APLICACIONES NO ELEMENTALES DE UN TEOREMA ELEMENTAL

J. ANDRÉS MONTOYA

ABSTRACT. In this brief paper we study some of the most beautiful applications, in Mathematics and Computer Sciences, of an elementary theorem of Polynomial Algebra. This theorem says that a polynomial of degree n has at most n roots in a field.

RESUMEN. En esta breve nota se estudian algunas de las más bellas aplicaciones, en Matemáticas y en Computación teórica, de un teorema elemental del Álgebra de polinomios. Dicho teorema afirma que un polinomio de grado n tiene a lo más n raíces en un campo.

1. INTRODUCCIÓN

El propósito de este trabajo es estudiar la riqueza combinatoria y algunas de las aplicaciones, en Matemáticas y en Computación Teórica, de un teorema elemental del álgebra de polinomios. El Teorema de las Raíces, como lo llamaremos, asegura que dado un campo $\mathbb{F}$, todo polinomio no nulo y de grado menor o igual que n tiene a lo más n raíces en $\mathbb{F}$. Sanjeev Arora, en el prefacio de su tesis doctoral, escribió lo siguiente:

"*Most readers should find that they can understand most of the dissertation on the basis of just the following mantra: A non-zero univariate polynomial of degree d has at most d roots.*"

Lo que puede resultar sorprendente de la afirmación de Arora, es que en su tesis doctoral se enuncia y prueba el Teorema PCP, considerado por algunos expertos, como el teorema mas difícil y el más profundo de la Teoría de la Complejidad Computacional.

La pequeña selección de aplicaciones presentadas en el artículo no pretende ser, y de hecho no es, un catálogo completo de las aplicaciones del Teorema de las Raíces en Matemáticas y en Computación Teórica. En el escrito hemos evitado entrar en detalles, cuando tales detalles se refieren a conceptos técnicos propios o de las Ciencias de la Computación o de áreas especializadas de las Matemáticas, a cambio hemos intentado explicar detalladamente el uso del teorema de las raíces en los argumentos y en las construcciones estudiadas (con ello hemos intentado escribir sólo lo esencial pero detalladamente).

1.1. **Organización del artículo.**

Este articulo está dividido en seis secciones incluyendo la introducción. En la sección 2 se enuncia el teorema de las raíces, se listan algunos de sus corolarios y se estudia la generalización del teorema de las

Key words and phrases. Campos, Anillos de polinomios, Complejidad Computacional, Combinatoria.

raíces al caso de polinomios multivariados. En la sección 3 se estudian algunas aplicaciones elementales del teorema de las raíces en el Álgebra Lineal, la Teoría Elemental de Números, la Teoría de Grupos, la Geometria Algebraica y la Teoria de la Aproximacion. En la sección 4 se estudia una aplicación del teorema de las raíces en combinatoria, específicamente en la construcción de códigos con buenos parámetros. En la sección 5 se estudia el núcleo algebraico de la prueba del teorema PCP, la cual es una ingeniosa aplicación del teorema de las raíces. Finalmente en la última sección se presentan algunas conclusiones.

Notación: Dado Ω un espacio de probabilidad y A un evento, $\Pr_{a\in\Omega}[a \in A]$ denotará la probabilidad de, al escoger al azar un elemento de Ω, escoger un elemento en A. A lo largo del escrito identificaremos a todo campo finito $\mathbb{F}$ con el espacio de probabilidad $(\mathbb{F}, \mu)$, donde μ es la distribución uniforme sobre $\mathbb{F}$.

2. Un viejo teorema revisitado

Dado $\mathbb{F}$ un campo, $\mathbb{F}[X]$ es el anillo de polinomios en la variable X con coeficientes en $\mathbb{F}$ y $\mathbb{F}[X_1, ..., X_n]$ es el anillo de polinomios en las variables $X_1, ..., X_n$ con coeficientes en $\mathbb{F}$. Dado d un número natural $\mathbb{F}_d[X_1, ..., X_n]$ es el conjunto de polinomios de grado total menor o igual que d, es decir el conjunto de los polinomios tales que el grado de cada uno de sus monomios es menor o igual que d. Dado p, el símbolo $gra(p)$ denotará el grado de p. Si p es un polinomio en varias variables, $gra(p)$ denotará el grado total de p.

Teorema 1 (Teorema de la división)**.** *Dados $p, q \in \mathbb{F}[X]$, con $q \neq 0$, existen $h, r \in \mathbb{F}[X]$ tales que*

1. $p = hq + r$.
2. $gra(r) \lneqq gra(q)$.

Corolario 1 (Teorema de las raíces)**.** *Dado $p \in \mathbb{F}[X]$, si $p \neq 0$ y $gra(p) \leq n$, entonces p tiene a lo más n raíces en $\mathbb{F}$.*

Demostración. Sea $a \in \mathbb{F}$ tal que $p(a) = 0$. Del teorema de la división tenemos que $p = h(X - a) + r$, con r constante. Se tiene entonces que $0 = p(a) = r$, esto es $p = h(X - a)$. De igual manera podemos probar que dados $a_1, ..., a_{n+1} \in \mathbb{F}$, $n+1$ elementos de $\mathbb{F}$ distintos dos a dos, si $p(a_1) = ... = p(a_{n+1}) = 0$. Existe entonces $g \in \mathbb{F}[X]$ tal que $p = g \prod_{i\leq n+1} (X - a_i)$. Pero esto último es una contradicción dado que $gra(p) \leq n$. □

Corolario 2. *Dados $p, q \in \mathbb{F}_d[X]$, si $|\{a \in \mathbb{F} : p(a) = q(a)\}| \geq d + 1$, entonces $p = q$.*

Teorema 2 (Interpolación)**.** *Dados $a_0, ..., a_d \in \mathbb{F}$ distintos dos a dos y dados $b_0, ..., b_d \in \mathbb{F}$. Existe un único $p \in \mathbb{F}_d[X]$ tal que $p(a_0) = b_0, ..., p(a_d) = b_d$.*

Demostración. La existencia es consecuencia de la siguiente fórmula de interpolación

$$p(X) = \sum_{0\leq i\leq d} \left(\prod_{j\neq i} \frac{(X - a_j)}{(a_i - a_j)} \right) b_i$$

La unicidad de p es una consecuencia inmediata del teorema de las raíces. □

Para concluir esta sección enunciaremos y probaremos el Teorema de Schwartz-Zippel para campos finitos, el cual es una generalización del teorema de las raíces para polinomios en varias variables.

Teorema 3. *Dado* $p \in \mathbb{F}_d[X_1, ..., X_n]$ *se tiene que* $\Pr_{\overrightarrow{a} \in F^n}[p(\overrightarrow{a}) = 0] \leq \frac{d}{|\mathbb{F}|}$.

Demostración. La prueba es por inducción en n

- El caso $n = 1$ es el teorema de las raíces.
- Dado $p \in \mathbb{F}_d[X_1, ..., X_n]$, p es igual a $\sum_{0 \leq i \leq d} X_n^i (p_i(X_1, ..., X_{n-1}))$, donde cada p_i es un polinomio de grado menor o igual que $d - i$. Si $p \neq 0$, existe un i tal que $p_i \neq 0$. Sea $k := \max\{i : p_i \neq 0\}$. Se tiene que

$$\Pr_{\overrightarrow{a} \in \mathbb{F}^{n-1}}[p_k(\overrightarrow{a}) = 0] \leq \frac{d-k}{|\mathbb{F}|}$$

  Sea ahora $\overrightarrow{a} \in \mathbb{F}^{n-1}$ tal que $p_k(\overrightarrow{a}) \neq 0$, es claro que $p(\overrightarrow{a}, X_n)$ es un polinomio de grado k en la variable X_n, por lo tanto

$$\Pr_{(\overrightarrow{a},a) \in \mathbb{F}^{n-1} \times \mathbb{F}}[p(\overrightarrow{a}, a) = 0] \leq \frac{d-k}{|\mathbb{F}|} \frac{k}{|\mathbb{F}|} \leq \frac{d^2}{|\mathbb{F}|^2}$$

  Para terminar basta notar que:
- Si $d \leq |\mathbb{F}|$, entonces $\frac{d^2}{|\mathbb{F}|^2} \leq \frac{d}{|\mathbb{F}|}$.
- Si $d \geq |\mathbb{F}|$, entonces $\Pr_{\overrightarrow{c} \in \mathbb{F}^n}[p(\overrightarrow{c}) = 0] \leq \frac{d}{|\mathbb{F}|}$.

□

En lo que sigue presentaremos una pequeña selección de aplicaciones del teorema de las raíces, (y de su versión multivariada, el teorema de Schwartz-Zippel), en diversas áreas de la Matemática y la Computación Teórica.

3. Calentamiento: Aplicaciones elementales

En esta sección estudiaremos algunas aplicaciones elementales del teorema de las raíces.

3.1. Aplicaciones en la Teoría de Matrices.

En esta subsección estudiaremos dos aplicaciones elementales del teorema de las raíces en la Teoría de Matrices.

Dados $a_1, ..., a_n$; n números reales distintos dos a dos, la matriz de Vandermonde $M(a_1, ..., a_n)$ es la matriz de $n \times n$ dada por

$$\begin{bmatrix} 1 & a_1 & a_1^2 & ... & a_1^{n-1} \\ 1 & a_2 & a_2^2 & ... & a_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & ... & a_n^{n-1} \end{bmatrix}$$

Un ejercicio típico de un curso de Álgebra Lineal consiste en probar que toda matriz de Vandermonde es invertible. La prueba usual consiste en probar que, para todo n y para toda n-tupla $a_1, ..., a_n$ de números reales distintos dos a dos

$$\det((M(a_1, ..., a_n))) = \prod_{1 \leq i \lneq j \leq n} (a_j - a_i) \neq 0$$

Nosotros presentaremos una prueba elemental basada en el teorema de las raíces. Lo que nosotros probaremos es que para todo n y para toda n-tupla $a_1, ..., a_n$ de números reales distintos dos a dos $N\acute{u}cleo\left(M\left(a_1, ..., a_n\right)\right) = \left\{\overrightarrow{0}\right\}$.

Sea $(b_0, ..., b_{n-1})$ un vector cualquiera de $\mathbb{R}^n$ y sea $p\left(X\right)$ el polinomio

$$p(X) = b_0 + b_1 X + ... + b_{n-1} X^{n-1}$$

Note que

$$\left(M\left(a_1, ..., a_n\right)\right) \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix} = \begin{bmatrix} p\left(a_1\right) \\ p\left(a_2\right) \\ \vdots \\ p\left(a_n\right) \end{bmatrix}$$

Supongamos que $(b_0, ..., b_{n-1}) \in N\acute{u}cleo\left(M\left(a_1, ..., a_n\right)\right)$. Esto implica que $p\left(a_1\right) = 0, ..., p\left(a_n\right) = 0$. Lo cual a su vez implica que el polinomio p de grado $n-1$ tiene al menos n raíces. De lo anterior, **e invocando el teorema de las raices**, podemos concluir que p es el polinomio cero y que por lo tanto, si $(b_0, ..., b_{n-1}) \in N\acute{u}cleo\left(M\left(a_1, ..., a_n\right)\right)$, entonces $(b_0, ..., b_{n-1}) = \overrightarrow{0}$.

En lo que sigue daremos un paso adelante, sean $a_1, ..., a_n$; n números reales distintos y sea $m \lneqq n$. Considere la matriz

$$A = \begin{bmatrix} 1 & a_1 & a_1^2 & \dots & a_1^m \\ 1 & a_2 & a_2^2 & \cdots & a_2^m \\ 1 & a_3 & a_3^2 & \dots & a_3^m \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^m \end{bmatrix}$$

El siguiente teorema es de gran importacia en la Teoría de Aproximación mediante mínimos cuadrados.

Teorema 4. *La matriz $A^T A$ es invertible.*

La prueba de este teorema es muy similar a la prueba del teorema anterior y es, por lo tanto, una nueva aplicación del teorema de las raíces. Note que las matrices de Vandermonde corresponden al caso límite $m = n - 1$ y esto, en términos de aproximación mediante mínimos cuadrados significa que las matrices de Vandermonde corresponden al caso límite de interpolación.

Demostración. Note primero que $A^T A$ es igual a

$$\begin{bmatrix} n & \sum a_i & \sum a_i^2 & \dots & \sum a_i^m \\ \sum a_i & \sum a_i^2 & \sum a_i^3 & \cdots & \sum a_i^{m+1} \\ \sum a_i^2 & \sum a_i^3 & \sum a_i^4 & \dots & \sum a_i^{m+2} \\ \vdots & \vdots & \vdots & & \vdots \\ \sum a_i^m & \sum a_i^{m+1} & \sum a_i^{m+2} & \dots & \sum a_i^{m+m} \end{bmatrix}$$

Sea $v = (b_0, ..., b_m)$ un elemento en el núcleo de $A^T A$ y sea $p(X)$ el polinomio $b_0 + b_1 X + ... + b_m X^m$. Note que $A^T Av$ es igual a

$$\begin{bmatrix} \sum p(a_i) \\ \sum (Xp(X))(a_i) \\ \sum \left(X^2 p(X)\right)(a_i) \\ \vdots \\ \sum (X^m p(X))(a_i) \end{bmatrix}$$

Si v pertenece al núcleo de $A^T A$, entonces $\sum p(a_i) = 0$, $\sum (Xp(X))(a_i) = 0, ...,$ $\sum (X^m p(X))(a_i) = 0$. Esto implica que $p(a_1) = 0, ..., p(a_n) = 0$, y que por lo tanto p tiene al menos n raíces. Ahora, como $gra(p) = m \lneqq n$, **el teorema de las raices implica que el polinomio p es idénticamente cero**, o lo que es lo mismo el vector v es el vector cero. En conclusión, hemos probado que el núcleo de $A^T A$ es trivial, i.e. $A^T A$ es invertible. □

3.2. **Aplicaciones en Teoría de Números.** El teorema de Wilson afirma que, dado p un número primo, $(p-1)!$ es congruente con -1 módulo p. En esta sección presentaremos una prueba elemental de dicho teorema. El argumento final, en la prueba, es una aplicación elemental del teorema de las raíces. Fijemos un primo p. Sea $\otimes$ la operación producto módulo p, esto es, dados $m, n \in \mathbb{N}$, $m \otimes n$ es igual a $(mn) \bmod (p)$. Es un hecho conocido que el par $(\{1, ..., p-1\}, \otimes)$ es un grupo al que suele denotarse con el símbolo $\mathbb{F}_p^*$. Por otro lado es también un hecho conocido que la tripla $(\{1, ..., p-1\}, \otimes, \oplus)$ es un campo al que suele denotarse con el símbolo $\mathbb{F}_p$ ($\oplus$ denota la suma módulo p).

Lema 1. *Dados $n_1, ..., n_m \in \mathbb{N}$, se tiene que* $\left(\prod_{i \leq m} n_i\right) \bmod (p) = \prod_{i \leq m} (n_i \bmod (p))$.

Teorema 5 (Teorema de Wilson)**.** $(p-1)! \equiv -1\,(p)$.

Demostración. $(p-1)! \bmod (p) = \left(\prod_{i \leq p-1} i\right) \bmod (p) = \prod_{i \leq m} (i \bmod (p)) = \bigotimes_{i \leq p-1} i$

Sea $A = \{a \in \mathbb{Z}_p : a \otimes a \neq 1\}$. Note que:

(1) $\bigotimes_{i \in A} i = 1$.

(2) $\bigotimes_{i \leq p-1} p = \left(\bigotimes_{i \in A} i\right) \otimes \left(\bigotimes_{i \notin A} i\right)$.

Tenemos entonces que $\bigotimes_{i \leq p-1} p = \bigotimes_{i \notin A} i$. Note ahora que $A^c = \{a \in \mathbb{Z}_p : p(a) = 0\}$, donde $p(X)$ es el polinomio $X^2 - 1$. **El teorema de las raíces implica que** $|A^c| = 2$, por lo tanto $A^c = \{1, -1\}$ y $\bigotimes_{i \notin A} i = 1 \otimes -1 = -1$. Tenemos entonces que $(p-1)!$ es congruente con -1 módulo p. □

Para finalizar esta seccion estudiaremos un teorema relativo al comportamiento de la funcion aritmetica conocida como *El simbolo de Legendre.* Sea $\mathcal{P}$ el conjunto

de los numeros primos, el simbolo de Legendre es la funcion $(-):\mathbb{N}\times\mathcal{P}\to\mathbb{N}$ definida por

$$\left(\frac{n}{p}\right)=\begin{cases}0 \text{ si } p \text{ divide a } n\\ 1 \text{ si } p \text{ no divide a } n \text{ y } n \text{ es un cuadrado en } \mathbb{F}_p\\ -1 \text{ en otro caso}\end{cases}$$

Teorema 6. *Para todo $n\geq 1$ y para todo $p\in\mathcal{P}-\{2\}$ se tiene que $n^{\frac{p-1}{2}}\equiv\left(\frac{n}{p}\right)\bmod p$.*

Proof. El resultado es obvio cuando p divide a n. Supongamos que p no divide a n. El pequeño teorema de Fermat afirma que $n^{p-1}\equiv 1\bmod p$. Esto implica que $n^{\frac{p-1}{2}}\in\{-1,1\}$ (esto de por si **es un corolario del teorema de las raices**, recuerde la prueba del teorema de Wilson). Suponga que n es un cuadrado en $\mathbb{F}_p$, esto es: suponga que existe m tal que $n\equiv m^2$. Se tiene que $n^{\frac{p-1}{2}}\equiv m^{p-1}\equiv 1\bmod p$, esto es: todo cuadrado en $\mathbb{F}_p$ satisface la ecuacion $n^{\frac{p-1}{2}}\equiv 1\equiv\left(\frac{n}{p}\right)\bmod p$. Suponga que n no es un cuadrado, nosotros sabemos que $n^{\frac{p-1}{2}}\bmod p\in\{1,-1\}$, como queremos probar que $n^{\frac{p-1}{2}}\equiv -1\equiv\left(\frac{n}{p}\right)\bmod p$, lo que debemos probar es que n no es una raiz del polinomio $X^{\frac{p-1}{2}}-1=0$. **El teorema de las raices nos dice que la ecuacion $X^{\frac{p-1}{2}}-1=0$ tiene a lo mas $\frac{p-1}{2}$ raices en $\mathbb{F}_p$.** Todo cuadrado en $\mathbb{F}_p$ es una raiz, y existen $\frac{p-1}{2}$ cuadrados en $\mathbb{F}_p$ es una raiz. Tenemos entonces que el conjunto de raices en $\mathbb{F}_p$ de la ecuacion $X^{\frac{p-1}{2}}-1=0$ es exactamente igual al conjunto de los cuadrados, por lo tanto si n no es un cuadrado $n^{\frac{p-1}{2}}\equiv -1\equiv\left(\frac{n}{p}\right)\bmod p$ y con esto queda probado el teorema □

3.3. **Aplicaciones en Teoría de Grupos.** Un teorema importante de la Teoría de Campos Finitos afirma que si $\mathbb{F}$ es un campo finito, el grupo multiplicativo de $\mathbb{F}$ es cíclico. En esta sección probaremos dicho teorema apoyándonos fuertemente en el teorema de las raíces.

Definición 1 (El tociente de Euler)**.** *Dado $m\geq 1$, la función $\phi:\mathbb{Z}\to\mathbb{Z}$ definida por $\phi(m)=|\{j\leq m: mcd(m,j)=1\}|$ es conocida como el tociente de Euler.*

Teorema 7 (Identidad de Euler)**.** *Para todo $m\geq 1$ se tiene que $m=\sum_{d/m}\phi(d)$.*

La identidad de Euler, el teorema de Lagrange de la Teoría de Grupos y el teorema de la raíces es todo lo que necesitamos para probar el siguiente teorema.

Teorema 8. *Dado $\mathbb{F}$ un campo finito, el grupo multiplicativo de $\mathbb{F}$, que denotaremos con el símbolo $\mathbb{F}^*$, es cíclico.*

Demostración. Sea $m=|\mathbb{F}^*|$. Dado $n\leq m$ se tiene lo siguiente:

- Si n no divide a m, el polinomio X^n-1 no tiene raíces en $\mathbb{F}$ diferentes de 1 (teorema de Lagrange).
- Si n divide a m, **el polinomio X^n-1 tiene a lo más n raíces en F (teorema de las raíces)**.

Sea $n\leq m$ un divisor de m y sea A_n el conjunto $\{a\in\mathbb{F}^*: a^n-1=0\}$. Note que $\mathbb{F}^*=\bigcup_{n/m}A_n$. Note también que para todo n divisor de m el conjunto A_n es en realidad un subgrupo de $\mathbb{F}^*$. Sea $B_n=\{a\in A_n: o(a)=n\}$. Note que

(1) $\mathbb{F}^* = \biguplus B_n$, donde el símbolo $\biguplus$ denota que la unión es disyunta.
(2) $|B_n| \leq \phi(n)$.

Es claro que $\mathbb{F}^*$ es cíclico si y solo si B_m es no vacío. Suponga que B_m es vacío. De 1 y 2 tenemos que

$$m = |\mathbb{F}^*| = \left|\biguplus B_n\right| = \sum_{n/m} |B_n| \leq \sum_{n/m:n\neq m} \phi(n) \lneqq \sum_{n/m} \phi(n) = m$$

Tenemos entonces que B_m es no vacío y que por lo tanto $\mathbb{F}^*$ es un grupo cíclico. □

3.4. **Aplicaciones elementales en Geometría Algebraica.** En esta sección estudiaremos algunas aplicaciones elementales del teorema de las raíces en la Geometria Algebraica.

Definición 2. *Dado $\mathbb{F}$ un campo y dados $p_1, ..., p_n \in \mathbb{F}[X_1, ..., X_k]$, el conjunto $Zero(p_1, ..., p_n)$ es el subconjunto de $\mathbb{F}^k$ definido por*

$$Zero(p_1, ..., p_n) := \left\{\overrightarrow{a} \in \mathbb{F}^k : p_1(\overrightarrow{a}) = 0, ..., p_n(\overrightarrow{a}) = 0\right\}$$

Esto es, el conjunto $Zero(p_1, ..., p_n)$ es el conjunto de los ceros comunes de los polinomios $p_1, ..., p_n$.

El objeto de estudio de la Geometría Algebraica son las variedades algebraicas.

Definición 3. *Un subconjunto V de $\mathbb{F}^k$ es una variedad algebraica en $\mathbb{F}^k$ si y solo si existen polinomios $p_1, ..., p_n \in \mathbb{F}[X_1, ..., X_k]$ tales que $V = Zero(p_1, ..., p_n)$.*

El problema que definiremos a continuación, es un primer y fundamental problema de la Geometría Algebraica.

Problema 1. *(Caracterización de Variedades)*

- *Instancia: $V \subset \mathbb{F}^k$, donde $\mathbb{F}$ es un campo y $k \in \mathbb{N}$.*
- *Problema: Decida si V es una variedad algebraica.*

Si la instancia V del problema es una instancia positiva, es decir si V es una variedad algebraica, la manera canónica de resolver el problema para V es encontrar polinomios $p_1, ..., p_n \in \mathbb{F}[X_1, ..., X_k]$ tales que V es igual a $Zero(p_1, ..., p_n)$, (lo cual no siempre es fácil). Consideremos ahora la otra cara de la moneda, ¿Cómo podemos resolver el problema para V, si V es una instancia negativa? En este caso el teorema de las raíces es, en esencia, la única herramienta disponible.

Definición 4. *Dado $\mathbb{F}$ un campo y dado $k \in \mathbb{N}$, una línea en $\mathbb{F}^k$ es un conjunto $L \subset \mathbb{F}^k$ tal que existen $a_1, ..., a_k, b_1, ..., b_k \in \mathbb{F}$ para los cuales se tiene que*

$$L = \{(a_1 + tb_1, ..., a_k + tb_k) : t \in \mathbb{F}\}$$

Lema 2. *Dado $V \subsetneqq \mathbb{F}^k$, si L es una línea en $\mathbb{F}^k$ y V es una variedad algebraica, entonces $V \cap L$ es finito.*

Demostración. Suponga que existen $p_1, ..., p_n \in \mathbb{F}[X_1, ..., X_k]$ polinomios no nulos y tales que V es igual a $Zero(p_1, ..., p_n)$. Sea L una línea en $\mathbb{F}^k$ determinada por la $2k$ tupla a_1, ... , a_k, b_1, ... , $b_k \in \mathbb{F}$. Note que $(c_1, ..., c_k) \in V \cap L$ si y solo si existe $t_{\overrightarrow{c}} \in \mathbb{F}$ tal que $(c_1, ..., c_k)$ es igual a $(a_1 + t_{\overrightarrow{c}} b_1, ..., a_k + t_{\overrightarrow{c}} b_k)$ y para todo $i \leq n$ se tiene que $\widetilde{p_i}(t_{\overrightarrow{c}}) = 0$, donde dado $i \leq n$, el polinomio $\widetilde{p_i}(X)$ es el polinomio univariado definido por

$$\widetilde{p_i}(X) := p_i(a_1 + Xb_1, ..., a_k + Xb_k)$$

Note que si $V \cap L$ es infinito cada uno de los polinomios $\widetilde{p_i}(X)$ tiene infinitas raíces, **pero esto obviamente contradice al teorema de las raíces** $\square$

Veamos ahora algunos ejemplos de la aplicación del lema. Para empezar probaremos que el conjunto $V := \left\{(x,y) \in \mathbb{R}^2 : y = \sin(x)\right\}$ no es una variedad algebraica, para ello es suficiente notar que la intersección de V y el eje X (¡ el eje X es una linea $\mathbb{R}^2$!) es un conjunto infinito. Consideremos ahora el conjunto

$$U := \left\{(x,y,t) \in \mathbb{R}^3 : x = \cos t \text{ y } y = \sin t\right\}$$

Note que la intersección de U y la línea $\left\{\left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, t\right) : t \in \mathbb{R}\right\}$ es también un conjunto infinito. Por lo tanto U tampoco puede ser una variedad algebraica.

Ejercicio 1. *Pruebe que el conjunto* $\left\{(w,z) \in \mathbb{C}^2 : |w|^2 + |z|^2 = 1\right\}$ *no es una variedad algebraica.*

3.5. **Aplicaciones en teoria de la aproximacion.** La teoria de la aproximacion polinomial [6] es una teoria que estudia la manera en que una funcion continua puede ser aproximada mediante polinomios de grado pequeño.

Dadas $f, g : [a,b] \to \mathbb{R}$ podemos medir la *distancia* entre f y g de la siguiente manera

$$d_{\max[a,b]}(f,g) = \sup\{|f(x) - g(x)| : x \in [a,b]\}$$

Calcular una buena aproximacion polinomial para f significa calcular un polinomio $p(X)$ tal que $d_{\max[a,b]}(f,p)$ sea tan pequeña como sea posible (el teorema de aproximacion de Weirstrass [6] implica que, si f es continua, es posible calcular aproximaciones polinomiales a f tan ajustadas como sea necesario).

Dada $f : [a,b] \to \mathbb{R}$ una funcion continua, una manera ingenua de calcular una aproximacion polinomial para f consiste en escoger $a_1, ..., a_n \in [a,b]$, y usar interpolacion (i.e. **usar el teorema de las raices**) para calcular un polinomio $p(X)$ que satisfaga las ecuaciones

$$p(a_i) = f(a_i) \text{ con } i = 1, ..., n$$

La intuicion nos dice que, si queremos calcular una mejor aproximacion basta con escoger mas puntos en el intervalo $[a,b]$ (i.e. basta con interpolar usando mas informacion). Tal intuicion, como suele suceder en matematicas, es falsa. La razon es que si aumentamos el numero de puntos sin usar una estrategia inteligente para escogerlos, terminamos calculando, con probabilidad 1, un polinomio $q(X)$ de grado muy alto que coincide con f en muchos puntos, pero que oscila *salvajemente*, lo que le permite alejarse *salvajemente* de f en algunos puntos del intervalo $[a,b]$, haciendo que $d_{\max[a,b]}(f,q)$ sea muy grande. De lo que se trata entonces no es de escoger muchos puntos sino de escogerlos inteligemente. Este es precisamente el contenido del teorema de Chebyshev, que probaremos en esta seccion. El teorema de Chebyshev es uno de los teorema fundamentales de la teoria de la aproximacion polinomial [6]. El teorema nos dice como, dado $n \geq 1$, escoger n puntos $x_1, ..., x_n \in [-1,1]$ de manera tal que la cantidad

$$\max\{|(x - x_1)...(x - x_n)| : x \in [-1,1]\}$$

sea tan pequeña como sea posible. La razon por la cual este teorema es importante en la teoria de la aproximacion polinomial, es porque dado $p(X)$ un polinomio

obtenido usando interpolacion y las ecuaciones $p(a_1) = f(a_1), ..., p(a_n) = f(a_n)$, la desigualdad

$$d_{\max[-1,1]}(f,q) \leq \frac{f^n(c)}{n!}\left(\max\left\{|(x-a_1)...(x-a_n)| : x \in [-1,1]\right\}\right)$$

es valida, para al menos un c en el intervalo $[-1,1]$. Si quiseramos calcular la mejor aproximacion posible a f, usando interpolacion y a lo mas n ecuaciones, lo que deberiamos hacer es encontrar una tupla $a_1, ..., a_n \in [-1,1]$ que minimize la cantidad $\max\left\{|(x-a_1)...(x-a_n)| : x \in [-1,1]\right\}$.

Teorema 9. *(Teorema de aproximacion de Chebyshev)*
Dado $n \geq 1$, la eleccion de numeros reales $a_1, ..., a_n \in [-1,1]$ que minimiza la cantidad

$$\max\left\{|(x-a_1)...(x-a_n)| : x \in [-1,1]\right\}$$

es

$$a_i = \cos\left(\frac{(2i-1)n}{2n}\right),\ i = 1, ..., n$$

Nota 1. *Es importante señalar que la aplicabilidad del teorema de Chebyshev no se reduce a la paroximacion de funciones continuas definidas en el intervalo $[-1,1]$. El mismo teorema puede ser usado, cuando se estudian aproximaciones a funciones continuas definidas sobre otros intervalos compactos, para ello es suficiente realizar un apropiado cambio de variables.*

Nota 2. *La prueba del teorema, que presentaremos a continuacion, se basa en algunas propiedades elementales de los polinomios de Chebyshev* [6]*, en algunos hechos elementales del analisis real, y por supuesto* ***en el teorema de las raices****, para ser mas especificos podriamos decir que la prueba se basa en un corolario del teorema de las raices, que llamaremos el teorema de cambio de signo, y que enunciaremos y probaremos a continuacion.*

Usaremos el simbolo *sign* para denotar la funcion de variable real definida por:

$$sign(x) = \begin{cases} 1 \text{ si } x \gneqq 0 \\ 0 \text{ si } x \leq 0 \end{cases}$$

Teorema 10. *(Teorema del cambio de signo)*
Sea $p(X)$ un polinomio real y sea $a_1 \lneqq a_2 \lneqq ... \lneqq a_{n+1}$ una secuencia estrictamente creciente de numeros reales tal que $1 = sign(a_1) \neq sign(a_2) \neq ... \neq sign(a_{n+1})$. Se tiene que el grado de $p(X)$ esta acotado inferiormente por n.

Proof. El teorema del valor intermedio (teorema de Bolzano) implica que existen $b_1, ..., b_n$ numeros reales tales que

(1) Para todo $i \leq n$ se tiene que $a_i \lneqq b_i \leq a_{i+1}$.
(2) Para todo $i \leq n$ se tiene que $p(b_i) = 0$.

Los dos hechos anteriores implican que $p(X)$ tiene al menos n raices en el campo $\mathbb{R}$, y esto implica (**el teorema de las raices implica**) que el grado de $p(X)$ es al menos n □

Ya estamos listos para presentar un esbozo de la prueba del teorema de Chebyshev.

Proof. (del teorema 9) Defina el n-esimo polinomio de Chebyshev mediante la ecuacion

$$T_n(X) = \cos\left(n\cos^{-1}(X)\right)$$

T_n es un polinomio de grado n cuyo coeficiente lider es 2^{n-1}. Sean $x_1, ..., x_n$ los ceros de $T_n(x)$, es facil ver que

$$x_i = \cos\left(\frac{(2i-1)\,n}{2n}\right)$$

Adicionalmente se tiene que

$$|(x-x_1)...(x-x_n)| \leq \frac{1}{2^{n-1}}$$

Suponga que existen $y_1, ..., y_n \in [-1,1]$ tales que

$$|(x-y_1)...(x-y_n)| \lneqq \frac{1}{2^{n-1}}$$

Y sea $P(X)$ el polinomio obtenido al interpolar usando las ecuaciones $P(y_1) = f(y_1), ..., P(y_n) = f(y_n)$. Se tiene que

- El termino lider de $P(X)$ es X^n (i.e. $P(X)$ es un polinomio monico de grado n).
- Para todo $x \in [-1,1]$ se tiene que $|P(x)| \lneqq \frac{1}{2^{n-1}}$.

Defina $F(X) = P(X) - \frac{T_n(X)}{2^{n-1}}$. Es claro que el grado de $F(X)$ esta acotado superiormente por $n-1$. Note que

$$\begin{aligned}
F(1) &= P(1) - \frac{1}{2^{n-1}} \lneqq 0 \\
F\left(\cos\left(\frac{\pi}{n}\right)\right) &= P\left(\cos\left(\frac{\pi}{n}\right)\right) + \frac{1}{2^{n-1}} \gneqq 0 \\
F\left(\cos\left(\frac{2\pi}{n}\right)\right) &= P\left(\cos\left(\frac{2\pi}{n}\right)\right) - \frac{1}{2^{n-1}} \lneqq 0 \\
&\vdots \\
F\left(\cos\left(\frac{n\pi}{n}\right)\right) &= P\left(\cos\left(\frac{n\pi}{n}\right)\right) + (-1)^{n+1}\frac{1}{2^{n-1}}
\end{aligned}$$

Se tiene entonces que, en el intervalo $[-1,1]$, el polinomio $F(X)$ experimenta al menos $n+1$ cambios de signo, esto implica que $F(X)$ tiene al menos n ceros. El teorema del cambio de signo implica (**El teorema de las raices implica)** que el grado de $F(X)$ es al menos n, pero esto es una contradiccion dado que el grado de $F(X)$ esta acotado superiormente por $n-1$. □

4. Acercándose al núcleo: aplicaciones en Combinatoria

En esta sección estudiaremos algunas aplicaciones en Combinatoria del teorema de las raíces.

4.1. **Códigos lineales.**

Una manera (digamos combinatorialista) de ver el teorema de las raíces es la siguiente: Dado $d \in \mathbb{N}$ y dado $\mathbb{F}$ un campo suficientemente grande, los elementos de $\mathbb{F}_d[X]$ son objetos muy distintos (o muy distantes) los unos de los otros. Dado que dos elementos distintos de $\mathbb{F}_d[X]$ coinciden a lo más en d puntos de $\mathbb{F}$.

Podemos precisar la anterior afirmación de la siguiente manera. Dados $p, q \in \mathbb{F}_d[X]$, la distancia entre p y q se define como $d(p,q) := |\{a \in \mathbb{F} : p(a) \neq q(a)\}|$.

Note que dados $p, q \in \mathbb{F}_d[X]$, si $p \neq q$, entonces $d(p,q) \geq |\mathbb{F}| - d$. (¡Los objetos de $\mathbb{F}_d[X]$ son muy distantes entre si!).

Esta manera combinatorialista de pensar el teorema de las raíces puede ser felizmente aplicada en la construcción de ciertos objetos combinatorios. En esta sección estudiaremos la construcción de códigos lineales con buenos parámetros. Tal construcción se basa completamente en el teorema de las raíces.

Los códigos lineales son artificios matemáticos usados en los sistemas de transmisión de información para detectar y corregir los errores que puedan ocurrir durante la transmisión de dicha información. La Teoría de Códigos Lineales se remonta al trabajo pionero de Shannon [9] quien además de proponer el uso de códigos lineales para tales fines probó la existencia de buenos códigos.

Sea m un número natural que es potencia de un número primo y sea $\mathbb{F}$ el campo de Galois $\mathbb{F}_m$, i.e. el campo finito con m elementos.

Definición 5 (Código lineal)**.** *Un $[k, n, d, m]$ código lineal es un subespacio vectorial E de $\mathbb{F}^n$ tal que:*

(1) $\dim(E) = k$.
(2) Para todo $v \in E$ se tiene que $||v|| \geq d$. Donde $||v|| := |\{i \leq n : v_i \neq 0\}|$.

Lema 3 (Reed-Solomon)**.** *Sean d, k, n, m numeros naturales, si*

(1) $d + k = n + 1 \lneqq m$.
(2) $m = p^r$ *para algún r y algún primo p.*

Es entonces posible construir velozmente un $[k, n, d, m]$ código.

Demostración. El anillo $\mathbb{F}_d[X]$ es un espacio vectorial sobre $\mathbb{F}$ de dimensión d. Dados $a_1, ..., a_n \in \mathbb{F}$, distintos dos a dos, $ev_{a_1,...,a_n} : \mathbb{F}_{k-1}[X] \to \mathbb{F}^n$ es la transformación lineal definida por

$$ev_{a_1,...,a_n}(p) := (p(a_1), ..., p(a_n))$$

Suponga ahora que $k \leq n$. Note que $ev_{a_1,...,a_n}$ satisface:

(1) Es inyectiva, **lo cual es consecuencia del teorema de las raíces** y lo cual implica que E, la imagen de $ev_{a_1,...,a_n}$, es un subespacio de $\mathbb{F}^n$ de dimensión k.
(2) Para todo $v \in E$, si $u \neq v$ se tiene que $||v|| \geq n - k + 1$. **Es fácil verificar esto último usando nuevamente el teorema de las raíces.**

De lo anterior se tiene que E es un $[k, n, d, m]$ código lineal sobre $\mathbb{F}$. □

Es importante anotar que los códigos óptimos de Reed-Solomon (óptimos dado que satisfacen la igualdad $d + k = n + 1$), construidos en la prueba, son los códigos algebraicos usados en la construcción del software corrector de errores que se utiliza por ejemplo en los procesos de grabación de la firma Phillips. El lector interesado en obtener más información acerca de códigos lineales y códigos de Reed-Solomon puede consultar [9].

Sea $m = p^s$ con p primo, dado E un $[d, k, n, m]$ código lineal, el código E está determinado por una tranformación lineal T de $\mathbb{F}^k$ en $\mathbb{F}^n$ tal que

(1) El rango de T es igual a k.
(2) Para todo $u, v \in \mathbb{F}^k$ se tiene que $\|T(u - v)\| \geq d$.

(3) E es igual a $\mathrm{Im}(T)$.

La función T es llamada **función de codificación** de E. Dado E un $[d,k,n,m]$ código lineal definido por una función de codificación T, es importante poder decodificar el código, es decir, poder encontrar algoritmos veloces M y N que resuelvan el siguiente par de problemas:

Problema 2 (Detección de errores)**.** *Sea E un $[k,n,d,m]$ código lineal sobre el campo $\mathbb{F}$, dado por una función de codificación T.*

- *Input: $u \in \mathbb{F}^n$.*
- *Problema: Decida si u es $\frac{d}{n}-$**cercano** a algún $v \in \mathrm{Im}(T)$, es decir, decida si existe $w \in \mathbb{F}^k$ tal que $\|u - T(w)\| \leq d$.*

Problema 3 (Corrección de errores)**.** *Sea E un $[d,k,n,m]$ código lineal E, sobre el campo finito $\mathbb{F}$, dado por una función de codificación T.*

- *Input: $u \in \mathbb{F}^n$.*
- *Problema: Si u es $\frac{d}{2n}-$**cercano** a un $v \in \mathrm{Im}(T)$, calcule v.*

La buena noticia es que los códigos de Reed-Soloman son decodificables. Una tal decodificación será estudiada en la última sección de este escrito (ya se imaginará el lector en que teorema elemental basaremos la construcción de dicho algoritmo decodificador).

Una generalización de los códigos de Reed-Solomon son los códigos de Reed-Muller, en los cuales se utilizan polinomios en varias variables, a cambio de los polinomios en una variable, usados en la construcción de los primeros. A continuación estudiaremos la construcción de los códigos de Reed-Muller en dos variables y algunas de sus propiedades

Sean $\mathbb{F}$ el campo finito con m elementos, $k = r^2$ y $m \geq r+1$. La función de codificación T tiene por dominio a $\mathbb{F}^k$, o equivalentemente, podemos considerar que la función de codificación tiene por dominio a $\mathbb{F}_r[X_1, X_2]$. Dado $p \in \mathbb{F}_r[X_1, X_2]$, tenemos que $T(p) := \langle p(\alpha,\beta)\rangle_{\alpha,\beta\in\mathbb{F}}$. Es claro que T es una transformación lineal de $\mathbb{F}^k$ en $\mathbb{F}^n$ con $n = m^2$. Además, dado que $\mathrm{Pr}_{\alpha,\beta\in\mathbb{F}}[p(\alpha,\beta) = 0] \leq \frac{r}{m}$ (teorema de las raíces versión multivariada) y $r \lneqq m$, se tiene que la función T es inyectiva. Nos queda por estimar el parámetro d, para ello podemos usar nuevamente el teorema de Scharwtz-Zippel. Dados $p, q \in \mathbb{F}_r[X_1, X_2]$, se tiene que $\mathrm{Pr}_{\alpha,\beta\in\mathbb{F}}[p(\alpha,\beta) = q(\alpha,\beta)] \leq \frac{r}{m}$ y esto implica a su vez que $\|p - q\| \geq (m-r)\cdot r$.

Los códigos de Reed-Muller, a diferencia de los códigos de Reed-Solomon, no optimizan el parámetro d, pero también a diferencia de estos, requieren vocabularios pequeños, donde el vocabulario de un código E es el campo $\mathbb{F}$ sobre el cual el código es construido, o lo que es lo mismo, el campo $\mathbb{F}$ respecto al cual consideramos a E como un espacio vectorial. En este punto, debe ser claro para el lector, como se construyen los códigos de Reed-Muller en n variables, para todo $n \geq 2$.

5. Clímax: aplicaciones en la Teoría de Algoritmos

En esta sección, la última del escrito, estudiaremos algunas aplicaciones del teorema de las raíces en la Teoría de Algoritmos. Las aplicaciones que estudiaremos están relacionadas con la decodificación de códigos algebraicos y la prueba del teorema PCP. Lo dijimos al comienzo y lo repetimos en este momento, las aplicaciones del teorema de las raíces incluidas en este escrito no constituyen (y están muy lejos de hacerlo), un catálogo exhaustivo de las aplicaciones del teorema de

las raíces. Este también es el caso en lo referente a las aplicaciones del teorema de las raíces en Computación Teórica. En este punto nos parece importante listar algunas de las aplicaciones, que pese a su importancia, no serán estudiadas en lo que resta del escrito.

(1) Algoritmos probabilísticos para Matching y para verificación de identidades algebraicas [5].
(2) Algoritmos interactivos para la permanente [4].
(3) Algoritmos de autocorrección y autoverificación [3].
(4) La prueba del teorema de Agrawal-Kayal-Saxena asegurando que el problema de reconocimento de primos está en P [2].

5.1. **El teorema PCP.** El Teorema PCP es uno de los teoremas más profundos de la Complejidad Computacional. El teorema PCP afirma que, todo problema $L \in NP$, tiene una verificación probabilística veloz, (¡en tiempo constante!). En esta sección no intentaremos profundizar en él, e incluso evitaremos enunciarlo de manera precisa, dado que esto está más allá de los alcances de este escrito. El lector interesado en obtener más información al respecto puede consultar [1]. En esta sección estudiaremos el que consideramos el núcleo algebraico de la prueba del teorema. Este núcleo, aunque puesto fuera de contexto, es una interesante aplicación del teorema de las raíces, aplicación que es de interés en sí misma, dado que corresponde a la decodificación de los códigos de Reed-Muller.

Las soluciones algorítmicas a los problemas de detección y corrección de errores que estudiaremos en lo que queda del escrito, son algoritmos probabilísticos [5].

En adelante fijaremos un campo finito $\mathbb{F}$. Dados $p, q : \mathbb{F}^n \to \mathbb{F}$ y $\delta \gneqq 0$. Diremos que p y q son δ–**cercanos** si y solo si $\Pr_{a \in \mathbb{F}^n} [p(a) \neq q(a)] \leq \delta$.

El núcleo algebraico de la prueba del teorema PCP consiste en el diseño de algoritmos probabilísticos veloces, que usan pocos bits aleatorios y que resuelven el siguiente par de problemas computacionales.

Problema 4. *(Low degree testing)*

- *Input:* $(\mathbb{F}, f : \mathbb{F}^n \to \mathbb{F}, d, \delta)$*, donde* $\mathbb{F}$ *es un campo finito;* $n, d \in \mathbb{N}$ *y* $\delta \in (0, 1)$.
- *Problema: Decida si* f *es* δ*-cercana a algún polinomio de grado total a lo más* d.

Note que si f es δ–cercana a dos polinomios p y q de grado a lo más d y $1 - 2\delta \gneqq \frac{d}{|\mathbb{F}|}$, entonces $p = q$.

Problema 5. *(Self correcting)*

- *Input:* $(\mathbb{F}, f : \mathbb{F}^n \to \mathbb{F}, d, a, \delta)$*, donde* $\mathbb{F}$ *es un campo finito;* $a \in \mathbb{F}^n$; $n, d \in \mathbb{N}$ *y* $0 \gneqq \delta \gneqq \frac{|\mathbb{F}|-d}{2|\mathbb{F}|}$.
- *Problema: Si* f *es* δ*-cercana a algún polinomio* p *de grado total a lo más* d*, (note que en caso afirmativo* p *es único) calcule* $p(a)$.

Es importante notar que los dos problemas anteriores corresponden a los problemas de detección y corrección de errores asociados a los códigos de Reed-Muller.

Es un poco más que sorprendente que existan algoritmos probabilístiscos que resuelven estos problemas cuyo tiempo de cómputo es polinomial en $|\mathbb{F}|^n$ y que sólo utilizan $O(n \log(|\mathbb{F}|))$ bits aleatorios. Más sorprendente aún es que estos algoritmos sólo sean una inteligente aplicación del teorema de las raíces.

5.1.1. *Decodificación de los códigos de Reed-Solomon y de Reed-Muller.* Al final del parágrafo anterior hacíamos notar que, existe una profunda relación entre los problemas *Low-degree Testing y Self-correcting* y los problemas de detección y de corrección de errores asociados a los códigos de Reed-Muller. En esta subsección analizaremos la decodificación de los códigos de Reed-Solomon y de Reed-Muller, derivando tal decodificación de una propiedad de los polinomios que llamaremos **autoreducibilidad – aleatoria**, *aa* para abreviar, y que es consecuencia del Teorema de las raíces.

El problema de la decodificación de los códigos de Reed-Solomon, puede ser entendido de la siguiente manera. Suponga que nosotros contamos con un algoritmo M, el cual supuestamente, con input $a \in \mathbb{F}$, calcula $p(a)$, donde p es algún polinomio de grado menor o igual que d. Suponga además que por alguna razón, nosotros no confiamos en la corrección del algoritmo y por ello quisieramos primero verificar, que la función calculada por M es δ–cercana a algún polinomio de grado menor o igual que d, habiendo elegido un δ tal que $0 \lneqq \delta \lneqq \frac{|\mathbb{F}|-d}{2|\mathbb{F}|}$. Recuerde que si la función calculada por M es δ–cercana a un polinomio de grado menor o igual que d, debido a la elección del δ, lo es a un único polinomio de tal grado (Teorema de las raíces).

Sea p tal que $\Pr_{a\in\mathbb{F}}[p(a) \neq M(a)] \leq \delta$, donde $M(a)$ es el output de M con input $a \in \mathbb{F}$. Note que:

$$\Pr_{a_1,\ldots,a_{d+1}\in\mathbb{F}}\left[\bigwedge_{i\leq d+1} p(a) = M(a)\right] \geq (1-\delta)^{d+1}.$$

Esto sugiere una solución algorítmica al problema de verificación antes propuesto.

Algoritmo 1. *(RS-Detector de errores)*

(1) *Elija al azar* $a_1, \ldots, a_{d+1}, a \in \mathbb{F}$.
(2) *Calcule* $M(a_1), \ldots, M(a_{d+1})$.
(3) *Usando interpolación calcule el único polinomio* h *de grado menor o igual que* d *tal que* $h(a_1) = M(a_1)$ *y* ... *y* $h(a_{d+1}) = M(a_{d+1})$.
(4) *Calcule* $M(a)$ *y* $h(a)$.
(5) *Si* $M(a) = h(a)$ *acepte a* M*, en caso contrario rechace a* M.

El algoritmo que acabamos de presentar es probabilísticamente correcto y su corrección es consecuencia de lo que llamaremos la autorreducibilidad aleatoria de los polinomios.

Definición 6 (Autorreducibilidad aleatoria)**.** *Sea* Ω *un conjunto y* $\mathcal{F}$ *una colección de funciones con dominio* Ω*, la colección* $\mathcal{F}$ *tiene la propiedad* $aa(d)$ *si y solo si para todo* $a \in \Omega$*, toda* $f \in \mathcal{F}$ *y toda escogencia aleatoria de* $a_1, \ldots a_{d+1}$*;* $d+1$ *elementos de* Ω *distintos dos a dos, el valor de* f *en* a *puede ser calculado usando únicamente la tupla* $(f(a_1), \ldots, f(a_{d+1}))$*, (esto es, sin conocer una definición analítica o algebraica de* f*).*

Es claro que, para todo campo $\mathbb{F}$ y todo $d \in \mathbb{N}$, la familia $\mathcal{F} = \mathbb{F}^d[X]$ tiene la propiedad $aa(d)$ (naturalmente como consecuencia del Teorema de las raíces). Tras verificar que el algoritmo M calcula una función δ–cercana a un único polinomio p de grado menor o igual que d, quisiéramos corregir el algoritmo M, es decir, quisiéramos poder calcular $p(a)$, dado cualquier $a \in \mathbb{F}$. Aunque esto suene a magia negra, (nosotros no conocemos el polinomio p y tan solo conocemos una versión corrupta de p, esto es, la función calculada por el algoritmo M), es posible diseñar

un algoritmo probabilísticamente correcto que resuelva, velozmente y usando pocos bits aleatorios, este problema de corrección.

Algoritmo 2. *(RS-Corrector de errores)*

- *Input:* (a, M^*). *Donde* $a \in \mathbb{F}$ *y* M^* *es el código del algoritmo* M.
- *Tarea: Calcular* $p(a)$.
  (1) *Elija al azar* $a_1, \ldots, a_{d+1} \in \mathbb{F}$.
  (2) *Usando* M^* *Calcule* $M(a_1), \ldots, M(a_{d+1})$.
  (3) *Usando interpolación calcule el único polinomio* h *de grado menor o igual que* d *tal que* $h(a_1) = M(a_1)$ *y ... y* $h(a_{d+1}) = M(a_{d+1})$.
  (4) *Calcule* $c := h(a)$.
  (5) *Imprima* c.

Teorema 11. *Los algoritmos RS-detector de errores y RS-corrector de errores son probabilísticamente correctos.*

Para una prueba el lector puede consultar [**?**]. Es importante anotar que existen decodificadores deterministas de los códigos de Reed-Solomon, un famoso ejemplo es el algoritmo decodificador de Berlekamp y Welch [**?**], pero también es importante anotar que no se conocen decodificadores deterministas eficientes de los códigos de Reed-Muller. En lo que sigue mostraremos como adaptar las ideas anteriores para el caso de los códigos de Reed-Muller.

Lema 4. *Dado* $f \in \mathbb{F}[X_1, \ldots, X_n]$. *El grado de* f *en cada variable es menor o igual que* d *si y solo si para todo* $\beta_1, \ldots, \beta_n \in F$ *y todo* $i \leq n$, *la función* $f_{i,\beta}(X_i)$ *definida por:*

$$f_{i,\beta}(X_i) = f\left(\beta_1, \ldots, \beta_{i-1}, X_i, \beta_{i+1}, \ldots, \beta_n\right)$$

Es un polinomio en X_i *de grado a lo más* d.

Demostración. Una de las dos implicaciones es obvia, probaremos la otra.

La prueba es por inducción en n.

El caso $n = 1$ es inmediato.

Sea $f \in \mathbb{F}[X_1, \ldots, X_n]$, tal que para todo $\beta_1, \ldots, \beta_n \in \mathbb{F}$ y todo $i \leq n$, la función

$$f_{i,\beta}(X_i) := f\left(\beta_1, \ldots, \beta_{i-1}, X_i, \beta_{i+1}, \ldots, \beta_n\right)$$

es un polinomio en X_i de grado a lo más d. Dado i, $0 \leq i \leq d$, la función $F_i(X_1, \ldots, X_{n-1})$ es el polinomio $f(X_1, \ldots, X_{n-1}, i)$.

La hipótesis de inducción implica que para todo $i \leq d$, el grado de F_i en cada variable es menor o igual que d. Sea δ^i el único polinomio de grado d, tal que para todo $j \leq d$, se tiene que $\delta^i(j) = \delta_{ij}$. Sea h la función

$$\sum_{0 \leq i \leq d} \delta^i(X_m) F_i(X_1, \ldots, X_{n-1})$$

Es claro que el grado de h en cada variable es menor o igual que d. Veamos ahora que f y h son iguales. Fijemos $\beta_1, \ldots, \beta_{n-1} \in \mathbb{F}$. Tenemos que $f\left(\beta_1, \ldots, \beta_{n-1}, X_n\right)$ y $h\left(\beta_1, \ldots, \beta_{n-1}, X_n\right)$ son polinomios de grado d en la variable X_n, además, para todo j tal que $0 \leq j \leq d$, se tiene la igualdad

$$h\left(\beta_1, \ldots, \beta_{n-1}, j\right) = f\left(\beta_1, \ldots, \beta_{n-1}, j\right)$$

En este punto podemos invocar el Teorema de las raíces y concluir que las funciones $f\left(\beta_1, \ldots, \beta_{n-1}, X_n\right)$ y $h\left(\beta_1, \ldots, \beta_{n-1}, X_n\right)$ son uno y el mismo

polinomio en la variable X_n. Tenemos entonces que, para todo $\beta_1, \ldots, \beta_{n-1} \in \mathbb{F}$ y todo $\beta \in \mathbb{F}$, se satisface la ecuación

$$f\left(\beta_1, \ldots, \beta_{n-1}, \beta\right) = h\left(\beta_1, \ldots, \beta_{n-1}, \beta\right)$$

Con lo cual podemos dar por probado el teorema. □

Dados $a, b \in \mathbb{F}^n$ y $p \in \mathbb{F}[X_1, \ldots, X_n]$, definimos una función $p_{a,b} : \mathbb{F} \to \mathbb{F}$ de la siguiente manera: $p_{a,b}(t) := p(a + tb)$.

Teorema 12. *Dado $p \in \mathbb{F}[X_1, ..., X_n]$ y dado $d \in \mathbb{N}$, tenemos que p es un polinomio de grado a lo más d si y solo si para todo $a, b \in \mathbb{F}^n$ se tiene que $p_{a,b}(t)$ es un polinomio de grado a lo más d.*

Demostración. Una de las dos direcciones es obvia, probaremos la otra.

La prueba es por inducción en n.

El caso $n = 1$ es trivial.

Sea $p \in \mathbb{F}[X_1, \ldots, X_n]$, tal que, para todo par $a, b \in \mathbb{F}^n$, se tiene que $p_{a,b}$ es un polinomio de grado menor o igual que d. Dado $\alpha \in \mathbb{F}$, el grado total del polinomio $p(X_1, \ldots, X_{n-1}, \alpha)$ es menor o igual que d (hipótesis de inducción). En consecuencia el grado total de p es menor o igual que $2d$. Sea $d^* \leq 2d$ el grado total de p. Supongamos que $d^* \gneqq d$. Dado $(c_1, \ldots, c_n) \in \mathbb{F}^n$, la función $f : \mathbb{F} \to \mathbb{F}$, definida por:

$$f(t) : = p(tc_1, \ldots, tc_n), \text{ para todo } t \in \mathbb{F}$$

Es un polinomio de grado d^* cuyo coeficiente director es un polinomio $q(c_1, \ldots, c_n)$ de grado a lo más d^*. Tenemos entonces que:

$$\Pr_{\vec{c} \in \mathbb{F}^n}\left[q(c) \neq 0\right] \geq 1 - \frac{d^*}{\mathbb{F}} \gneqq 0$$

Lo anterior nos permite elegir un $c \in \mathbb{F}^n$, tal que $q(c) \neq 0$. Con esto hemos llegado a una contradicción, dado que la función $p_{0,c}$ es un polinomio de grado $d^* \gneqq d$. □

El teorema anterior sugiere un algoritmo probabilístico M para el problema *Low degree Testing (RM-Detección de errores).*

Sea M el siguiente algoritmo

Algoritmo 3. *Con input* $(\mathbb{F},\ f : \mathbb{F}^n \to \mathbb{F},\ d)$

1. *M escoge uniformemente al azar $a, b \in \mathbb{F}^n$ y $t_0 \in \mathbb{F}$.*
2. *Usando interpolación M calcula el polinomio q que coincide con $f_{a,b}$ en los puntos $1, \ldots, d + 1$.*
3. *M verifica que $f_{a,b}(t)$ y $q(t)$ coinciden.*

Note que el número de bits aleatorios empleados por M es $O(n \log(|\mathbb{F}|))$.

Teorema 13. *M es probabilísticamente correcto y su tiempo de cómputo es polinomial en $|\mathbb{F}|$.*

La prueba del teorema anterior puede ser consultada en [1] o en [**?**].

Con las herramientas ahora disponibles, podemos diseñar también, un algoritmo para el problema *Self-correcting.* Sea N el siguiente algoritmo

Algoritmo 4. *Con input* $(\mathbb{F},\ f : \mathbb{F}^n \to \mathbb{F}, d, a, \delta)$

1. *N escoge uniformemente al azar $b \in \mathbb{F}^n$.*

(2) *N calcula* $f(a+b), \ldots, f(a+(d+1)b)$.
(3) *Usando interpolación N encuentra h, el único polinomio de grado a lo más d tal que* $f(a+b) = h(1), \ldots, f(a+(d+1)b) = h(d+1)$.
(4) *N calcula* $h(0)$.

Note que el número de bits aleatorios empleados por N es $O(n \log(|\mathbb{F}|))$.

Teorema 14. *N es probabilísticamente correcto y su tiempo de cómputo es polinomial en* $|\mathbb{F}|$.

La prueba del teorema anterior puede ser consultada en [1] o en [**?**].

6. Conclusión

Más que cerrar con una conclusión, cerramos con una moraleja.

> *Nunca desprecies un teorema, ya que, incluso aquellos que parecen pequeños e insignificantes pueden contener a un gigante.*

Referencias

[1] **S. Arora.** *Probabilistic Cheking of proofs and the Hardness of approximation problems.* PhD thesis, University of California at Berkeley, August 1994.
[2] **A. Agrawal, N. Saxena and N. Kayal.** *PRIMES is in P. Annals of Mathematics.* **160** (2004), 781-793.
[3] **M. Blum, M. Luby and R. Rubinfeld.** *Self-testing/correcting with applications to numerical problems.* Journal of Computer and Systems Science. **47** (1993), 549-595.
[4] **C. Lund et al.** *Algebraic methods for interactive proof systems.* Journal of the ACM **39** (1992), 859-868.
[5] **C. Papadimitriou.** *Computational Complexity.* Addison-Wesley, NY, 1994.
[6] **T. Rivlin.** *Chebyshev Polynomials: From approximation theory to algebra and number theory.* Second edition. Pure and Applied Mathematics. John Wiley & Sons, Inc., New York, 1990.
[7] **C. Shannon.** *A mathematical theory of communication.* Bell Systems Technical Journal. **27** (1948), 379-423.
[8] **M. Sudan.** *Efficient Cheking of polynomials and proofs and the Hardness of approximation problems.* PhD thesis, University of California at Berkeley, October 1992.
[9] **M. Sudan.** *Algorithmic Introduction to Coding Theory*, available at http://theory.lcs.mit.edu.co/~madhu/FT01/course.html.

E-mail address: amontoyaa@googlemail.com, juamonto@uis.edu.co

Universidad Industrial de Santander