An etude on polynomials over finite rings in Computational Complexity Theory

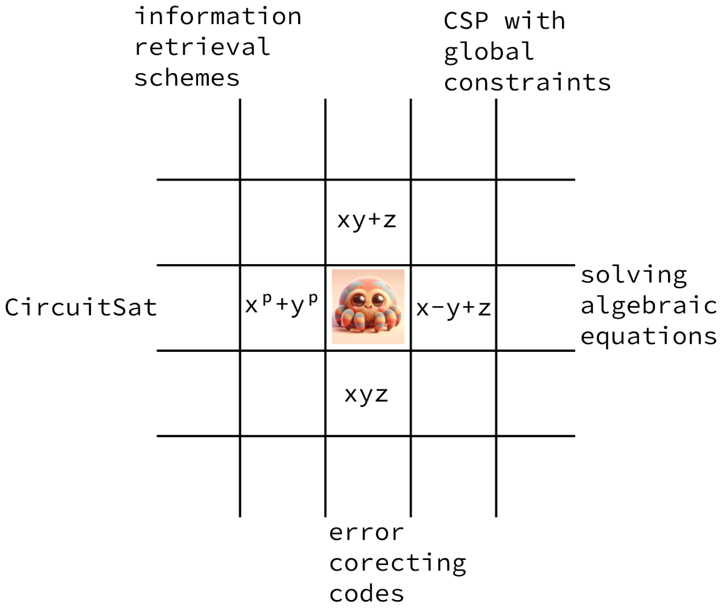
Piotr Kawałek

TU Wien

28 XI 2023

European Research Council
Established by the European Commission

ERC Synergy Grant POCOCOP (GA 101071674)


information retrieval schemes
CSP with global constraints
xy+z
CircuitSat
x^p+y^p
x-y+z
solving algebraic equations
xyz
error corecting codes

Quick reminder

We consider polynomials over the ring $(\mathbb{Z}_m, +, \cdot)$, where m - integer.

Polynomials of arity n are expressions from $\mathbb{Z}_m[x_1, \ldots, x_n]$

- Polynomial naturally represents a function $(\mathbb{Z}_m)^n \longmapsto \mathbb{Z}_m$
- Polynomials can also represent a function $\{0, 1\}^n \longmapsto \mathbb{Z}_m$

Polynomials in sparse form

We say a polynomial is written in an s-sparse form if it is presented as a sum of s monomials.

4-sparse form:

$$xz + xt + yz + yt$$

Not s-sparse form:

$$(x + y)(z + t)$$

Representing Boolean functions

Polynomials over $(\mathbb{Z}_m, +, \cdot)$ can be used to represent Boolean functions $\{0,1\}^n \longmapsto \{0,1\} \subseteq \mathbb{Z}_m$:

Negation: $\mathbf{f}(x) = 1 - x$

NOR: $\mathbf{f}(x, y) = xy - x - y + 1$

AND$_n$: $\mathbf{f}(x_1, \ldots, x_n) = x_1 \cdot \ldots \cdot x_n$

In fact every Boolean function can be represented as a polynomial over $(\mathbb{Z}_m, +, \cdot)$. However, most of the n-ary functions require large degree (close to n).

Uniqueness

Every function $\{0,1\}^n \longmapsto \mathbb{Z}_m$ has a unique representation as a sparse multilinear polynomial. To get this representation just:

1. Perform all the multiplications to get sparse form
2. Replace each occurance of x^k with x (on Boolean domain $x^k \equiv x$)

Why is it unique?

- Every n-ary function has a representation,
- there is the same number of functions and representations.

Degree for the conjunction

$\mathrm{AND}_n \rightarrow \quad \mathbf{f}(x_1, \ldots, x_n) = x_1 \cdot \ldots \cdot x_n$ of degree n.

What does it even mean that we represent AND_n in $(\mathbb{Z}_m, +, \cdot)$?

Strong representation:

$$\begin{aligned} \mathbf{f}(x_1, \ldots, x_n) = 1 \quad & \text{if } x_i = 1 \text{ for all } i \\ \mathbf{f}(x_1, \ldots, x_n) = 0 \quad & \text{if } x_i = 0 \text{ for some } i \end{aligned}$$

Degree for the conjunction

$\mathrm{AND}_n \rightarrow \quad \mathbf{f}(x_1, \ldots, x_n) = x_1 \cdot \ldots \cdot x_n$ of degree n.

What does it even mean that we represent AND_n in $(\mathbb{Z}_m, +, \cdot)$?

Weak representation:

$$\begin{aligned} \mathbf{f}(x_1, \ldots, x_n) &= a \quad \text{if } x_i = 1 \text{ for all } i \\ \mathbf{f}(x_1, \ldots, x_n) &\neq a \quad \text{if } x_i = 0 \text{ for some } i \end{aligned}$$

Weak representation for conjunction

Ring: $(\mathbb{Z}_m, +, \cdot)$

With weak representation we can get smaller degree than n:

$$x_1 \cdot \ldots x_{n/2} + x_{1+n/2} \cdot \ldots \cdot x_n$$

value 2 is achieved only for $x_1 = \ldots = x_n = 1$.

But by spliting variables uniformly into $m-1$ monomials we can achieve degree $\frac{n}{m-1}$.

Weak representation - optimal for a prime p

Ring: $(\mathbb{Z}_p, +, \cdot)$

When $m = p$ is a prime the degree $\frac{n}{p-1}$ is optimal. Why?

Let $\mathbf{q}(x_1, \ldots, x_n)$ weakly represent AND_n, let $\mathbf{q}(1, \ldots, 1) = a$.

Define a new polynomial $\mathbf{p}(\overline{x}) = 1 - (\mathbf{q}(\overline{x}) - a)^{p-1}$. Notice that:

$$\begin{aligned} \mathbf{p}(x_1, \ldots, x_n) &= 1 \quad \text{if } x_i = 1 \text{ for all } i \\ \mathbf{p}(x_1, \ldots, x_n) &= 0 \quad \text{if } x_i = 0 \text{ for some } i \end{aligned}$$

So $\mathbf{p}$ strongly represents AND_n! The unique sparse multilinear form of $\mathbf{p}$ must be $x_1 \cdot \ldots \cdot x_n$. So $\deg \mathbf{p} = n$ but

$$n = \deg \mathbf{p} \leqslant \deg \mathbf{q} \cdot (p-1)$$

hence $\deg \mathbf{q} \geqslant \frac{n}{p-1}$

Weak representation - $m = 6$

Ring: $(\mathbb{Z}_6, +, \cdot)$

Barrington, Beigel, Rudrich, *1994*

There is a polynomial $\mathbf{p}(\overline{x})$ over $(\mathbb{Z}_6, +, \cdot)$ weakly representing AND_n of degree $O(\sqrt{n})$.

Or more generally:

Barrington, Beigel, Rudrich, *1994*

Let m have r distinct prime divisors.

There is a polynomial $\mathbf{p}(\overline{x})$ over $(\mathbb{Z}_m, +, \cdot)$ weakly representing AND_n of degree $O(\sqrt[r]{n})$.

We will see the construction at the end!

Weak representation - lower bounds

Barrington, Tardos, *1998*

Let m have r distinct prime divisors.

Any polynomial $\mathbf{p}(\overline{x})$ over $(\mathbb{Z}_m, +, \cdot)$ weakly representing AND_n must have degree at least $\Omega((\log n)^{1/r-1})$.

We have exponential gap between lower bound and upper bound!

$$(\log n)^{1/r-1} \quad \text{vs} \quad n^{1/r}$$

No progress for > 20 years despite many potential applications

Degree vs length

Ring: $(\mathbb{Z}_p, +, \cdot)$

$$\mathbf{p}(x_1, \ldots, x_n) = x_1 \cdot \ldots \cdot x_n$$

Degree: n (in range $0 - n$)

Length: 1 (in range $0 - 2^n$)

The degree is large while length (sparsity) is low. This is a problem.

Solution: redefine what we mean by monomial.

Old s-sparse form vs new s-sparse form

Let $X = \{x_1, \dots, x_n\}$.

Old sparse form:

$$\sum_{V \subseteq X} \alpha_V \prod_{v \in V} v$$

New sparse form:

$$\sum_{V \subseteq X} \alpha_V \prod_{v \in V} (-1)^v$$

In both cases we measure length (sparsity s) with the number of non-zero α_V

Values $\{0, 1\}$ are now naturally interpreted as a multiplicative subgroup of $(\mathbb{Z}_m^*, \cdot)$ isomorphic to $(\mathbb{Z}_2, +)$.

Old s-sparse form vs new s-sparse form

Whem m is odd, the degree of a function $\{0,1\}^n \longmapsto \mathbb{Z}_m$ is the same in old and a new representation.
Reason: the mapping $x \longmapsto 2^{-1} \cdot (x+1)$.
Corollary: all functions $\{0,1\}^n \longmapsto \mathbb{Z}_m$ have a unique, new s-sparse form.

Degree vs length

Ring: $(\mathbb{Z}_p, +, \cdot)$

$$\mathbf{p}(x_1, \ldots, x_n) \text{ weakly representing } \mathrm{AND}_n$$

Degree: $\Omega(n)$ (in old and new form)

Length: $2^{\Omega(n)}$ (in new form)

The proof is by Barrington, Straubing and Thérien (1990).

Results on length

Barrington, Beigel, Rudrich, *1994*

Let m have r distinct prime divisors.

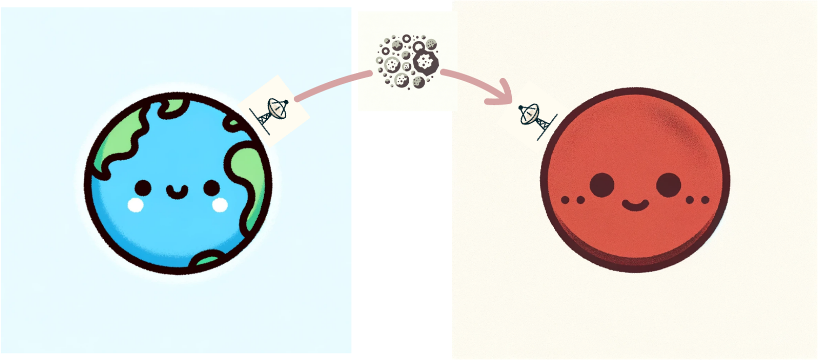
There is a polynomial $\mathbf{p}(\overline{x})$ over $(\mathbb{Z}_m, +, \cdot)$ weakly representing AND_n of length $2^{O(n^{1/r} \log n)}$.

Chattopadhyay, Goyal, Pudlak, Therien, *2006*

Let m have r distinct prime divisors.

Any polynomial $\mathbf{p}(\overline{x})$ over $(\mathbb{Z}_m, +, \cdot)$ weakly representing AND_n must have length at least $\Omega(n)$.

Error correcting codes



Error correcting codes - applications

1. digital communication systems
2. computer memory
3. data storage devices
4. internet and network transmission
5. broadcasting
6. QR codes and barcodes
7. deep space missions
8. secure communication
9. warfare devices

Error correcting codes - parameters

1. We want to encode k-bit message x into N-bit codeword $C(x)$.
2. We assume that at most δ fraction of bits can be corrupted, so at least $(1-\delta)|C(x)|$ bits are correct.
3. Additionally we want the code to be **locally decodable**, i.e. to find an i-th bit of x we read r bits of $C(x)$ using some probabilistic procedure. We succeed with probability at least $1-\epsilon$.

Error correcting codes - parameters

(r, δ, ϵ)-localy decodable code translates k-bit message to $f(k)$-bit code.

- We want δ, ϵ to be constant, preferably δ around $\frac{1}{4}$
- r also should be constant, or at least some small function of k
- $f(k)$ should be some very small function of k.

Matching Vector Codes

BBR94 construction of AND_n using polynomial over $\mathbb{Z}_m$ of degree $O(\sqrt[r]{n})$ leads to so-called Matching Vector Codes.

This codes are based on 2 families of vectors $u_1, \ldots, u_k$ and $v_1, \ldots, v_k$ over $\mathbb{Z}_m^n$. They are matching in a sense that $(u_i, v_i) = 0$ while $(u_i, v_j) \neq 0$ for $i \neq j$.

Dvir, Gopalan, Yekhanin, 2011

There are good (r, δ, ϵ)-locally decodable Matching Vector codes with δ being constant and ϵ being constant if r is small enough. There is a complicated trade-off between r and the size of the code.

Parameters

The (r, δ, ϵ)-code is parametrized with $\delta \in (0, 1)$ and $t \in \mathbb{N}$.

- number of trials $r = t^{O(t)}$
- probability of failure $\epsilon = 4\delta(1 + 1/(\log t))$
- size of the code is $\exp\exp((\log k)^{1/t}(\log\log k)^{1-1/t})$.

Ramsey Graphs

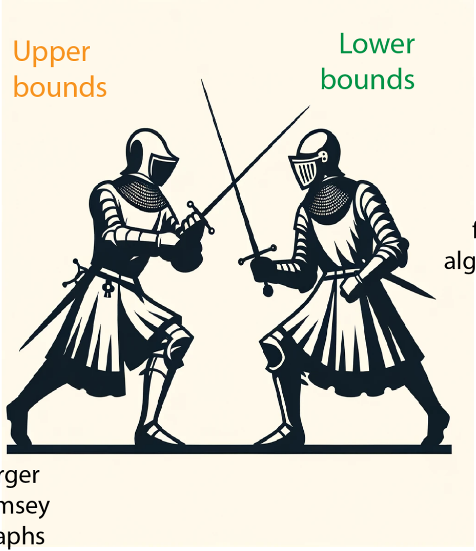
Fix k.

How to contruct a large graph,
which does not have k-clique nor k-independent set?

Grolmusz, 2000

There is explicit construction of graphs of size $2^{\Omega((\log k)^2/\log\log k)}$.

But also: if we construct AND_n with degree n^ϵ over $\mathbb{Z}_6$
we get a Ramsey graph of size $2^{\Omega((\log k)^{1/\epsilon}/(\log\log k)^{1/\epsilon-1}}$



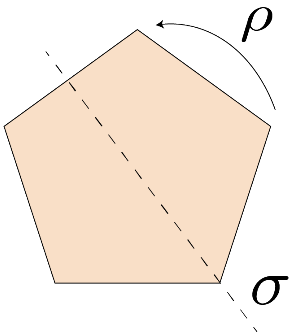
error
correcting
codes

anonymous
databases

larger
Ramsey
graphs

faster
algorithms

$\mathbf{D}_m$ - group of symmetry of regular m-gon



Elements of $\mathbf{D}_m$

Rotations: $\rho^0, \rho^1, \ldots, \rho^{m-1}$

Reflections $\sigma, \sigma \circ \rho, \ldots, \sigma \circ \rho^{m-1}$

Equations - examples

Has solution:

$$x \circ \sigma \circ y = \rho$$

Has no solution:

$$x \circ y \circ x^{-1} \circ y^{-1} = \sigma$$

Equations - algorithm

Random Sampling: just put random values for variables.

Assume you have lower bound $s(n)$ for the **length** of polynomial over $\mathbb{Z}_m$ representing AND_n.

Idziak, PK, Krzaczkowski, 2022

For equation of length l in the group $\mathbb{D}_m$ the random sampling algorithm with $O(2^{s^{-1}(l)})$ trials finds a solution if it exists with probability $1-\epsilon$.

If $s(n) = 2^{\sqrt[r]{n}}$ then algorithm needs $n^{(\log n)^r}$ samples.

Solving systems of linear equations

Consider systems of linear equations over domain $\{0, 1\}$.

$$
\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &\equiv b_1 \pmod 2,\\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &\equiv b_2 \pmod 2,\\
&\vdots\\
a_{(k-1)1}x_1 + a_{(k-1)2}x_2 + \cdots + a_{(k-1)n}x_n &\equiv b_{k-1} \pmod 2,\\
a_{k1}x_1 + a_{k2}x_2 + \cdots + a_{kn}x_n &\equiv b_k \pmod m.
\end{aligned}
$$

How to solve them when 1 equation is modulo m?

This problem enebles to classify Boolean CSP's with global modular constraints which admit polynomial-time solution.

Algorithm

Random Sampling:

1. Ignore the equation modulo m.
2. Compute affine subspace of solutions to the system modulo 2.
3. In the subspace, take R random points.
4. If some of the random points satisfies also the last equation we return a solution.
5. Otherwise we say there is no solution.

Brakensiek, Gopi, Guruswami, 2019

The better lower bounds for the length of AND_n,
the smaller R is required.

Upper bounds

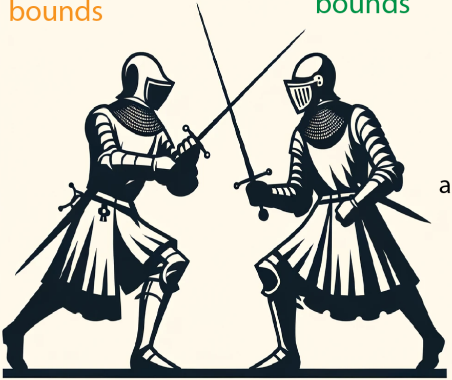
Lower bounds

error correcting codes

anonymous databases

larger Ramsey graphs

faster algorithms



Weak representation - $m = 6$

Ring: $(\mathbb{Z}_6, +, \cdot)$

Barrington, Beigel, Rudrich, *1994*

There is a polynomial $\mathbf{p}(\overline{x})$ over $(\mathbb{Z}_6, +, \cdot)$ weakly representing AND_n of degree $O(\sqrt{n})$.

Or more generally:

Barrington, Beigel, Rudrich, *1994*

Let m have r distinct prime divisors.

There is a polynomial $\mathbf{p}(\overline{x})$ over $(\mathbb{Z}_m, +, \cdot)$ weakly representing AND_n of degree $O(\sqrt[r]{n})$.

Funding

Funding statement: Funded by the European Union (ERC, POCOCOP, 101071674). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.