{q-k}(Y_1(0))H_k\big(Y_1'(0)\big)H_{q-k}(Y_2(s))H_k\big(Y_2'(s)\big)\Big]ds \tag{26}$$

where the processes $Y_1(t)$ and $Y_2(t)$ are chosen among $\{X(t), X^\varepsilon(t)\}$. It suffices to prove that all these terms have the same limit, as $t \to +\infty$ and then $\varepsilon \to 0$ whatever the choice is.

Applying Lemma 5, the expectation in(26) is equal to

$$\int_0^t \frac{t-s}{t}\sum_{d_1,\dots,d_4\in Z}\frac{(q-k)!^2k!^2}{d_1!d_2!d_3!d_4!}(\rho(s))^{d_1}(\rho'(s))^{d_2}(-\rho'(s))^{d_3}(-\rho''(s))^{d_4}ds,$$

where $\rho(.)$ is the covariance function between the processes Y_1 and Y_2 and Z is defined as in Lemma 5. Again, since the number of terms in Z is finite, it suffices to prove that

$$\lim_{\varepsilon\to 0}\lim_{t\to\infty}\int_0^t \frac{t-s}{t}(\rho(s))^{d_1}(\rho'(s))^{d_2+d_3}(\rho''(s))^{d_4}ds,$$

where $(d_1,\dots,d_4)$ is chosen in Z, does not depend on the way to choose Y_1 and Y_2. ρ is the Fourier transform of (say) $g(\lambda)$ which is taken among $f(\lambda)$; $f * \widehat{\psi}_\varepsilon(\lambda)$ or $\sqrt{f(\lambda)}\sqrt{f * \widehat{\psi}_\varepsilon(\lambda)}$. Define $\overline{g}(\lambda) = i\lambda g(\lambda)$ and $\overline{\overline{g}}(\lambda) = -\lambda^2 g(\lambda)$. Then $(\rho(s))^{d_1}(\rho'(s))^{d_2+d_3}(\rho''(s))^{d_4}$ is the Fourier transform of the function

$$h(\lambda) = g^{*d_1}(\lambda) * \overline{g}^{*(d_2+d_3)}(\lambda) * \overline{\overline{g}}^{*d_4}(\lambda).$$

The continuity and boundedness of f imply that all the functions above are bounded and continuous. The Fubini theorem shows that

$$\int_0^t \frac{t-s}{t}\rho(s)^{d_1}\rho'(s)^{d_2+d_3}(\rho''(s))^{d_4}ds = \int_{-\infty}^{+\infty}\frac{1-\cos\lambda}{\lambda^2}h(\frac{\lambda}{t}),$$

As $t \to +\infty$, the right-hand side converges, using dominated convergence, to

$$\int_{-\infty}^{+\infty}\frac{1-\cos\lambda}{\lambda^2}h(0)d\lambda.$$

The continuity of f now gives the result, as in Proposition 8.

∎

Proof of Corollary 12:

Some attention must be payed to the fact that the coefficients

$$d_j(u) = \frac{1}{j!}\phi(u)H_j(u)$$

do not satisfy $\sum_{j=0}^{\infty} j! d_j^2(u) < \infty$. They only satisfy the relation

$$j! d_j^2(u) \text{ is bounded} \tag{27}$$

First, considering the bound given by the right-hand side of (22), we can improve it by reintroducing the factor $q2^{-q}$ that had been bound by 1. We get that in its new expression this right-hand side is bounded by

$$\begin{aligned}
&(const) q 2^{-q} \sum_{k,k'=0}^{q} |d_{q-k}(u)||a_k||d_{q-k'}(u')||a_{k'}| \sqrt{(k')!(q-k')!(k)!(q-k)!} \\
&\leq (const) q^2 2^{-q} \sum_{k=0}^{q} \big(d_{q-k}(u)\big)^2 a_k^2 (k)!(q-k)! \\
&\leq (const) q^2 2^{-q} \sum_{k=0}^{q} a_k^2 k! \leq (const) q^2 2^{-q}.
\end{aligned}$$

Second we have to replace the bound (23). Since the series in (17) is convergent $\mathrm{E}\Big(\big(G_{2T_0}^q\big)^2\Big)$ is the term of a convergent series and this in enough to conclude. ∎

.

4. Applications and extensions

In an unpublished manuscript, Stephane Mourareau has extended the result of Corollary 12 to the case of moving level u_T.

Theorem 13. *Let u_T be a moving level that tends to infinity with T. Suppose that*

- *The process $X(t)$ is m-dependent*
- $$\mathrm{E}(U_t) \to \infty$$

Then

$$\frac{1}{\sqrt{T\phi(u_T)}} \left(U_{u_T}(T) - \sqrt{\frac{\lambda_2}{2\pi}} T \phi(u_T) \right) \Rightarrow \mathcal{N}\big(0, \frac{\lambda_2}{2\pi}\big)$$

The variance is now simple and explicit and it corresponds to the Poissonian limit (the variance is equal to the expectation) known as the Vlokonskii- Rozanov theorem.

Theorem 14. *Assume the conditions of Theorem 11 except* (18) *which is now replaced by the very weak Berman's condition*

$$\Gamma(\tau) \log(\tau) \to 0 \text{ as } \tau \to \infty.$$

Let u_T be a movinf level such that $\mathrm{E}\big(U_{u_t}\big) = \lambda$ where λ is some constant. Then U_{u_t} converges to a Poisson distribution with parameter λ.

This is a simplified version, the full one establishes a functional convergence of the point process itself.

4.1. **Random trigonometric polynomials.** Let $X(t)$ be the stochastic process with covariance

$$\Gamma(t) = \frac{\sin(t)}{t}$$

Since the covariance is not summable in the Lebesgue sense, it does not satisfy strictly the conditions of Corollary 12. But in fact the integral

$$\int_{\mathbb{R}} \Gamma(t)dt$$

can be defined by passage to the limit and it can be checked that the result holds true.

Let $X_N(t)$ the sequences of random trigonometric polynomials given by

$$X_N(t) = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} (a_n \sin nt + b_n \cos nt),$$

where the a_n, b_n's are independent standard normal.

it is easy to check that for each N, $X_N(t)$ is a stationary Gaussian process with covariance:

$$\Gamma_{X_N}(\tau) := \mathbb{E}[X_N(0)X_N(\tau)] = \frac{1}{N} \sum_{n=1}^{N} \cos n\tau = \frac{1}{N} \cos(\frac{(N+1)\tau}{2}) \frac{\sin(\frac{N\tau}{2})}{\sin \frac{\tau}{2}}. \tag{28}$$

We define the process

$$Y_N(t) = X_N(t/N),$$

with covariance

$$\Gamma_{Y_N}(\tau) = \Gamma_{X_N}(\tau/N).$$

The convergence of the Rieman sum to the intergral implies that

$$\Gamma_{Y_N}(\tau) \to \Gamma(\tau) := \sin(\tau)/\tau \text{ as } N \to +\infty$$

And the have the same type of control for the derivatives. The main argument of Azaïs and León [1] is a construction of the process $X_N(t)$ as well as the limit $X(t)$ in the same probability space to get that the Central limit theorem for the crossings of $X(t)$ pass to those of $X_N(t)$. It gives a generalization of a paper by Grandville and Wigman [8]

Theorem 15. *With the notation above*

$$(1)\ \frac{1}{\sqrt{N\pi}} \big(N^{Y_N}_{[0,N\pi]}(u) - \mathrm{E}(N^{Y_N}_{[0,N\pi]}(u)) \big) \Rightarrow N(0, \frac{1}{3}u^2\phi^2(u) + \sum_{q=2}^{\infty} \sigma_q^2(u)),$$

$$(2)\ \frac{1}{\sqrt{2N\pi}} \big(N^{Y_N}_{[0,2N\pi]}(u) - \mathrm{E}(N^{Y_N}_{[0,2N\pi]}(u)) \big) \Rightarrow N(0, \frac{2}{3}u^2\phi^2(u) + \sum_{q=2}^{\infty} \sigma_q^2(u)),$$

where $\Rightarrow$ is the convergence in distribution as $N \to \infty$ and $\sigma_q^2(u)$ is the variance of the part in the qth chaos.

4.2. **Specular points.** A different case of central limit theorem is given by the number of specular points. These are point of the surface of the sea that appear in bright on a photo. We use a cylinder model: time is fixed; the variation of the elevation of the sea $W(x)$ as a function of the space variable x is modeled by a smooth stationary Gaussian process; as a function of the second space variable y the elevation of the sea is supposed to be constant.

Suppose that a source of light is located at $(0, h_1)$ and that an observer is located at $(0, h_2)$ where h_1 and h_2 are big with respect to $W(x)$ and x. Only the variable x has to be taken into account and the following approximation, was introduced long ago by Longuett-Higgins [14]: the point x is a specular point if

$$W'(x) \simeq kx, \text{ with } k := \frac{1}{2}\Big(\frac{1}{h_1} + \frac{1}{h_2}\Big).$$

This is a non stationary case: there are more specular points underneath the observer. In particular if $SP(I)$ s the number of specular points contained in the interval I,

$$\mathrm{E}(SP(I)) = \int_I G(-k, \sqrt{\lambda_4})\frac{1}{\sqrt{\lambda_2}}\varphi(\frac{kx}{\sqrt{\lambda_2}})dx, \tag{29}$$

where λ_2, λ_4 are the spectral moments of order 2 and 4 respectively that are assumed to be finite; $G(\mu, \sigma) := \mathrm{E}(|Z|)$, Z with distribution $N(\mu, \sigma^2)$.

An easy consequence of that formula is that

$$\mathrm{E}(SP) := \mathrm{E}(SP(\mathbb{R})) = \frac{G(k, \sqrt{\lambda 4})}{k} \simeq \sqrt{\frac{2\lambda_4}{\pi}}\frac{1}{k},$$

as k tends to 0.

As a consequence the number of specular point is almost surely finite and the Central Limit Theorem may only happen in the case where $k \to 0$,i.e. when the locations of the observer an the source of light are infinitely far from the surface of the sea.

The central limit theorem is now established using Lyapounov type conditions for Lindeberg type Central Limit Theorem for triangular arrays.

Theorem 16. *Under some conditions (see Azaïs León and Wschebor* [2] *for details), as* $k \to 0$,

$$\frac{S - \sqrt{\frac{2\lambda_4}{\pi}}\frac{1}{k}}{\sqrt{\theta/k}} \Rightarrow N(0,1), \text{ in distribution,}$$

where θ *is some (complicated) constant.*

References

[1] J-M. Azaïs and J. León. CLT for Crossings of random trigonometric Polynomials. Electronic Journal of Probability, 18 (2013), paper 68.

[2] J-M. Azaïs, J. León and M. Wschebor. Rice formulae and Gaussian waves Bernoulli Volume 17, Number 1 (2011), 170-193.

[3] J-M. Azaïs and M. Wschebor. Level sets and Extrema of Random Processes and Fields. Wiley (2009).

[4] S.M. Berman. Ocupation times for stationary Gaussian process *J. Applied Probability.* 7, 721-733 (1970).

[5] D. Geman. (1972). On the variance of the number of zeros of stationary Gaussian process, Ann. Math. Statist., Vol 43, N 3, 977-982.

[6] J. Cuzick. A Central Limit Theorem for the Number of Zeros of a Stationary Gaussian Process, *The Annals of Probability.* Volume 4, Number 4 (1976), 547-556.
[7] W. Hoeffding and H. Robbins. (1948).The Central Limit Theorem for dependent random variables, *Duke Math- J.* 15, 773-730 .
[8] A. Granville and I. Wigman. The distribution of the zeros of Random Trigonometric Polynomials. *American Journal of Mathematics.* 133, 295-357 (2011).
[9] M.F. Kratz. Level crossings and other level functionals of stationary Gaussian processes. Probability Surveys Vol. 3, 230-288 (2006)
[10] M. Kratz and J.R. León. Hermite polynominal expansion for non-smooth functionals of stationary Gaussian processes: Crossings and extremes. *Stoch. Proc. Applic.* 66, 237-252, (1997).
[11] M. Kratz and J.R. León. Central Limit Theorems for Level Functionals of Stationary Gaussian Processes and Fields. *Journal of Theoretical Probability.* Vol. 14, No. 3, (2001).
[12] J. León. A note on Breuer-Major CLT for non-linear functionals of continuous time stationary Gaussian processes. Preprint (2006)
[13] J. León and J. Ortega. Weak convergence of different types of variation for biparametric Gaussian processes, Colloquia Math. Soc. J. Bolyai, n 57, 1989, Limit theorems in Proba. and Stat. Pecs. (1989)
[14] M.S. Longuett-Higgins. Reflection and refraction at a random surface. I, II, III, Journal of the Optical Society of America, vol. 50, No.9, 838-856 (1960).
[15] T.L. Malevich. Asymptotic normality of the number of crossings of the level zero by a Gaussian process. *Theor. Probability Appli.* 14, 287-295 (1969).
[16] D. Nualart. The Malliavin Calculus and Related Topics. Springer-Verlag, (2006).

Institut de Mathématiques de Toulouse (CNRS UMR 5219)
Université Paul Sabatier, 118 route de Narbonne,
31062 Toulouse, France
E-mail address: jean-marc.azais@math.univ-toulouse.fr

Publicaciones Matemáticas del Uruguay
Volumen 15, Junio 2016, Páginas 109–122
S 0797-1443

K-TEORÍA ALGEBRAICA Y CONJETURAS DE ISOMORFISMO

EUGENIA ELLIS

1. Introducción

La K-teoría algebraica es una rama del álgebra que le asocia a un anillo R una sucesión de grupos abelianos $K_i(R)$, $i \in \mathbb{Z}$. Esta teoría juega un rol importante en varias áreas, especialmente en teoría de números, topología algebraica y geometría algebraica. En este curso nos detendremos a estudiar los grupos $K_0(R)$ y $K_1(R)$ y su conexión con algunos problemas clásicos de la topología algebraica. Nos preguntaremos cuando un CW-complejo X finitamente dominado es homotópicamente equivalente a un CW-complejo finito. Responderemos esta pregunta calculando $K_0(\mathbb{Z}G)$, siendo $G = \pi_1(X)$. También nos preguntaremos cuando un h-cobordismo W es trivial y resolveremos el problema calculando el grupo de Whitehead del grupo fundamental de W. La conjetura de Farrell-Jones tiene como objetivo facilitar el cálculo de los grupos $K_i(RG)$ en donde R es un anillo y G es un grupo. Usando este resultado se pueden probar otras conjeturas más clásicas como la conjetura de Poincaré, la conjetura de Borel y la conjetura de Novikov. Si bien esta conjetura ha sido recientemente probada para una larga lista de grupos (grupos hiperbólicos, grupos CAT(0), $SL_n(R)$, $GL_n(R)$, etc [3]), aún esta abierta para otra lista de grupos (grupos amenables, grupos de automorfismos de una superficie $MCG(S)$, $Out(F_n)$). Tampoco se tiene un contraejemplo o un posible candidato.

Estas notas fueron realizadas para complementar el curso "Introducción a la K-teoría y conjeturas de isomorfismo" que se dictará en el Congreso Uruguayo de Matemática y cuyo objetivo es dar un pantallazo de estos temas. Para una introducción completa a la K-teoría algebraica ver [13] y [19]. Para una introducción completa a las conjeturas de isomorfismo ver [2] y [8]. Para los concéptos básicos de topología algebraica ver [7] y [16].

1.1. Notaciones. Denotaremos por R a un anillo con unidad no necesariamente conmutativo. Los espacios son espacios topológicos de Hausdorff y localmente compactos. Un morfismo entre espacios topológicos siempre será una función continua.

2. El grupo $K_0(R)$ y la obstrucción de finitud de Wall

La K-teoría surge de la necesidad de poner en términos algebraicos ciertos invariantes y obstrucciones que aparecen en la topología. En esta sección presentamos el problema geométrico que lleva a definir la obstrucción de Wall. Definimos el grupo $K_0(R)$, algunas propiedades y su relación con el problema de ver cuando un CW-complejo finitamente dominado es homotópicamente equivalente a un CW-complejo finito.

2.1. CW-complejos. La clasificación de espacios con igual forma puede realizarse de varias maneras. Si X e Y son variedades diferenciables, decimos que son difeomorfas si existe un difeomorfismo $f : X \to Y$ (función diferenciable, invertible y con inversa diferenciable). Si X e Y son espacios topológicos, decimos que son homeomorfos si existe un homeomorfismo $f : X \to Y$ (función continua, invertible y con inversa continua). Existe una relación entre espacios aún más laxa, la equivalencia homotópica. Dos morfismos $f, g : X \to Y$ son homotópicos si existe un morfismo $H : X \times [0,1] \to Y$ tal que $H(x,0) = f(x)$ y $H(x,1) = g(x)$, lo notamos $f \simeq g$. Dos espacios X e Y son homotópicamente equivalentes si existen morfismos $f : X \to Y$ y $g : Y \to X$ tales que $f \circ g \simeq \mathrm{id}_Y$ y $g \circ f \simeq \mathrm{id}_X$.

Si X es un espacio con un punto distinguido x_0 y $n \in \mathbb{N}$ se definen los grupos de homotopía $\pi_n(X, x_0)$, ver [7], [16]. Si $f : (X, x_0) \to (Y, f(x_0))$ es un morfismo de espacios también se define $f_n : \pi_n(X, x_0) \to \pi_n(Y, f(x_0))$ un morfismo de grupos. Cuando f_n es un isomorfismo para todo $n \in \mathbb{N}$ decimos que f es una equivalencia débil de homotopía. Si X es conexo por caminos, los grupos $\pi_n(X, x_0)$ para diferentes x_0 son isomorfos y por ese motivo omitiremos el punto distinguido en nuestra notación.

Los CW-complejos son espacios con buen comportamiento en la teoría de homotopía y se forman construyendo bloques llamados *celdas*.

Definición 2.1. Sea X^0 un conjunto discreto. Los puntos de X^0 son las 0-celdas. Definimos el n-esqueleto X^n inductivamente. Supongamos que tenemos construido X^{n-1}. Le pegamos a X^{n-1} discos D^n_α de dimensión n por el borde $\partial D^n_\alpha = S^{n-1}_\alpha$. Las funciones de pegado son morfismos $\varphi_\alpha : S^{n-1}_\alpha \to X^{n-1}$ y la acción de pegado es considerar el sigiente producto cocartesiano

$$\begin{array}{ccc} \coprod_\alpha S^{n-1}_\alpha & \xrightarrow{\varphi_\alpha} & X^{n-1} \\ \downarrow & & \downarrow \\ \coprod_\alpha D^n_\alpha & \longrightarrow & X^n \end{array}$$

En otras palabras X^n es el espacio cociente de $X^{n-1} \coprod_\alpha D^n_\alpha$ via las identificaciones $x \sim \varphi_\alpha(x)$ para todo $x \in \partial D^n_\alpha$. La n-celda e^n_α es la imagen de $D^n_\alpha - \partial D^n_\alpha$ por el morfismo cociente. Consideramos $X = \bigcup_n X^n$ con la topología débil, i.e. $A \subset X$ es un conjunto abierto (cerrado) sii $A \cap X^n$ es abierto (cerrado) en X^n para cada n. Si $X = X^n$ para algún $n \in \mathbb{N}$ decimos que X es de dimensión finita y n es la dimensión. Si la cantidad de celdas que pegamos es finita decimos que X es un CW-complejo finito.

Un teorema básico nos dice que todo espacio X tiene una CW-aproximación Y, es decir existe un CW-complejo Y y una equivalencia débil de homotopía $f : X \to Y$. Entonces si estamos estudiando las clases de equivalencia débil de homotopía, siempre podremos considerar un CW-complejo como representante de dicha clase. Decimos que un espacio X es dominado por un espacio Y si existen morfismos $f : X \to Y$ y $g : Y \to X$ tales que $g \circ f \simeq \mathrm{id}_X$. Notemos que esta condición es necesaria pero no suficiente para que f sea una equivalencia homotópica. Un corolario del teorema de CW-aproximación dice que si X es dominado por un CW-complejo entonces es homotópicamente equivalente a un CW-complejo. Un espacio X es finitamente dominado si es dominado por un CW-complejo finito. Es claro

que esta condición es necesaria para que X sea homotópicamente equivalente a un CW-complejo finito. La pregunta es cuándo esta condición es suficiente:

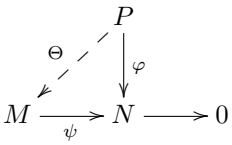
¿Cuándo un espacio X finitamente dominado es homotópicamente equivalente a un CW-complejo finito?

Ejercicio 2.2. *Probar que un espacio X es finitamente dominado si y solamente si $X \times S^1$ es homotópicamente equivalente a un CW-complejo finito.*

2.2. Módulos proyectivos. Para contestar esta pregunta de origen topológico introducimos algunos objetos algebraicos.

Proposición 2.3. *Sea P un R-módulo. Son equivalentes las siguientes afirmaciones:*

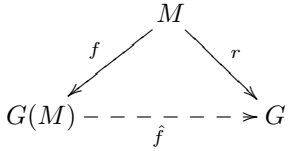
1. *Existe un R-módulo Q tal que $P \oplus Q$ es un R-módulo libre.*
2. *Todo R-homomorfismo de módulos sobreyectivo $\alpha : M \to P$ tiene inversa a derecha $\beta : P \to M$, i.e. $\alpha \circ \beta = \mathrm{id}_P$.*
3. *Si $\varphi : P \to N$ es un homomorfismo de R-módulos y $\psi : M \to N$ es un homomorfismo de R-módulos sobreyectivo*



4. *Si $0 \to M_0 \to M_1 \to M_2 \to 0$ es una sucesión exacta de R-módulos, entonces*
$$0 \to \hom_R(P, M_0) \to \hom_R(P, M_1) \to \hom_R(P, M_2) \to 0$$
es exacta.

Definición 2.4. Un R-módulo P es proyectivo si satisface las condiciones de la proposición 2.3.

2.3. El grupo $K_0(R)$. Sea M un monoide abeliano. El grupo de Grothendieck asociado a M es un grupo $G(M)$ y una aplicación $g : M \to G(M)$ tales que se verifica la siguiente propiedad universal: si G es un grupo y $f : M \to G$ es un morfismo de monoides entonces existe un único morfismo de grupos $\hat{f} : G(M) \to G$ tal que el siguiente diagrama conmuta



El grupo de Grothendieck asociado a un monoide abeliano M existe y es único a menos de isomorfismos (ver [13] pag. 3).

Consideramos la colección de clases de isomorfismos de R-módulos proyectivos finitamente generados:

$$\mathcal{P}(R) := \{[M] : \ M \text{ es un } R\text{-módulo finitamente generado}\}.$$

La suma directa de R-módulos le da a $\mathcal{P}(R)$ una estructura de monoide abeliano

$$[M] \oplus [N] := [M \oplus N].$$

Definición 2.5. Definimos el K_0 de un anillo R como el grupo de Grothendieck del monoide $(\mathcal{P}(R), \oplus)$

$$K_0(R) := G(\mathcal{P}(R), \oplus)$$

Sea $f : R \to R'$ un morfismo de anillos. Consideramos la siguiente estructura de R-módulo a derecha de R',

$$r' \cdot r := r' f(r).$$

Definimos el morfismo de monoides abeliano

$$\mathcal{P}(f) : \mathcal{P}(R) \to \mathcal{P}(R') \qquad \mathcal{P}(f)[M] = [R' \otimes_R M],$$

por propiedad universal del grupo de Grothendieck tenemos que existe un morfismo de grupos al cual llamamos $K_0(f) : K_0(R) \to K_0(R')$ tal que el siguiente diagrama conmuta

$$\begin{array}{ccc} \mathcal{P}(R) & \xrightarrow{\mathcal{P}(f)} & \mathcal{P}(R') \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g'} \\ K_0(R) & \xrightarrow[K_0(f)]{} & K_0(R'). \end{array}$$

Observación 2.6. El grupo de clases proyectivas $K_0(R)$ es el grupo abeliano generado por las clases de isomorfismo $[P]$ de R-módulos proyectivos finitamente generados tal que para cada sucesión exacta corta

$$0 \to P_0 \to P_1 \to P_2 \to 0$$

de R-módulos proyectivos finitamente generados resulta que $[P_1] = [P_0] + [P_2]$.

Como R es un anillo con unidad, existe un único homomorfismo unital de anillos $j : \mathbb{Z} \to R$. Definimos el grupo reducido de clases proyectivas $\tilde{K}_0(R)$ al conúcleo de $K_0(j) : K_0(\mathbb{Z}) \to K_0(R)$. En otras palabras, $\tilde{K}_0(R)$ es el cociente de $K_0(R)$ por el subgrupo generado por las clases de R-módulos libres finitiamente generados. Un R-módulo proyectivo y finitamente generado P es establemente libre si existen $m, n \in \mathbb{N}$ tal que $P \oplus R^m \simeq R^n$ y esto sucede si y solamente si $[P] = 0$ en $\tilde{K}_0(R)$. Es así que $\tilde{K}_0(R)$ mide la desviación de P de ser un R-módulo establemente libre.

Observación 2.7. Se cumple que $\tilde{K}_0(R) = 0$, si R es algunos de los siguientes anillos,

- Un anillo con división, ver [13, Example 1.1.6].
- Un dominio de ideales principales, ver [13, Theorem 1.3.1].
- Un anillo local, ver [13, Theorem 1.3.11].

2.4. Complejos de cadenas de R-módulos. Sea R un anillo. Un complejo de cadenas de R-módulos $(C_\bullet, d)$ es una familia $\{C_k\}_{k\in\mathbb{Z}}$ de R-módulos junto con morfismos de R-módulos $d_k : C_k \to C_{k-1}$ tales que $d_{k-1} \circ d_k = 0$ para todo $k \in \mathbb{Z}$. Un morfismo de complejos $\varphi : (C_\bullet, d) \to (\hat{C}_\bullet, \hat{d})$ es una familia de morfismos de R-módulos $\varphi_k : C_k \to \hat{C}_k$ tales que $\hat{d}_k \circ \varphi_k = \varphi_{k-1} \circ d_k$. Dos morfismos $\varphi, \tilde{\varphi} : (C_\bullet, d) \to (\hat{C}_\bullet, \hat{d})$ son homotópicos si existe una familia $s_k : C_k \to \hat{C}_{k+1}$ de morfismos de R-módulos tales que

$$\hat{d}_{k+1} \circ s_k + s_{k-1} \circ d_k = \varphi_k - \hat{\varphi}_k \quad \forall k \in \mathbb{Z}$$

Decimos que $s : C_\bullet \to \hat{C}_{\bullet+1}$ es una homotopía de cadenas. Dos complejos de cadenas $(C_\bullet, d)$ y $(\hat{C}_\bullet, \hat{d})$ son homotópicos si existen morfismos $\varphi : (C_\bullet, d) \to (\hat{C}_\bullet, \hat{d})$ y $\psi : (\hat{C}_\bullet, \hat{d}) \to (C_\bullet, d)$ tales que $\varphi \circ \psi$ y $\psi \circ \varphi$ son homotópicos a $\mathrm{id}_{\hat{C}_\bullet}$ e $\mathrm{id}_{C_\bullet}$

respectivamente. El complejo de cadenas $(C_\bullet, d)$ es contráctil si $\mathrm{id}_{C_\bullet}$ y el morfismo nulo son homotópicos.

Decimos que $(C_\bullet, d)$ es proyectivo si C_k es un R-módulo proyectivo para todo $k \in \mathbb{Z}$. Decimos que $(C_\bullet, d)$ es libre (con base) si C_k es un R-módulo libre (con una base distinguida) para todo $k \in \mathbb{Z}$. Si solamente hay una candidad finita de C_k no nulos decimos que $(C_\bullet, d)$ es acotado. El complejo $(C_\bullet, d)$ es de tipo finito si es acotado y cada C_k es finitamente generado.

Los grupos de homología de un complejo de cadenas $(C_\bullet, d)$ se definen de la siguiente manera

$$H_k(C_\bullet, d) = \mathrm{Ker}(d_k)/\,\mathrm{Im}(d_{k+1}) \qquad d_k : C_k \to C_{k+1}.$$

Ejercicio 2.8. *Probar que un complejo de cadenas $(C_\bullet, d)$ proyectivo y tal que $C_k = 0$ para $k < 0$, es contráctil si y solamente si $H_k(C_\bullet, d) = 0$ para todo $k \geq 0$.*

Si X es un espacio podemos considerar su complejo de cadenas singular asociado $C_*(X)$, ver [7]. Si X un CW-complejo, se puede considerar $C_*(X)$ como el complejo de cadenas tal que $C_n(X)$ es el grupo abeliano libre generado por las n-celdas, ver [7, Sec. 2.2] por más detalles.

2.5. Obstrucción de finitud de Wall. Si $(C_\bullet, d)$ es un complejo de cadenas proyectivo y de tipo finito tiene sentido considerar $[C_j] \in K_0(R)$ y $[C_j] \in \tilde{K}_0(R)$. La característica de Euler de $(C_\bullet, d)$ es

$$\chi((C_\bullet, d)) = \sum_{j\in\mathbb{Z}} (-1)^j [C_j] \in K_0(R)$$

y la característica de Euler reducida de $(C_\bullet, d)$ es

$$\tilde{\chi}((C_\bullet, d)) = \sum_{j\in\mathbb{Z}} (-1)^j [C_j] \in \tilde{K}_0(R)$$

Sea X un espacio conexo por caminos y localmente simplemente conexo y $C_*(X)$ su complejo de cadenas singular. Si $\tilde{X}$ es su revestimiento universal obtenemos que $C_*(X) = \mathbb{Z} \otimes_{\mathbb{Z}G} C_*(\tilde{X})$ en donde $G = \pi_1(X)$, ver [7, Sec 3.H].

Teorema 2.9. *(Wall,* [17],[18]*)*

1. *Sea X un espacio finitamente dominado, entonces $\pi_1(X)$ es finitamente presentado y $C_*(\tilde{X})$ es homotópico (como complejo de cadenas) a un complejo de tipo finito C_* de R-módulos proyectivos finitamente generados. La característica de Euler de X queda bien definida de la siguiente manera*

$$\tilde{\chi}(X) = \sum_{j\in\mathbb{Z}} (-1)^j [C_j] \in \tilde{K}_0(RG).$$

   Además, $\tilde{\chi}(X) = 0$ si y solamente si X es homotópicamente equivalente a un CW-complejo finito.
2. *Sea G un grupo finitamente presentado. Todo elemento $\sigma \in \tilde{K}_0(RG)$ es la obstrucción finita de un CW-complejo finitamente dominado X con $\tilde{\chi}(X) = \sigma$ y $\pi_1(X) = G$.*
3. *Un CW-complejo X es finitamente dominado si y solamente si $G = \pi_1(X)$ es finitamente presentado y el complejo de cadenas de $\mathbb{Z}G$-módulos $C_*(\tilde{X})$ es homotópicamente equivalente a un complejo de cadenas $\mathcal{P}$ de tipo finito de $\mathbb{Z}G$-módulos proyectivos finitamente generados.*

Corolario 2.10. *Sea G un grupo finitamente presentado.*

Todo CW-complejo X finitamente dominado con $\pi_1(X) = G \quad \Leftrightarrow \quad \tilde{K}_0(RG) = 0$ es homotópicamente equivalente a un CW-complejo finito.

Conjetura 2.11. *Si G es finitamente presentado y libre de torsión entonces*

$$\tilde{K}_0(\mathbb{Z}G) = 0$$

3. El grupo $K_1(R)$ y torsión de Whitehead

3.1. Homotopías simples. En esta sección nos vamos a detener en el problema de clasificación de equivalencias homotópicas entre CW-complejos finitos.

El par (D^n, S^{n-1}_+) tiene una estructura de CW-complejo relativo. El disco D^n se obtiene de S^{n-1}_+ pegando el casco de abajo S^{n-1}_- que es una $n-1$-celda y rellenando con una n-celda. Sea X un CW-complejo y $q : S^{n-1}_+ \to X$ un morfismo tal que $q(S^{n-2}) \subseteq X^{n-2}$ y $q(S^{n-1}_+) \subseteq X^{n-1}$. Sea $Y = D^n \cup_q X$ el espacio obtenido del siguiente diagrama de push out

$$\begin{array}{ccc} S^{n-1}_+ & \xrightarrow{q} & X \\ {\scriptstyle \iota}\downarrow & & \downarrow{\scriptstyle \alpha} \\ D^n & \xrightarrow[\beta]{} & Y \end{array}$$

El espacio Y se obtiene de X mediante el pegado de una celda de dimensión $n-1$ y otra de dimensión n y hereda una estructura de CW-complejo

$$Y^k = \alpha(X^k) \qquad k \leq n-2$$

$$Y^{n-1} = \alpha(X^{n-1}) \cup \beta(S^{n-1})$$

$$Y^k = \alpha(X^k) \cup \beta(D^n) \qquad k \geq n$$

El morfismo $\iota : S^{n-1}_+ \to D^n$ es una equivalencia homotópica entonces $\alpha : X \to Y$ también. Decimos que α es una expansión elemental y que Y es obtenido de X por una expansión elemental. El morfismo $r : Y \to X$ con $r \circ \alpha = \mathrm{id}_X$ es único a menos de homotopías relativas a $\alpha(X)$, decimos que r es un colapso elemental y decimos que X es obtenido de Y via un colapso elemental.

Una equivalencia homotópica $f : X \to Y$ es simple si existe una sucesión de morfismos

$$X = X[0] \xrightarrow{f_0} X[1] \xrightarrow{f_1} X[2] \xrightarrow{f_2} \ldots \xrightarrow{f_{n-1}} X[n] = Y$$

tal que f_i es una expasión o un colapso elemental y la compsosición de las f_i es un morfismo homotópico a f.

¿Cuándo una equivalencia homotópica es simple?

3.2. $K_1(R)$.

Definición 3.1. El grupo $K_1(R)$ está definido como el grupo abeliano cuyos generadores son las clases de conjugación $[f]$ de automorfismos $f : P \to P$ de R-módulos proyectivos finitamente generados y que satisfacen las siguientes relaciones:

- Para cada diagrama conmutativo de R-módulos proyectivos finitamente generados con filas exactas y columnas con automorfismos

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P_0 & \xrightarrow{i} & P_1 & \xrightarrow{p} & P_2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_0}\cong & & \downarrow{\scriptstyle f_1}\cong & & \downarrow{\scriptstyle f_2}\cong & & \\ 0 & \longrightarrow & P_0 & \xrightarrow{i} & P_1 & \xrightarrow{p} & P_2 & \longrightarrow & 0 \end{array}$$

  tenemos que $[f_0] + [f_2] = [f_1]$.
- Si $f, g : P \to P$ son dos automorfismos de un mismo R-módulo proyectivo finitamente generado P entonces $[f \circ g] = [f] + [g]$.

Otra manera de definir $K_1(R)$ es la siguiente. Sea $GL_n(R)$ el grupo de matrices invertibles de $n \times n$ con coeficientes en R. Consideramos la inclusión $GL_n(R) \subset GL_{n+1}(R)$ como

$$A \mapsto \begin{pmatrix} A & 0 \\ 0 & 1 \end{pmatrix}$$

y al colímite de este sistema le llamamos $GL(R)$:

$$GL(R) = \operatorname{colim} GL_n(R) = \bigcup_{n\in\mathbb{N}} GL_n(R).$$

Se puede probar que, (ver [8, Theorem 5.14])

$$K_1(R) = GL(R)_{ab} = GL(R)/[GL(R), GL(R)].$$

Sea $j : \mathbb{Z} \to R$ el único morfismo de anillos unital. El grupo K_1 reducido $\tilde{K}_1(R)$ es el conúcleo del morfismo $j_* : K_1(\mathbb{Z}) \to K_1(R)$.

3.3. Torsion de Whitehead. En esta sección veremos la definición algebraica de la torsión de Whitehead presentada en [9].

Definición 3.2. Sea G un grupo. Sea $< \pm[g] : g \in G >$ el subgrupo de $K_1(\mathbb{Z}G)$ generado por las 1×1-matrices de la forma $(\pm g)$. El grupo de Whitehead de G es

$$Wh(G) = K_1(\mathbb{Z}G)/ < \pm[g] : g \in G > .$$

La torsión de Whitehead de una equivalencia homotópica $f : X \to Y$ de CW-complejos finitos y conexos es un elemento $\tau(f) \in Wh(\pi_1(X))$ y este elemento nos dirá si f es una homotopía simple. Empezaremos por definir la torsión de Whitehead para una equivalencia de homotopía de complejos de cadena.

Supongamos que $(C_\bullet, c)$ es un complejo de cadenas de R-módulos tal que $C_p = 0$ para $p < 0$. Sea $f_\bullet : (C_\bullet, c) \to (D_\bullet, d)$ un morfismo de complejo de cadenas. El mapping cylinder de $f_\bullet$, denotado por $\operatorname{cyl}_*(f_\bullet)$ es

$$\operatorname{cyl}_p(f_\bullet) = C_{p-1} \oplus C_p \oplus D_p \qquad \partial_p^{\text{cyl}} = \begin{pmatrix} -c_{p-1} & 0 & 0 \\ -\operatorname{id} & c_p & 0 \\ f_{p-1} & 0 & d_p \end{pmatrix}$$

El mapping cone de $f_\bullet$, denotado por $\operatorname{cone}_*(f_\bullet)$, es el cociente de $\operatorname{cyl}_*(f_\bullet)$ por la copia de $C_\bullet$

$$\operatorname{cone}_p(f) = C_{p-1} \oplus D_p \qquad \partial_p^{\text{cone}} = \begin{pmatrix} -c_{p-1} & 0 \\ f_{p-1} & d_p \end{pmatrix}$$

La suspensión de $C_\bullet$, denotada por $\sum C_\bullet$, es el cociente de $\mathrm{cone}_*(\mathrm{id}_{C_\bullet})$ por la copia de $C_\bullet$

$$(\sum C_\bullet)_p = C_{p-1} \qquad \partial^{\Sigma} = -c_{p-1}$$

Proposición 3.3. *Un morfismo de complejo de cadenas $f : C_\bullet \to D_\bullet$ es una equivalencia homotópica si y solamente si $\mathrm{cone}_\bullet(f)$ es contráctil.*

Sea $\gamma_\bullet : \mathrm{cone}_\bullet(f) \to \mathrm{cone}_\bullet(f)$ una contracción, es decir, una homotopía entre el morfismo identidad y el morfismo nulo:
(3.4)

$$\gamma_n : \mathrm{cone}_n(f) \to \mathrm{cone}_{n-1}(f) \quad \gamma_n = \begin{pmatrix} h_{n-1} & g_n \\ l_{n-1} & k_n \end{pmatrix} : C_{n-1} \oplus D_n \to C_n \oplus D_{n+1}$$

tal que

$$\begin{array}{ccc} & \overset{\begin{pmatrix} -c_{n-1} & 0 \\ f_{n-1} & d_n \end{pmatrix}}{\longrightarrow} & \\ \begin{pmatrix} h_{n-1} & g_n \\ l_{n-1} & k_n \end{pmatrix} \swarrow & C_{n-1} \oplus D_n \quad \downarrow \mathrm{id} & \searrow \begin{pmatrix} h_{n-2} & g_{n-1} \\ l_{n-2} & k_{n-1} \end{pmatrix} \\ C_n \oplus D_{n+1} & \underset{\begin{pmatrix} -c_n & 0 \\ f_n & d_{n+1} \end{pmatrix}}{\longrightarrow} & C_{n-1} \oplus D_n \end{array} \qquad C_{n-1} \oplus D_{n-1}$$

entonces

$$-c_n h_{n-1} - h_{n-2} c_{n-1} + g_{n-1} f_{n-1} = \mathrm{id}_{C_{n-1}} \tag{3.5}$$

$$f_n g_n + d_{n+1} k_n + k_{n-1} d_n = \mathrm{id}_{D_n} \tag{3.6}$$

$$-c_n g_n + g_{n-1} d_n = 0 \tag{3.7}$$

De (3.7) obtenemos que los morfismos g_n forman un morfismo de complejo de cadenas, $g_\bullet : D_\bullet \to C_\bullet$. De (3.5) obtenemos que los morfismos $h_{n-1} : C_{n-1} \to C_n$ son una homotopía de cadenas de $g \circ f$ a id_C. De (3.6) obtenemos que los morfismos $k_n : D_n \to D_{n+1}$ forman una homotopía de cadenas de id_D a $f \circ g$.

Recíprocamente, dados g, h, k definimos γ como en (3.4) tomando $l = 0$. Luego γ es una homotopía de cadenas entre el siguiente morfismo

$$F_\bullet : \mathrm{cone}_\bullet(f) \to \mathrm{cone}_\bullet(f) \qquad F_n = \begin{pmatrix} \mathrm{id}_{C_{n-1}} & 0 \\ f_n h_{n-1} + k_{n-1} f_{n-1} & \mathrm{id}_{D_n} \end{pmatrix}$$

y el morfismo nulo. Obtenemos la contracción de cadenas considerando $F^{-1} \circ \gamma$. □

Proposición 3.8. *Sea $(C_\bullet, c)$ un complejo contráctil. Sean γ y $\tilde{\gamma}$ dos contracciones, entonces*

1. *Los siguientes son isomorfismos*

$$c + \gamma : C_{\mathrm{odd}} = \bigoplus_{i \geq 0} C_{2i+1} \to C_{\mathrm{even}} = \bigoplus_{i \geq 0} C_{2i} \quad c + \tilde{\gamma} : C_{\mathrm{even}} \to C_{\mathrm{odd}}$$

2. *Si $C_\bullet$ es proyectivo y de tipo finito, la composición*

$$(c + \tilde{\gamma}) \circ (c + \gamma) : C_{\mathrm{odd}} \to C_{\mathrm{odd}}$$

es un automorfismo de un R-módulo proyectivo finitamente generado cuya clase en $K_1(R)$ es cero.

Sea $\Delta_\bullet : C_\bullet \to C_{\bullet+2}$ el morfismo definido por $(\gamma - \tilde{\gamma}) \circ \gamma$. Consideremos el isomorfismo $f : C_{\text{even}} \to C_{\text{even}}$ definido por a siguiente matriz

$$\begin{pmatrix} \text{id} & 0 & 0 & \dots \\ \Delta & \text{id} & 0 & \dots \\ 0 & \Delta & \text{id} & \dots \\ \vdots & \vdots & \vdots & \end{pmatrix}$$

La composición

$$g : C_{\text{odd}} \xrightarrow{c+\gamma} C_{\text{even}} \xrightarrow{f} C_{\text{even}} \xrightarrow{c+\tilde{\gamma}} C_{\text{odd}}$$

esta dada por la siguiente matriz

$$\begin{pmatrix} c & 0 & 0 & ... \\ \gamma & c & 0 & ... \\ 0 & \gamma & c & ... \\ \vdots & \vdots & \vdots & \end{pmatrix} \begin{pmatrix} \text{id} & 0 & 0 & ... \\ \Delta & \text{id} & 0 & ... \\ 0 & \Delta & \text{id} & ... \\ \vdots & \vdots & \vdots & \end{pmatrix} \begin{pmatrix} \tilde{\gamma} & c & 0 & ... \\ 0 & \tilde{\gamma} & c & ... \\ 0 & 0 & \tilde{\gamma} & ... \\ \vdots & \vdots & \vdots & \end{pmatrix} = \begin{pmatrix} \alpha & 0 & 0 & \dots \\ \beta & \alpha & 0 & \dots \\ \xi & \beta & \alpha & \dots \\ \vdots & \vdots & \vdots & \end{pmatrix}$$

con $\alpha = \gamma c + c\Delta c + c\tilde{\gamma}$. Es fácil ver que

$$c\Delta - \Delta c = \tilde{\gamma} - \gamma$$

entonces

$$c\Delta c = \tilde{\gamma} c - \gamma c = \text{id} - c\tilde{\gamma} - \gamma c \quad \Rightarrow \quad \alpha = \text{id}\,.$$

Obviamente f y g representan a la clase nula en $K_1(R)$. □

Sea $(C_\bullet, c)$ un complejo de cadenas libre con base de tipo finito de R-módulos y contráctil. Por proposición 3.8,

$$c + \gamma : C_{\text{odd}} \to C_{\text{even}}$$

es un isomorfismo. Identificamos C_{odd} y C_{even} con R^n para algún $n \in \mathbb{N}$. Esta identificación esta determinada por la base distinguida. Entonces $[c+\gamma]$ representa un elemento en $K_1(R)$. Por proposición 3.8, si $\tilde{\gamma}$ es otra contracción de cadenas entonces $[c+\gamma] = -[c+\tilde{\gamma}]$. Definimos

$$\tau(C_\bullet) := [c+\gamma] \in \tilde{K}_1(R) = K_1(R)/\{\pm 1\}.$$

Esta definición depende de las bases distinguidas en cada R-módulo C_k pero no en la contracción elegida.

Sea $f_\bullet : C_\bullet \to D_\bullet$ una equivalencia de homotopía de complejos de cadenas libre, con base, de tipo finito de R-módulos. Observemos que $\text{cone}(f_\bullet)$ es un complejo de cadenas libre, con base, de tipo finito y contráctil. Definimos la torsión de Whitehead de $f_\bullet$ como

$$\tau(f_\bullet) = \tau(\text{cone}(f_\bullet)) \in \tilde{K}_1(R). \tag{3.9}$$

Supongamos ahora que $f : X \to Y$ es una equivalencia homotópica de CW-complejos conexos y finitos. Sea $p_X : \tilde{X} \to X$ y $p_Y : \tilde{Y} \to Y$ los revestimientos universales. Fijemos puntos base $\tilde{x} \in \tilde{X}$ e $\tilde{y} \in Y$ tales que si $p_X(\tilde{x}) = x$ y $p_Y(\tilde{y}) = y$ entonces $f(x) = y$. Sea $\tilde{f} : \tilde{X} \to \tilde{Y}$ el único levantado de f que satisface $\tilde{f}(\tilde{x}) = \tilde{y}$. Sea $G = \pi_1(X, x) = \pi_1(Y, y)$. Luego de tener fijados $\tilde{x}$ e $\tilde{y}$ la acción de G en $\tilde{X}$ e $\tilde{Y}$ queda determinada. El morfismo $\tilde{f}$ es G-equivariante. Consideramos la equivalencia de homotopía entre $\mathbb{Z}G$-complejos de cadenas $C_\bullet(\tilde{f}) : C_*(\tilde{X}) \to C_*(\tilde{Y})$. Equipamos

los $\mathbb{Z}G$-módulos $C_*(\tilde{X})$ y $C_*(\tilde{Y})$ con la bases que corresponden a las celdas. Usando (3.9) definimos

$$\tau(f) = \tau(C_\bullet(\tilde{f})) \in Wh(G)$$

Observar que estamos considerando la torsión en el cociente de $K_1(\mathbb{Z}G)$ por el subgrupo $< \pm[g] : g \in G >$, esto nos garantiza que la definición no depende de las bases elegidas.

Teorema 3.10. [4] *Sea $f : X \to Y$ una equivalencia homotópica de CW-complejos finitos. Entonces f es una equivalencia homotópica simple si y solamente si su torsión de Whitehead $\tau(f) \in Wh(\pi_1(Y))$ es nula.*

Conjetura 3.11. *Si G es finitamente presentado y libre de torsión entonces*

$$Wh(G) = 0$$

3.4. Teorema del s-cobordismo. Un cobordismo de dimensión n sobre M^- es $(W; M^-, f^-, M^+, f^+)$ en donde W es una variedad diferenciable compacta n-dimensional, junto con una descomposición de su borde ∂W en dos variedades cerradas $(n-1)$-dimensionales $\partial^- W$ y $\partial^+ W$, dos variedades cerradas $(n-1)$-dimensionales M^- y M^+ y difeomorfismos $f^- : M^- \to \partial^- W$ y $f^+ : M^+ \to \partial^+ W$. Un cobordismo es un h-cobordismo si las inclusiones $i^- : \partial^- W \to W$ y $i^+ : \partial^+ W \to W$ son equivalencias homotópicas.

Dos cobordismos $(W; M^-, f^-, M^+, f^+)$ y $(W'; M^-, f'^-, M'^+, f'^+)$ sobre M^- son difeomorfos relativos a M^- si existe un difeomorfismo $F : W \to W'$ tal que $F \circ f^- = f'^-$. Decimos que un cobordismo sobre M^- es trivial si es difeomorfo relativo a M^- al h-cobordismo trivial dado por el cilindro $M^- \times [0,1]$ junto con las inclusiones obvias de $M^- \times \{0\}$ y $M^+ \times \{1\}$.

¿Cuándo un h-cobordismo es trivial?.

La respuesta a la pregunta anterior esta facilitada por la torsión de Whitehead de un h-cobordismo $\tau(M^-, W)$. En dicho caso, la torsión de Whitehead está bien definida y se realiza considerando una estructura de CW-complejo de la variedad, ver [8, Sec. 6.3].

Teorema 3.12 (Teorema del s-cobordismo)**.** *Sea M^- una variadad diferenciable cerrada, orientada y conexa de dimensión ≥ 5 con grupo fundamental $G = \pi_1(M^-)$. Entonces*

i) *Un h-cobordismo W sobre M^- es trivial si y solamente si $\tau(W, M^-) \in Wh(G)$ se anula.*
ii) *Las clases de difeomorfismos relativas a M^- de h-cobordismos sobre M^- estan en biyección con los elementos de $Wh(G)$ via la torsión de Whitehead.*

Corolario 3.13. *Sea G un grupo finitamente presentado.*

Todo h-cobordismo sobre una variedad cerrada y conexa M^- $\Leftrightarrow$ $Wh(G) = 0$ con $\dim(M^-) \geq 5$ y $\pi_1(M^-) = G$ es trivial.

4. Conjetura de Farrell-Jones

Las conjeturas de isomorfismo tienen como objetivo facilitar el cálculo de ciertos invariantes. Hemos visto el interés que hay en calcular $\tilde{K}_0(\mathbb{Z}G)$ y $Wh(G)$ y hemos formulado las conjeturas 2.11 y 3.11. La conjetura de Farrell-Jones tiene como

objetivo calcular $K_n(RG)$ y la veracidad de dicha conjetura implica otras conjeturas más conocidas como la conjetura de Poincaré y la conjetura de Borel. Para una exposición completa ver el artículo [10].

4.1. Conjetura de Farrell-Jones: caso K_n, $n = 0, 1$. Sea R un anillo y G un grupo. Denotamos por

$$A_0 = K_0(i) : K_0(R) \to K_0(RG)$$

el morfismo inducido por la inclusión $i : R \to RG$. Sea G_{ab} el grupo abelianizado de G. Definimos $\phi : G_{ab} \otimes K_0(R) \to K_1(RG)$ el morfismo inducido por la aplicación que manda un elemento $(g, [P]) \in G \times K_0(R)$ a la siguiente clase de RG-automorfismo

$$R[G] \otimes_R P \to R[G] \otimes_R P, \qquad u \otimes x \mapsto ug^{-1} \otimes x$$

Definimos

$$A_1 = \phi \oplus K_1(i) : G_{ab} \otimes_{\mathbb{Z}} K_0(R) \oplus K_1(R) \to K_1(RG)$$

Un anillo R es Noetheriano si todo submódulo de un R-módulo finitamente generado es también finitamente generado. Decimos que R es regular si es Noetheriano y todo R-módulo tiene una resolución proyectiva de dimensión finita.

Conjetura 4.1. *Sea R un anillo regular y G un grupo libre de torsión entonces los siguientes son isomorfismos*

$$K_0(R) \xrightarrow{A_0} K_0(RG) \qquad G_{ab} \otimes_{\mathbb{Z}} K_0(R) \oplus K_1(R) \xrightarrow{A_1} K_1(RG)$$

Observemos que si $R = \mathbb{Z}$ entonces la conjetura 4.1, es exactamente la unión de las conjeturas 2.11 y 3.11.

4.2. Conjetura de Farrell-Jones: caso libre de torsión. Enunciaremos la conjetura para todas las dimensiones. El objetivo es calcular $K_n(RG)$ para todo $n \in \mathbb{Z}$. Los grupos K_n con $n < 0$ se llaman grupos de K-teoría negativa y la definición se puede consultar en [13]. Los grupos K_n con $n \geq 1$ son los grupos de K-teoría superior y la definición de Quillen se puede ver en [12], [19]. Denotaremos por $\mathbf{K}_R$ al espectro de K-teoría no conectivo de R que verifica

$$\pi_n(\mathbf{K}_R) = K_n(R) \qquad \forall n \in \mathbb{Z}.$$

Para ver la definición de dicho espectro consultar [11]. La conjetura de Farrell-Jones consiste en relacionar $K_n(RG)$ con el grupo de homología del espacio clasificante BG con coeficientes en el espectro $\mathbf{K}_R$, que notamos por $H_n(BG; \mathbf{K}_R)$. El espacio clasificante de un grupo G, es un CW-complejo BG tal que $\pi_1(BG) \cong G$ cuyo revestimiento universal es contráctil. Esta propiedad caracteriza a BG a menos de equivalencias homotópicas.

Conjetura 4.2. *Sea G un grupo libre de torsión y R un anillo regular. Entonces existe un morfismo, llamado morfismo de asemblaje,*

$$H_n(BG; \mathbf{K}_R) \to K_n(RG)$$

que es un isomorfismo para todo $n \in \mathbb{Z}$.

4.3. Conjetura de Farrell-Jones: caso general. Supongamos que tenemos:

- Un grupo discreto G.
- Una familia $\mathcal{F}$ de subgrupos de G, es decir, un conjunto de subgrupos de G que es cerrado por conjugación y por intersecciones finitas.
- Una teoría de G-homología, $\mathcal{H}^G_*(-)$.

El espacio clasificante de G para la familia $\mathcal{F}$ es un G-CW-complejo $E_{\mathcal{F}}G$ tal que $(E_{\mathcal{F}}(G))^H$, la parte fija de $E_{\mathcal{F}}G$ por un subrgupo H de G, es un conjunto vacío si $H \notin \mathcal{F}$ y es un espacio contráctil si $H \in \mathcal{F}$. Este espacio queda unicamente determinado a menos de G-homotopías. El morfismo de asemblaje asociado a $(G, \mathcal{F}, \mathcal{H}^G_*(-))$ es la imagen de la proyección $E_{\mathcal{F}} \to pt$ por la teoría de homología

$$\mathcal{A}_{\mathcal{F}} : \mathcal{H}^G_*(E_{\mathcal{F}}G) \to \mathcal{H}^G_*(pt).$$

Sea R es un anillo, consideramos la una G-teoría de homología $H^G_*(-; \mathbf{K}_R)$ definida en [6] que verifica que $H^G_*(pt; \mathbf{KR}) = K_*(RG)$. Un grupo es virtualmente cíclico si contiene un subgrupo cíclico de indice finito. Denotemos por Vyc a la familia de subgrupos cíclicos de G.

Conjetura 4.3. *Sea R un anillo y G un grupo, el morfismo de asemblaje*

$$\mathcal{A}_{Vyc} : H^G_n(E_{Vyc}G; \mathbf{K}_R) \to H^G_n(pt; \mathbf{K}_R) = K_n(RG)$$

es un isomorfismo para todo $n \in \mathbb{Z}$

4.4. Relación con otras conjeturas. Las siguientes conjeturas pueden ser probadas usando la conjetura de Farrell-Jones

Conjetura 4.4 (Conjetura de Poincaré)**.** *Supongamos que $n \geq 5$. Si M es una variedad diferenciable cerrada homotópicamente equivalente a S^n, entonces es homeomorfa a S^n*

Decimos que una variedad diferenciable o un CW-complejo es aesférico si su revestimiento universal es contráctil.

Conjetura 4.5 (Conjetura de Borel)**.** *Sea $f : M \to N$ una equivalencia de homotopía entre variedades topológicas cerradas, entonces f es homotópico a un homeomorfismo. En particular, dos variedades cerradas y aesféricas con grupos fundamentales isomorfos son homeomorfas.*

Conjetura 4.6 (Conjetura de idempotencia)**.** *Sea R un dominio de integridad y G un grupo libre de torsión. Los únicos idempotentes en RG son 0 y 1.*

H. Apéndice: Propiedades de K_0 y K_1

En esta sección enunciaremos algunas de las propiedades de los funtores K_0 y K_1. Para más detalles se puede consultar los dos primeros capítulos de [13]. Denotemos por **PRng** a la categoría de anillos sin unidad y por **Ring** a la subcategoría plena de **PRng** formada por los anillos con unidad.

- **Aditividad.** Sean R_1 y R_2 anillos con unidad. Consideramos $R = R_1 \times R_2$ y $p_i : R \to R_i$ las proyecciones correspondientes. Se verifica que el morfismo

  $$K_i(R) \to K_i(R_1) \oplus K_i(R_2) \qquad i = 0, 1$$

  es un isomorfismo.

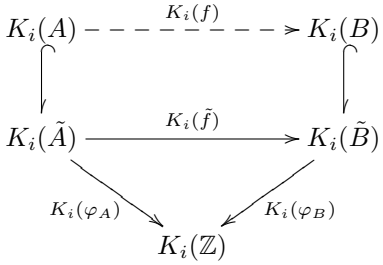
- **Extensión a anillos sin unidad.** Podemos extender la definición de los funtores K_0 y K_1 a la categoría **PRng** de anillos sin unidad. Sea A un anillo (no necesariamente con unidad); consideramos

$$\varphi_A : \tilde{A} \to \mathbb{Z} \qquad \varphi(a, n) = n.$$

  Definimos

$$K_i(A) := \ker(K_i(\varphi_A)) \subseteq K_i(\tilde{A}) \qquad i = 0, 1.$$

  Sea $f : A \to B$ un morfismo de anillos, definimos $K_i(f)$ $i = 0, 1$ de manera tal que el siguiente diagrama conmuta



  Si A tiene unidad, ésta definición coincide con las realizadas para anillos con unidad. En efecto, consideramos el isomorfismo $\psi : \tilde{A} \to A \times \mathbb{Z}$

$$\psi : A \times \mathbb{Z} \to \tilde{A} \qquad \psi(a, n) = (a + n \cdot 1_A, n).$$

  Por aditividad $K_i(\tilde{A}) \cong K_i(A) \oplus K_i(\mathbb{Z})$. Luego $\ker(K_i(\varphi_A)) = K_i(A)$.
- $\mathcal{M}_p$ **estabilidad.** Sea K_i : **Ring** $\to$ **Ab**. Denotemos por $\mathrm{diag}(r_1, \ldots, r_p)$ a la matriz diagonal de $\mathcal{M}_p(R)$ cuyas entradas en la diagonal son $r_1, \ldots, r_p$. La imagen por K_i del morfismo

$$r \mapsto \mathrm{diag}(r, 0, \ldots, 0)$$

  es un isomorfismo. Luego si R es un anillo con unidad,

$$K_i(R) \cong K_i(\mathcal{M}_p(R)).$$

- **Continuidad.** Los funtores K_i : **PRng** $\to$ **Ab** preservan colímites de sistemas filtrantes. Es decir el morfismo canónico

$$\mathrm{colim}_j\, K_i(A_j) \to K_i(\mathrm{colim}_j(A_j))$$

  es un isomorfismo.
- $\mathcal{M}_\infty$**-estabilidad.** Combinando la continuidad y la $\mathcal{M}_p$-estabilidad del funtor K_i : **PRng** $\to$ **Ab**, obtenemos que si R es un anillo con unidad

$$K_i(\mathcal{M}_\infty(R)) \cong K_n(R).$$

- K_0 **es nilinvariante.** Consideramos K_0 : **Ring** $\to$ **Ab**. Si $I \lhd R$ es un ideal nilpotente, entonces $K_0(R) \to K_0(R/I)$ es un isomorfismo. El funtor K_1 no tiene esta propiedad, ver ejemplo 1.3.1 en [5].
- **Semi-Exactitud.** Varios ejemplos muestran que funtores K_i : **PRng** $\to$ **Ab** no son exactos. Sin embargo, son semi-exactos: Si

(H.1) $$0 \to A \to B \to C \to 0$$

  es una sucesión exacta de anillos, entonces

(H.2) $$K_i(A) \to K_i(B) \to K_i(C)$$

es exacta. Además si (H.1) se parte, entonces

$$0 \to K_0(A) \to K_0(B) \to K_0(C) \to 0$$

es una sucesión exacta que se parte. Esta última propiedad no es verficada por K_1, ver contraejemplo en [15].

- **Sucesión exacta.** La razón por la cual se consideran a los funtores K_0 y K_1 como parte de una misma teoría, es porque podemos conectar ambas sucesiones de (H.2), formando así una sucesión exacta de seis términos. En efecto, existe $\partial : K_1(C) \to K_0(A)$ tal que

$$K_1(A) \to K_1(B) \to K_1(C) \xrightarrow{\partial} K_0(A) \to K_0(B) \to K_0(C) \tag{H.3}$$

es exacta.

Referencias

[1] A. Bartels, On proofs of the Farrell-Jones conjecture. `http://arxiv.org/abs/1210.1044v2`, *2013*

[2] A. Bartels and W. Lück, The Borel conjecture for hyperbolic and CAT(0)-groups. *Ann. of Math. (2) 175 (2012), no. 2, 631–689.*

[3] A. Bartels; W. Lück and H. Reich, The K-theoretic Farrell-Jones conjecture for hyperbolic groups. Invent. Math. 172 (2008), no. 1, 29–70.

[4] M. M. Cohen, A course in simply-homotopy theory *Springer-Verlag, New York, 1973. Graduate Texts in Mathematics, Vol. 10.*

[5] G. Cortiñas, Algebraic v. topological K-theory: a friendly match. *Topics in algebraic and topological K-theory, 103–165, Lecture Notes in Math., 2008, Springer, Berlin, 2011.*

[6] J. Davis and W. Lück. Spaces over a category and assembly maps in isomorphism conjectures in K- and L-theory. *K-theory*, 15:241–291, 1998.

[7] A. Hatcher, Algebraic Topology `http://www.math.cornell.edu/~hatcher/AT/AT.pdf`

[8] M. Kreck and W. Lück, The Novikov conjecture. *Geometry and algebra. Oberwolfach Seminars, 33. Birkhäuser Verlag, Basel, 2005.*

[9] W. Lück, Transformation groups and algebraic K-theory. *Lecture Notes in Mathematics, 1408. Mathematica Gottingensis. Springer-Verlag, Berlin, 1989.*

[10] W. Lück and H. Reich, The Baum-Connes and the Farrell-Jones conjectures in K- and L-theory. *Handbook of K-theory. Vol. 1, 2, 703–842, Springer, Berlin, 2005.*

[11] E. Pedersen, C. Weibel. A nonconnective delooping of algebraic K-theory. Algebraic and geometric topology (New Brunswick, N.J., 1983) 166–181, *Lecture Notes in Math., 1126, Springer, Berlin, 1985.*

[12] D. Quillen, Higher algebraic K-theory I *In Algebraic K-theory, I: Higher K-theories (Proc. Conf., Battelle Memorial Inst., Seattle, Wash., 1972), pages 85–147. Lectures Notes in Math., Vol 341. Springer-Verlag, Berlin, 1973.*

[13] J. Rosenberg. Algebraic K-theory and its applications. *Graduate texts in Mathematics, 147. Springer-Verlag, New York, 1994.*

[14] J. Rosenberg. K-theory and Geometric Topology. *Handbook of K-theory. Vol. 1, 2, 577–610, Springer, Berlin, 2005.*

[15] A. Swan Excision in algebraic K-theory J. Pure Appl. Algebra, 1:221–252, 1971.

[16] R. M. Switzer Algebraic topology - homology and homotopy. Reprint of the 1975 edition. Classics in Mathematics. Berlin. Springer. xii, 526, 2002.

[17] C.T.C. Wall, Finiteness condition for CW-complex. Ann. of Math. 81 (1965), 56–69.

[18] C.T.C. Wall, Finiteness condition for CW-complex II. Proc. Roy. Soc. Ser. A, 295:129–139, 1966

[19] C. A. Weibel, The K-book. An introduction to algebraic K-theory. Graduate Studies in Mathematics, 145. American Mathematical Society, Providence, RI, 2013

IMERL, Facultad de Ingeniería, Universidad de la República
Julio Herrera y Reissig 565, 11.300, Montevideo, Uruguay
E-mail address: `eellis@fing.edu.uy`

Publicaciones Matemáticas del Uruguay
Volumen 15, Junio 2016, Páginas 123–139
S 0797-1443

CÓDIGOS Y CRIPTOGRAFÍA: LA TEORÍA DE NÚMEROS APLICADA A TRES VIÑETAS DE AMOR

NATHAN C. RYAN

Resumen. La criptografía y la teoría de códigos son dos áreas de la teoría de números que tienen mucha aplicación a la comunicación. Describimos unos ejemplos destacados de las áreas nombradas, ejemplos que dan una vista panorámica de que ellas consisten.

1. Un cuento de amor y de códigos...

Nuestro héroe tímido Miguel toma el ómnibus. Una chica, desconocida para Miguel toma el mismo ómnibus. Desde el otro lado del bus Miguel la ve y piensa que es la chica más bonita que jamás haya visto. Ella está leyendo un libro, completamente absorta. Siendo nerd, además de ser tímido, Miguel logra memorizar el número ISBN del libro y anota

$$849838285X$$

después de que la chica se baja del ómnibus.

Miguel arma un plan: va a comprar el mismo libro y usará esta cosa en común para iniciar una conversación la próxima vez que ve a la chica en el ómnibus.

Pero...

Cuando llega a casa, entra el número de ISBN que escribió en un buscador de ISBN y lee

```
‘‘El número de ISBN ingresado tiene una cantidad incorrecta de
        dígitos o la suma verificadora equivocada.’’
```

¿Qué es un número de ISBN?. Un *International Standard Book Number* (ISBN) es una cadena de diez símbolos que únicamente identifica un libro. Los primeros nueve símbolos son dígitos y el décimo, un 'símbolo verificador' viene del conjunto

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X\}.$$

¿Qué hace este símbolo verificador?

Divisibilidad. Arrancamos con un hecho que el lector ya debería saber del liceo, enunciado y nombrado como un teorema:

Teorema (El teorema cociente-resto)**.** *Sea* a *un entero y* x *un entero positivo. Existen enteros* q *y* r *únicos tal que*

1. $a = qx + r$*;*
2. $0 \leq r < x$.

Decimos que q es el *cociente* y r el *resto* cuando se divide a por x.

Sean $x_1, x_2, \ldots, x_9$ los primeros nueve símbolo en el número ISBN. Sea c el resto cuando la suma

$$\sum_{k=1}^{9} kx_k = 1 \cdot x_1 + 2 \cdot x_2 + 3 \cdot x_3 + 4 \cdot x_4 + 5 \cdot x_5 + 6 \cdot x_6 + 7 \cdot x_7 + 8 \cdot x_8 + 9 \cdot x_9$$

es dividida por 11. Como c es el resto que resulta de una división por 11, c es un elemento del conjunto

$$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

El símbolo verificador x_{10} del ISBN es determinado por la regla:

$$x_{10} = \begin{cases} c & \text{si } 0 \leq c \leq 9 \\ X & \text{si } c = 10. \end{cases}$$

Se usa el símbolo X como lo usaba los romanos.

Ahora se nota que la suma $-c + \sum_{k=1}^{9} kx_k$ es divisible por 11.

Máximo común divisor y mínimo común múltiplo. El *maximal común divisor* de dos enteros a y b, denotado $\mathrm{mcd}(a, b)$ es un entero g que cumple

- $g \mid a$ y $g \mid b$;
- si $d \mid a$ y $d \mid b$, también $d \mid g$.

El *mínimo común múltiplo* de dos enteros a y b, denotado $\mathrm{mcm}(a, b)$ es un entero ℓ que cumple

- ℓ es un múltiplo de a y ℓ es un múltiplo de b;
- si x es un múltiplo de a y x es un múltiplo de b, también x es un múltiplo de ℓ.

Se puede probar que

$$a \cdot b = \mathrm{mcm}(a, b) \cdot \mathrm{mcd}(a, b).$$

Regresando al cuento de amor... Se puede ver que el número que anotó Miguel es incorrecto porque la suma

$$\sum_{k=1}^{9} kx_k = 1 \cdot \mathbf{8} + 2 \cdot \mathbf{4} + 3 \cdot \mathbf{9} + 4 \cdot \mathbf{8} + 5 \cdot \mathbf{3} + 6 \cdot \mathbf{8} + 7 \cdot \mathbf{2} + 8 \cdot \mathbf{8} + 9 \cdot \mathbf{5} = 261$$

que da un resto de 8 cuando se divide por 11, hecho que implica el símbolo verificador debería ser un 8 y no un X o que haya un error en los primeros nueve dígitos.

Si Miguel no tuviera mala suerte, no tendría ningún tipo de suerte...

Detectando errores comunes. El número de ISBN consiste de 10 símbolos, pero con los primeros nueve se puede únicamente identificar el libro. El décimo símbolo, el símbolo verificador es redundante. ¿Por qué se usan más símbolos de los que se precisa? Debería haber buena razón para justificar lo extra.

Los dos errores más comunes en manejando números de ISBN son un símbolo alterado y la transposición de dos símbolos adyacentes. Por ejemplo, quiero escribir

$$556176988\mathrm{X},$$

pero escribo

$$556\mathbf{2}76988\mathrm{X} \quad \text{o} \quad 556\mathbf{71}6988\mathrm{X}.$$

En cada caso el símbolo verificador está mal considerando los primeros nueve símbolos, sugiriendo que hay un error en los primeros nueve símbolos.

Hay errores que no se puede detectar con este método. Por ejemplo, si quiero escribir

$$673329141X,$$

pero escribo

$$672329341X,$$

el símbolo verificador no me dice nada porque en cada caso el 'X' sí es el símbolo correcto.

Afirmación. *El número ISBN puede detectar un símbolo incorrecto.*

Es decir, sean $x_1, x_2, \ldots, x_9$ y $y_1, y_2, \ldots, y_9$ los primeros nueve símbolos de dos candidatos para un ISBN. Y sea i un entero tal que

1. $1 \leq i \leq 9$;
2. $x_i \neq y_i$;
3. $x_k = y_k$ para $k \neq i$.

Entonces

$$\sum_{k=1}^{9} kx_k \text{ y } \sum_{k=1}^{9} ky_k$$

tienen restos diferentes cuando se dividen por 11.

Entonces, si, en vez de escribir

$$x_1 \ldots x_{i-1} x_i x_{i+1} \ldots x_{10},$$

escribo

$$x_1 \ldots x_{i-1} y_i x_{i+1} \ldots x_{10},$$

voy a saber que algo está mal porque x_{10} no es el símbolo verificador correcto para

$$x_1 \ldots x_{i-1} y_i x_{i+1} \ldots x_{10}.$$

Vamos a demostrar esta afirmación. Pero primero, tenemos que hablar de divisibilidad y la aritmética modular.

Divisibilidad.

Definición (a divide b)**.** Sea a un entero distinto de cero y sea b cualquier entero. Decimos que a *divide* b, y escribimos $a \mid b$, si existe un entero m tal que $b = am$; si no, decimos que a *no divide* a b y escribimos $a \nmid b$.

Ejemplo. Entonces $a \mid b$ si y solo si 0 es el resto cuando se divide b por a. Por ejemplo $7 \mid 35$ porque $35 = 7 \cdot 5$; $7 \mid (-14)$ porque $-14 = 7 \cdot (-2)$; $7 \nmid 11$ porque $11 = 7 \cdot 1 + 4$.

Regresando al cuento de amor... Quizás, no se ha perdido toda la esperanza...

Propiedades de la divisibilidad. Un *primo* es un entero p divisible por exactamente dos enteros. Los primos son como los átomos de los enteros; esta idea se encapsula en:

Proposición. *Sean a y b enteros y sea p un primo. Si $p \mid ab$, entonces $p \mid a$ o $p \mid b$.*

Demostración. Si a o b es cero, entonces p trivialmente divide el producto. Supongamos que $p \nmid a$ y vamos a probar que $p \mid b$. Sea $\ell = \text{mcm}(p, a)$. Como $\text{mcd}(p, a) = 1$, $\ell = |pa|$. Como $p \mid ab$ y $a \mid ab$, vemos que ab es un múltiplo común de p y a. Entonces

$$(\ell \mid ab) \to (pa \mid ab) \to (p \mid b).$$

□

Otra propiedad útil de los primos con respeto a la divisibilidad:

Proposición. *Sean a y b enteros y sea x un entero positivo. Entonces, a y b tienen el mismo resto con dividir por x si y sólo si $x \mid (a - b)$.*

Demostración. Probamos la parte directa primero: usando el teorema cociente-resto, tenemos:

$$a = q_1 x + r_1 \text{ y } b = q_2 x + r_2.$$

Como $r_1 = r_2$, tenemos:

$$a - b = q_1 x - q_2 x = x(q_1 - q_2)$$

y con esto concluimos que $x \mid (a - b)$.

Recíprocamente, usando el teorema cociente-resto, $a = q_1 x + r_1$ y $b = q_2 x + r_2$ donde $r_1 \neq r_2$. Entonces $(a - b) = (q_1 - q_2)x + r_1 - r_2$. Como $r_1 \neq r_2$, vemos que $x \nmid (a - b)$. □

Detectando errores.

Afirmación (De vuelta)**.** *El código ISBN detecta una dígito incorrecto.*

Sean $x_1, x_2, \ldots, x_9$ y $y_1, y_2, \ldots, y_9$ los primeros nueve símbolo y sea i un entero tal que

1. $1 \leq i \leq 9$;
2. $x_i \neq y_i$;
3. $x_k = y_k$ para $k \neq i$.

Entonces

$$\sum_{k=1}^{9} k x_k \text{ y } \sum_{k=1}^{9} k y_k$$

tienen restos diferentes cuando se dividen por 11. Esta condición es equivalente a

$$11 \nmid \left(\sum_{k=1}^{9} k x_k - \sum_{k=1}^{9} k y_k \right).$$

¿Por qué nos ayuda esta observación? Primero introducimos una notación útil: escribimos $a \equiv b \pmod{n}$ (se lea a y b son iguales módulo n) si $n \mid b - a$ o,

equivalentemente, que a y b, después de dividir por n tienen el mismo resto. Se nota que $a \equiv 0 \pmod{n}$ es equivalente a $n \mid a$. La relación

$$11 \nmid \left(\sum_{k=1}^{9} k x_k - \sum_{k=1}^{9} k y_k \right)$$

se puede escribir como

$$\left(\sum_{k=1}^{9} k x_k - \sum_{k=1}^{9} k y_k \right) \not\equiv 0 \pmod{11}.$$

Se puede hacer aritmética módulo n: si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, sabemos

- $a + c \equiv b + d \pmod{n}$;
- $a - c \equiv b - d \pmod{n}$; y
- $a \cdot c \equiv b \cdot d \pmod{n}$.

División es un poco más complicado porque, por ejemplo, no se puede dividir por algunos números. División es igual a multiplicar por el inverso y el inverso de un numero x es un número $y (= x^{-1})$ tal que $xy = 1$. En la notación de aritmética modular, trabajando, por ejemplo, módulo 30:

$$\begin{aligned}
7^{-1} &\equiv 13 \pmod{30} \text{ porque } 7 \cdot 13 = 91 \equiv 1 \pmod{30} \\
1^{-1} &\equiv 1 \pmod{30} \text{ porque } 1 \cdot 1 \equiv 1 \pmod{30} \\
29^{-1} &\equiv 29 \pmod{30} \text{ porque } 29 \equiv -1 \pmod{30} \text{ y } (-1)^2 \equiv 1 \pmod{30}
\end{aligned}$$

Usando fuerza bruta se puede ver que 2 no tiene inverso. En general, cuando $\mathrm{mcd}(x, 30) \neq 1$, x no tiene un inverso módulo 30. Este ejemplo es una instancia de un fenómeno bastante general:

Proposición. *Sea n un entero positivo y sea a y b dos enteros. Entonces la ecuación*

$$ax \equiv b \pmod{n}$$

tiene una solución única si y solo si $\mathrm{mcd}(a, n) = 1$. *Y esta solución es* $a^{-1}b \pmod{n}$.

Ahora se puede terminar con el análisis de lo que pasa cuando uno escribe un símbolo mal en el ISBN. Si el x_i de un número de ISBN se cambia por un y_i entonces la suma $\sum_{k=1}^{10} k x_k$ cambia por $i(y_i - x_i)$. ¿La suma

$$S' = 1 \cdot x_1 + 2 \cdot x_2 + \cdots + i \cdot y_i + \cdots 9 \cdot x_9$$

puede ser igual al símbolo verificador módulo 11? Para fijar ideas, sea c el símbolo verificador. Entonces esta suma debería ser igual a c módulo 11 y la suma $S = \sum_{k=1}^{9} k x_k$ también debería ser igual a c módulo 11. Entonces la diferencia $S' - S$ debería ser igual a 0 módulo 11. La diferencia $S' - S$ es $i(y_i - x_i)$ y la pregunta es: ¿Esta diferencia puede ser 0 módulo 11?

Supongamos que

$$i(y_i - x_i) \equiv 0 \pmod{11}.$$

Como $1 \leq i < 10$, el inverso i^{-1} de i existe y podemos multiplicar cada lado por i^{-1}:

$$i^{-1} \cdot i(y_i - x_i) \equiv i^{-1} \cdot 0 \pmod{11}$$
$$(y_i - x_i) \equiv 0 \pmod{11}.$$

Como $0 \leq y_i, x_i \leq 9$, esta última ecuación implica que $x_i = y_i$. Entonces se puede concluir que si uno cambia exactamente uno de los primeros nueve símbolos se puede detectar el error.

Si por alguna razón el recipiente del mensaje supiera que hay un solo error en el mensaje, el recipiente pudiera encontrar el i que contiene el error y corregir el mensaje.

Regresando al cuento de amor... Miguel supone que hay un sólo error en lo que anotó y usa el código que detecta errores como un código que corrige errores. Encuentra que hay varias maneras de como corregir el número de ISBN para que tenga un X como el símbolo verificador. Va a Amazon y mira cada ISBN que genera usando este método y cuando ingresa el ISBN 849838205X, inmediatamente reconoce la tapa del libro como la misma del libro que tenía el amor de su vida.

Va corriendo a la librería esa misma noche y compra el libro.

El día siguiente en el ómnibus.

Ella: ¡Wow! Tenemos el mismo libro!

Él : ¡Qué casualidad! Me llamo Miguel.

Ella: Me llamo Yésica...

2. El lenguaje secreto del amor.

En los siguientes meses el amor de Miguel y Yésica florece. Les encanta pensar y hablar de la matemática. Como suele suceder, el primer amor matemático para ambos era la teoría de números.

Cifrados de César. Un cifrado de César es, en un sentido, el cifrado más clásico de todos – clásico no solo porque viene del periodo clásico de la historia pero también su puesto en el panteón de los cifrados es parecido al puesto que el David de Rafael tiene en el panteón de la escultura. Mostramos como funciona usando un ejemplo. Supongamos que tenemos el *texto plano*:

¿SABÍA YO LO QUE ES AMOR? OJOS JURAD QUE NO PORQUE NUNCA HABÍA VISTO UNA BELLEZA ASÍ.

El cifrado de César procede así: pensamos la letra A como 0, B como 1, C como 2, etc, hasta Z como 26. Entonces la primera palabra del texto plano de arriba se *preprocesa* como

19 0 1 9 0

Entonces, para generar el *texto cifrado* se elige una *clave* que, en este caso es un resto módulo 27; es decir un número de 0 a 26. Por ejemplo si se elige la clave 10 el cifrado de César dice que se suma 10 a cada número en el texto plano preprocesado y se anota el resto módulo 27. Para nuestro ejemplo tenemos

19+10 0+10 1+10 9+10 0+10

que son, módulo 27,

2 10 11 19 10.

Con estos números se determina el texto cifrado usando la misma correspondencia de antes:

C J K S J.

Si Miguel manda un mensaje cifrado, Yésica, para poder leer el mensaje en la manera más eficiente posible, tendría que saber la clave. ¿Qué descifrado debería usar? Empieza con el texto cifrado, lo convierta en números, resta la clave módulo 27, y convierta los números que quedan otra vez en letras. Para hacerlo en una manera eficiente, Yésica tiene que saber la clave.

¿Cuáles son algunos de los problemas con este cifrado (¡Hay muchos!)? Para empezar solamente hay 27 claves distintas y, entonces, la clave para el descifrado es fácil de encontrar usando fuerza bruta. Una segunda limitación de este cifrado es que uno puede usar el método llamado 'análisis frecuencial' para determinar la clave. Si uno ve un mensaje cifrado lo primero que haría es contar que letras aparecen y con que frecuencia lo hacen. La letra en el texto cifrado con la frecuencia más alta probablemente corresponde o a la A o a la E y de ahí se calcula la clave fácilmente. Por ejemplo si la Ñ es la letra más común en el texto cifrado, entonces se adivinaría que la clave c fuera determinado por una de estas relaciones:

$$0 + \mathsf{c} \equiv 14 \pmod{27} \text{ o } 4 + \mathsf{c} \equiv 14 \pmod{27},$$

(el 0 corresponde a la A, el 4 a la E y el 14 a la Ñ). Si el texto plano que resulta no tiene sentido, se adivina una clave nueva y se repita el proceso.

Este cifrado es un cifrado de tipo sustitución *monoalfabética* porque con aplicar la operación de sustitución se conserva siempre a lo largo de todo el mensaje; en oposición a la sustitución polialfabética. Es decir, por ejemplo, cada E en el texto plano se convierte en la misma letra en el texto cifrado.

Regresando al cuento de amor... Los jóvenes pasan todo su tiempo juntos, leyendo libros, hablando de la matemática y paseando por la ciudad. Sus padres, pensando que son demasiados jóvenes, comienzan a prohibir que se vean. Como son padres muy controladores, monitorean las interacciones entre nuestros héroes y, entonces, Miguel y Yésica, enfocan todo su poder matemático para desarrollar métodos para comunicarse en secreto. Ya saben un poco del cifrado de César, incluyendo lo fácil que es para romper, y, entonces inventan un cifrado nuevo. Lo llaman el cifrado de Miguésica. Y deciden que, a partir de ese momento van a comunicar solamente en textos usando ese cifrado. Cada día que se ven en el liceo, compartan la clave que van a usar ese día.

El cifrado Vigenère. El cifrado que inventaron también se conoce como el cifrado de Vigenère (según la revista *Scientific American*, aún en el año 1917, casi 400 años después de que fue inventado, se pensaba que era imposible descifrar sin saber la clave). El cifrado funciona así. Consideramos el texto plano

LO ÚNICO QUE ME DUELE DE MORIR, ES QUE NO SEA DE AMOR;

y la clave

LIMON

Preprocesamos el texto plano un poco y repetimos la clave debajo del texto plano

LOUNICOQUEMEDUELEDEMORIRESQUENOSEADEAMOR
LIMONLIMONLIMONLIMONLIMONLIMONLIMONLIMON.

Para calcular el texto de cifrado, de acá se procede como en el cifrado de César. Si la i-ésima letra corresponde al número $x_i \in \{0, 1, \ldots, 26\}$ y la i-ésima letra de la clave repetida es y_i, la i-ésima letra z_i del texto de cifrado es la que corresponde a $x_i + y_i \pmod{27}$. Haciéndolo así, llegamos al siguiente texto de cifrado:

VWGBUNWCGQWQOGQVQOQWWZUZQDCGQBWDQOOQOWWZ.

¿Cómo es el descifrado de este cifrado? Si uno conoce la clave, el descifrado es muy parecido al descifrado del cifrado de César: usando la notación del párrafo anterior, simplemente se calcula $z_i - y_i \pmod{27}$.

Este cifrado es más difícil de romper que el cifrado de César porque es un cifrado con sustitución polialfabética: cada ocurrencia de la letra 'E', por ejemplo, en el texto plano, no tiene que ser sustituida por la misma letra en el texto cifrado porque depende de la letra de la clave que corresponde.

Regresando a nuestro cuento de amor... Los padres de nuestros héroes se enloquecen por no saber lo que está ocurriendo entre Miguel y Yésica. Deciden contratar a los conocidos matemáticos Dr Friedrich Kasiski y Dr Edward Friedman para romper el cifrado.

Los métodos de Kasiski y de Friedman. La prueba de Kasiski toma ventaja de que palabras (o partes de palabras) repetidas pueden ser, por casualidad, cifradas por las mismas letras de la clave. Esto implica que habrán repeticiones en el texto cifrado. Entonces, si uno podría determinar lo largo de la clave, el cifrado se convierte en un cifrado de César con período. El método de Kasiski nos da una manera de encontrar cuantas letras tiene la clave.

Por ejemplo, si consideramos el texto cifrado

RFVSM SFIUO MCCMA CZWKO FGYGR JIVBL RVZCU BLDMF
DGEMG WDWWZ VDSJG MFJGT ZZSFM QHZZS GUDSE ODSCV
EIGWP IZQRG AANQR JWVNX QRCOK QYMUL SDYUY YASJL
ZMWTW FNXAT FFKHV DMCZG SIEJF FAPIP IDSFG YOEJW
WKWXE DCWAO ZEIFW OUFSU SSZID WZZGS OQWVG XRUYE
IWSGY MQRFA NWAQF HWNGA EYCJN WAQFS KZCPI JHAAI
MQRFL RBMWK OENMM PCOVR YEXRJ AQUEM YOQNF SSDOK
NFXEU SWYFM JVFFN HPSUW BBFML VFEBM MIEHG AWQWT
CFHHM ZFNKR GQNRB LRUGR RAMFC OEPCL RUYSD OKNOZ
ULSLH GQEDO KLICY VRWFW UIERG UUEXR IFZID XRZKV
YZHFI FRMBM IWLHJ GVFBG FIKYE OEHDQ VTCEB FMWHI
WRRUW KSFRH XEKWW ELMWF MMAUY YASJQ CSRRR WGCCY
VSJRM EYGSJ VIDEC CKQYY EJVGZ VDIJM GICHS VBWYZ
ARUCV RYEXR GSTOM WZBUB LBSIS SPIYS VZDNM RYXOR
LNDEJ DSEYZ XVVSO FAGFB KHMDY DCJRM KSERM YIOSE
GMFJX MVUMR MKSEC UNMFM XCSYK GIFGS GODFR FDNZG
IEHWQ IZHVA GEIMR KSKYY BVVAA BWARD WSZID GFAGN
OZQFF LNFEY GSJVI DECOK FOBII GLVWU SESKQ YXZLZ
YBWAQ FOMAU YEEHW PUBEQ RWPIY TISFQ YDQZQ SECZS
VLLEU ZSPAA FNQVZ CKBGU IEHJN MQPCO ZNVXE SOSFC

```
QPACN RHMFJ CJGIQ RCOUB HFIDD DNWUS ERWFO REEHS
FNUGR VWEGA WLFSN NDEZR GPIYS GCJHH MJLSJ MUPIJ
QGAIO MUOKR UBVFL AZUNE DOKLG MWRZT BLPIU SDNLA
GRZSZ OVIIR WYIES ACKIY DHVGH EIEMX IABUE MMSKI
YEICZ AZJUH FTGAX AHVSK RFMKF JWFYE EJDDN HFEJR
WYUDK RGQIY DHVGZ BDMWH IWFYM KZHSA YZWLT GAXAI
CZSFH AWUOJ NHGRC SUUIP IVGER LMPUO KLWAV RZWFS
KSPCL RXMVV IFNZQ PZQAQ UPWZB FBGNV VSKNZ QPZQA
QUPUL SZNME SEOVB YZXLG ZBLMW USVRF UVZCQ DOQRF
DMRXQ SWFWP YDXVB SQCQZ VBDNH UISZS QYXPR UGSFA
XRGGO LQRLS KGLMW WFWAN QWTCE BOZTR PWYFA RUSDV
HAPRG GAXMW ECKYF MQRBU BHEYJ JGPYE MEQGZ JDIEG
AOFQW VZNVY ZXFSE CCQDR SFGLQ PFGSY UYSJG MFBUQ
ECKQY MQFFN RHHIE
```

y buscamos conjuntos de letras repetidos como los que ilustramos en el texto cifrado. En este texto se pueden encontrar más de 240 conjuntos de tres, cuatro o cinco letras repetidas. Un tabla de ejemplos:

Conjunto	Separación	Divisores hasta 20
HHM	2, 3, 6, 7, 13, 14	
IYS	315	3, 5, 7, 9, 15
IYDH	70	2, 5, 7
NZQPZ	21	3, 7

Suponiendo que los conjuntos repetidos representan la igualdad del texto plano, la primera fila de la tabla indica que la clave es 2, 3, 6, 7, 13, o 14 de largo, la segunda fila que la clave es 3, 5, 7, 9 o 15 de largo. Entonces adivinamos que es 7 de largo porque en todas la filas en tabla y en más de 200 de las 240 filas de la tabla completa, aparece el divisor 7.

Sabiendo el largo de la clave, ahora se rompe el cifrado de César pensando que el texto cifrado está compuesto por una de cada 7 letras.

Para textos planos más cortos se puede usar el método de Friedman basado en el índice de coincidencia. Este índice da una medida de la variación en la distribución de las letras del texto cifrado. Supongamos que el texto plano tiene N letras: hay $\binom{N}{2}$ maneras de elegir dos letras del texto. Sean $f_1, f_2, \ldots, f_{27}$ las frecuencias con que las letras A, B,..., Z aparecen en el texto plano y $p_1, p_2, \ldots, p_{27}$ las probabilidades de que las letras A, B,..., Z aparezcan en el texto. El índice de coincidencia de un texto $\mathcal{X} = x_1x_2x_3\cdots x_N$ es

$$I_c(\mathcal{X}) = \frac{\sum_{i=1}^{27}\binom{f_i}{2}}{\binom{N}{2}} = \frac{\sum_{i=1}^{27} f_i(f_i-1)}{N(N-1)}$$

que se aproxima con

$$\frac{\sum_{i=1}^{27} f_i^2}{N^2}.$$

Es la probabilidad que dos letras elegidas de un texto son iguales.

Si el texto plano es "natural" en el sentido de que la frecuencia f_1 de los A en $\mathcal{X}$ es igual a la frecuencia universal de los A en el castellano, esta suma se estima

como

$$\frac{\sum_{i=1}^{27} f_i^2}{N^2} = \sum_{i=1}^{27} \left(\frac{f_i}{N}\right)^2 \approx \sum_{i=1}^{27} p_i^2.$$

Para el castellano, esta invariante "natural" sería $0,075$. El otro extremo de la invariante es cuando las letras son uniformemente elegidas al azar del alfabeto de 27 letras. En ese caso el índice sería $1/27 \approx 0,037$. La observación clave en lo que sigue es si el cifrado era monoalfabético, se conservaría el índice de coincidencia: el índice del texto del texto plano es igual al índice del texto cifrado. En particular, el texto cifrado bajo un cifrado de César debería tener un índice de coincidencia muy cerca a $0,075$.

Ahora, para adivinar el largo de la clave se hace lo siguiente. Se repartan las letras $x_1, \ldots, x_N$ del texto cifrado entre r columnas (r será el largo de la clave). Entonces hay más o menos

$$r\binom{N/r}{2} = \frac{N(N/r-1)}{2}$$

maneras de elegir dos letras de la misma columna y hay

$$\frac{r \cdot (N/r) \cdot (N - N/r)}{2} = \frac{N(N - N/r)}{2}$$

maneras de elegir dos letras de distintas columnas.

Entonces, uno esperaría tener

$$E = (0,075) \cdot \left(\frac{N(N/r-1)}{2}\right) + (0,037) \cdot \left(\frac{N(N-N/r)}{2}\right)$$

pares iguales y la probabilidad de elegir un par de letras iguales sería

$$\frac{E}{\binom{N}{2}} = \frac{1}{r(N-1)}(0,038N + r(0,037N - 0,075)).$$

Pero el resultado de esta cuenta también es el índice de coincidencia del texto. Entonces,

$$I_c(\mathcal{X}) \approx \frac{1}{r(N-1)}(0,038N + r(0,037N - 0,075))$$

y de aquí se puede resolver para la r.

Regresando a nuestro cuento de amor... Con la ayuda de los terribles Dres Kasiski y Friedman, los padres ya pueden romper toda la comunicación entre Miguel y Yésica. Tienen una intervención familiar y los padres de Miguel anuncian que están mandando Miguel al exterior para terminar el liceo. Miguel y Yésica piden media hora más, para tener una última oportunidad para estar juntos. Los padres dicen que sí.

Miguel y Yésica van al cuarto de Miguel y empiezan a planear como van a seguir en contacto sin que su padres se enteren. Se dan cuenta de dos cosas: necesitan un cifrado nuevo y una nueva manera de como compartir claves ya que nunca se van a ver y ya que sus padres van a monitorear todos los mensajes no cifrados.

Yésica dice que ella tiene un método para compartir claves.

Diffie-Hellman. Este protocolo criptográfico permite que dos personas desconocidas una para la otra puedan establecer una clave secreta y compartida. Mostramos como funciona con un ejemplo, pero primero tenemos que hablar un poco de multiplicación módulo un primo p.

Consideramos el conjunto $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ de enteros módulo p. Todo elemento de este conjunto menos cero tiene un recíproco multiplicativo (porque p es primo y todo n positivo menor que p es coprimo con p). El conjunto $\mathbb{Z}_p^\times = \{1, \ldots, p-1\}$ tiene la estructura de un *grupo*: hay una operación binaria (en nuestro caso multiplicación módulo p denotada $\cdot$) tal que:

1. existe un elemento nulo e tal que $a \cdot e \equiv e \cdot a \equiv a \pmod{p}$ para todo $a \in \mathbb{Z}_p^\times$ (en nuestro caso $e = 1$);
2. la operación binaria es asociativa (o sea $a \cdot (b \cdot c) \equiv (a \cdot b) \cdot c \pmod{p}$ para toda $a, b, c \in \mathbb{Z}_p^\times$;
3. cada elemento de $\mathbb{Z}_p^\times$ tiene un recíproco multiplicativo (o sea, para cada $a \in \mathbb{Z}_p^\times$ existe una $b \in Z_p^\times$ tal que $a \cdot b \equiv 1 \pmod{p}$.

Se dice que el elemento $g \in \mathbb{Z}_p^\times$ *genera* el grupo si cada elemento del grupo se puede escribir como una potencia de g. En este caso particular tal g también se llama una *raíz primitiva módulo* p.

Miguel y Yésica eligen y publican dos números: un primo p y una raíz primitiva g módulo p. Miguel elige un entero a al azar y calcula $u \equiv g^a \pmod{p}$; manda u a Yésica. Yésica elige un entero b al azar y calcula $v \equiv g^b \pmod{p}$; manda v a Miguel. Yésica, entonces, puede calcular la clave $k \equiv u^b \equiv (g^a)^b \pmod{p}$ y Miguel también: $k \equiv v^a \equiv (g^b)^a \pmod{p}$. Ahora tienen la misma clave.

Si sus padres quisieran conocer la clava precisan a o b. Sin esos datos, tendrían que resolver el *problema del logaritmo discreto*, un problema para cual no se conoce un algoritmo que lo resuelva en una cantidad de tiempo razonable. El problema es: encontrar x dado y, g, p y $y \equiv g^x \pmod{p}$. El algoritmo de Shanks para resolver este problema usando un primo con 300 dígitos y a y b con 100 dígitos tomaría más tiempo que la edad del universo para romper el protocolo.

Regresando a nuestro cuento de amor... Ahora que tienen el método para intercambiar claves, empiezan a discutir el cifrado. Pero en ese momento los padres de Yésica entran y se la llevan. Y Miguel se queda ahí, sentado, sin manera de comunicarse con el amor de su vida.

Nuestros héroes siguen comunicándose en claro, sin un cifrado, pero no pueden hablar como quieren. Hay cosas que solo quieren compartir con el otro, pero ya no pueden. Los padres de Yésica siguen leyendo su mail. Entonces, con la comunicación sofocada, con tiempo, la intimidad de su amor decae. Siguen adelante con sus vidas separadas, trabajando en la matemática y siempre pensando en el otro.

3. Como comparar secretamente los amores...

Después de la abrupta separación de nuestros héroes, se dedican independientemente a la matemática en general y la criptografía en particular. Algunas de las cosas que aprendieron, las ilustramos acá.

Grupos. Antes de introducir al nuevo sistema criptográfico, se precisan unas ideas básicas. Pensamos de vuelta en equivalencia módulo n y un poco más acerca de grupos. En particular, se sabe que

- un entero m es equivalente módulo n a uno de los enteros $\{0, 1, \ldots, n-1\}$;
- la aritmética funciona en una manera razonable: si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, sabemos
  - $a + c \equiv b + d \pmod{n}$;
  - $a - c \equiv b - d \pmod{n}$; y
  - $a \times c \equiv b \times d \pmod{n}$;
- la ecuación $ax \equiv b \pmod{n}$ tiene una solución si y solo si $\mcd(a, n) = 1$.

Un grupo es un par de objetos $(G, \star)$ donde G es un conjunto y $\star$ es una operación binaria que cumple

1. [**Clausura**] para toda $x, y \in G$, $x \star y \in G$;
2. [**Elemento nulo**] existe un elemento $e \in G$ tal que $e \star x = x \star e = x$ para todo $x \in G$;
3. [**Asociatividad**] para toda $x, y, z \in G$, $x \star (y \star z) = (x \star y) \star z$;
4. [**Inversos**] para toda $x \in G$, existe $y \in G$ tal que $x \star y = e = y \star x$.

Dos ejemplos relevantes. Sean $\mathbb{Z}/n\mathbb{Z}$ el conjunto $\{0, 1, 2, \ldots, n-1\}$ y $\star$ la operación de sumar módulo n. Entonces: sabemos de los hechos de arriba que la operación es cerrada; sabemos que $0 \in \mathbb{Z}/n\mathbb{Z}$ sirve como el elemento nulo; una cuenta fea nos deja concluir que la operación es asociativa; y para cada x el elemento $-x \pmod{n}$ es el inverso de x.

Sean $(\mathbb{Z}/n\mathbb{Z})^\times = \{x \in \mathbb{Z}/n\mathbb{Z} : \mcd(x, n) = 1\}$ y $\star$ la operación de multiplicar módulo n. Entonces: la operación es cerrada porque el producto de dos números coprimos con n es coprimo con n; el elemento $1 \in (\mathbb{Z}/n\mathbb{Z})^\times$ es el elemento nulo; una cuenta fea nos dea concluir que la operación es asociativa; y para cada x coprimo con n existe un elemento y tal que $xy \equiv 1 \pmod{n}$.

La función ϕ de Euler. Varias veces vamos a tener que hablar del tamaño del conjunto $(\mathbb{Z}/n\mathbb{Z})^\times$. Definimos la función

$$\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$$

por $\phi(n) = \#\{x \in \mathbb{Z}/n\mathbb{Z} : \mcd(x, n) = 1\}$. Se puede probar lo siguiente:

Lema. *La función ϕ es multiplicativa; o sea, si $\mcd(m, n) = 1$, tenemos $\phi(mn) = \phi(m)\phi(n)$. También, si n se factoriza como $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, tenemos*

$$\phi(n) = n \prod_{p \mid n} \left(1 - \frac{1}{p}\right).$$

Obviamente, $\phi(n)$ es el tamaño del conjunto $(\mathbb{Z}/n\mathbb{Z})^\times$.

El algoritmo extendido de Euclides. Para el grupo $(\mathbb{Z}/n\mathbb{Z}, +)$ encontrar el elemento inverso de un elemento dado es fácil y obvio de hacer; para el grupo $((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ también es fácil de hacer pero no tan obvio. Arrancamos con la identidad de Bezout: dado dos enteros x, y, existen dos enteros a, b tal que

$$ax + by = \mcd(x, y).$$

Supongamos que queremos encontrar el inverso (multiplicativo) de x módulo n; o sea, dado x y n coprimos, ¿cómo encontramos la y tal que $xy \equiv 1 \pmod{n}$?; o sea, ¿como encontramos el entero k tal que $xy + kn = 1 (= \mcd(x, n))$? Según la identidad de Bezout tal k e y existen pero ahora hablamos de como encontrarlo.

Algoritmo 1. *Supongamos que* x *e* y *son enteros y sea* $m = \mathrm{mcd}(x, y)$. *Este algoritmo encuentra enteros* a *y* b *tal que* $xa + yb = m$.

1. ***[Inicializar]*** *Sean* $a = 1$, $b = 0$, $r = 0$, $s = 1$.
2. ***[¿Terminado?]*** *Si* $y = 0$, *sea* $m = x$ *y terminar.*
3. ***[Cociente y resto]*** *Escribir* $x = qy + c$ *con* $0 \leq c < y$.
4. ***[Shiftear]*** *Sea* $(x, y, r, s, a, b) = (y, c, a - qr, b - qs, r, s)$ *y seguir a paso (2).*

Ahora un ejemplo:

Ejemplo 3.1. Resolvemos la ecuación $17x \equiv 1 \pmod{17}$. Primero usamos el algoritmo recién descrito para encontrar a y b tal que $17x + 61y = 1$:

$$\begin{aligned} \underline{61} &= 3 \cdot \underline{17} + \underline{10} \\ \underline{17} &= 1 \cdot \underline{10} + \underline{7} \\ \underline{10} &= 1 \cdot \underline{7} + \underline{3} \\ \underline{7} &= 2 \cdot \underline{3} + \underline{1}. \end{aligned}$$

Trabajando con estas cuentas pero trabajando al revés, tenemos,

$$\begin{aligned} \underline{1} &= \underline{7} - 2 \cdot \underline{3} \\ &= \underline{7} - 2 \cdot (\underline{10} - 1 \cdot \underline{7}) \\ &= 3 \cdot \underline{7} - 2 \cdot \underline{10} \\ &= 3 \cdot (\underline{17} - 1 \cdot \underline{10}) - 2 \cdot (\underline{61} - 3 \cdot \underline{17}) \\ &= 9 \cdot \underline{17} - 2 \cdot \underline{61} - 3 \cdot \underline{10} \\ &= 9 \cdot \underline{17} - 2 \cdot \underline{61} - 3 \cdot (\underline{61} - 3 \cdot \underline{17}) \\ &= 18 \cdot \underline{17} - 5 \cdot \underline{61}. \end{aligned}$$

O sea

$$1 \equiv 18 \cdot 17 \pmod{61}.$$

En particular, esto quiere decir que el inverso multiplicativo de 17 módulo 61 es 18 módulo 61.

Calcular el inverso así es fácil (o, mejor dicho, rápido) por este teorema de Lamé:

Teorema. *La cantidad de pasos requerido por el algoritmo de arriba es menor o igual a 5 por el número de dígitos en* $\max\{x, y\}$.

El pequeño teorema de Fermat. Este teorema tiene muchas aplicaciones por todos lados de la matemática.

Teorema. *Sea* p *un primo y* a *un entero tal que* $\mathrm{mcd}(a, p) = 1$. *Entonces* $a^{p-1} \equiv 1 \pmod{p}$.

Demostración. Miramos la sucesión $a, 2a, 3a, \ldots, (p-1)a$. Ninguno de los enteros son congruentes módulo p: si lo fueran, $ma \equiv na \pmod{p}$ y, como a es coprimo con p se puede "dividir" por a y deducir que $m \equiv n \pmod{p}$, un absurdo. Además, como a y p son coprimos, ninguno de los números ma es equivalente a cero módulo p. Entonces

$$\begin{aligned} 1 \cdot 2 \cdot \cdots \cdot (p-1) &\equiv a \cdot 2a \cdot \cdots \cdot (p-1)a \pmod{p} \\ (p-1)! &\equiv a^{p-1}(p-1)! \pmod{p}. \end{aligned}$$

Como p y $(p-1)!$ son coprimos, se puede dividir por $(p-1)!$ y llegamos a

$$1 \equiv a^{p-1} \pmod{p}.$$

□

El sistema RSA. El sistema criptográfico asimétrico RSA fue desarrollado en 1977 por Rivest, Shamir y Adleman. Se llama asimétrico porque de los dos participantes, solamente uno tiene control de las claves. Por ejemplo si el sistema es de Yésica, ella genera dos claves: una clave pública para que cualquiera otra persona puede comunicarse con Yésica en una forma privada y, para cada clave pública, genera una clave privada que ella usa para el descifrado.

Los detalles del sistema RSA. La idea fundamental que forma la base de RSA es la construcción por Yésica de una función invertible

$$E : X \to X$$

tal que cualquiera persona puede calcular $E(x)$ pero solamente Yésica puede calcular $E^{-1}(x)$. Yésica construye tal función de esta manera:

1. Yésica elige dos primos grandes p y q; calcula $n = pq$.
2. Yésica puede calcular
$$\phi(n) = (p-1)(q-1).$$
3. Yésica elige un entero e al azar tal que
$$1 < e < \phi(n) \text{ y } \operatorname{mcd}(e, \phi(n)) = 1.$$
4. Yésica calcula una solución $x = d$ a la congruencia
$$ex \equiv 1 \pmod{\phi(n)}.$$
5. Finalmente, Yésica define una función $E : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ por
$$E(x) = x^e \in \mathbb{Z}/n\mathbb{Z}.$$

Para mandar un mensaje a Yésica se procede así. Se traduce el mensaje, de alguna manera, a una sucesión de números módulo n:

$$m_1, \ldots, m_r \in \mathbb{Z}/n\mathbb{Z}$$

y se manda

$$E(m_1), \ldots, E(m_r)$$

o sea,

$$m_1^e \pmod{n}, \ldots, m_r^e \pmod{n}.$$

Cuando los $E(m_i)$ llegan a Yésica, ella puede calcular $E^{-1}(m) = m^d \pmod{n}$. El hecho que el inverso se calcula usando el d viene del siguiente resultado.

Proposición. *Sea n un entero que es un producto de primos distintos y sean $d, e \in \mathbb{Z}_+$ tal que $p - 1 \mid de - 1$ para cada primo que divide a n. Entonces $a^{de} \equiv a \pmod{n}$ para todo $a \in \mathbb{Z}$.*

Demostración. Como $n | a^{de} - a$ si y solo si para cada $p \mid n$ tenemos que $p \mid a^{de} - a$, es suficiente probar que $a^{de} \equiv a \pmod{p}$ para cada $p \mid n$. Entonces hay dos casos: (1) $\operatorname{mcd}(a, p) \neq 1$: en este caso $a \equiv 0 \pmod{p}$ y, entonces, $a^{de} \equiv a \pmod{p}$; (2) $\operatorname{mcd}(a, p) = 1$: en este caso, el pequeño teorema de Fermat afirma que $a^{p-1} \equiv 1 \pmod{p}$. Ahora, como para algún k tenemos $k(p-1) = de - 1$, se ve que

$$1 \equiv 1^k \equiv (a^{p-1})^k \equiv a^{de-1} \pmod{p}$$

Multiplicando cada lado por a nos da

$$a^{de} \equiv a \pmod{n}.$$

□

Entonces, para calcular el descifrado se calcula

$$E^{-1}(m) \equiv E(m_i)^d \equiv (m_i^e)^d \equiv m_i \pmod{n}.$$

Convirtiendo un texto plano a un número. Hay varias maneras de hacerlo y para hacerlo de verdad es mucho más complicado de los que vamos a ver ahora. Por ejemplo, hay que "rellenar" el texto plano con caracteres aleatorios para evitar ciertos ataques.

Sea s una cadena de letras mayúsculas y espacios tal que no empieza con un espacio. Se convierte s a un número de esta manera: un espacio corresponde a 0, la letra A a 1, ..., Z a 27, y escribimos el número en base 28. Entonces

YESICA

corresponde a

$$28^5 \cdot 26 + 28^4 \cdot 5 + 28^3 \cdot 20 + 28^2 \cdot 9 + 28^1 \cdot 3 + 28^0 \cdot 1 = 450989029.$$

Para ir al revés, se tiene que dividir por potencias sucesivas de 28.

Si $28^k \leq n$ se puede cifrar cualquier sucesión de k letras tal que el resultado, después de aplicar el método de arriba, es menor o igual a n. Entonces, si se puede cifrar números de tamaño no mayor que n, se tiene que separar el mensaje original en bloques m_i de tamaño no mayor que $\log_{28}(n)$.

Un ejemplo completo de RSA.

1. Sean

$$p = 503294209384574398578 1 \text{ y } q = 1403294209384574398576 9.$$

2. Entonces

$$\begin{aligned}\phi(n) &= \phi(p)\phi(q)\\ &= (p-1)(q-1)\\ &= 706269849646160775335423984594368919143790 40.\end{aligned}$$

3. Elegir al azar un $e < \phi(n)$:

$$e = 69418451666598544362041409492071945586962923$$

y publicar la clave pública: $(e, \phi(n))$.

4. Calcular el $d \pmod{\phi(n)}$ tal que $e \cdot d \equiv 1 \pmod{\phi(n)}$:

$$d = 2361722340165447943045881988667204910167430 7.$$

5. Cifrar la letra X, que corresponde al número 25:

$$E(X) \equiv 25^e \equiv 168288943432844302785435735710046928575453 85 \pmod{\phi(n)}$$

6. Para descifrar, se calcula $E(X)^d$ y se puede ver (usando una calculadora) que

$$E(X)^d = X.$$

Exponenciación rápida. Supongamos que queremos calcular 2^{17}. El algoritmo obvio de como hacerlo es multiplicar dos por dos 16 veces:

$$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$$

Mejor sería

$$\left(\left((2 \cdot 2)^2\right)^2\right)^2 \cdot 2$$

que requiere cinco multiplicaciones solamente. Además si uno estuviera calculando el resto de la potencia módulo n, se reduciría módulo n después de cada producto. Entonces se calcula $b^m \pmod n$ de esta manera:

Algoritmo 2. *Dado enteros b, m y n, este algoritmo calcula $x = b^m \pmod n$ en una manera eficiente.*

1. ***[Inicializar]*** *Poner $x = 1$ y escribir m en base 2: $(m)_2$.*
2. ***[Seguir?]*** *$m > 0$? Si no, devolver el valor de x.*
3. ***[Caso impar]*** *Si el último dígito de $(m)_2$ es 1, poner $x = x \cdot b \pmod n$.*
4. ***[Move a la izquierda]*** *Sacar el último dígito de $(m)_2$ y hacer el cambio correspondiente a m (dividir por 2, o restar 1 y después dividir por 2).*
5. ***[Cuadrar la base]*** *Poner $b = b^2 \pmod n$.*
6. ***[Continuar]*** *Regresar a paso (2).*

Hay que tener cuidado con las claves. Describimos dos ejemplos donde uno puede, sin tanto esfuerzo, encontrar la clave privada.

Factorizando n dado $\phi(n)$. Sabemos que $\phi(n) = pq - p - q + 1$ y que $pq = n$. Entonces, si consideramos el polinomio

$$x^2 - (p + q)x + pq = x^2 - (n - \phi(n) + 1)x + n$$

se ve que las raíces del polinomio son p y q y, usando propiedades de la función ϕ, sabemos los coeficientes del polinomio. Las raíces se pueden encontrar usando la fórmula cuadrática.

Factorizando n dado que p y q están cercas. Éste es el método de factorización de Fermat: sean $p > q$ y $n = pq$. Entonces

$$n = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2.$$

Ahora si $p \approx q$, la cantidad $\left(\frac{p-q}{2}\right)^2$ es muy pequeña, la cantidad $\left(\frac{p+q}{2}\right)$ es aproximadamente el tamaño de $\sqrt{n}$ y $t^2 - n = s^2$ es un cuadrado perfecto. Entonces probamos

$$t = \lceil\sqrt{n}\rceil,\ t = \lceil\sqrt{n}\rceil + 1,\ \lceil\sqrt{n}\rceil + 2, \ldots$$

hasta que $t^2 - n$ sea un cuadrado. Entonces

$$p = t + s \text{ y } q = t - s.$$

Regresando a nuestro cuento de amor... Después de haber pasado tantos años separados, después que ambos habían ganado sus doctorados en matemática, se ven en una fiesta tirada por un amigo común. Cuando se ven, es como si el tiempo no se había movido en los años desde la última vez que pasaron unos momentos juntos. Miguel siente que sigue enamorado de Yésica pero no quiere anunciar que sigue con estos sentimientos sin saber que Yésica siente lo mismo. Entonces pasa un rato pensando en como resolver el problema de saber si Yésica está enamorado de él en una manera que se quedaría sin pedir la ayuda de ninguna otra persona.

Comunicación segura entres varios partidos. Supongamos que hay dos millonarios y quieren saber cual de los dos es el más rico pero sin revelar la cantidad de plata que tienen ni al otro ni a cualquier otra persona. ¿Cómo se puede resolver la duda sin revelar nada?

Millonario 1 tiene I millones de dólares y Millonario 2 tiene J millones de dólares. Quieren averiguar si $I \leq J$ pero al final del protocolo ninguno de los dos debería haber aprendido nada con respeto a la riqueza de la otra persona salvo la información implicada por $I \geq J$. Para simplicidad, supongamos que $I, J \in \{1, \ldots, 10\}$.

Supongamos que el millonario 2 tiene una clave privada y pública de RSA: (d, n) y (e, n), respectivamente y usa la función E_2 para cifrar y D_2 para descifrar. El protocolo es el siguiente:

1. Millonario 1 elige un número grande x y lo cifra usando el cifrado de Millonario 2: $c = E_2(x)$.
2. Millonario 1 calcula $c - I$ y manda el resultado a millonario 2.
3. Millonario 2 calcula $y_u = D_2(c - I + u)$ para cada $1 \leq u \leq 10$.
4. Millonario 2 elige un primo p de tamaño aproximadamente $x/2$ tal que $|z_u - z_v| \geq 2$ para $u \neq v$ $(u, v \in \{1, \ldots, 10\})$ donde $z_u \equiv y_u \pmod{p}$ para $u \in \{1, \ldots, 10\}$.
5. Millonario 2 manda a millonario 1 esta sucesión de números en este orden:
$$z_1, z_2, \ldots, z_J, z_{J+1} + 1, z_{J+2} + 1, \ldots, z_{10} + 1, p.$$
6. Millonario 1 verifica si el I-ésimo número de esta sucesión es equivalente a x módulo p. Si lo es, deduce que $I \leq J$; sino, deduce que $I > J$.

Regresando a nuestro cuento de amor... Miguel se acuerda del protocolo para resolver el problema de los dos millonarios, se acerca a Yésica, y le dice:

Él: Elegí un número: 3 si sigues enamorado de mí y 5 si no. Yo elijo 4 si estoy enamorado de ti y 2 si no. Sin contarme tu número vamos a deducir que hacer con lo que hay entre nosotros dos...

Ella: ¿Cómo vas a poder hacer eso?

Él: Si el número que estás pensando es mayor de la que yo estoy pensando, seguimos enamorados. ¿Lo probamos?

Instituto de Matemática y Estadística Rafael Laguardia
Universidad de la República, Uruguay
E-mail address: nryan@fing.edu.uy

ARTÍCULOS ARBITRADOS

Publicaciones Matemáticas del Uruguay
Volumen 15, Junio 2016, Páginas 143–155
S 0797-1443

COALITIONS OF PULSE-INTERACTING DYNAMICAL UNITS

ELEONORA CATSIGERAS

Abstract. We prove that large global systems of interacting (non necessarily similar) dynamical units that are coupled by cooperative impulses, recurrently exhibit the so called *grand coalition* for which all the units arrive to their respective goals simultaneously. We bound from above the waiting time until the first grand coalition appears. Finally, we prove that if besides the units are mutually similar, then the grand coalition is the unique subset of goal-synchronized units that is recurrently shown by the global dynamics.

1. Introduction

We study the global dynamics of a network N composed by a large number m of dynamical units that mutually interact by cooperative (i.e. positive) instantaneous pulses.

One of the most cited examples of the type of phenomena that we are contributing to explain mathematically along this work, is the large scale synchronization of the flashes of the fireflies "Pteroptyx malaccae": a large number of individuals flash periodically all together after a waiting time when they meet together on trees, with neither an external clock nor privileged individuals mastering the global synchronization [11].

We are motivated on the study of the dynamics of such global systems to obtain abstract and very general mathematical results, that are independent of the concrete formulae governing the dynamics, and require very few hypothesis. They prove at once the synchronization phenomena found in many particular cases whose previous study were based on and used concrete formulae and restrictive hypothesis. For instance, they are applicable to some models used in Neuroscience for which numerical formulae were needed to know the individual dynamics of the neurons (see for instance [2, 12, 14, 18, 24]).

The mathematical study of the global dynamics of abstract and general networks composed by mutually interacting units has a large diversity of concrete applications to other sciences and technology. As said above, they are widely used in Neuroscience. They have also applications to Engineering, for instance in the design and construction of some systems used in communications [28, 29]; also in Physics, for instance to study systems of light controlled oscillators [22, 23], and

Received by the editors February 9, 2014; accepted after revision November 2, 2014.

2010 *Mathematics Subject Classification.* Primary: 37NXX, 92B20; Secondary: 34D06, 05C82, 94A17, 92B25.

Key words and phrases. Pulse-coupled networks, interacting dynamical units, coalitions, synchronization.

EC was partially supported by CSIC of Universidad de la República, ANII and L'Oreal-UNESCO, Uruguay.

in the research of the evolution of physical lattices of coupled dynamical units of different nature [8, 27]. They have other important applications to Biology, for instance in the research of mathematical models of genetic regulatory networks [9]; to Ecology, in the study of the equilibria of some eco-systems evolving on time [13, 26]; to Economy and other Social Sciences in the research of coupled networks of different agents, individuals or coalitions of individuals, for instance by means of evolutive Game Theory [19, 1].

While not interacting with other units of the network, each unit $i \in \{1, 2, \dots, m\}$, which we also call "cell", evolves governed by two rules that determine the "free dynamics of i": the *relaxation rule* and the *update rule,* which we will precisely define in Subsection 2.1. While the units are not interacting, the dynamics of the network is the product dynamics of its m units, which evolve independently one from the other. But at certain instants, at least one unit i changes the dynamical rules that govern the other units $j \neq i$. The instants when each unit i acts on the others are exclusively determined by the state x_i of i. The pulsed coupling hypothesis assumes that any action from i to $j \neq i$ is a discontinuity jump in the instantaneous state of the cell j according to the *interactions rules* which we will precisely define in Subsection 2.1.

The free dynamics rules and the instantaneous interactions rules, as well as the mathematical results that we obtain from them, generalize to a wide context the particular cases that were studied for instance in [20, 3, 7, 15, 6].

The results that we prove along the paper deal with the spontaneous formation of *coalitions* (subsets) of dynamical units during the dynamical evolution of the network, provided that the interactions among the units are all "cooperative" (i.e. positively signed). Roughly speaking, each coalition is a subset of units that synchronize certain milestones of their respective individual dynamics, which we call goals, and do that spontaneously without any external clock or master unit, infinitely many times in the future. In particular the formation of the so called *grand coalition* (i.e. the simultaneous arrival to a certain goal of all the units of the network) is spontaneously and recurrently exhibited from any initial state (Theorem 2.8). The synchronization of the grand coalition was initially proved in 1992 by Mirollo and Strogatz [20], under restrictive hypothesis requiring that the units were identical, the interactions were also identical, and that the free dynamics of the units were one-dimensional oscillators whose evolution were linear on time. Later, in 1996, Bottani [3] proved the synchronization of the grand coalition requiring that the units were similar (non necessarily identical), but still one dimensional oscillators although their evolution were not necessarily linear on time. In Theorem 2.8 we will generalize the result to any network of non necessarily similar units with cooperative interactions that depend on the pair of interacting cells, with general free dynamics of each unit i, on any finite dimension (depending on i), and such that the cells do not necessarily behave as oscillators. The price to pay for such a general result is that the network has to be large enough, and, unless the units were mutually similar (Theorem 2.10), the grand coalition is not necessarily the unique coalition that is exhibited recurrently in the future.

Due to the fact that the units may be very different and that the grand coalition is not necessarily the unique coalition that is exhibited in the future, the word "synchronization" in Theorem 2.8, if applied, it is not in its classical meaning ([21]). In fact, the orbits of each of the units that recurrently exhibit the grand

coalition, are not synchronized in the strict sense since they do not show the same state for all the instants $t \geq 0$. The states of two or more units may sensibly differ one from the others, at some instants between two consecutive formations of the grand coalition.

On the one hand, the synchronization in the strict or wide sense, for models of pulsed coupled dynamical units, were up to now proved for particular examples in which the free dynamics of each cell is governed by a differential equation or a discrete time mapping with *a concrete formulae.* For instance, the free dynamics is governed by affine mapping in [7], by linear differential equations in [22, 23], and by piecewise contracting maps in [27] [15],[6] or using known results about piecewise contractions in [4]. In this sense, the novelty of the results here is that their proofs work independently of the concrete formulation of the free dynamics of the cells. They have almost no hypothesis about the second term of the differential equation governing the free dynamics of each of the cells.

On the other hand, the results along this paper hold independently of the dimension of the space X_i where the state of each unit evolves, and they do not require the free dynamics of each unit to make it an oscillator. This freedom allows the results to be applied for instance to multidimensional chaotic free dynamics of the cells that recurrently shear certain milestones in the global collective dynamics ([16, 17]).

The paper is organized as follows: in Section 2 we state the mathematical definitions and theorems to be proved. In Section 3 we write the proofs.

2. Definitions and statements of the results

2.1. **Definitions and hypothesis.**

The relaxation rule of the free dynamics of i:

The relaxation rule of the free dynamics of the cell i determines the evolution on time $t \geq 0$ of the state x_i on a compact finite-dimensional manifold X_i (whose dimension may depend of i). It is defined as the solution of any differential equation:

$$\frac{dx_i}{dt} = f_i(x_i), \quad x_i \in X_i \tag{1}$$

satisfying just one condition as follows:

There exists a Lyapunov real function $S_i : X_i \mapsto \mathbb{R}$, which we call *the satisfaction level* of i, such that:

$$\frac{dS_i(x_i(t))}{dt} = \bigtriangledown S_i(x_i(t)) \cdot f_i(x_i(t)) > v_i > 0 \ \ \forall\, t \text{ such that } S_i(x_i(t)) < \theta_i, \tag{2}$$

where θ_i is a positive constant (for each unit i) which we call the *goal* of i. (In formula (2) $\bigtriangledown S_i \cdot f_i$ denotes the inner product in the tangent bundle of the manifold X_i).

In other words, the free dynamics of i holds at all the instants for which i is uncoupled to the network and its state is unchanged by interferences that may come from outside i. It is described by a finite dimensional variable x_i evolving on time t in such a way that the satisfaction level $S_i(x_i)$, while it does not reach the goal value θ_i, is strictly increasing with t and its (positive) velocity is bounded away from zero.

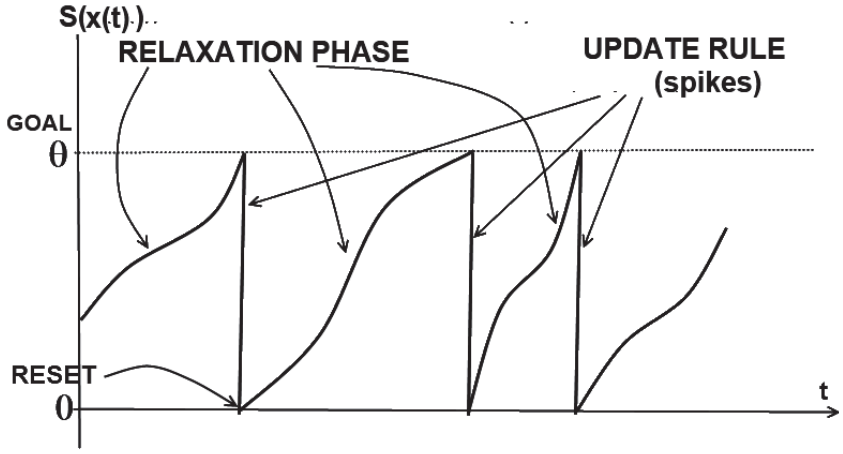


FIGURE 1. The evolution on time t of the satisfaction variable $S(x(t))$ of a dynamical unit while not interacting with the other units of the network.

The update rule of the free dynamics of i:

The update rule is a discontinuity jump in the state x_i of the cell i that is produced whenever the satisfaction variable $S_i(x_i(t))$ reaches (or is larger than) the goal level θ_i. This discontinuity jump instantaneously resets the satisfaction level $S_i(x_i(t))$ to a "reset value", which is strictly smaller than θ_i. With no loss of generality, we assume that the reset value is zero (see Figure 1). Precisely:

$$S_i(x_i(t_0^-)) \geq \theta_i \quad \Rightarrow \quad S_i(x_i(t_0)) = 0, \tag{3}$$

where $S_i(x_i(t_0^-))$ denotes $\lim_{t \to t_0^-} S_i(x_i(t))$.

Note that the alternation between the relaxation and update rules of the free dynamics of i will occur while no interferences come from outside i forcing its satisfaction variable to decrease (see Figure 1). Nevertheless, the free evolution $S_i(x_i(t))$ is not necessarily periodic if $\dim(X_i) \geq 2$. In fact, the set $S_i^{-1}(\{0\}) \subset X_i$ of states with constant null satisfaction may be for instance a curve: there may exist infinitely many points in X_i for which $S_i = 0$. So, each state $x_i(t)$ obtained by the reset rule $S_i(x_i(t)) = 0$ from the goal $S_i(x_i(t^-)) = \theta_i$, does not necessarily repeat in the future to make the evolution $S_i(x_i(t))$ periodic. On the contrary, if the set of all the possible reset states $x_i \in S_i^{-1}(\{0\})$ were finite (this can occur even if $S_i^{-1}(\{0\})$ is infinite), then the free dynamics of i would be periodic, i.e. an oscillator.

Definition 2.1. (Spikes) Taking the name from Neuroscience, we call *spike* of the cell i to the discontinuity jump of its satisfaction state from the goal value θ_i (which in Neuroscience is called "threshold level") to its reset value (which is assumed to be zero). Note that the instants when each cell i spikes, while not interacting with the other units of the network, are defined just by the value of its own satisfaction variable. There is not a master clock to force the spikes of the many cells of the network happen simultaneously.

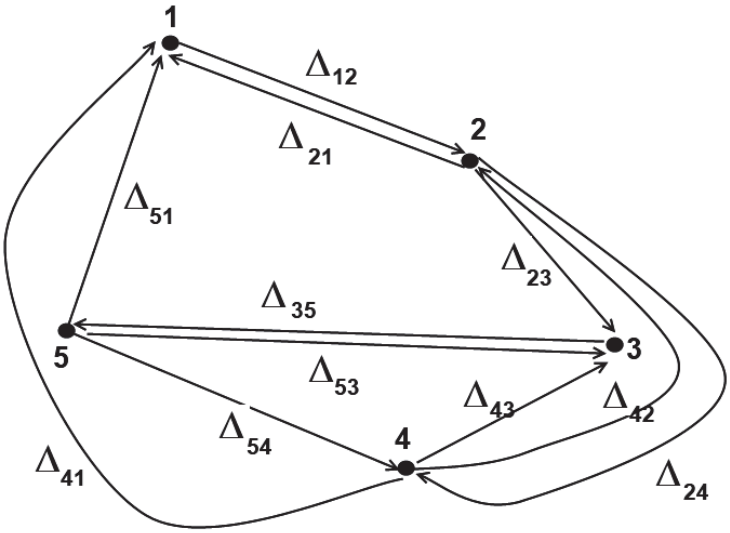


FIGURE 2. The graph of interactions of a global system of instantaneously coupled units $1, 2, \ldots, 5$. The oriented and nonzero weighted edges are denoted by Δ_{ij}.

The interactions rules among the units:

Now, let us define the rules that govern the mutual interactions among the units, to compose a global dynamical system which we call network N. Consider a system composed by $m \geq 2$ dynamical units with the free dynamics as described above.

Definition 2.2. (Spiking instants and inter-spike intervals) We denote by $\{t_n\}_{n\geq 0}$ the sequence of instants $0 \leq t_n < t_{n+1}$ for which at least one cell of the system spikes. We call t_n the *n-th. spiking instant* of the global system.

We call (t_{n+1}, t_n) the *n-th. inter-spike interval of the global system.*

First, by hypothesis, the interactions among the units of the global system are produced only at the spiking instants. In other words, during the inter-spike intervals the cells evolve independently one from the others. Hence, the dynamics of the global system along the inter-spike time intervals is the product dynamics of those of its units.

Second, at each instant t_n the possible action from a cell i to $j \neq i$ is weighted by a real number Δ_{ij}. The interactions in the network are represented by the edges of a finite graph, whose vertices are the cells $i \in \{1, \ldots, m\}$ and whose edges (i, j) are oriented and weighted by $\Delta_{i,j}$ respectively (see Figure 2). We call $\Delta_{i,j}$ the interaction weight. We say that the graph of interactions is *complete* if $\Delta_{i,j} \neq 0$ for all $i \neq j$.

Third and finally, the satisfaction value of any cell j, at any spiking instant t_n is defined by the following rule:

$$S_j(x_j(t_n)) = \begin{cases} S_j(x_j(t_n^-)) + \sum\limits_{i\in I(t_n),\, i\neq j} \Delta_{ij} & \text{if } S_j(x_j(t_n^-)) + \sum\limits_{i\in I(t_n),\, i\neq j} \Delta_{ij} < \theta_j, \\ 0 & \text{otherwise,} \end{cases} \tag{4}$$

where $I(t_n)$ is the set of neurons that spike at instant t_n.

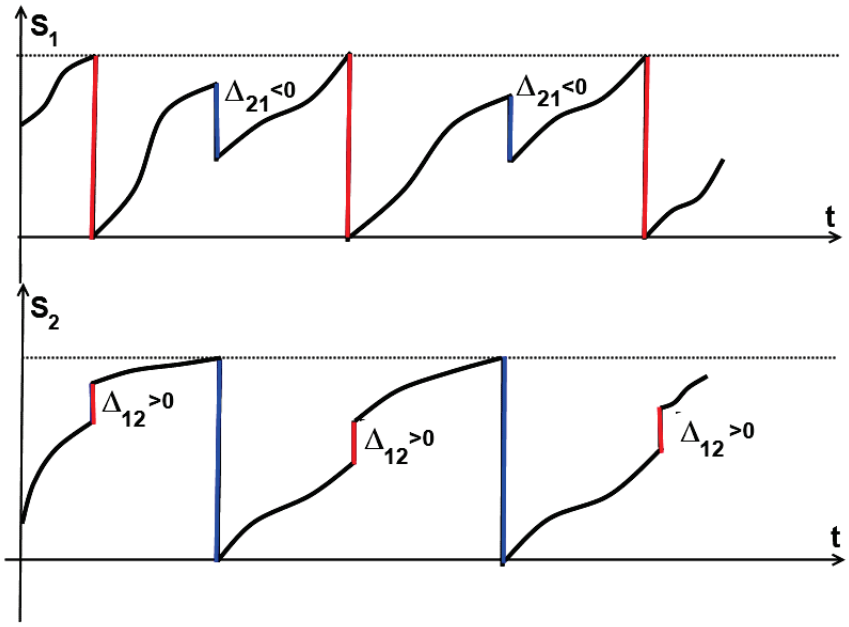


FIGURE 3. Evolution on time t of the satisfaction variable of two interacting units. One cell is cooperative and the other is antagonist.

Definition 2.3. (Coalition) We call the set $I(t_n)$ *the coalition* at the spiking instant t_n. A coalition I is a singleton if $\#I = 1$. From the definition of the spiking instant, no coalition is empty.

If the interactions weights $\Delta_{i,j}$ are all positive and large enough, the coalition $I(t_n)$ may be the result of an avalanche process that makes more and more cells spike at the same instant t_n when at least one cell spikes. In fact, we can always decompose $I(t_n)$ as the following union of pairwise disjoint subsets of cells:

$$I(t_n) = \bigcup_{p\geq 0} I_p(t_n),$$

where $I_0(t_n)$ is the set of cells i such that $S_i(x_i(t_n^-)) = \theta_i$, and for all $p \geq 1$, the set $I_p(t_n)$ is composed by the cells $j \notin \cup_{k=0}^{p-1} I_k(t_n)$ such that $x_j(t_n^-) + \sum_{k=0}^{k=p-1} \sum_{i\in I_k(t_n)} \Delta_{ij} \geq \theta_j$.

Definition 2.4. (Cooperative and antagonist cells)
A cell i is called *cooperative* if $\Delta_{ij} \geq 0$ for all $j \neq i$. It is called *antagonist* if $\Delta_{ij} \leq 0$ for all $j \neq i$. It is called *mixed* if it is neither cooperative nor antagonist.

In Figure 3 we draw the evolution on time of the satisfaction variables of two interacting dynamical units: one of the units is cooperative and the other is antagonist.

From the rule (4), when a cooperative cells spikes, it helps the other cells to increase the values of their respective satisfaction variables. So it shortens the time that the other cells must wait to arrive to their respective goals. On the contrary,

an antagonist cell diminishes the values of the satisfaction variables of the other cells, opposing to them and enlarging the time they must wait to arrive to their goals.

Experimentally in Neuroscience, the nervous system of animals rarely show the existence of mixed cells. This is a reason why one usually assumes the so called Dale's Principle [25, 2]: any cell in the network is either cooperative or antagonist. In [5] abstract mathematical reasons that support Dale's principle were proved: it is a necessary condition for a maximum dynamical richness in the network. Precisely, the amount of information that the network can exhibit along its temporal evolution in the future acquires its maximum restricted to a constant number of nonzero interactions, only if Dale's principle holds.

Along this work we focus on the global dynamics of networks that are composed by cooperative cells in a complete graph of interactions.

The global state and the vectorial satisfaction variable

We denote by

$$\mathbf{x}(t) = (x_1(t), \dots, x_m(t)) \in \prod_{i=1}^{m} X_i$$

the state of the global system at instant $t \geq 0$. We denote by

$$\mathbf{S}(\mathbf{x}(t)) = (S_1(x_1(t)), \dots, S_m(x_m(t))) \in \mathbb{R}^m$$

the vectorial satisfaction variable of the global system at instant t. We consider the cube

$$Q := \prod_{i=1}^{m} [0, \theta_i) \subset \mathbb{R}^m.$$

From the hypothesis of the free dynamics of the cells and of the mutual interactions, if all the cells are cooperative then

$$\mathbf{S}(\mathbf{x}(t)) \in Q \quad \forall\, t \geq 0$$

provided that

$$\mathbf{x}(0) \in \mathbf{S}^{-1}(Q). \tag{5}$$

Along this paper we will assume condition (5). This assumption is not a restriction for the study of all the orbits of the global autonomous system. In fact, if $\mathbf{S}(\mathbf{x}(0)) \notin Q$, then, applying the inequality (2) and the reset rule (3), and taking into account that the interactions are non negative, we deduce that there exists a minimum positive instant t_0 such that $\mathbf{S}(\mathbf{x}(t_0)) \in Q$. So, translating the origin of the time axis to t_0, we have reduced the problem to the case for which the vectorial satisfaction value initially belongs to Q.

Definition 2.5. (Grand coalition) We call $I(t_n)$, defined in 2.3, the *grand coalition* if all the cells of the system spike at instant t_n. Namely, the grand coalition is exhibited at instant t_n if $I(t_n) = \{1, 2, \dots, m\}$.

Definition 2.6. (Waiting time) If from some initial state of the global system the grand coalition is exhibited at some spiking instant $t_n \geq 0$, we call the minimum such an instant *the waiting time* until the grand coalition occurs. Note that in general, if existing, the finite waiting time depends on the initial state.

Weak interactions: We will not need to assume the following condition (6) as an hypothesis. So, it is not an assumption in any part of this paper. Nevertheless, we pose condition (6) just because some of the theorems that we will prove along the work become more interesting for networks that satisfy it:

$$\max_{i\neq j} |\Delta_{ij}| \ll \min_i \theta_i, \tag{6}$$

where $\ll$ denotes "much smaller than". For instance, one may be interested in considering $a \ll b$ (where $0 < a < b$) if $a/b < 10^{-3}$. Condition (6) says that the interactions weights are relatively very weak.

Definition 2.7. (Large networks)

Let N be a network composed by m cooperative units. We say that N is *large enough* in relation to the cooperative interactions if the following inequality holds:

$$\sqrt{m} \geq 1 + \frac{\max_i \theta_i}{\min_{i\neq j} \Delta_{ij}}. \tag{7}$$

Note that, inequality (7) implies that the graph of interactions is complete. In fact $\Delta_{ij} \geq 0$ for all $i \neq j$ because the cells are all cooperative, but

$$\Delta_{ij} \neq 0 \ \forall \ i \neq j$$

to make the minimum in formula (7) be nonzero and make this formula hold for a finite value of m.

2.2. **Statements of the results.** The purpose of this paper is to prove the following results:

Theorem 2.8. *If the network is cooperative and large enough, then from any initial state the grand coalition is exhibited infinitely many times in the future.*

Theorem 2.9. *If the network is cooperative and large enough, then from any initial state in $\mathbf{S}^{-1}(Q)$ the waiting time t_{n_0} before the grand coalition appears for the first time is upper bounded by:*

$$t_{n_0} \leq \max_i \ \frac{\theta_i}{\min_{x_i \in S_i^{-1}[0,\theta_i]} \bigtriangledown S_i(x_i) \cdot f_i(x_i)}.$$

Theorem 2.10. *If the network is cooperative, large enough and if besides all the cells are mutually similar, i.e.*

$$\frac{\min_i \left(\theta_i / \max_{x_i \in S_i^{-1}[0,\theta_i]} \bigtriangledown S_i(x_i) \cdot f_i(x_i)\right)}{\max_i \left(\theta_i / \min_{x_i \in S_i^{-1}[0,\theta_i]} \bigtriangledown S_i(x_i) \cdot f_i(x_i)\right)} \geq 1 - \frac{\min_{i\neq j} \Delta_{ij}}{\max_i \theta_i} \tag{8}$$

then, from any initial state and after a waiting time the grand coalition appears at every spiking instant of the system.

Inequality (8) is satisfied for instance if the cells have mutually identical free dynamics and besides, for each cell i, the maximum and minimum velocities $\bigtriangledown S_i(x_i) \cdot f_i(x_i)$ - according to which the satisfaction variable S_i increases - are not very different. Hypothesis (8) also holds if the cells are not identical but their differences are small enough so the quotient at left in inequality (8) - which is strictly smaller than 1 - differs from 1 less than $\dfrac{\min_{i\neq j} \Delta_{ij}}{\max_i \theta_i}$. If besides the interactions weights $\Delta_{i,j}$ are much smaller than θ_i - cf. condition (6) -, then the similarity among the cells must be very notorious to satisfy the hypothesis of Theorem 2.10.

Roughly speaking, Theorem 2.10 states that if the cells are similar enough then, after a waiting time which depends on the initial state of the global system, the spike of one cell makes all the other cells also spike at the same instant. In other words, the only recurrent coalition is the grand coalition.

3. The proofs

3.1. **Proof of Theorem 2.8.** Let $\{t_n\}_{n\geq 0}$ the strictly increasing sequence of spiking instants, as defined in 2.2. Let

$$r := 1 + \operatorname{int}\Big(\frac{\max_i \theta_i}{\min_{i\neq j} \Delta_{ij}}\Big),$$

where int denotes the lower integer part. Since by hypothesis the network is large, from Definition 2.7 we obtain:

$$r^2 \leq m,$$

where m is the number of units in the system.

As remarked in assertion (5) of Section 2, it is not restrictive to assume that the initial state $\mathbf{x}(0)$ belongs to the set $\mathbf{S}^{-1}(Q)$. In other words $S_i(x_i(0)) \in [0, \theta_i)$ for any unit i.

Assertion (A) *During the time interval* $[0, t_{r-1}]$ *all the units of the system have spiked at least once.*

To prove Assertion (A), let argue by contradiction. Assume that there is a cell, say j, such that $x_j(t) < \theta_j$ for all $t \in [0, t_{r-1}]$. By the interactions rule (4), and since at least one cell spikes at instant t_k for all $k = 0, \ldots, r-1$, we have:

$$S_j(x_j(t_{r-1})) \geq S_j(x_j(0)) + r \min_{i\neq j} \Delta_{ij} \geq S_j(x_j(0)) + \theta_j \geq \theta_j,$$

contradicting the initial assumption. So Assertion (A) is proved.

Now, we state

Assertion (B) *If at some instant* t_n *at least* r *cells spike simultaneously, then all the cells spike simultaneously at* t_n.

To prove Assertion (B) we have, by hypothesis, $\#I(t_n) \geq r$. Due to the interactions rule (4), for any cell $j \notin I(t_n)$ we obtain:

$$S_j(x_j(t_n)) \geq S_j(x_j(t_n^-)) + r \min_{i\neq j} \Delta_{ij} \geq \theta_j,$$

contradicting the assumption that $j \notin I(t_n)$. Therefore, all cells are in $I(t_n)$ proving Assertion (B).

Consider the r coalitions $I(t_0), I(t_1), \ldots, I(t_{r-1})$. Assertion (A) states that each cell i belongs to at least one of those coalitions. Since the number of different cells is $m \geq r^2$, and the number of coalitions in the above list is r, there exists at least one of such coalitions, say $I(t_k)$ having at least r different cells. In other words, there exists a spiking instant t_k such that at least r cells spike simultaneously at t_k. Applying Assertion (B) we deduce that all the cells spike simultaneously at t_k. We have proved that the grand coalition $I(t_k) = \{1, \ldots, m\}$ is spontaneously formed at the instant $t_0^* := t_k > 0$. Since this assertion holds for any initial state, we now translate the origin of the time axis to t_0^*, adopting a new initial state from which the grand coalition will be formed again at some future instant $t_1^* > t_0^*$. By induction on n, the grand coalition will be exhibited recurrently in the future at an increasing sequence of instants t_n^*, ending the proof of Theorem 2.8. □

3.2. **Proof of Theorem 2.9.** From the proof of Theorem 2.8, the waiting time t_0^* until the first grand coalition appears is not larger than the instant t_{r-1} such that all the cells have spiked at least once during the time interval $[0, t_{r-1}]$. Since all the interactions are positive, t_{r-1} is not larger than the time T_i that the slowest cell, say i, would take to arrive to its goal θ_i if it were not coupled to the network, i.e. under the free dynamics:

$$t_0^* \leq t_{r-1} \leq T_i.$$

From the relaxation rules (1) and (2) we get

$$\theta_i = S_i(x_i(T_i^-)) = \int_0^{T_i} \bigtriangledown S_i(x_i(t)) \cdot f_i(x_i(t))\, dt \geq \Big(\min_{x_i \in S_i^{-1}([0,\theta_i])} \bigtriangledown S_i(x_i) \cdot f_i(x_i) \Big)\, T_i$$

Thus

$$t_0^* \leq T_i \leq \frac{\theta_i}{\min_{x_i \in S_i^{-1}[0,\theta_i]} \bigtriangledown S_i(x_i) \cdot f_i(x_i)} \leq \max_i \ \frac{\theta_i}{\min_{x_i \in S_i^{-1}[0,\theta_i]} \bigtriangledown S_i(x_i) \cdot f_i(x_i)},$$

ending the proof of Theorem 2.9. □

3.3. **Proof of Theorem 2.10.** From Theorem 2.8, there exists a first instant t_0^* such that the grand coalition is exhibited. From the update rule (3, the state $\mathbf{x}(t_0^*)$ of the global system is such that $\mathbf{S}(\mathbf{x}(t_0^*)) = \mathbf{0}$. We now translate the origin of the time axis to t_0^*. So, the initial state is now $\mathbf{x}(0)$ such that $\mathbf{S}(\mathbf{x}(0)) = \mathbf{0}$.

Hence, to prove Theorem 2.10 it is enough to show that, if the hypothesis of inequality (8) holds, then for any initial state $\mathbf{x}(0)$ such that $\mathbf{S}(\mathbf{x}(0)) = \mathbf{0}$, all the cells spikes simultaneously at the minimum instant $t_1 > 0$ such at least one cell, say i, spikes.

So, let us compute the values of the satisfaction variables of all the cells at the instant t_1^-. Due to the relaxation rules (1) and (2) we have

$$(9)\quad S_j(x_j(t_1^-)) = \int_0^{t_1} \bigtriangledown S_j(x_j(t)) \cdot f_j(x_j(t))\, dt \geq \Big(\min_{x_j \in S_j^{-1}([0,\theta_j]} \bigtriangledown S_j(x_j) \cdot f_j(x_j) \Big)\, t_1,$$

for all $1 \leq j \leq m$. In particular for the spiking cell i we have

(10)

$$\theta_i = S_i(x_i(t_1^-)) = \int_0^{t_1} \bigtriangledown S_i(x_j(t)) \cdot f_i(x_j(t))\, dt \leq \Big(\max_{x_i \in S_i^{-1}([0,\theta_i])} \bigtriangledown S_i(x_i) \cdot f_i(x_i) \Big)\, t_1.$$

Combining inequalities (9) and (10) we deduce:

$$\begin{aligned} S_j(x_j(t_1^-)) &\geq \theta_i \ \frac{\min_{x_j \in S_j^{-1}([0,\theta_j])} \bigtriangledown S_j(x_j) \cdot f_j(x_j)}{\max_{x_i \in S_i^{-1}([0,\theta_i])} \bigtriangledown S_i(x_i) \cdot f_i(x_i)} \\ &\geq \theta_j \ \frac{\min_i \left(\theta_i / \max_{x_i \in S_i^{-1}[0,\theta_i]} \bigtriangledown S_i(x_i) \cdot f_i(x_i) \right)}{\max_j \left(\theta_j / \min_{x_j \in S_j^{-1}[0,\theta_j]} \bigtriangledown S_j(x_j) \cdot f_j(x_j) \right)} \qquad \forall\ j \neq i. \end{aligned}$$

Using now the hypothesis of inequality (8), we obtain:

$$S_j(x_j(t_1^-)) \geq \theta_j \ \Big(1 - \frac{\min_{i \neq j} \Delta_{ij}}{\max_i \theta_i} \Big) \geq \theta_j - \min_{i \neq j} \Delta_{ij} \qquad \forall\ j \neq i.$$

Since at least the cell i spikes at instant t_1 we have

$$S_j(x_j(t_1^-)) + \sum_{i \in I(t_1),\ i \neq j} \Delta_{ij} \geq S_j(x_j(t_1^-)) + \min_{i \neq j} \Delta_{ij} \geq \theta_j.$$

So, applying the interaction rule (4) we deduce that the cell j spikes at instant t_1. This result holds for all the cells $j \neq i$. Thus, all the cells spike when at least one spikes, ending the proof of Theorem 2.10. □

4. Example

To illustrate Theorems 2.9 and 2.10 we consider the following phenomenon described and mathematically modeled in [10]: the spontaneous synchronization of the step of the walkers on the Millennium footbridge over the River Thames of London, which occurred on June 2000.

On the one hand, in [10] the interaction among the pedestrians was modeled through the acceleration of the lateral bridge displacement, which was itself produced by the sum of the actions of the walkers on the bridge. Nevertheless, this model can be translated to positive interactions that occur directly among the pedestrians, by considering the composition of the actions of the walkers on the bridge with the action of the bridge backwards to the walkers.

On the other hand, in [10] the model is non-impulsive but continuous on time: the mutual interactions are considered as a continuous and differentiable change of the velocity of each pedestrian, which is itself modeled as a one-dimensional oscillator. Nevertheless, one can equivalently substitute this continuous-time model by an integrate-pulsed oscillator. In fact, one can change the state variable artificially to consider each walker's equation as follows: First it is governed by a continuous-time integrator according to its own free dynamics without perturbations. Second, a pulsed action is added to its instantaneous phase. This pulse should be computed as the result of integrating separately the continuous change of its velocity during the prior interval of time.

The results reported by Eckhardt et al. [10] were obtained from the analysis of their mathematical model, to explain the real phenomenon that occurred during the opening of the Millennium bridge: once the number of pedestrians exceeded a critical number and after a waiting time, many started to move in synchronized step. In Figure 4 Eckhardt et al. show the graphics obtained by computer simulation of the steps of 80 walkers, under different interaction weights.

Acknowledgements

We thank the scientific and organizing committees of the IV Coloquio Uruguayo de Matemática for the invitation to give a talk on the subject of this paper. We thank the editors of Publicaciones Matemáticas del Uruguay and the anonymous referees for their valuable suggestions and comments. We thank B. Eckhardt, E. Ott, S.H. Strogatz. D.M. Abrams, A. Mc.Robie for providing the original files of Figure 4. We thank the editors of the journal Physical Review E and the American Physical Society for the permission to reproduce this figure.

References

[1] E. Accinelli, S. London, and E. Sánchez Carrera, *A Model of Imitative Behavior in the Population of Firms and Workers*, Quaderni del Dipartimento di Economia Politica **554**, University of Siena, Siena, 2009

[2] M.F. Bear, B.W. Connors, M.A. Paradiso: *Neuroscience - Exploring the Brain*, 3rd. Edition, Lippincott, Williams & Wilkins, Philadelphia, 2007

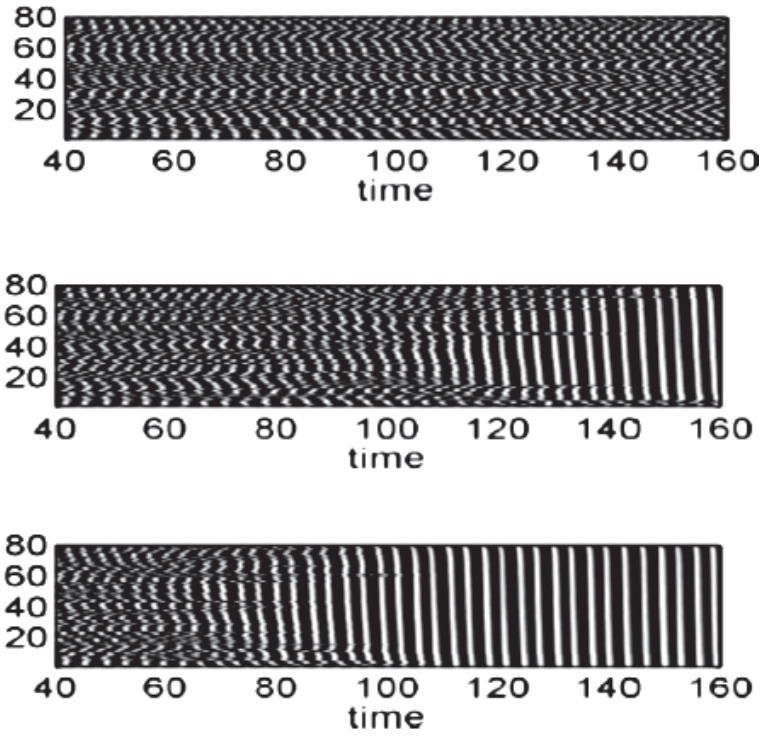


FIGURE 4. Computer simulation of non-synchronized and synchronized step of a group of 80 walkers modeled as identical oscillators. The upper frame corresponds to a low interaction weight. It shows no synchronization within the time interval of observation. The middle frame corresponds to middle interaction weight. It shows almost synchronization (up to a certain deviation) but a rather long waiting time to synchronize. The lower frame corresponds to a large interaction weight. It shows synchronization after a shorter waiting time.

---

[3] S. Bottani, *Synchronization of integrate and fire oscillators with global coupling*, Physical Review E, **54** (1996), 2334–2350 doi: 10.1103/PhysRevE.54.2334

[4] J. Bremont, *Dynamics of injective quasi-contractions*, Erg. Theor. Dyn. Syst. **26** (2006) 19–44

[5] E. Catsigeras: *Dale's Principle is Necessary for an Optimal Neural Network's Dynamics* Appl. Math. (Irvine)**4** (2013) 15–29 doi: 10.4236/am.2013.410A2002

[6] E. Catsigeras and P. Guiraud *Integrate and Fire Neural Networks, Piecewise Contractive Maps and Limit Cycles.* Journ. Math. Biol. **67**(3), (2013) 609–655, doi: 10.1007/s00285-012-0560-7

[7] B. Cessac, *A discrete time neural network model with spiking neurons. Rigorous results on the spontaneous dynamics*, Journ. Math. Biol. **56** (2008) 311–345.

[8] J.R. Chazottes and B. Fernandez (Eds), *Dynamics of coupled map lattices and of related spatially extended systems*, Lecture Notes in Physics **671** Springer Berlin, 2005
[9] R. Coutinho, B. Fernandez, R. Lima and A. Meyroneinc, *Discrete time piecewise affine models of genetic regulatory networks*, Journ. Math. Biol. **52** (2006), 524-570 doi: 10.1007/s00285-005-0359-x
[10] B. Eckhardt, E. Ott, S.H. Strogatz, D.M. Abrams, A. McRobie, *Modeling walker synchronization on the Milennium Bridge* Phys. Rev. E **75** 021110 (2007), pp. 1–10
[11] G.B. Ermentrout, *An adaptive model for syncrhony in the firefly Pteroptyx malaccae* Journ. Math. Biol. **29** (1991), pp. 571–585
[12] G.B. Ermentrout and D.H. Terman, *Mathematical Foundations of Neuroscience.* Springer, 2010
[13] J. Feng, L. Zhu and H. Wang, *Stability of Ecosystem induced by mutual interference between predators*, Procedia Environmental Sciences **2** (2010) 42-48
[14] E.M. Izhikevich, *Dynamical Systems in Neuroscience: The Geometry of Excitability and Bursting.* MIT Press, 2007
[15] N. Jiménez, S. Mihalas, R. Brown, E. Niebur and J. Rubin, *Locally contractive dynamics in generalized integrate-and-fire neuron models* Preprint Johns Hopkins Univ., Univ. of Pittsburgh and Allen Institute for Brain Science, (2013) `http://www.math.pitt.edu/~rubin/pub/pub.html` (Last retrieved February 7th., 2013)
[16] K.K. Lin and L.S. Young, *Shear-induced chaos.* Nonlinearity **21** (2008) 899–922.
[17] K.K. Lin, K.C.A. Wedgwood, S. Coombes and L-S Young, *Limitations of perturbative techniques in the analysis of rhythms and oscillations,* Journal of Mathematical Biology **66** (2013), 139–161
[18] W. Mass and C.M. Bishop (Eds), *Pulsed Neural Networks*, MIT Press, Cambridge, 2001.
[19] I. Milchtaich, *Representation of finite games as network of congestion*, Int. Journ. Game Theory **42** (2013) 1085–1096 doi: 10.1007/s00182-012-0363-5
[20] R.E. Mirollo and S.H. Strogatz, *Synchronization of pulse-coupled biological oscillators*, SIAM J. Appl. Math. **50** (1990) 1645–1662.
[21] A. Pikovsky and Y. Maistrenko (Editors), *Synchronization: Theory and Application*, Kluwer Academic Publ, Dordrecht, 2003.
[22] G.M. Ramírez Ávila, J.L. Guisset and J.L. Deneubourg, *Synchronization in light-controlled oscillators*, Physica D, **182** (2003) 254–273
[23] N. Rubido, C. Cabeza, S. Kahan, G.M. Ramírez Ávila and A. C. Marti, *Synchronization regions of two pulse-coupled electronic piecewise linear oscillators*, Europ. Phys. Journ. D **62** (2011), 51–56 doi: 10.1140/epjd/e2010-00215-4
[24] G.T. Stamov and I. Stamova, *Almost periodic solutions for impulsive neural networks with delay*, Applied Mathematical Modelling **31** (2007) 1263–1270
[25] P. Strata, R. Harvey: *Dale's Principle*, Brain Res. Bull. **50** (5-6) (1999) 349–350 doi:10.1016/S0361-9230(99)00100-8
[26] D.A. Vasseur and J. Fox, *Phase-locking and environmental fluctuations generate synchrony in a predatorprey community*, Nature **460** (2009) Issue 7258, 1007–1010 doi:10.1038/nature08208
[27] W. Wang and J.J.E. Slotine, *On partial contraction analysis for coupled nonlinear oscillators*, Biolog. Cybernetics **92** (2005) 38–53
[28] T. Yang and L.O. Chua, *Impulsive stabilization for control and synchronization of chaotic systems: theory and application to secure communication*, IEEE Trans. Circuits Syst. **44** (1997), 976–988.
[29] X. Yang, C. Huang, Q. Zhu, *Synchronization of swiched neural networks with mixed delays via impulsive control*, Chaos Solit and Frac. **44** (2011), 817–826.

Instituto de Matemática y Estadística Rafael Laguardia (IMERL)
Fac. Ingeniería, Universidad de la República, Uruguay.
E-mail address: `eleonora@fing.edu.uy`

Las Publicaciones Matemáticas del Uruguay (PMU) tienen como objetivo reflejar parte de las actividades de investigación matemática que se lleva a cabo en Uruguay. Nuestro interés es publicar artículos de investigación, así como artículos de tipo survey, anuncios, y otros trabajos que el Consejo Editor considere adecuado.

Los volúmenes no necesariamente serán arbitrados. Esto se indicará cuidadosamente en cada volumen.

Este volumen contiene notas de cursos, y un artículo arbitrado.

The goal of Publicaciones Matemáticas del Uruguay (PMU) is to reflect part of the mathematics research activities taking place in Uruguay. It is our interest to publish research articles, survey-type articles, research announcements and other papers considered suitable by the Editorial Board.

The editorial process may or may not involve a revision by referees. This will be carefully indicated in each volume.

This volume contains course notes, and a peer-reviewed article.

Publicaciones Matemáticas del Uruguay

Volumen 15 Junio 2016