Polynomial Methods (aka Algebra for Computer Scientist)

Goal: Modelize discrete combinatorial [pbs] by (multivariate) polynomials to either show the existence of solutions, or design algorithms

☹ Usually difficult to use, but the "polynomial method" is very much used these 10 last years.

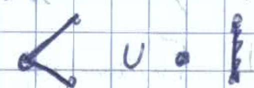
☺ Often the only known tools, and works as pure magic

[0] Introductory example: | Algebraic Geometry: Solve $P(x)=0$
This course: Solve $P=0$

▶ I will ~~[illegible]~~ often use graphs problems to serve as examples.

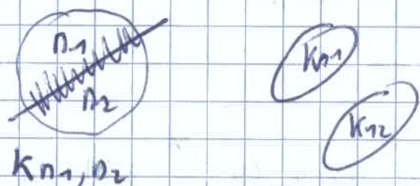
Def: Complete graph K_5  Complete bipartite graph $K_{3,3}$ 

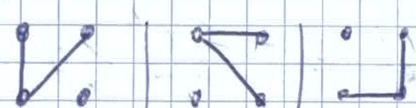
Th (Graham-Pollak '72) The minimum number of cbg edge-partitioning K_n is ~~[illegible]~~ $n-1$.

Remark: . K_3 is  K_4 is 

. Any binary search tree is a solution

$n = n_1 + n_2$ ~~[illegible]~~



. Special cuts:  "not binary type".

. If only want to cover edges of K_n by ~~[illegible]~~ $K_{a,b}$, only need $\lceil \log_2 n \rceil$ (exercise)

▼ ~50 years without a combinatorial proof, only algebraic one exists.

Proof: (Tverberg) Idea is to modelize pb with polynomials; like in LP, we must introduce . variables & constraints.

. ~~[illegible]~~ Every vertex of K_n is a variable: $x_1, x_2, \dots, x_n$

$\rightarrow$ Every edge corresponds to a monomial $x_i x_j$ $i \neq j$

How to express the edges of ~~the~~ K_n?

$$(x_1+\dots+x_n)^2 - \sum_{i=1}^{n} x_i^2 = 2\sum_{i\neq j} x_i x_j \rightarrow \text{disjoint union is sum}$$

Assume now for contradiction that K_n is edge-partioned into ℓ complete bipartite $(A_k,B_k)_{k=1..\ell}$ where $\ell < n-1$.

▷ edges of (A_k, B_k) are $\displaystyle\sum_{x_i\in A_k}\sum_{x_j\in B_k} x_i x_j = \left(\sum_{x_i\in A_k} x_i\right)\left(\sum_{x_j\in B_k} x_j\right)$

We then get the polynomial identity:

$$P(x) = \frac{(x_1+x_2+\dots+x_n)^2 - \sum_{i=1}^{n} x_i^2}{2} = \sum_{k=1}^{\ell}\left(\sum_{x_i\in A_k} x_i\right)\left(\sum_{x_j\in B_k} x_j\right) = Q(x)$$

The modelization step is done ~ constraints ~ polynomial equalities.

|| How to get contradiction? usually, everything boils down to show that one side is (or evaluate to) 0 and the other does not.

Consider $(\overset{*}{x}_1,\dots,\overset{*}{x}_n)\in\mathbb{R}^n$ with the following pties:

- $\forall k=1..\ell$, we have $\displaystyle\sum_{x_i\in A_k} x_i = 0$
- $\displaystyle\sum_{i=1}^{n} x_i = 0$

This is $\ell+1<n$ constraints, so such an $\overset{*}{x}$ exists.

However $Q(\overset{*}{x})=0$ & $P(\overset{*}{x}) = \dfrac{-\sum \overset{*}{x}_i^{\,2}}{2} < 0$, contradiction ⊠

The crucial fact here is to be able to show that $P\neq Q$, or in other words, $P-Q\neq 0$.

---

1 Polynomial Identity testing

▷ Given a multivariate polynomial P of degree d, how to ~~show that~~ test if $P\neq 0$? | $\deg_{x_i} P$

Def: Let $\mathbb{F}$ be a field. A polynomial $P\in\mathbb{F}[x_1,\dots,x_n]$ is a finite sum of terms of the form $C_\alpha x^\alpha$ where $\alpha=(\alpha_1,\dots,\alpha_n)\in\mathbb{N}^n$ and $C_\alpha\in\mathbb{F}$ is the coefficient of the monomial $x^\alpha := x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$. The degree of the x^α is $\sum\alpha_i$. The degree of P is max degree of its monomials. We denote it $\deg P$. *, **

~~The key idea~~ One of the key tool in the polynomial method is that if P and Q have low degree, and agree on many points, then they are equal. Considering $P-Q$, this says that a non zero poly of low degree cannot ~~have too many roots~~ vanish on a large set.

$\boxed{\text{Lem}}$ If $P \in \mathbb{K}[x]$ ~~has deg P+1~~ of degree d has at most $d+1$ roots, then $P=0$

Factor Th: Hence, if P, Q have degree at most d and satisfy $f(a)=g(a)$ for at least $d+1$ values $a \in \mathbb{K}$, then $P=Q$.

The generalization to multivariate is:

$\boxed{\text{Th}}$ (Schwartz - Zippel) Let S be a finite subset of $\mathbb{K}$. For every nonzero polynomial $P \in \mathbb{K}[x_1, \dots, x_n]$ with degree d, the number of n-tuples $(r_1, \dots, r_n) \in S^n$ for which $P(r_1, \dots, r_n) = 0$ is $\leq d\,|S|^{n-1}$.

$\boxed{\text{Cor}}$ Hence, if we pick independently and uniformly at random the values of $x_1, \dots, x_n$ in S, the probability that $P(r_1, \dots, r_n) = 0$ is at most $\dfrac{d}{|S|}$

S.Z. says we can efficiently test if P is 0, or equivalently that $P=Q$.

Proof: Induction on n. For $n=1$, this is the previous lemma. If $n>1$, we assume wlog that x_1 appears in one term of P (i.e. with nonzero coef). Let us write P as a polynomial with coefs in $\mathbb{F}[x_2, \dots, x_n]$

$$P = \sum_{i=0}^{k} P_i x_1^i \quad \text{where } P_i \in \mathbb{F}[x_2, \dots, x_n]$$

* coef are in a ring, not a field.

** If $S \subseteq$ ~~$\mathbb{F}$~~ $\mathbb{F}^n$ is such that $P(s_1, \dots, s_n) = 0 \ \forall$ ~~s~~ $(s_1, \dots, s_n) \in S$, we say that P vanishes on S.

Let $r = (r_1, \dots, r_n)$ s.t. $P(r_1, \dots, r_n) = 0$.

- r is of type 1 if $P_k(r_2, \dots, r_n) = 0$. Since $P_k \neq 0$ and P_k has degree at most $d-k$, the number of such $(r_2, \dots, r_n)$ is at most $(d-k) \cdot |S|^{n-2}$. Hence the # type 1 is $\leq (d-k)\,|S|^{n-1}$
- r is of type 2 if $P_k(r_2, \dots, r_n) \neq 0$. The total number of choices for $(r_2, \dots, r_n)$ is $|S|^{n-1}$, and for each choice P_i evaluates as an elt of $\mathbb{F}$.

hence for each such choice P is now a polynomial in $\mathbb{F}[x_1]$ with degree k, so at most k values r_1 can extend $(r_2, .., r_n)$. In all #type 2 is $\leq k.|S|$

Altogether $(d-k)|S|^{n-1} + k|S|^{n-1}$ ☒

Proof seems generous counting, but ~~can~~ Th can be sharp (Cf ex).

<u>Applications to perfect matching</u>. $|E| = m$

Let $G = (A, B, E)$ be a bipartite graph  $\leftarrow E$ where $|A| = |B| = n$.

A <u>perfect matching</u> is a set of n disjoint edges . By flows, or LP, we can ~~show~~ test in polynomial time if a graph has a perfect matching. Best algo in $O(\sqrt{n}.m) = O(n^{2,5})$ when $m = \Theta(n^2)$

<u>Polynomial Modelization</u>: Assume $A = \{a_1, .., a_n\}$ and $B = \{b_1, .., b_n\}$, a perfect matching is a permutation $\sigma \in S_n$ such that $a_i b_{\sigma(i)} \in E$ for all $i = 1..n$.

We now express the existence of a perfect matching by a determinant ~~det~~ of a matrix ~~with~~ which entries are variables. Namely:

- For every edge $a_i b_j \in E$, we introduce a variable x_{ij}.
- Define the $n \times n$ matrix $M = (m_{ij})$ where $\begin{cases} m_{ij} = 0 & \text{if } a_i b_j \notin E \\ m_{ij} = x_{ij} & \text{if } \quad " \in E \end{cases}$

By definition of determinant, we have:

$$\det M = \sum_{\pi \in S_n} \operatorname{sgn}(\pi)\, m_{1,\pi(1)} \cdot m_{2,\pi(2)} \cdot \ldots \cdot m_{n,\pi(n)}$$

$$= \sum_{\pi \text{ is a perfect matching}} \operatorname{sgn}(\pi)\, x_{1\pi(1)}\, x_{2\pi(2)} \ldots x_{n\pi(n)}$$

the polynomial identity

<u>Observation</u>: we have $\det M = 0$ iff G has no perfect matching.

(all monomials of this sum are $\neq$, no cancellation occur)

$\boxed{\text{Th}}$ There is a randomized algo for bip matching in time $O(n^{2,376})$.

which answer $\begin{cases} \text{YES if } G \text{ has a p.m. with proba } \frac{1}{2} \\ \text{NO if } G \text{ has no } \quad " \quad " \quad " \quad 1. \end{cases}$

(Pf) Independently & uniformly assign every x_{ij} to a value r_{ij} in $S = \{1, \dots, 2n\}$.

Since $\det \Pi$ has degree n, by SZ we have probability at most $\frac{d}{|S|} = \frac{1}{2}$ that $\det \Pi$ evaluates to 0 when G has a p.m.

Since ~~the~~ evaluating $\det \Pi$ is just computing the determinant of an integer matrix $\Rightarrow O(n^\omega)$ ⊠

<u>Remarks</u>
- Allows // computing
- Same approach works for perfect matching in g^{al} graphs (which is in P, but <u>much</u> harder: Edmond's Blossom Algo)

2 Quick remark on Error Correcting Codes

The fact that (univariate) low degree <u>distinct</u> polynomials P, Q must be very different appeared in the IT course.

Assume $\mathbb{F}$ has q elts and P is a polynomial in $\mathbb{F}[x]$ with degree at most $q^{1/2}$. Here P is the information one want to transmit (there are $q^{q^{1/2}}$ such possible P's). ~~As~~ the channel is heavily noisy ($\leq 49\%$ of errors). What to do?

$\rightarrow$ Transmit all values $P(r) : r \in \mathbb{F}$

Th If $q > 10^4$, for any function $f : \mathbb{F} \to \mathbb{F}$, there is at most one $P \in \mathbb{F}[x]$ with degree $\leq \sqrt{q}$ such that $f(r) = P(r)$ for at least 51% of r in $\mathbb{F}$.

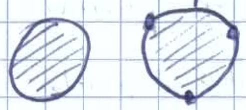
(Pf) Assume P_1 & P_2 agree on 51% of f. Then P_1 & P_2 agree on $\frac{2q}{100}$ values. So $P_1 - P_2$ has $\frac{2q}{100}$ zeroes, but $\frac{2q}{100} > \sqrt{q}$ so $P_1 = P_2$ ⊠

Th (Berlekamp-Welch 1986) One can recover P from F in polytime.

Method seems blocked by 50% since one need common agreement, but the very surprising result holds:

Th (Sudan '97) ~~Let $\mathbb{F}$ be a field on q~~ Given $f : \mathbb{F} \to \mathbb{F}$, there is an efficient algo retrieving all P with degree $\leq \frac{\sqrt{q}}{200}$ with 1% agreement with f.

[3] The Kakeya pb *

Given a needle on the plane, what is the minimum area needed to return it?  Reuleaux (SF) ... Besicovitch showed measure 0. However such a **Besicovitch set** (subset of the plane containing all unit segment with all orientation) has dimension 2 (for various dimension). The **Kakeya conjecture** asserts that in $\mathbb{R}^n$, a B Set has dimension n. (Big open problem).

Wolff proposed the following version in finite fields $\mathbb{F}$

- A B set $B \in \mathbb{F}^n$ is a set containing all lines, ie. $\forall \epsilon \in \mathbb{F}$ $\exists$ $b \in B$ s.t. $\{b + \epsilon . f : f \in \mathbb{F}\} \subseteq B$.

Conj (Wolff '99) $\exists$ constant C_n only depending on n s.t. $\forall \mathbb{F}$ finite, and for every B set $B \subseteq \mathbb{F}^n$, we have $|B| > C_N |\mathbb{F}|^n$

{ In other words, every B set in dimension n must occupy a positive fraction of the space.

Th (Dvir, '09) C_n exists $\forall n$.

We need two Tools: "Interpolation with low degree"

Lemma 1 Let $S \subseteq \mathbb{F}^n$ be a finite set and d integer such that $|S| < \binom{n+d}{n}$, then there exists non zero $P \in \mathbb{F}(x_1, \dots, x_n)$ with degree at most d which vanishes on S.

Pf: The set W of all $P \in \mathbb{F}[x_1 \dots x_n]$ with $d^0 \leq d$ is an $\mathbb{F}$-vector space, with dimension $\binom{n+d}{n}$. (A basis is provided by monomials)

{ Rem: $d^0 \leq 7$ x_1, x_2, x_3 gives bijection:

$x_1^2 x_2^2 x_3^3 \to 00|00|000|$

$x_2^3 x_3^2 \to |000|00|00$

{ 01 words of l^0 $n+d$ with n "0"s.

---

* We now turn to another application of poly method: How to prove ~~statements~~ ~~there~~ via polynomials? Usually by contradiction: Show first that a low d^0 poly modelize pb, and then show that it must be 0.

Now consider the linear map Φ from $\mathbb{F}(x_1,\dots,x_n) \longrightarrow \mathbb{F}^S$

$$P \longmapsto (P(\alpha))_{\alpha\in S}$$

$\dim(W) > \dim(\mathbb{F}^S) = |S|$, thus $\mathrm{Ker}(\Phi) \neq \{0\}$. So there is $P \in W$ s.t. P vanishes on S. ⊠

<u>Remark:</u> Using polynomials $\{1, X, Y, X^2+Y^2\}$, show that every three points in the plane are contained in a line of a circle.

The second tool: "Low degree nonzero poly do not vanish too much".

$\left\{ \begin{array}{l} \deg_{x_i}(P) := \\ \text{max power} \\ \text{of } x_i \end{array} \right.$

$\boxed{\text{Th}}$ (Alon-Tarsi) Let $\mathbb{F}$ be a field and $P \in \mathbb{F}(x_1,\dots,x_n)$ be nonzero. Suppose $S_1,\dots,S_n \subseteq \mathbb{F}$ with $\deg_{x_i}(P) < |S_i|$ for all $i = 1\dots n$. Then P cannot vanish on $S_1 \times S_2 \times \dots \times S_n$.

(Pf) Induction on n. Exercise ~ Schwartz-Zippel.

<u>Proof of finite field Kakeya:</u> Let $B \subseteq \mathbb{F}^n$ be a B-set. Let us show first that a polynomial $P \in \mathbb{F}[x_1,\dots,x_n]$ with degree $d < |\mathbb{F}|$ and vanishing on B must be the 0 polynomial. Let us write $P = \sum_{i=0}^{d} P_i$ where P_i consists of the sum of all terms of P with degree i.

Let $v \in \mathbb{F}^n \setminus \{0\}$ be some direction. Since B is a B-set, $\exists\, a \in \mathbb{F}^n$ s.t. $a + tv \in B$ for all $t \in \mathbb{F}$. Since P vanishes on B, we have $P(a+tv) = 0 \ \forall t \in \mathbb{F}$.

Consider the (univariate) polynomial $Q \in \mathbb{F}[t]$ s.t.

$$Q(t) := P(a+tv) = P(a_1+tv_1, a_2+tv_2, \dots, a_n+tv_n)$$

and note that $\deg Q < |\mathbb{F}|$. Since Q vanishes on $\mathbb{F}$, we must have $Q=0$. In particular, its t^d coefficient is 0.

|| The key-observation is that the coefficient of t^d is exactly $P_d(v)$, which means that P_d vanishes on all $v \in \mathbb{F}^n \setminus \{0\}$. Since $d>0$, P_d vanishes on $\{\mathbb{F}\}^n$, thus by Alon-Tarsi, ~~vanishes on~~ is 0, contradiction. ⊠

Now, why C_n exist? Consider n fixed and $q := |\mathbb{F}|$ arbitrarily large

If $c_n \cdot q^n < \binom{n+q-1}{n}$, there is a $P \in \mathbb{F}(x_1, \dots, x_n)$ of degree $q-1$ & non trivial which vanishes on any given set of size $c_n q^n$.

Note that $\binom{n+q-1}{n} \sim \frac{(n+q-1)^n}{n!} \sim \frac{q^n}{n!}$ when $q \to \infty$.

$\exists q_0$ s.t. $\forall q > q_0$, $\binom{n+q-1}{n} > \frac{q^n}{2 \cdot n!}$

Pick now $c_n = \min\left(\frac{1}{2n!}, \frac{1}{q_0^n}\right)$ to conclude ⊗

$\boxed{4}$ Additive Number Theory – Cauchy Davenport.

One of the oldest result in additive combinatorics is Cauchy-Davenport:

$\boxed{\text{Th}}$ (Cauchy-Davenport) If p is a prime and $A, B \subseteq \mathbb{Z}_p$, then $|A+B| \geq \min(p, |A|+|B|-1)$

where $A+B := \{a+b : a \in A, b \in B\}$.

<u>Rem</u>
- p is necessary since we could have $A = B = \mathbb{Z}_p$ for inst.
- when $A = \{1, \dots, K-1\} = B$ we have $A+B = \{2, \dots, 2K-2\}$ (sharp).
- A <u>much</u> more complex theory asks for the structure of A, B when $|A+B|$ close to $|A|+|B|$.

Before giving an elegant proof via polynomials, we need yet another non-vanishing lemma:

$\boxed{\text{Th}}$ (Alon's combinatorial Nullstellensatz) Given $S_1, \dots, S_n \subseteq \mathbb{F}$ and $P \in \mathbb{F}[x_1, \dots, x_n]$ such that the coefficient of $x_1^{d_1} \dots x_n^{d_n}$ is non zero & P has total degree $d = d_1 + \dots + d_n$. If $|S_i| > d_i$ for all i, then P cannot vanish on all $S_1 \times S_2 \times \dots \times S_n$

(Pf) Induction on d. Clearly true for $d = 0$ since P is non zero constant & all $S_i \neq \emptyset$. Assume for contradiction that P vanishes on $S_1 \times \dots \times S_n$. Wlog we can assume $d_1 > 0$. Take $a \in S_1$.

$P = (x_1 - a) Q + R$ where $Q \in \mathbb{F}[x_1, \dots, x_n]$ & $R \in \mathbb{F}[x_1, \dots, x_n]$
(exo)

Since P vanishes on $\{a\} \times S_2 \times \cdots \times S_n$, R vanishes on $S_2 \times \cdots \times S_n$

Since both P & R vanish on $(S_1 \setminus \{a\}) \times S_2 \times \cdots \times S_n$, so does Q.

Note that ~~Q is non zero~~ the coef of $x_1^{d_1-1} x_2^{d_2} \cdots x_n^{d_n}$ in Q is non zero.
and Q has total degree $d-1$. Thus by induction, there exists
$s_1 \in S_1 \setminus \{a\}$; $s_2 \in S_2, \dots, s_n \in S_n$ s.t. $Q(\vec{s}) \neq 0$. But then

$$\underbrace{P(s_1, \dots, s_n)}_{0} = \underbrace{(s_1 - a)}_{\neq 0} \underbrace{Q(s_1, \dots, s_n)}_{\neq 0} + \underbrace{R(s_1, \dots, s_n)}_{0}$$ is contradiction. ⊠

proof of CD (by Alon, Nathanson, Ruzsa)

Let $A, B \subseteq \mathbb{Z}_p$. We assume $|A| + |B| \leq p$ since if $|A| + |B| > p$, we have always $A \cap (x - B) \neq \emptyset$, and thus $x \in A+B$, hence $A+B = \mathbb{Z}_p$.
Suppose for contradiction that $|A+B| \leq |A| + |B| - 2$. Let $E \subseteq \mathbb{Z}_p$ s.t. $A+B \subseteq E$ & $|E| = |A| + |B| - 2$. Consider the bivariate polynomial

$$P(x, y) = \prod_{e \in E} (x + y - e) \quad \text{where } P \in \mathbb{Z}_p[x, y] \text{ \& } \deg P = |A| + |B| - 2$$

Note that P vanishes on $A \times B$. Set $d_1 = |A| - 1$ and $d_2 = |B| - 1$.
Observe that P has total degree $d_1 + d_2$ and that the coefficient of $x^{d_1} y^{d_2}$ is $\binom{d_1 + d_2}{d_1}$ which is non zero mod p since $d_1 + d_2 \leq p - 2 < p$
$\rightarrow$ contradiction via Nullstellensatz. ⊠

$\boxed{5}$ Graph Theory - Olson lemma.

Recall that a graph $G = (V, E)$ with at least $|V|$ edges always contain a cycle. (Exo: find an algebraic proof by considering the incidence $E \times V$ matrix). Hence, when $|E| \geq |V|$, ~~we have~~ the graph G has a subgraph H which is non trivial & such that all degrees are even.
Remarquably, a generalization exist for all ~~divisibilities~~ primes:

$\boxed{\text{Th}}$ (Alon, adapting Olson) If p is a prime, and $|E| \geq (p-1)|V| + 1$ then G has a non trivial subgraph H in which all degrees are ~~[illegible]~~ $0\,[p]$.

- Sharp for $p=3$ for instance  $|E| = 2|V|$
  no subgraph $0[3]$
- Implies in particular that every 5-regular graph has a 3-regular subgraph. | No non algebraic proof known
  | No algo to find it in polytime

Proof: Assume $|E| \geq (p-1)|V|+1$ and consider the following:
$P \in \mathbb{F}_p[x_1, .., x_n]$ where each x_i corresponds to a vertex i of V:

$$P = \prod_{ij \in E} (1 - x_i x_j)$$

We moreover quotient P by the polynomials $x_i^p - 1$, for all $i = 1..n$. (this amount to reduce every degree d_i mod p). We denote this quotient by $\mathring{P}$.

Fact: $\mathring{P} = 0$

(Pf) Rewrite $P = \prod_{ij \in E} (1 - x_i + x_i - x_i x_j)$

$$= \prod_{ij \in E} \left(\underbrace{(1-x_i)} + \underbrace{x_i (1-x_j)} \right)$$

Now develop the product w.r.t. each of the two terms. We obtain that $P = \sum_{\alpha = \alpha_1 .. \alpha_n} Q_\alpha (1-x_1)^{\alpha_1} (1-x_2)^{\alpha_2} .. (1-x_n)^{\alpha_n}$

where $\sum \alpha_i = |E|$. Since $|E| \geq (p-1)|V| + 1$, one of the α_i is at least p in each of the poly of the sum. But recall that in $\mathbb{F}_p$ we have $(1-x_i)^p = 1 - x_i^p$ ($= 0$ since we quotiented)

So $\mathring{P} = 0$. ☒

But P has the constant term 1 which must then be cancelled by some other monomial(s) of $\prod (1 - x_i x_j)$. Such a monomial precisely corresponds to a subgraph of G whose all degrees are $0[p]$ ☒ (*)

(6) AI - Perceptrons

In 1969, Minsky & Pappert were studying the computational power of perceptron, w.r.t. Boolean functions.

A <u>K-perceptron</u> is a boolean function $f : \{0,1\}^n \to \{0,1\}$ which can be expressed as a ~~major~~ threshold ~~function~~ of a sum of simpler functions, i.e. defined on only K entries.

<u>Precisely</u>: $\exists\, S_1, \dots, S_m$, each $S_i \subseteq [n]$ & $|S_i| = K$ and functions $f_i : \{0,1\}^{S_i} \to \mathbb{R}$ s.t.

$$f(x) = 1 \text{ iff } \sum_{i=1}^{m} f_i(x_{|S_i}) \geqslant 0$$

$\boxed{\text{Th}}$ (Minsky-Papert '69) The PARITY function $x_1 \oplus \dots \oplus x_n$ is not a K perceptron, when $K < n$.

<u>Proof</u>: ① First observe that there exists for each i, a polynomial P_i of $\mathbb{R}^{S_i}$ which satisfies $P_i = f_i$ on $\{0,1\}^{S_i}$

<u>Magic</u>: we can take P_i with degree K, since ~~reducing any~~ the equality $x_j^2 = x_j$ is valid when $x_j = 0$ or 1, we can reduce every monomial to a product of variables:

$$\boxed{P_i \text{ has degree } \leq K}$$

$$\boxed{P(x) = \sum_{\substack{S \subseteq [n] \\ |S| \leq K}} \alpha_S \prod_{i \in S} x_i}$$

Now $f(x) = 1$ iff $P(x) = \underbrace{\sum_{i=1}^{m} P_i(x_{|S_i})}_{\text{poly of degree } K.} \geq 0$

② $f(x)$ is invariant under permutations of indices, we can symmetrize P:

$$Q(t) := \mathbb{E}\left(P(x_1, \dots, x_n) \mid x_1 + \dots + x_n = t \;\&\; x \in \{0,1\}^n\right)$$

$$:= \sum_S \alpha_S\, \mathbb{E}\left(\prod_{i \in S} x_i \mid \dots\right)$$

$$\mathbb{E}\left(\prod_{i\in S} x_i \;\middle|\; \begin{matrix}\sum x_i = t\\ x_i = 0 \text{ or } 1\end{matrix}\right) = \begin{cases} 0 \text{ if } t < S \\ \dfrac{\binom{n-|S|}{t-|S|}}{\binom{n}{t}} & t \geq |S| \end{cases}$$

$(S\, t)\, n$

$$Q(t) = \sum_S$$

$$= \frac{(n-|S|)!}{(n-t)!\,(t-|S|)!} \cdot \frac{(n-t)!\; t!}{n!} = \boxed{\frac{(n-|S|)!}{n!}}\;\underbrace{t\cdot(t-1)\cdots(t-|S|+1)}_{\text{degree} \leq k \text{ in } t}$$

"Cste"

$\rightarrow$ $Q(t)$ has degree $\leq k$.

But $Q(0)<0$, $Q(1)\geq 0$, $Q(2)<0$, $\ldots$, $Q(n)$ thus Q has n roots, so $k \geq n$. $\boxtimes$

☹ for perceptrons.

Later, (M&P) found two 1-perceptrons f_1, f_2 s.t. $f_1 \wedge f_2$ was not $O(1)$ perceptron.

(7) Error Correcting Codes - Berlekamp Welch

Assume that you have
- a heavily noisy channel (49% error)
- a large alphabet of size q ~~(power of prime)~~

How to transmit information?, i.e. sequence of letters $a_0, \ldots, a_\ell$?

$\longmapsto$ Idea is to consider $P \in \mathbb{F}_q[x]$, $P = a_0 + a_1 x + a_2 x^2 + \ldots + a_\ell x^\ell$ & send all: $P(t) : t \in \mathbb{F}_q$.

If the degree of P is low enough, many redundant info.

$\boxed{\text{Th}}$ (Berlekamp - Welch '86)

If $P \in \mathbb{F}_q[x]$ has degree $< \frac{q}{100}$ and we are given a function $F : \mathbb{F}_q \to \mathbb{F}_q$ such that $\{t : P(t) = F(t)\}$ has size at least $\frac{51q}{100}$, then we can compute in poly time the polynomial P.

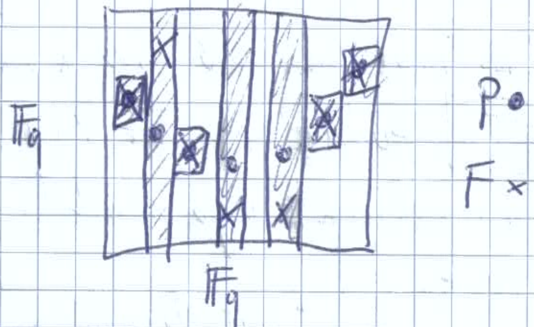
$E = \{e : F(e) \neq P(e)\}$
$G = \mathbb{F}_q \setminus E$

Rem: Observe that in particular, there is a unique solution. This part is clear since if P & Q are solutions, they coincide on $\frac{2q}{100}$ entries

- Thus $P-Q$ is identically 0. $\boxtimes$

Given F, how to retrieve P?

<u>Poly method</u>:
- Define poly low degree
- Show that it is $=0$



- Input is function $(x, F(x))$
- Define $R(x,y)$ which vanishes on $(x, F(x))$ (size q)

Choose R of the form $R_0(x) + y R_1(x)$ where $d^\circ(R_0) \le \frac{q}{2}$, $d^\circ(R_1) \le \frac{q}{2}$

The dimension of this space is $\lfloor \frac{q}{2} \rfloor + 1 + \lfloor \frac{q}{2} \rfloor + 1 > q$

so such an R exists. *

<u>Lemma</u>: ~~R is the 0 polynomial~~ $R(x, P(x))$ is the 0 polynomial.

$\boxed{\text{PF}}$ On $\frac{51q}{100}$ entries, we have $R(x, P(x)) = 0$. But the degree of $R(x, P(x))$ is $\le \frac{q}{2} + \frac{q}{100}$. $\boxtimes$

Thus $R_0(x) + P(x) R_1(x) = 0$ and then $P(x) = \frac{-R_0(x)}{R_1(x)}$ $\otimes$

<u>Can we say more about R?</u>

<u>Lemma</u>: $\forall e \in \mathbb{F}_q$ s.t. $P(e) \neq F(e)$, we have that R vanishes on all (e, f), $f \in \mathbb{F}_p$.

PF $R(e, y) \in \mathbb{F}_p[y]$ & $d^\circ \le 1$. But $R(e, F(e)) = R(e, P(e)) = 0$ $\otimes$

Moreover, if R is chosen with minimum degree, we have that
$$R(x,y) = c \cdot (y - P(x)) \prod_{e \in E} (x - e)$$
where $E = \{e : P(e) \neq F(e)\}$.

Given R, to test if entry erroneous, $R(e, F(e)+1)$ $\nearrow 0$ erroneous, $\searrow \neq 0$ $F(e) = P(e)$

---

* not only R exists, but it is easy to compute: set its coefficient as variables, and solve a linear system.