Cotas inferiores para sumas de potencias afines

Buscando paja en un pajar y pinchándome con las agujas

Ignacio García Marco

Universidad de La Laguna

Seminario GASIULL - 18/02/2019

Based on joint work with:

Pascal Koiran & **Timothée Pecatte**

ENS Lyon

The affine powers model: a way of expressing polynomials

Let $\mathbb{F}$ be a characteristic zero field and $f \in \mathbb{F}[x]$.

Example: $f = 3x^4 + 12x^3 + 1 \in \mathbb{C}[x]$

The affine powers model: a way of expressing polynomials

Let $\mathbb{F}$ be a characteristic zero field and $f \in \mathbb{F}[x]$.

We consider expressions of f as:

$$f = \sum_{i=1}^{s} \alpha_i (x + a_i)^{e_i},$$

with $\alpha_i, a_i \in \mathbb{F}$, and $e_i \in \mathbb{N}$

Example: $f = 3x^4 + 12x^3 + 1 \in \mathbb{C}[x]$

The affine powers model: a way of expressing polynomials

Let $\mathbb{F}$ be a characteristic zero field and $f \in \mathbb{F}[x]$.

We consider expressions of f as:

$$f = \sum_{i=1}^{s} \alpha_i (x + a_i)^{e_i},$$

with $\alpha_i, a_i \in \mathbb{F}$, and $e_i \in \mathbb{N}$

Example: $f = 3x^4 + 12x^3 + 1 \in \mathbb{C}[x]$

$$f = \quad 3\,(x+0)^4 \quad + \quad 12\,(x+0)^3 \quad + \quad (x+0)^0$$

The affine powers model: a way of expressing polynomials

Let $\mathbb{F}$ be a characteristic zero field and $f \in \mathbb{F}[x]$.

We consider expressions of f as:

$$f = \sum_{i=1}^{s} \alpha_i (x + a_i)^{e_i},$$

with $\alpha_i, a_i \in \mathbb{F}$, and $e_i \in \mathbb{N}$

Example: $f = 3x^4 + 12x^3 + 1 \in \mathbb{C}[x]$

$$f = \quad 3\,(x+0)^4 \quad + \quad 12\,(x+0)^3 \quad + \quad (x+0)^0 =$$

$$= \quad 3(x+1)^4 \quad - \quad 18(x+\tfrac{1}{3})^2$$

The affine powers model: a way of expressing polynomials

Let $\mathbb{F}$ be a characteristic zero field and $f \in \mathbb{F}[x]$.

We consider expressions of f as:

$$f = \sum_{i=1}^{s} \alpha_i (x + a_i)^{e_i},$$

with $\alpha_i, a_i \in \mathbb{F}$, and $e_i \in \mathbb{N}$

Example: $f = 3x^4 + 12x^3 + 1 \in \mathbb{C}[x]$

$$f = 3\,(x+0)^4 + 12\,(x+0)^3 + (x+0)^0 =$$

$$= 3(x+1)^4 - 18(x+\tfrac{1}{3})^2$$

This is better!

The affine powers model: a way of expressing polynomials

Let $\mathbb{F}$ be a characteristic zero field and $f \in \mathbb{F}[x]$.

We consider expressions of f as:

$$f = \sum_{i=1}^{s} \alpha_i (x + a_i)^{e_i},$$

with $\alpha_i, a_i \in \mathbb{F}$, and $e_i \in \mathbb{N}$

Example: $f = 3x^4 + 12x^3 + 1 \in \mathbb{C}[x]$

$$f = 3\,(x+0)^4 + 12\,(x+0)^3 + (x+0)^0 =$$

$$= 3(x+1)^4 - 18(x+\tfrac{1}{3})^2$$

This is better!

A complexity measure

For all $f \in \mathbb{F}[x]$, we set

$$c(f) := \min\{s \mid \quad f = \textstyle\sum_{i=1}^{s} \alpha_i (x + a_i)^{e_i} \text{ with } \alpha_i, a_i \in \mathbb{F} \text{ and } e_i \in \mathbb{N}\}$$

A complexity measure

For all $f \in \mathbb{F}[x]$, we set

$$c(f) := \min\{s \mid \quad f = \sum_{i=1}^{s} \alpha_i (x + a_i)^{e_i} \text{ with } \alpha_i, a_i \in \mathbb{F} \text{ and } e_i \in \mathbb{N}\}$$

Example: $f = 3x^4 + 12x^3 + 1 \in \mathbb{C}[x]$

$$f = 3(x+1)^4 - 18(x + \tfrac{1}{3})^2 \Longrightarrow c(f) \leq 2$$

A complexity measure

For all $f \in \mathbb{F}[x]$, we set

$$c(f) := \min\{s \mid \quad f = \sum_{i=1}^{s} \alpha_i (x + a_i)^{e_i} \text{ with } \alpha_i, a_i \in \mathbb{F} \text{ and } e_i \in \mathbb{N}\}$$

Example: $f = 3x^4 + 12x^3 + 1 \in \mathbb{C}[x]$

$f = 3(x+1)^4 - 18(x + \frac{1}{3})^2 \Longrightarrow c(f) \leq 2$

Indeed, $c(f) = 2$.

An upper bound for $c(f)$

Lemma. Let $f \in \mathbb{F}[x]$ a (nonzero) polynomial of degree d. Then,

$$c(f) \leq d + 1$$

An upper bound for $c(f)$

Lemma. Let $f \in \mathbb{F}[x]$ a (nonzero) polynomial of degree d. Then,

$$c(f) \leq \left\lceil \frac{d+1}{2} \right\rceil$$

An upper bound for $c(f)$

Lemma. Let $f \in \mathbb{F}[x]$ a (nonzero) polynomial of degree d. Then,

$$c(f) \leq \left\lceil \frac{d+1}{2} \right\rceil$$

Proof. By induction over d:

$$\left.\begin{array}{l} \text{If } d = 0,\ f = a_0 = a_0 x^0 \\ \text{if } d = 1,\ f = a_1 x + a_0 = a_1(x + (a_0/a_1))^1 \end{array}\right\} \Rightarrow c(f) = 1$$

An upper bound for $c(f)$

Lemma. Let $f \in \mathbb{F}[x]$ a (nonzero) polynomial of degree d. Then,

$$c(f) \leq \left\lceil \frac{d+1}{2} \right\rceil$$

Proof. By induction over d:

$$\left.\begin{array}{l} \text{If } d = 0,\ f = a_0 = a_0 x^0 \\ \text{if } d = 1,\ f = a_1 x + a_0 = a_1(x + (a_0/a_1))^1 \end{array}\right\} \Rightarrow c(f) = 1$$

If $f = \sum_{i=0}^{d} a_i x^i$ has degree d. Let

$$g := f - a_d \left(x + \frac{a_{d-1}}{d a_d} \right)^d$$

An upper bound for $c(f)$

Lemma. Let $f \in \mathbb{F}[x]$ a (nonzero) polynomial of degree d. Then,

$$c(f) \leq \left\lceil \frac{d+1}{2} \right\rceil$$

Proof. By induction over d:

$$\left.\begin{array}{l} \text{If } d = 0,\ f = a_0 = a_0 x^0 \\ \text{if } d = 1,\ f = a_1 x + a_0 = a_1(x + (a_0/a_1))^1 \end{array}\right\} \Rightarrow c(f) = 1$$

If $f = \sum_{i=0}^{d} a_i x^i$ has degree d. Let

$$g := f - a_d \left(x + \frac{a_{d-1}}{d a_d} \right)^d$$

$$\boxed{\begin{array}{c}\text{Tschirnhausen} \\ \text{Transformation} \\ \deg(g) \leq d-2\end{array}}$$

An upper bound for $c(f)$

Lemma. Let $f \in \mathbb{F}[x]$ a (nonzero) polynomial of degree d. Then,

$$c(f) \leq \left\lceil \frac{d+1}{2} \right\rceil$$

Proof. By induction over d:

$$\left.\begin{array}{l} \text{If } d = 0,\ f = a_0 = a_0 x^0 \\ \text{if } d = 1,\ f = a_1 x + a_0 = a_1(x + (a_0/a_1))^1 \end{array}\right\} \Rightarrow c(f) = 1$$

If $f = \sum_{i=0}^{d} a_i x^i$ has degree d. Let

$$g := f - a_d \left(x + \frac{a_{d-1}}{d a_d} \right)^d$$

Tschirnhausen Transformation
$\deg(g) \leq d - 2$

Then, $c(f) \leq c(g) + 1 \leq \left\lceil \frac{d-1}{2} \right\rceil + 1 = \left\lceil \frac{d+1}{2} \right\rceil$ $\square$

The generic case

Theorem If $f \in \mathbb{F}[x]$ is a **generic** polynomial of degree d, then

$$c(f) = \left\lceil \frac{d+1}{2} \right\rceil$$

The generic case

Theorem If $f \in \mathbb{F}[x]$ is a **generic** polynomial of degree d, then

$$c(f) = \left\lceil \frac{d+1}{2} \right\rceil$$

In other words

$$\left\{ (a_0, \ldots, a_d) \in \mathbb{F}^{d+1} \mid c\left(\sum_{i=0}^{d} a_i x^i \right) < \left\lceil \frac{d+1}{2} \right\rceil \right\} \subset X,$$

where $X \subsetneq \mathbb{F}^{d+1}$ is an algebraic set.

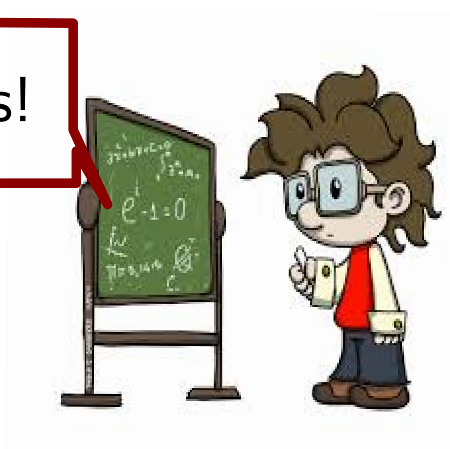
The generic case

Theorem If $f \in \mathbb{F}[x]$ is a **generic** polynomial of degree d, then

$$c(f) = \left\lceil \frac{d+1}{2} \right\rceil$$

So, tell me one polynomial $f \in \mathbb{C}[x]$ of degree 100 such that $c(f) = 51$.

Almost anyone works!



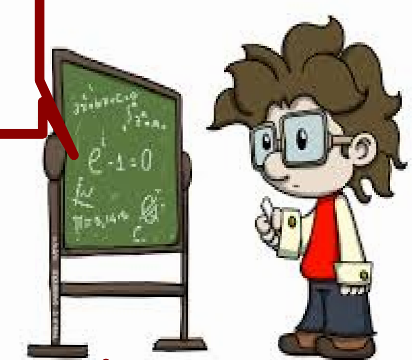
The generic case

Theorem If $f \in \mathbb{F}[x]$ is a **generic** polynomial of degree d, then

$$c(f) = \left\lceil \frac{d+1}{2} \right\rceil$$

So, tell me one polynomial $f \in \mathbb{C}[x]$ of degree 100 such that $c(f) = 51$.

Almost anyone works!



But, could you tell me one explicitly.

Mmmmmm, ...

The problem

For every $d \in \mathbb{N}$, find an **explicit** $f_d \in \mathbb{C}[x]$, such that

- f_d has degree d, and
- $c(f_d) = \lceil (d+1)/2 \rceil$.

The problem

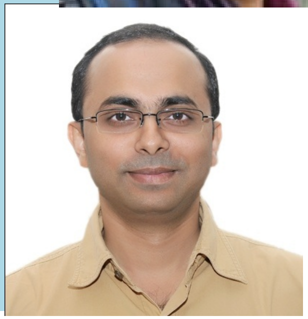
For every $d \in \mathbb{N}$, find an **explicit** $f_d \in \mathbb{C}[x]$, such that
- f_d has degree d, and
- $c(f_d) = \lceil (d+1)/2 \rceil$.

Theorem [Kayal, Koiran, Pecatte & Saha (2015)]

For all $k \in \mathbb{N}$ and all $a_1 \neq a_2 \in \mathbb{C}$, the polynomial

$$f = [(x+a_1)(x+a_2)]^k$$

of degree $d = 2k$ satisfies that $c(f) \geq (\sqrt{d})/2$.



The problem

For every $d \in \mathbb{N}$, find an **explicit** $f_d \in \mathbb{C}[x]$, such that

- f_d has degree d, and
- $c(f_d) = \lceil (d+1)/2 \rceil$.

Theorem [Kayal, Koiran, Pecatte & Saha (2015)]

For all $k \in \mathbb{N}$ and all $a_1 \neq a_2 \in \mathbb{C}$, the polynomial

$$f = [(x+a_1)(x+a_2)]^k$$

of degree $d = 2k$ satisfies that $c(f) \geq (\sqrt{d})/2$.

Today's goal: Improve this result for $\mathbb{F} = \mathbb{R}$.

This is, provide **explicit polynomials** $f \in \mathbb{R}[x]$ of degree d such that $c(f)$ is equal (or close) to $\lceil (d+1)/2 \rceil$.

An easy observation

Let $f \in \mathbb{F}[x]$, if:

$$f = \sum_{i=1}^{s} \alpha_i (x + a_i)^{e_i}$$

and

$$f = \sum_{j=1}^{\ell} \beta_j (x + b_j)^{d_j}.$$

An easy observation

Let $f \in \mathbb{F}[x]$, if:

$$f = \sum_{i=1}^{s} \alpha_i (x + a_i)^{e_i}$$

and

$$f = \sum_{j=1}^{\ell} \beta_j (x + b_j)^{d_j}.$$

Then,

$$\left\{(x + a_i)^{e_i} \,|\, 1 \le i \le s\right\} \cup \left\{(x + b_j)^{d_j} \,|\, 1 \le j \le \ell\right\},$$

is a **linearly dependent** set.

Our approach

If $I := \{(x + a_i)^{e_i} \mid 1 \leq i \leq s\}$ satisfies the following **nice property**:

For **all** $L = \{(x + b_i)^{d_i} \mid 1 \leq i \leq \ell\}$ $\mathbb{F}$-linearly independent with $\ell < s \Rightarrow\ L \cup I$ is also $\mathbb{F}$-linearly independent.

Our approach

If $I := \{(x+a_i)^{e_i} \mid 1 \leq i \leq s\}$ satisfies the following **nice property**:

For **all** $L = \{(x+b_i)^{d_i} \mid 1 \leq i \leq \ell\}$ $\mathbb{F}$-linearly independent with $\ell < s \Rightarrow\ L \cup I$ is also $\mathbb{F}$-linearly independent.

$$\Downarrow$$

Taking $\alpha_1, \ldots, \alpha_s \in \mathbb{F} \setminus \{0\}$ and setting

$$f = \sum_{i=1}^{s} \alpha_i (x+a_i)^{e_i}$$

we have that $c(f) = s$.

Our approach

If $I := \{(x+a_i)^{e_i} \mid 1 \le i \le s\}$ satisfies the following **nice property**:

For **all** $L = \{(x+b_i)^{d_i} \mid 1 \le i \le \ell\}$ $\mathbb{F}$-linearly independent with $\ell < s \Rightarrow\ L \cup I$ is also $\mathbb{F}$-linearly independent.

$\Downarrow$

Taking $\alpha_1, \ldots, \alpha_s \in \mathbb{F} \setminus \{0\}$ and setting

$$f = \sum_{i=1}^{s} \alpha_i (x+a_i)^{e_i}$$

we have that $c(f) = s$.

Goal: find a set I with the **nice property** and s large.

To carry out this, we need a **good criterion for deciding $\mathbb{F}$-linear independence** of polynomials of the form $(x+a_i)^{e_i}$.

Our approach: study linear independence of affine powers

Let $\ell_1, \ldots, \ell_s \in \mathbb{F}[x]$ be affine powers:

$$\ell_i = (x + a_i)^{e_i} = \sum_{j=0}^{e_i} \binom{e_i}{j} a_i^{e_i - j} x^j.$$

Are $\ell_1, \ldots, \ell_s$ linearly independent?

Our approach: study linear independence of affine powers

Let $\ell_1, \ldots, \ell_s \in \mathbb{F}[x]$ be affine powers:

$$\ell_i = (x + a_i)^{e_i} = \sum_{j=0}^{e_i} \binom{e_i}{j} a_i^{e_i - j} x^j.$$

Are $\ell_1, \ldots, \ell_s$ linearly independent?

Take $d := \max(e_i)$, $B := \{1, \frac{x}{1!}, \ldots, \frac{x^j}{j!}, \ldots, \frac{x^d}{d!}\}$ and set A_i the vector of coordinates of ℓ_i with respect to B, that is

$$A_i = \left(a_i^{e_i}, \ldots, \frac{e_i!}{(e_i - j)!} a_i^{e_i - j}, \ldots, e_i!, 0, \ldots, 0 \right) \in \mathbb{F}^{d+1}$$

Let A be the matrix with rows $A_1, \ldots, A_s$. Then,

$$\dim_{\mathbb{F}} \langle \ell_1, \ldots, \ell_s \rangle = \mathrm{rk}(A).$$

Our approach: study linear independence of affine powers

Let $\ell_1, \ldots, \ell_s \in \mathbb{F}[x]$ be affine powers:

$$\ell_i = (x + a_i)^{e_i} = \sum_{j=0}^{e_i} \binom{e_i}{j} a_i^{e_i - j} x^j.$$

Are $\ell_1, \ldots, \ell_s$ linearly independent?

Take $d := \max(e_i)$, $B := \{1, \frac{x}{1!}, \ldots, \frac{x^j}{j!}, \ldots, \frac{x^d}{d!}\}$ and set A_i the vector of coordinates of ℓ_i with respect to B, that is

$$A_i = \left(a_i^{e_i}, \ldots, \frac{e_i!}{(e_i - j)!} a_i^{e_i - j}, \ldots, e_i!, 0, \ldots, 0 \right) \in \mathbb{F}^{d+1}$$

Let A be the matrix with rows $A_1, \ldots, A_s$. Then,

$$\dim_{\mathbb{F}} \langle \ell_1, \ldots, \ell_s \rangle = \mathrm{rk}(A).$$

It is not easy to determine when A has maximal row rank!!!

Birkhoff interpolation

Birkhoff interpolation studies the set of polynomials $g \in \mathbb{F}[x]$ of degree $\leq d$ satisfying a system of equations of the form

$$\left.\begin{array}{rcl} g^{(k_1)}(a_1) & = & 0 \\ \cdots & & \\ g^{(k_s)}(a_s) & = & 0 \end{array}\right\}$$

with $0 \leq k_i \leq d$, $a_i \in \mathbb{F}$.

Birkhoff interpolation

Birkhoff interpolation studies the set of polynomials $g \in \mathbb{F}[x]$ of degree $\leq d$ satisfying a system of equations of the form

$$\left.\begin{array}{rcl} g^{(k_1)}(a_1) & = & 0 \\ \cdots & & \\ g^{(k_s)}(a_s) & = & 0 \end{array}\right\}$$

with $0 \leq k_i \leq d$, $a_i \in \mathbb{F}$.

Definition.

The **Birkhoff interpolation problem** is **regular** if its set of solutions $g \in \mathbb{F}[x]_{\leq d}$ is a vector space of dimension $d + 1 - s$.

From linear independence to Birkhoff interpolation

Example: Consider the affine powers $(x+1)^4, (x-1)^4, x^3, x$.

From linear independence to Birkhoff interpolation

Example: Consider the affine powers $(x+1)^4, (x-1)^4, x^3, x$.

They are **linearly dependent** because:

$$(x+1)^4 - (x-1)^4 = 8x^3 + 8x$$

From linear independence to Birkhoff interpolation

Example: Consider the affine powers $(x+1)^4, (x-1)^4, x^3, x$.

They are **linearly dependent** because:

$$(x+1)^4 - (x-1)^4 = 8x^3 + 8x$$

We associate the following interpolation problem:

We look for polynomials $g \in \mathbb{F}[x]$ of degree $d \leq 4$ such that

$$\left.\begin{array}{lcrcl} (x+1)^4 & \rightsquigarrow & g(1) & = & 0 \\ (x-1)^4 & \rightsquigarrow & g(-1) & = & 0 \\ x^3 & \rightsquigarrow & g'(0) & = & 0 \\ x & \rightsquigarrow & g^{(3)}(0) & = & 0 \end{array}\right\}$$

From linear independence to Birkhoff interpolation

Example: Consider the affine powers $(x+1)^4, (x-1)^4, x^3, x$.

They are **linearly dependent** because:

$$(x+1)^4 - (x-1)^4 = 8x^3 + 8x$$

We associate the following interpolation problem:

We look for polynomials $g \in \mathbb{F}[x]$ of degree $d \leq 4$ such that

$$\left.\begin{array}{lcrcl}
(x+1)^4 & \rightsquigarrow & g(1) & = & 0 \\
(x-1)^4 & \rightsquigarrow & g(-1) & = & 0 \\
x^3 & \rightsquigarrow & g'(0) & = & 0 \\
x & \rightsquigarrow & g^{(3)}(0) & = & 0
\end{array}\right\}$$

The set of solutions is $\langle x^4 - 1, x^2 - 1 \rangle$.

The **Birkhoff interpolation problem** is **not regular**.

From linear independence to Birkhoff interpolation

Given $\ell_1, \dots, \ell_s \in \mathbb{F}[x]$ with $\ell_i = (x + a_i)^{e_i}$ and $d := \max(e_i)$.
We associate the following **Birkhoff interpolation problem**:

Find $g \in \mathbb{F}_{\le d}[x]$ such that

$$g^{(d-e_i)}(a_i) = 0 \text{ for } 1 \le i \le s.$$

From linear independence to Birkhoff interpolation

Given $\ell_1, \ldots, \ell_s \in \mathbb{F}[x]$ with $\ell_i = (x + a_i)^{e_i}$ and $d := \max(e_i)$. We associate the following **Birkhoff interpolation problem**:

Find $g \in \mathbb{F}_{\leq d}[x]$ such that

$$g^{(d-e_i)}(a_i) = 0 \text{ for } 1 \leq i \leq s.$$

Proposition

Set $r := \dim_{\mathbb{F}} \langle \ell_1, \ldots, \ell_s \rangle$ with $\ell_i = (x + a_i)^{e_i}$. Then,

$$\dim_{\mathbb{F}} \{g \in \mathbb{F}_{\leq d}[x];\ g^{(d-e_i)}(a_i) = 0 \text{ for all } i\} = d + 1 - r.$$

From linear independence to Birkhoff interpolation

Given $\ell_1, \ldots, \ell_s \in \mathbb{F}[x]$ with $\ell_i = (x + a_i)^{e_i}$ and $d := \max(e_i)$. We associate the following **Birkhoff interpolation problem**:

Find $g \in \mathbb{F}_{\leq d}[x]$ such that

$$g^{(d-e_i)}(a_i) = 0 \text{ for } 1 \leq i \leq s.$$

Proposition

Set $r := \dim_{\mathbb{F}} \langle \ell_1, \ldots, \ell_s \rangle$ with $\ell_i = (x + a_i)^{e_i}$. Then,

$$\dim_{\mathbb{F}} \{ g \in \mathbb{F}_{\leq d}[x];\ g^{(d-e_i)}(a_i) = 0 \text{ for all } i \} = d + 1 - r.$$

Proof. We know that $r = \mathrm{rk}(A)$.

If $g = \sum_{j=0}^{d} g_j \frac{x^j}{j!}$ with $g_j \in \mathbb{F}$

$\Searrow$

$$g^{(d-e_i)} = \sum_{j=0}^{e_i} g_{d-e_i+j} \frac{x^j}{j!}.$$

From linear independence to Birkhoff interpolation

Then,

$$g^{(d-e_i)}(a_i) = 0 \text{ for all } 1 \leq i \leq s \Longleftrightarrow B \cdot \begin{pmatrix} g_d \\ g_{d-1} \\ \vdots \\ g_0 \end{pmatrix} = 0,$$

where B is the $s \times (d+1)$ matrix whose i-th row is

$$B_i := \left(\frac{a_i^{e_i}}{e_i!}, \ldots, \frac{a_i^{e_i - j}}{(e_i - j)!}, \ldots, a_i, 1, 0, \ldots, 0 \right) \in \mathbb{F}^{d+1}.$$

From linear independence to Birkhoff interpolation

Then,

$$g^{(d-e_i)}(a_i) = 0 \text{ for all } 1 \le i \le s \iff B \cdot \begin{pmatrix} g_d \\ g_{d-1} \\ \vdots \\ g_0 \end{pmatrix} = 0,$$

where B is the $s \times (d+1)$ matrix whose i-th row is

$$B_i := \left(\frac{a_i^{e_i}}{e_i!}, \ldots, \frac{a_i^{e_i-j}}{(e_i-j)!}, \ldots, a_i, 1, 0, \ldots, 0 \right) \in \mathbb{F}^{d+1}.$$

Then,

$$\dim\{g \in \mathbb{F}_{\le d}[x]\, ;\, g^{(d-e_i)}(a_i) = 0 \text{ for } 1 \le i \le s\} = d+1-\mathrm{rk}(B).$$

We observe that $A_i = e_i!\, B_i \Longrightarrow r = \mathrm{rk}(A) = \mathrm{rk}(B)$. $\square$

From linear independence to Birkhoff interpolation

Proposition

Set $r := \dim_{\mathbb{F}}\langle \ell_1, \ldots, \ell_s \rangle$ with $\ell_i = (x + a_i)^{e_i}$. Then,

$$\dim_{\mathbb{F}}\{g \in \mathbb{F}_{\leq d}[x];\ g^{(d-e_i)}(a_i) = 0 \text{ for all } i\} = d + 1 - r.$$

From linear independence to Birkhoff interpolation

Proposition
Set $r := \dim_{\mathbb{F}}\langle \ell_1, \ldots, \ell_s\rangle$ with $\ell_i = (x + a_i)^{e_i}$. Then,

$$\dim_{\mathbb{F}}\{g \in \mathbb{F}_{\leq d}[x];\ g^{(d-e_i)}(a_i) = 0 \text{ for all } i\} = d + 1 - r.$$

Corollary
The set $\{\ell_1, \ldots, \ell_s\}$ is **linearly independent** if and only if the **Birkhoff interpolation problem**

$$g \in \mathbb{F}_{\leq d}[x];\ g^{(d-e_i)}(a_i) = 0\ for\ 1 \leq i \leq s$$

is **regular**.

From linear independence to Birkhoff interpolation

Example: Consider the affine powers $(x+1)^4, (x-1)^4, x^3, x$.

They are **linearly dependent** because:

$$(x+1)^4 - (x-1)^4 = 8x^3 + 8x$$

We associate the following interpolation problem:

We look for polynomials $g \in \mathbb{F}[x]$ of degree $d \leq 4$ such that

$$\left.\begin{array}{lcrcl}
(x+1)^4 & \rightsquigarrow & g(1) & = & 0 \\
(x-1)^4 & \rightsquigarrow & g(-1) & = & 0 \\
x^3 & \rightsquigarrow & g'(0) & = & 0 \\
x & \rightsquigarrow & g^{(3)}(0) & = & 0
\end{array}\right\}$$

The set of solutions is $\langle x^4 - 1, x^2 - 1 \rangle$.

The **Birkhoff interpolation problem** is **not regular**.

Bringing results from Birkhoff interpolation

Given $\ell_1, \ldots, \ell_s$ with $\ell_i = (x + a_i)^{e_i}$.

Set $N_j := \sharp\{i \mid e_i < j\}$.

number of polynomials
of degree $< j$

Bringing results from Birkhoff interpolation

Given $\ell_1, \ldots, \ell_s$ with $\ell_i = (x + a_i)^{e_i}$.

Set $N_j := \sharp\{i \mid e_i < j\}$.

number of polynomials
of degree $< j$

Remark:

If $\{\ell_1, \ldots, \ell_s\}$ are lin. indep. $\Longrightarrow$ $N_j \leq j$ for all $j \geq 1$

Bringing results from Birkhoff interpolation

Given $\ell_1, \ldots, \ell_s$ with $\ell_i = (x + a_i)^{e_i}$.

Set $N_j := \sharp\{i \,|\, e_i < j\}$.

number of polynomials of degree $< j$

Remark:

If $\{\ell_1, \ldots, \ell_s\}$ are lin. indep. $\implies$ $N_j \leq j$ for all $j \geq 1$

And as a consequence of **Atkinson-Sharma theorem (1969)** for **real Birkhoff interpolation**:

Theorem. For $\mathbb{F} = \mathbb{R}$.

If $N_j + N_{j-1} \leq j$ for all $j \geq 1$ $\implies$ $\{\ell_1, \ldots, \ell_s\}$ are lin. indep.

Bringing results from Birkhoff interpolation

Given $\ell_1, \dots, \ell_s$ with $\ell_i = (x + a_i)^{e_i}$.

Set $N_j := \sharp\{i \mid e_i < j\}$.

number of polynomials of degree $< j$

> **Remark:**
>
> If $\{\ell_1, \dots, \ell_s\}$ are lin. indep. $\implies$ $N_j \le j$ for all $j \ge 1$

And as a consequence of **Atkinson-Sharma theorem (1969)** for **real Birkhoff interpolation**:

Theorem. For $\mathbb{F} = \mathbb{R}$.

If $N_j + N_{j-1} \le$ … $\{\ell_1, \dots, \ell_s\}$ are lin. indep.

Not true for $\mathbb{F} = \mathbb{C}$

Main results

Theorem. Let $e, s \in \mathbb{N}$ with $s \leq (e+2)/4$, $a_1, \ldots, a_s \in \mathbb{R}$ distinct. Then,

$$I := \{(x + a_i)^e \mid 1 \leq i \leq s\}$$

has the *nice* property.

Main results

Theorem. Let $e, s \in \mathbb{N}$ with $s \leq (e+2)/4$, $a_1, \ldots, a_s \in \mathbb{R}$ distinct and $\alpha_1, \ldots, \alpha_s \in \mathbb{R} \setminus \{0\}$. Then,

$$f := \sum_{i=1}^{s} \alpha_i (x + a_i)^e$$

satisfies that $c(f) = s$.

Main results

Theorem. Let $e, s \in \mathbb{N}$ with $s \leq (e+2)/4$, $a_1, \ldots, a_s \in \mathbb{R}$ distinct and $\alpha_1, \ldots, \alpha_s \in \mathbb{R} \setminus \{0\}$. Then,

$$f := \sum_{i=1}^{s} \alpha_i (x + a_i)^e$$

satisfies that $c(f) = s$.

Choosing $s := (e+2)/4$. Then,

a) $c(f) = (e+2)/4$

Main results

Theorem. Let $e, s \in \mathbb{N}$ with $s \leq (e+2)/4$, $a_1, \ldots, a_s \in \mathbb{R}$ distinct and $\alpha_1, \ldots, \alpha_s \in \mathbb{R} \setminus \{0\}$. Then,

$$f := \sum_{i=1}^{s} \alpha_i (x + a_i)^e$$

satisfies that $c(f) = s$.

Choosing $s := (e+2)/4$. Then,

a) $c(f) = (e+2)/4$

b) The degree of f is $\leq e$

Main results

Theorem. Let $e, s \in \mathbb{N}$ with $s \leq (e+2)/4$, $a_1, \ldots, a_s \in \mathbb{R}$ distinct and $\alpha_1, \ldots, \alpha_s \in \mathbb{R} \setminus \{0\}$. Then,

$$f := \sum_{i=1}^{s} \alpha_i (x + a_i)^e$$

satisfies that $c(f) = s$.

Choosing $s := (e+2)/4$. Then,

a) $c(f) = (e+2)/4$

b) The degree of f is $\leq e$

One can choose α_i, a_i so that $\deg(f) = e - ((e-2)/4)$

Main results

Theorem. Let $e, s \in \mathbb{N}$ with $s \leq (e+2)/4$, $a_1, \ldots, a_s \in \mathbb{R}$ distinct and $\alpha_1, \ldots, \alpha_s \in \mathbb{R} \setminus \{0\}$. Then,

$$f := \sum_{i=1}^{s} \alpha_i (x + a_i)^e$$

satisfies that $c(f) = s$.

Choosing $s := (e+2)/4$. Then,

a) $c(f) = (e+2)/4$

b) The degree of f is $\leq e$

One can choose α_i, a_i so that $\deg(f) = e - ((e-2)/4)$

Corollary 1. For each $d \in \mathbb{N}$, there is an **explicit** polynomial $f_d \in \mathbb{R}[x]$ of degree d and

$$c(f_d) = d/3$$

Main results

Theorem. Let $e, s \in \mathbb{N}$ with $s \leq (e+2)/4$, $a_1, \ldots, a_s \in \mathbb{R}$ distinct and $\alpha_1, \ldots, \alpha_s \in \mathbb{R} \setminus \{0\}$. Then,

$$f := \sum_{i=1}^{s} \alpha_i (x + a_i)^e$$

satisfies that $c(f) = s$.

Not true for $\mathbb{F} = \mathbb{C}$

Choosing $s := (e+2)/4$. Then,

a) $c(f) = (e+2)/4$

b) The degree of f is $\leq e$

One can choose α_i, a_i so that $\deg(f) = e - ((e-2)/4)$

Corollary 1. For each $d \in \mathbb{N}$, there is an **explicit** polynomial $f_d \in \mathbb{R}[x]$ of degree d and

$$c(f_d) = d/3$$

Main results

Corollary 2. For each $d \in \mathbb{N}$, we consider

$$g_d := (x+1)^{d+1} - (x-1)^{d+1}.$$

Main results

Corollary 2. For each $d \in \mathbb{N}$, we consider

$$g_d := (x+1)^{d+1} - (x-1)^{d+1}.$$

Then,

- $\deg(g_d) = d$, and
- if $g_d = \sum_{i=1}^{s} \alpha_i (x + a_i)^{e_i}$ with $\alpha_i, a_i \in \mathbb{R}$ and $e_i \leq d$; then $s \geq \lceil \frac{d+1}{2} \rceil$.

Main results

Corollary 2. For each $d \in \mathbb{N}$, we consider

$$g_d := (x+1)^{d+1} - (x-1)^{d+1}.$$

Then,

- $\deg(g_d) = d$, and
- if $g_d = \sum_{i=1}^{s} \alpha_i (x+a_i)^{e_i}$ with $\alpha_i, a_i \in \mathbb{R}$ and $e_i \leq d$; then $s \geq \lceil \frac{d+1}{2} \rceil$.

Moreover,

$$(x+1)^{d+1} - (x-1)^{d+1} = \sum_{\substack{i\ odd \\ 1 \leq i \leq d+1}} 2\binom{d}{i} x^{d+1-i}.$$

$\lceil \frac{d+1}{2} \rceil$ affine powers

The complex case

Over $\mathbb{C}$ one can generalize the identity:

$$(x+1)^d - (x-1)^d = \sum_{\substack{i\ odd \\ 1\leq i\leq d}} 2\binom{d}{i} x^{d-i}.$$

Proposition

Take $k \in \mathbb{Z}^+$ and let ξ be a **k-th primitive root of unity**. Then, for all $d \in \mathbb{Z}^+$ the following equality holds:

$$\sum_{j=1}^{k} \xi^j (x+\xi^j)^d = \sum_{\substack{i\equiv -1 \pmod{k} \\ 0\leq i\leq d}} k\binom{d}{i} x^{d-i} \in \mathbb{R}[x]$$

Open questions

- Find explicit $f \in \mathbb{C}[x]$ such that $c(f)$ is linear in d.
- Find a *good* sufficient condition for $\ell_1, \ldots, \ell_s \in \mathbb{C}[x]$ to be $\mathbb{C}$-linearly independent with $\ell_i = (x + a_i)^{e_i}$, $a_i \in \mathbb{C}$.
- Find a *good* sufficient condition for a Birkhoff interpolation problem to be regular over $\mathbb{C}$.
- Does Corollary 1 hold over $\mathbb{C}$? and Corollary 2?
- Devise algorithms computing $c(f)$ for a given polynomial f.
- What about multivariate polynomials?

Open questions

Proposition 1

For any family $F = \{(x - a_i)^{e_i} \mid 1 \leq i \leq s\}$ with $a_i \in \mathbb{R}$. If $e_i \geq 2s - 4$, then F is linearly independent.

Open questions

Proposition 1

For any family $F = \{(x - a_i)^{e_i} \,|\, 1 \leq i \leq s\}$ with $a_i \in \mathbb{R}$. If $e_i \geq 2s - 4$, then F is linearly independent.

Proposition 2

For any family $F = \{(x - a_i)^{e_i} \,|\, 1 \leq i \leq s\}$ with $a_i \in \mathbb{C}$. If $e_i \geq s^2$, then F is linearly independent.

Open questions

Proposition 1
For any family $F = \{(x - a_i)^{e_i} \,|\, 1 \leq i \leq s\}$ with $a_i \in \mathbb{R}$. If $e_i \geq 2s - 4$, then F is linearly independent.

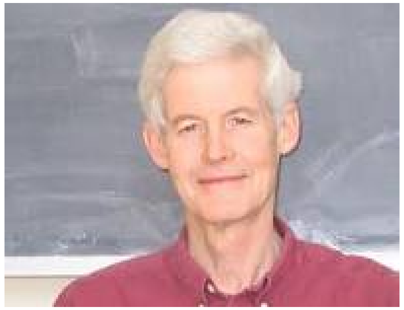
Proposition 2
For any family $F = \{(x - a_i)^{e_i} \,|\, 1 \leq i \leq s\}$ with $a_i \in \mathbb{C}$. If $e_i \geq s^2$, then F is linearly independent.

Conjecture. There are constants a and b such that Proposition 2 can be proved for $e_i \geq as + b$

Motivation

In 1971, Stephen Cook introduces: 'Is $P = NP$?'

P y NP are complexity clases of **decision problems**

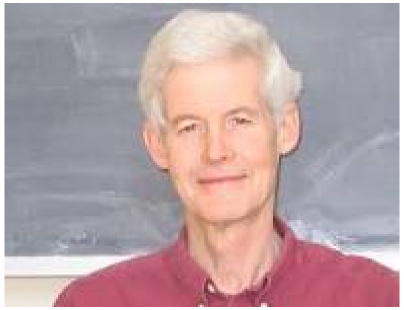


Motivation

In 1971, Stephen Cook introduces: ‘Is $\mathsf{P} = \mathsf{NP}$?’

P y NP are complexity clases of **decision problems**

P $\hookrightarrow$ easy to solve

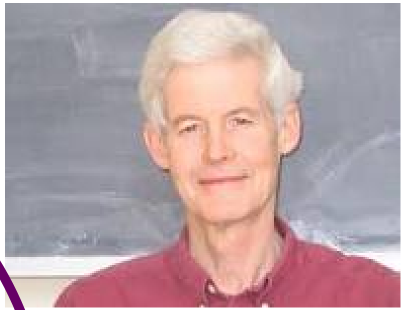


Motivation

In 1971, Stephen Cook introduces: 'Is $\mathsf{P} = \mathsf{NP}$?'

P y NP are complexity clases of **decision problems**

$\mathsf{P} \quad \hookrightarrow \quad$ easy to solve



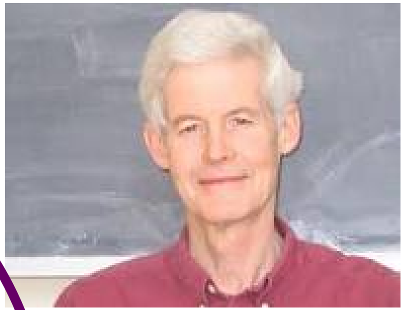
Input: $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$
Problem: Is v ordered?

Motivation

In 1971, Stephen Cook introduces: 'Is $\mathsf{P} = \mathsf{NP}$?'

P y NP are complexity clases of **decision problems**

P	$\hookrightarrow$	easy to solve
NP	$\hookrightarrow$	easy to verify with a witness if the answer is YES



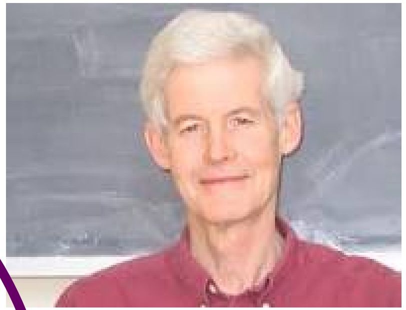
Input: $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$
Problem: Is v ordered?

Motivation

In 1971, Stephen Cook introduces: 'Is $\mathsf{P} = \mathsf{NP}$?'

P y NP are complexity clases of **decision problems**

P	$\hookrightarrow$	easy to solve
NP	$\hookrightarrow$	easy to verify with a witness if the answer is YES



Input: $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$
Problem: Is v ordered?

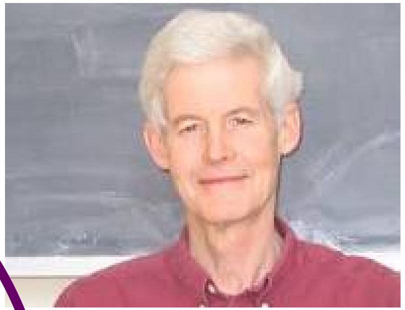
Input: $A = \{a_1, \ldots, a_n\} \subset \mathbb{Z}$
Problem: Is there a $B \subseteq A$ so that $\sum_{b \in B} b = 0$?

Motivation

In 1971, Stephen Cook introduces: 'Is P $=$ NP?'

P y NP are complexity clases of **decision problems**

P	$\hookrightarrow$	easy to solve
NP	$\hookrightarrow$	easy to verify with a witness if the answer is YES



Input: $v = (v_1, \ldots, v_n) \in \mathbb{Z}^n$
Problem: Is v ordered?

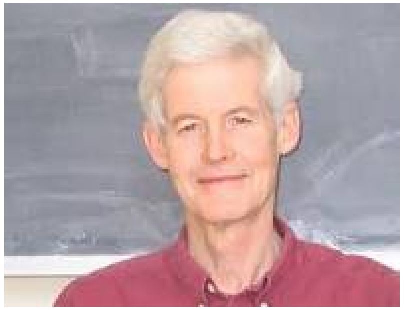
Input: $A = \{a_1, \ldots, a_n\} \subset \mathbb{Z}$
Problem: Is there a $B \subseteq A$ so that $\sum_{b \in B} b = 0$?

Clearly P $\subseteq$ NP

Motivation

In 1971, Stephen Cook introduces: 'Is $\mathsf{P} = \mathsf{NP}$?'

P y NP are complexity clases of **decision problems**

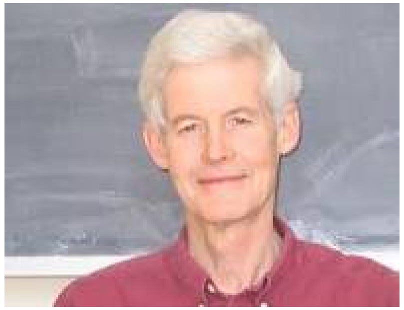


- One of the *millenium problems* of Clay Math Institute
- General thought: $\mathsf{P} \subsetneq \mathsf{NP}$
- Second general thought: we are far from a proof

Motivation

In 1971, Stephen Cook introduces: 'Is $\mathsf{P} = \mathsf{NP}$?'

P y NP are complexity clases of **decision problems**



- One of the *millenium problems* of Clay Math Institute
- General thought: $\mathsf{P} \subsetneq \mathsf{NP}$
- Second general thought: we are far from a proof

- 45 before 2050
- 17 before 2100
- 12 after 2100
- 5 never
- 21 don't know

- 61 believe $\mathsf{P} \neq \mathsf{NP}$
- 9 believe $\mathsf{P} = \mathsf{NP}$
- 8 believe it is not decidable
- 22 don't know

Survey by W.I. Gasarch

An algebraic variant of P vs. NP

In 1979, Leslie Valiant presents the problem: Is $\mathsf{VP} = \mathsf{VNP}$?

Elements of VP and VNP: families of polynomials

VP	$\hookrightarrow$	easy to compute
VNP	$\hookrightarrow$	explicit

An algebraic variant of P vs. NP

In 1979, Leslie Valiant presents the problem: Is VP $=$ VNP?

Elements of VP and VNP: families of polynomials

VP	$\hookrightarrow$	easy to compute
VNP	$\hookrightarrow$	explicit

$$\boxed{f_n = \sum_{i=1}^{n} x_i^n, \text{ for all } n \in \mathbb{Z}^+}$$

An algebraic variant of P vs. NP

In 1979, Leslie Valiant presents the problem: Is VP $=$ VNP?

Elements of VP and VNP: families of polynomials

VP	$\hookrightarrow$	easy to compute
VNP	$\hookrightarrow$	explicit

$f_n = \sum_{i=1}^{n} x_i^n$, for all $n \in \mathbb{Z}^+$

$$\mathrm{Det}_n := \det \begin{bmatrix} x_{1,1} & \cdots & x_{1,n} \\ x_{2,1} & \cdots & x_{2,n} \\ \cdots & \cdots & \cdots \\ x_{n,1} & \cdots & x_{n,n} \end{bmatrix} = \sum_{\sigma \in S_n} (-1)^{\mathrm{sign}(\omega)} x_{1\sigma(1)} \cdots x_{n\sigma(n)}$$

An algebraic variant of P vs. NP

In 1979, Leslie Valiant presents the problem: Is VP $=$ VNP?

Elements of VP and VNP: families of polynomials

VP	$\hookrightarrow$	easy to compute
VNP	$\hookrightarrow$	explicit

$f_n = \sum_{i=1}^{n} x_i^n$, for all $n \in \mathbb{Z}^+$

$$\mathrm{Det}_n := \det \begin{bmatrix} x_{1,1} & \cdots & x_{1,n} \\ x_{2,1} & \cdots & x_{2,n} \\ \cdots & \cdots & \cdots \\ x_{n,1} & \cdots & x_{n,n} \end{bmatrix} = \sum_{\sigma \in S_n} (-1)^{\mathrm{sign}(\omega)} x_{1\sigma(1)} \cdots x_{n\sigma(n)}$$

$$\mathrm{Perm}_n = \sum_{\sigma \in S_n} x_{1\sigma(1)} \cdots x_{n\sigma(n)}$$

An algebraic variant of P vs. NP

In 1979, Leslie Valiant presents the problem: Is VP $=$ VNP?

Elements of VP and VNP: families of polynomials

VP $\hookrightarrow$ easy to compute

VNP $\hookrightarrow$ explicit

$f_n = \sum_{i=1}^{n} x_i^n$, for all $n \in \mathbb{Z}^+$

$$\mathrm{Det}_n := \det \begin{bmatrix} x_{1,1} & \cdots & x_{1,n} \\ x_{2,1} & \cdots & x_{2,n} \\ \cdots & \cdots & \cdots \\ x_{n,1} & \cdots & x_{n,n} \end{bmatrix} = \sum_{\sigma \in S_n} (-1)^{\mathrm{sign}(\omega)}\, x_{1\sigma(1)} \cdots x_{n\sigma(n)}$$

$$\mathrm{Perm}_n = \sum_{\sigma \in S_n} x_{1\sigma(1)} \cdots x_{n\sigma(n)}$$

Clearly, VP $\subseteq$ VNP

An algebraic variant of P vs. NP

In 1979, Leslie Valiant presents the problem: Is $\mathsf{VP} = \mathsf{VNP}$?

Elements of VP and VNP: families of polynomials

VP	$\hookrightarrow$	easy to compute
VNP	$\hookrightarrow$	explicit

- Widely thought that: $\mathsf{VP} \subsetneq \mathsf{VNP}$
- Kayal (2009) introduces the method of *shifted partial derivatives*. This method (and its improvements) are very close to solve the problem.

An algebraic variant of P vs. NP

In 1979, Leslie Valiant presents the problem: Is $\mathsf{VP} = \mathsf{VNP}$?

Elements of VP and VNP: families of polynomials

VP	$\hookrightarrow$	easy to compute
VNP	$\hookrightarrow$	explicit

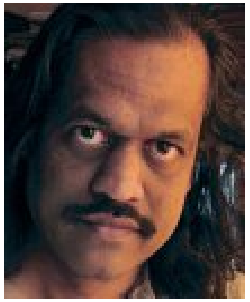
- Widely thought that: $\mathsf{VP} \subsetneq \mathsf{VNP}$
- Kayal (2009) introduces the method of *shifted partial derivatives*. This method (and its improvements) are very close to solve the problem.

Bad news:

Landsberg et al. (2016) show that the *shifted partial derivatives method* is not enough to separate VP from VNP.

Good news:

Results by [Agrawal & Vinay (2008), Tavenas (2014)] show that a **generic vs. explicit** result for any of the following model of computation of polynomials imply that VP $\subsetneq$ VNP.



1. $f = \sum_{i=1}^{k} f_i^{e_i} \in \mathbb{C}[x]$
   where f_i have at most t monomials and $e_i \in \mathbb{N}$
2. $f = \sum_{i=1}^{k} a_i f_i^{e_i} \in \mathbb{F}[x_1, \ldots, x_n]$
   where $a_i \in k$ and f_i have at most t monomials
3. $f = \sum_{i=1}^{s} \prod_{j=1}^{m} L_{i,j} \in \mathbb{F}[x_1, \ldots, x_n]$
   where $L_{i,j}$ are linear forms.

Si $P = NP$ el mundo sería muy diferente de como creemos que es. La creatividad no tendría un valor especial: no habría diferencia entre alguien que sepa apreciar a Mozart y el propio genio, todo el que pudiera entender una demostración sería Gauss...

Scott Aaronson

¡Muchas gracias!