What is...the Schwartz–Zippel lemma?

Or: The art of not solving equations

Polynomial identity testing (PIT)

Polynomial $f(x_1, ..., x_n)$, polynomial $g(x_1, ..., x_n)$

Question. Is $f = g$? Equivalently, is $f - g = 0$?

Problem 1. The polynomials might come in disguise

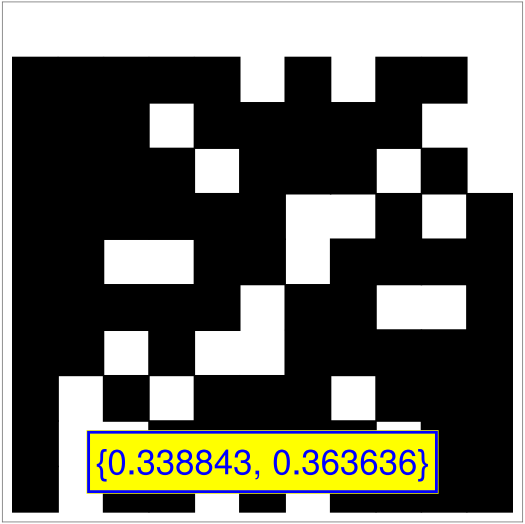
- $f = (x_1 - x_2)(x_1 + x_2)$, $g = x_1^2 - x_2^2$
- These are equal but one needs to factor f into monomials to see this

Problem 2. Factoring polynomials is costly

- $f = \prod_{i=1}^{n}(x_i + x_{i+1})$ has length $O(n)$
- f expands into $O(2^n)$ monomials

A threshold for being a root

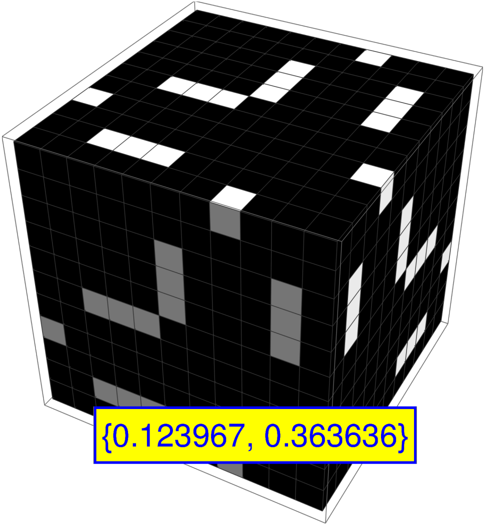
$f(x, y) = \prod_{i=0}^{d-1}(x + i \cdot y)$ and its roots in $\mathbb{F}_p^2$, for $p = 11, d = 4$:



Left number: percentage of roots; right number: d/p

The threshold does not depend on the number of variables?

$f(x, y, z) = x^d + y^d + z^d + x + y + z + 1$ and its roots in $\mathbb{F}_p^3$, for $p = 11, d = 4$:



Left number: percentage of roots; right number: d/p

Enter, the theorem!

(a) $f(x_1, \ldots, x_n)$ a degree $d > 1$ polynomial with coefficients in some field $\mathbb{K}$

(b) $S \subset \mathbb{K}$

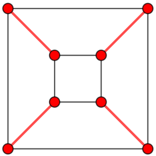
(c) $r_1, \ldots, r_n \in S$ chosen randomly

If f is non-zero, then $f(r_1, \ldots, r_n) = 0$ holds with probability $\leq d/|S|$

The point is:

- Repeat k times, get $r_1^k, \ldots, r_n^k$
- The probability that $f(r_1^k, \ldots, r_n^k) = 0$ always holds is $\leq (d/|S|)^k$
- For big S the value $(d/|S|)^k$ goes to zero
- If $f(r_1^k, \ldots, r_n^k) = 0$ all the time, then it almost certainly is constant zero

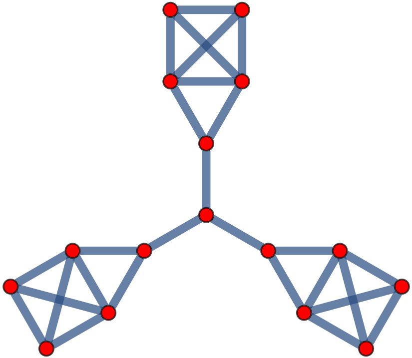
Count matchings



$$\det(\text{Tutte matrix}) = \det\left(\begin{pmatrix} 0 & x_{12} & 0 & x_{14} & x_{15} & 0 & 0 & 0 \\ -x_{12} & 0 & x_{23} & 0 & 0 & x_{26} & 0 & 0 \\ 0 & -x_{23} & 0 & x_{34} & 0 & 0 & x_{37} & 0 \\ -x_{14} & 0 & -x_{34} & 0 & 0 & 0 & 0 & x_{48} \\ -x_{15} & 0 & 0 & 0 & 0 & x_{56} & 0 & x_{58} \\ 0 & -x_{26} & 0 & 0 & -x_{56} & 0 & x_{67} & 0 \\ 0 & 0 & -x_{37} & 0 & 0 & -x_{67} & 0 & x_{78} \\ 0 & 0 & 0 & -x_{48} & -x_{58} & 0 & -x_{78} & 0 \end{pmatrix}\right)$$

Fact. det(Tutte matrix) is zero if and only if there are no perfect matchings

We can check heuristically that the graph below has no perfect matching!



Thank you for your attention!

I hope that was of some help.