Covering the hypercube with geometry and algebra

Yuval Wigderson (Stanford)

Joint with Lisa Sauermann

April 1, 2021

ἐζητεῖτο δὲ καὶ παρὰ τοῖς γεωμέτραις… καὶ ἐκαλεῖτο τὸ τοιοῦτον πρόβλημα κύβον διπλασιασμός… πάντων δὲ διαπορούντων ἐπὶ πολὺν χρόνον πρῶτος Ἱπποκράτης ὁ Χῖος… τὸ ἀπόρημα αὐτῷ εἰς ἕτερον οὐκ ἔλασσον ἀπόρημα κατέστρεφεν.

This was investigated by the geometers… and they called this problem "duplication of a cube"… And, after they were all puzzled by this for a long time, Hippocrates of Chios… converted the puzzle into another, no smaller puzzle.

Eratosthenes of Cyrene (translated by Reviel Netz)

Outline

Introduction: constrained covers of the hypercube

Covering with multiplicity

Our results

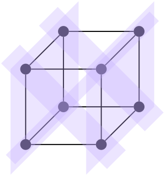
Proof sketch

Concluding remarks

Covering the hypercube by skew hyperplanes

Question

What is the minimum number of skew hyperplanes needed to cover the vertices of the hypercube $\{0, 1\}^n$? Two.



Skew: all normal vector coordinates $\neq 0$

Folklore, Yehuda–Yehudayoff 2021:

$$cn^{0.51} \leq \#(\text{skew hyperplanes}) \leq n.$$

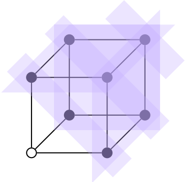
Open problem: Improve either bound.

This has connections to certain lower bounds in complexity theory.

Covering the hypercube minus a point

Question

What is the minimum number of hyperplanes needed to cover the vertices of the hypercube $\{0,1\}^n$ except $\vec{0}$ (without covering $\vec{0}$)?



There are at least 2 ways of doing it with n hyperplanes:

$$x_1 = 1, x_2 = 1, \ldots, x_n = 1 \qquad \text{and} \qquad \sum_{i=1}^{n} x_i = 1, \; \ldots, \; \sum_{i=1}^{n} x_i = n.$$

Theorem (Alon–Füredi 1993)

At least n hyperplanes are needed to cover $\{0,1\}^n \setminus \{\vec{0}\}$.

This answers a question of Komjáth arising in infinite Ramsey theory.

The Alon–Füredi theorem: geometry vs. algebra

Theorem (Alon–Füredi 1993)

At least n hyperplanes are needed to cover $\{0,1\}^n \setminus \{\vec{0}\}$.

The statement is geometric, but all known proofs are algebraic.

Theorem (Alon–Füredi 1993)

Let $P \in \mathbb{R}[x_1, \dots, x_n]$ be a polynomial with zeroes at all points in $\{0,1\}^n \setminus \{\vec{0}\}$, but such that $P(\vec{0}) \neq 0$. Then $\deg P \geq n$.

This is a stronger statement: any hyperplane cover can be converted into a polynomial cover by multiplying together all defining equations of the hyperplanes.

Luckily, the geometric and algebraic questions have the same answer!

This is a special case of Alon's Combinatorial Nullstellensatz, which has many other applications in combinatorics.

Proof of the Alon–Füredi theorem

Theorem (Alon–Füredi 1993)

Let $P \in \mathbb{R}[x_1, \ldots, x_n]$ be a polynomial with zeroes at all points in $\{0, 1\}^n \setminus \{\vec{0}\}$, but such that $P(\vec{0}) \neq 0$. Then $\deg P \geq n$.

Step 0: Assume WLOG that $P(\vec{0}) = 1$.

Step 1: Convert P to reduced form $\overline{P}$: replace each x_i^m by x_i.

Note that $\deg \overline{P} \leq \deg P$ and $\overline{P}$ agrees with P on $\{0, 1\}^n$.

Step 2: Every function $\{0, 1\}^n \to \mathbb{R}$ has a unique representation as a reduced polynomial.

This follows from dimension counting.

Step 3: One representation of the function P is as

$$\widetilde{P} = (1 - x_1)(1 - x_2) \cdots (1 - x_n),$$

which is reduced. So $\overline{P} = \widetilde{P}$, and $\deg P \geq \deg \widetilde{P} = n$. $\square$

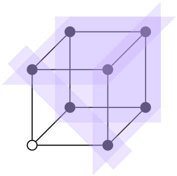
Outline

Covering with multiplicity

Question (Clifton–Huang 2020)

What is the minimum number of hyperplanes needed to cover every point of $\{0,1\}^n \setminus \{\vec{0}\}$ at least k times (without covering $\vec{0}$)?

$k = 2$: $n + 1$ hyperplanes are necessary and sufficient.



Theorem (Clifton–Huang 2020)

For fixed n and $k \to \infty$,

$$\left(1 + \frac{1}{2} + \cdots + \frac{1}{n} + o(1)\right) k$$

hyperplanes are necessary and sufficient.

From now on: k is fixed and $n \to \infty$.

A simple upper bound

Question (Clifton–Huang 2020)

What is the minimum number of hyperplanes needed to cover every point of $\{0,1\}^n \setminus \{\vec{0}\}$ at least k times (without covering $\vec{0}$)?

Start with the n hyperplanes

$$x_1 = 1, \quad x_2 = 1, \quad \dots \quad x_n = 1.$$

A vector with t ones is covered t times. Add the hyperplanes

$$\underbrace{\sum_{i=1}^{n} x_i = 1,}_{k-1 \text{ times}} \quad \underbrace{\sum_{i=1}^{n} x_i = 2,}_{k-2 \text{ times}} \quad \dots \quad \underbrace{\sum_{i=1}^{n} x_i = k-1\,.}_{1 \text{ time}}$$

This uses $n + (k-1) + (k-2) + \cdots + 1 = n + \binom{k}{2}$ hyperplanes.

Conjecture (Clifton–Huang 2020)

$n + \binom{k}{2}$ hyperplanes are also necessary for n sufficiently large.

Lower bounds

Question (Clifton–Huang 2020)

What is the minimum number of hyperplanes needed to cover every point of $\{0, 1\}^n \setminus \{\vec{0}\}$ at least k times (without covering $\vec{0}$)?

	Lower bound	Upper bound: $n + \binom{k}{2}$
$k = 1$	n	n
$k = 2$	$n + 1$	$n + 1$
$k = 3$	$n + 3$	$n + 3$
$k \geq 4$	$n + k + 1$	$n + \binom{k}{2}$

These statements are geometric, but all known proofs are algebraic.

Question

What is the minimum degree of a polynomial $P \in \mathbb{R}[x_1, \ldots, x_n]$ with zeroes of multiplicity $\geq k$ at all points in $\{0, 1\}^n \setminus \{\vec{0}\}$, but $P(\vec{0}) \neq 0$?

This is a more general notion: any hyperplane cover yields such a P.

Algebraically covering with multiplicities

Question

What is the minimum degree of a polynomial $P \in \mathbb{R}[x_1, \ldots, x_n]$ with zeroes of multiplicity $\geq k$ at all points in $\{0, 1\}^n \setminus \{\vec{0}\}$, but $P(\vec{0}) \neq 0$?

Recall: P has a zero of multiplicity $\geq k$ at $a \in \mathbb{R}^n$ if all derivatives of P of order $\leq k - 1$ vanish at a.

Theorem (Ball–Serra 2009, Clifton–Huang 2020)

For $n \geq 3$,

- *Any such P must have degree $\geq n + k - 1$.*
- *For $k = 3$, any such P must have degree $\geq n + 3$.*
- *For $k \geq 4$, any such P must have degree $\geq n + k + 1$.*

All these proofs use a higher-order ("punctured") version of the Combinatorial Nullstellensatz, due to Ball and Serra.

A more general question

Question

What is the minimum number of hyperplanes needed to cover every point of $\{0,1\}^n \setminus \{\vec{0}\}$ at least k times while covering $\vec{0}$ exactly ℓ times (for fixed $0 \leq \ell < k$)?

For $\ell = 0$, this is exactly the same problem as before.

Upper bound: $n + \binom{k-\ell}{2} + 2\ell$ hyperplanes suffice.

(Add ℓ copies of $x_1 = 0$ and $x_1 = 1$ to the $(k-\ell)$-cover above.)

- $\ell = k-3$: $n + 2k - 3$ hyperplanes suffice.
- $\ell = k-2$: $n + 2k - 3$ hyperplanes suffice.
- $\ell = k-1$: $n + 2k - 2$ hyperplanes suffice.

Question

What is the minimum degree of a polynomial $P \in \mathbb{R}[x_1, \dots, x_n]$ with zeroes of multiplicity $\geq k$ on $\{0,1\}^n \setminus \{\vec{0}\}$, and multiplicity $= \ell$ at $\vec{0}$?

Outline

Exact answers to the algebraic questions

Question

What is the minimum degree of a polynomial $P \in \mathbb{R}[x_1, \dots, x_n]$ with zeroes of multiplicity $\geq k$ at all points in $\{0, 1\}^n \setminus \{\vec{0}\}$, but $P(\vec{0}) \neq 0$?

Theorem (Sauermann–W. 2020)

For any $k \geq 2$ and $n \geq 2k - 3$, any such P has $\deg P \geq n + 2k - 3$. Moreover, there exists such a P with $\deg P \leq n + 2k - 3$.

Question

What is the minimum degree of a polynomial $P \in \mathbb{R}[x_1, \dots, x_n]$ with zeroes of multiplicity $\geq k$ on $\{0, 1\}^n \setminus \{\vec{0}\}$, and multiplicity $= \ell$ at $\vec{0}$?

Theorem (Sauermann-W. 2020)

For $0 \leq \ell \leq k - 2$, the answer is $n + 2k - 3$.
For $\ell = k - 1$, the answer is $n + 2k - 2$.

Lower bounds for hyperplane coverings

Question (Clifton–Huang 2020)

What is the minimum number of hyperplanes needed to cover every point of $\{0, 1\}^n \setminus \{\vec{0}\}$ at least k times (without covering $\vec{0}$)?

Our theorem implies that $\geq n + 2k - 3$ hyperplanes are necessary.

Question

What is the minimum number of hyperplanes needed to cover every point of $\{0, 1\}^n \setminus \{\vec{0}\}$ at least k times while covering $\vec{0}$ exactly ℓ times (for fixed $0 \leq \ell < k$)?

- $\ell \leq k - 2$: $\geq n + 2k - 3$ hyperplanes are necessary
- $\ell = k - 1$: $\geq n + 2k - 2$ hyperplanes are necessary

In particular, the hyperplane problem is resolved for $\ell \geq k - 3$.
(Since we previously saw matching upper bounds.)

Algebra (maybe) isn't enough!

Question (Clifton–Huang 2020)

What is the minimum number of hyperplanes needed to cover every point of $\{0, 1\}^n \setminus \{\vec{0}\}$ at least k times (without covering $\vec{0}$)?

Conjecture (Clifton–Huang 2020)

The answer is $n + \binom{k}{2}$ for n sufficiently large.

Either this conjecture is false, or it cannot be proved via "purely algebraic" techniques!

("Purely algebraic" = techniques that work for all polynomials)

To my knowledge, all lower bounds for such problems are "purely algebraic".

Outline

Proof sketch

Theorem (Sauermann–W. 2020)

Fix $k \geq 2$ and $n \geq 2k-3$. If $P \in \mathbb{R}[x_1, \dots, x_n]$ has $P(\vec{0}) \neq 0$ but P has zeroes of multiplicity $\geq k$ on $\{0,1\}^n \setminus \{\vec{0}\}$, then $\deg P \geq n + 2k - 3$.

(Along the way, we'll construct such a P with $\deg P \leq n + 2k - 3$.)

Recall Alon–Füredi: for $k = 1$, we have $\deg P \geq n$.

The proof had three steps:

1. Convert P to reduced form $\overline{P}$, such that $\deg \overline{P} \leq \deg P$ and $\overline{P}$ agrees with P on $\{0,1\}^n$.
2. Every function $\{0,1\}^n \to \mathbb{R}$ has a unique representation as a reduced polynomial.
3. Find a reduced representation of P with degree n.

Step 1: reduced form

Alon–Füredi

Replacing x_i^2 by x_i does not change the evaluation on $\{0,1\}^n$.

This is because

$$(x_i^2 - x_i)Q(x_1, \dots, x_n)$$

vanishes on $\{0,1\}^n$, so subtracting such terms from P does not change the evaluation on $\{0,1\}^n$.

By repeatedly doing this, we can eliminate all monomials divisible by x_i^2.

Our setting

We want to convert P to $\overline{P}$ such that the property of vanishing to multiplicity $\geq k$ on $\{0,1\}^n \setminus \{\vec{0}\}$ is preserved (as is the property $\overline{P}(\vec{0}) \neq 0$).

We can subtract

$$(x_{i_1}^2 - x_{i_1}) \cdots (x_{i_k}^2 - x_{i_k})Q, \quad \text{or}$$

$$(x_{i_1}^2 - x_{i_1}) \cdots (x_{i_{k-1}}^2 - x_{i_{k-1}}) \cdot (x_1 - 1) \cdots (x_n - 1)Q$$

for (not necessarily distinct) $i_1, \dots, i_k \in [n]$, and any Q.

We can eliminate all monomials divisible by $x_{i_1}^2 \cdots x_{i_k}^2$ or by $x_{i_1}^2 \cdots x_{i_{k-1}}^2 \cdot x_1 \cdots x_n$.

Such polynomials are reduced.

Reduced polynomials

A polynomial is reduced if it has no monomial divisible by

$$x_{i_1}^2 \cdots x_{i_k}^2 \qquad \text{or} \qquad x_{i_1}^2 \cdots x_{i_{k-1}}^2 \cdot x_1 \cdots x_n.$$

Every reduced polynomial has degree $\leq n + 2k - 3$ (pigeonhole).

Lemma

For any $P \in \mathbb{R}[x_1, \ldots, x_n]$, there exists a reduced $\overline{P}$ with $\deg \overline{P} \leq \deg P$ such that

- *All derivatives of order $\leq k - 1$ of P and $\overline{P}$ agree on $\{0, 1\}^n \setminus \{\vec{0}\}$*
- *All derivatives of order $\leq k - 2$ of P and $\overline{P}$ agree on $\vec{0}$.*

This implies the second part of our theorem: there exists a polynomial with zeroes of multiplicity $\geq k$ on $\{0, 1\}^n \setminus \{\vec{0}\}$ but not vanishing on $\vec{0}$ with degree $\leq n + 2k - 3$.

Proof: Simply pick your favorite high-degree polynomial with this property, and reduce it!

Step 2: Unique representation in reduced form

Alon–Füredi

Every function $\{0, 1\}^n \to \mathbb{R}$ has a unique representation as a reduced polynomial.

In other words: given desired values at each point of $\{0, 1\}^n$, there is a unique reduced polynomial taking these values.

Proof: Dimension counting, and the linear map

$$\{\text{reduced polys}\} \to \{\text{values}\}$$

is surjective.

Our setting

Given values for all derivatives

- Of order $\leq k - 1$ on $\{0, 1\}^n \setminus \{\vec{0}\}$,
- Of order $\leq k - 2$ on $\vec{0}$,

there is a unique reduced polynomial taking these values.

Proof: Dimension counting, and the linear map

$$\{\text{reduced polys}\} \to \{\text{values}\}$$

is surjective.

Step 3: Finishing the proof

Alon–Füredi

We want to show that any P that vanishes on $\{0,1\}^n \setminus \{\vec{0}\}$ with $P(\vec{0}) = 1$ has $\deg P \geq n$.

We write down the polynomial

$$\widetilde{P} = (1 - x_1) \cdots (1 - x_n)$$

which is reduced and agrees with P on $\{0,1\}^n$.

Since $\deg \widetilde{P} = n$, we are done by Steps 1 and 2.

Our setting

We want to show that any P that vanishes to multiplicity $\geq k$ on $\{0,1\}^n \setminus \{\vec{0}\}$ with $P(\vec{0}) \neq 0$ has $\deg P \geq n + 2k - 3$.

It suffices to prove this for reduced P.

This is hard!

In the Alon–Füredi setting, there was one reduced polynomial with this property, $\widetilde{P}$.

In our setting, there are very many.

Linear algebra to the rescue

Let V_k be the vector space of reduced polynomials with zeroes of multiplicity $\geq k$ on $\{0,1\}^n \setminus \{\vec{0}\}$. Recall that $\deg P \leq n+2k-3$ for all $P \in V_k$. To finish, it suffices to prove:

Lemma

$\deg P = n+2k-3$ *for every non-zero* $P \in V_k$.

Let $H_k : V_k \to \mathbb{R}[x_1, \ldots, x_n]$ be the linear map sending a polynomial to its homogeneous part of degree $n+2k-3$.

$$\text{Lemma} \iff H_k \text{ is injective} \iff \dim(\operatorname{im} H_k) \geq \dim V_k$$

So it suffices to identify $W_k \subseteq \mathbb{R}[x_1, \ldots, x_n]$ with $\dim W_k = \dim V_k$ such that H_k is surjective onto W_k.

Identifying the image

It suffices to identify $W_k \subseteq \mathbb{R}[x_1, \ldots, x_n]$ with $\dim W_k = \dim V_k$ such that H_k is surjective onto W_k.

Let W_k be the subspace spanned by all polynomials of the form

$$x_1 \cdots x_n \cdot (x_1^m + \cdots + x_n^m) \cdot x_1^{2d_1} \cdots x_n^{2d_n} \qquad (\star)$$

for non-negative $(m, d_1, \ldots, d_n)$ with $m + 2(d_1 + \cdots + d_n) = 2k - 3$.

Fact: $\dim W_k = \dim V_k = \binom{n+k-2}{n}$.

So it suffices to show that H_k is surjective onto W_k.

Surjectivity onto basis elements $(\star)$ with some $d_i > 0$ is straightforward by induction on k. So it suffices to prove:

Key lemma

There is a polynomial $R \in V_k$ with $H_k(R) \in W_k$ and the coefficient of the basis element $x_1 \cdots x_n \cdot (x_1^{2k-3} + \cdots + x_n^{2k-3})$ in $H_k(R)$ is non-zero.

Proof of the key lemma

Key lemma

There is a polynomial $R \in V_k$ with $H_k(R) \in W_k$ and the coefficient of the basis element $x_1 \cdots x_n \cdot (x_1^{2k-3} + \cdots + x_n^{2k-3})$ in $H_k(R)$ is non-zero.

Writing down an explicit such R is hard!

Instead, we start with the high-degree polynomial

$$(x_1 - 1)^k \cdots (x_n - 1)^k$$

and apply the reduction algorithm to get an element of V_k.

When we do this and apply H_k, the relevant basis coefficient is

$$\sum_{(s_1,\dots,s_t)} (-1)^t \cdot \binom{k-1-s_1}{s_1-1} \binom{k-1-s_2}{s_2} \cdots \binom{k-1-s_t}{s_t},$$

where the sum is over all sequences $(s_1, \dots, s_t)$ of positive integers with $s_1 + \cdots + s_t = k - 1$.

The sum is non-zero

To conclude, it suffices to prove:

Lemma

For $k \geq 2$, we have

$$\sum (-1)^t \binom{k-1-s_1}{s_1-1} \binom{k-1-s_2}{s_2} \cdots \binom{k-1-s_t}{s_t} = (-1)^{k-1} C_{k-2}$$

where the sum is over all sequences $(s_1, \dots, s_t)$ of positive integers with $s_1 + \cdots + s_t = k-1$.

> *"You have to check that something is non-zero, and that can be very hard... There are very many numbers, and if it's not zero it can be any of them."* –June Huh

The values of this sum are

$$-1,\ 1,\ -2,\ 5,\ -14,\ 42,\ -132,\ 429,\ -1430,\ 4862,\ -16796\dots$$

These are the Catalan numbers! They're given by $C_i = \frac{1}{i+1}\binom{2i}{i}$.

Proof summary

- The sum on the previous slide is non-zero.
- There is some $R \in V_k$ whose homogeneous part $H_k(R)$ has a non-zero coefficient of the basis element $x_1 \cdots x_n \cdot (x_1^{2k-3} + \cdots + x_n^{2k-3})$ of W_k.
- Together with induction on k, this shows that $\operatorname{im} H_k \supseteq W_k$.
- Since $\dim V_k = \dim W_k$, H_k must be injective.
- V_k was defined as the space of reduced polynomials with zeroes of multiplicity $\geq k$ on $\{0,1\}^n \setminus \{\vec{0}\}$. So every such polynomial has degree $n + 2k - 3$.
- Combining this with Steps 1 and 2, we conclude that every polynomial P with zeroes of multiplicity $\geq k$ on $\{0,1\}^n \setminus \{\vec{0}\}$ and $P(\vec{0}) \neq 0$ must have $\deg P \geq n + 2k - 3$.

Outline

Other fields

Question

What is the minimum number of hyperplanes in $\mathbb{F}^n$ needed to cover every point of $\{0,1\}^n \setminus \{\vec{0}\}$ at least k times (without covering $\vec{0}$)?

Theorem (Bishnoi–Boyadzhiyska–Das–Mészáros 2021)

Over $\mathbb{F}_2$, the answer is in $\left[n + \lfloor \frac{k-1}{2} \rfloor \log \frac{2n}{k-1}\ ,\ n + (k-1)\log(2n)\right]$.

Question

What is the minimum degree of a polynomial $P \in \mathbb{F}[x_1, \ldots, x_n]$ with zeroes of multiplicity $\geq k$ at all points in $\{0,1\}^n \setminus \{\vec{0}\}$, but $P(\vec{0}) \neq 0$?

Theorem (Sauermann–W. 2020)

If $\operatorname{char} \mathbb{F} \nmid C_{k-2}$, *the answer is* $n + 2k - 3$.
If k is minimal such that $\operatorname{char} \mathbb{F} \mid C_{k-2}$, *the answer is* $\leq n + 2k - 4$.

$\mathbb{F}_2$ is different from $\mathbb{R}$, and geometry is different from algebra!

Open problems

Conjecture (Clifton–Huang 2020)

$n + \binom{k}{2}$ hyperplanes are necessary to cover $\{0, 1\}^n \setminus \{\vec{0}\}$ with multiplicity $\geq k$, while not covering $\vec{0}$ (for n sufficiently large).

- Prove this conjecture!
  - Find a non-algebraic proof for the Alon–Füredi theorem (n hyperplanes are needed for $k = 1$).
  - Prove strengthenings of the Combinatorial Nullstellensatz under strengthened assumptions on the polynomial (e.g. it splits into linear factors).
- Understand what happens over finite fields.
  - If char $\mathbb{F} \mid C_{k-2}$, then the answer to the polynomial problem is $n + 2k - 3$. Is the converse true?
  - Combinatorial techniques may be more fruitful for the hyperplane problem in finite fields.

Thank you!