Goal: Modelize discrete combinatorial 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 often use graphs problems to serve as examples

- Def: Complete graph $K_n$  
- Complete bipartite graph $K_{3,3}$

- If (Graham-Pollak '72) The minimum number of $C^6$ edge-partitioning $K_n$ is $n - 1$.
- Remark: $K_n$ is $\leq \frac{n(n-1)}{2}$
- $K_n$ is $\leq \frac{n^2}{2}$
- What is $\leq$ in this case?

Any binary search tree is a solution

- $n = n_1 + n_2$
- $K_{n_1}$
- $K_{n_2}$
- $K_n$

- Special cases: $V = \{ 0 \} \cup \{ 1 \}$  
  "not binary type"

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

- In 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

- Every vertex of $K_n$ is a variable: $x_1, x_2, \ldots, x_n$
- Every edge corresponds to a monomial $x_i x_j$  
  if
How to express the edges of the $K_n$?

$$(x_1 + \ldots + x_n)^2 - \sum_{i=1}^{n} x_i^2 = 2 \sum_{i \neq j} x_i x_j$$

disjoint union is sum

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

$\Delta$ edges of $(A_k, B_k)$ are

$$\sum_{i \in A_k, j \in B_k} x_i x_j = \left( \sum_{i \in A_k} x_i \right) \left( \sum_{j \in B_k} x_j \right)$$

We then get the polynomial identity:

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

The modelization step is done. Constraints are polynomial equalities.

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

Consider $(x_1, \ldots, x_n) \in \mathbb{R}^n$ with the following properties:

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

This is $l+1 < n$ constraints, so such an $x$ exists.

However $Q(x) = 0 \Rightarrow P(x) = -\frac{\sum_{i=1}^{n} x_i^2}{2} < 0$, contradiction.

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


Given a multivariate polynomial, how to show that $P \neq 0$?

Def: Let $F$ be a field. A polynomial $P \in F[x_1, \ldots, x_n]$ is a finite sum of terms of the form $c \cdot x^d$ where $d = (d_1, \ldots, d_n) \in \mathbb{N}^n$ and $c \in F$ is the coefficient of the monomial $x^d = x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}$. The degree of the term $x^d$ is $\sum_{i=1}^{n} d_i$. The degree of the polynomial $P$ is the maximum degree of the terms of $P$.
degree of \( P \) is max degree of its monomials. We denote it \( \deg P \).

The key idea 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.

**Theorem** If \( P \in \mathbb{K}[x] \) has \( \deg P + 1 \) of degree \( d \) has \( d + 1 \) roots, then \( P = 0 \).

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

The generalization to multivariate is:

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

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

\[
P = \sum_{i=0}^{d} P_i x_i^d \quad \text{where} \quad P_i \in \mathbb{F}[x_1, \ldots, x_n]
\]

We let \( r = (r_1, \ldots, r_n) \) st. \( P(r_1, \ldots, r_n) = 0 \). Since \( P_k \neq 0 \) and \( P_k \) has degree at most \( d - k \), the number of such \( (r_1, \ldots, r_n) \) is at most \( (d - k)|S|^{n-2} \). Hence the # type 1 is \( \leq (d-k)|S|^{n-1} \).

- If \( P_k(r_1, \ldots, r_n) \neq 0 \). The total number of choices for \( (r_1, \ldots, r_n) \) is \( |S|^{n-1} \) and for each choice \( P_i \) evaluates as an elt of \( \mathbb{K} \).
hence for each such choice \( P \) is now a polynomial in \( \mathbb{F}[x_1] \) with degree \( k \), so at most \( k \) values \( r_n \) can extend \((r_1 \ldots r_n)\). In all \#type \( 2 \) is \( \leq k, k \).

 Altogether \( (d-k)!s^{n-k} + k!s^{n-k} \).

Proof seems generous counting, but I don't see the sharp \( (C+\varepsilon) \).

Applications to perfect matching.

Let \( G = (A \cup B, E) \) be a bipartite graph, \( E \subseteq \mathcal{E} \) where \(|A| = |B| = n\).

A perfect matching is a set of \( n \) disjoint edges. By Flow, or LP, we can test in polynomial time if a graph has a perfect matching. Best algo in \( O(\sqrt{n}m \cdot n) = O(n^{2.5}) \) when \( m = \Theta(n^3) \).

Polynomial Method of Focussing: Assume \( A = \{a_1, \ldots, a_m\} \) and \( B = \{b_1, \ldots, b_n\} \), a perfect matching is a permutation \( \pi \in S_n \) such that \( a_i b_{\pi(i)} \in E \) for all \( i = 1 \ldots n \).

We now express the existence of a perfect matching by a determinant of a matrix whose entries are variables. Namely:

- For every edge \( a_i b_j \in E \), we introduce a variable \( x_{ij} \).
- Define the \( m \times n \) matrix \( M = (m_{ij}) \) where \( m_{ij} = 0 \) if \( a_i b_j \notin E \) \( m_{ij} = x_{ij} \) if \( a_i b_j \in E \).

By definition of determinant, we have:

\[
\det N = \sum_{\pi \in S_n} \text{sgn}(\pi) M_{1,\pi(1)} \cdot M_{2,\pi(2)} \cdots M_{n,\pi(n)}
\]

\[
= \sum_{\pi \text{ is a perfect matching}} x_{\pi(1)} \cdot x_{\pi(2)} \cdots x_{\pi(n)}
\]

Observation: we have \( \det N = 0 \) if and only if \( G \) has no perfect matching.

(all monomials of this sum are \( \neq 0 \), no cancellation occurs.)

[?There is a randomized algo for bipartite matching in time \( O(n^{2.376}) \).

which answer: yes if \( G \) has a p.m. with proba \( \frac{1}{2} \)

no if \( G \) has no p.m. with proba \( \frac{1}{2} \).}
Independently & uniformly assign every $x_{ij}$ to a value in $S = \{1, \ldots, 2n\}$

Since det $N$ has degree $n$, by Szemerédi we have probability at most

$$\frac{1}{151} = \frac{1}{2}$$

that det $N$ evaluates to 0 when $G$ has a p.m.

Since evaluating det $N$ is just computing the determinant of an
integer matrix $\Rightarrow O(n^4)$

Remarks
- Allows non-repeating coded
- Same approach works for matching in $q$-ary graphs (which is in $P$, but much harder: Edmond's Blossom Alg.)

Quick remark on Error Correcting Codes

The fact that (min-max) low degree polynomials $P, Q$ must be different
appeared in the IT course.

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

\[ \rightarrow \text{ Transmit all values } P(r); r \in F \]

\[ \text{[Th]} \quad \text{If } q > 10^6, \text{ for any function } f: F \rightarrow F, \text{ there is at most one } P \in F[x] \]
with degree $\leq \sqrt{q}$ such that $f(r) = P(r)$ for at least $51\%$ of $r$ in $F$.

\[ \text{[Pf]} \quad \text{Assume } P_1 \text{ & } P_2 \text{ agree on } 51\% \text{ of } F. \text{ Then } P_1 \equiv P_2 \text{ on } \frac{2q}{100} \text{ values.} \]

\[ \text{Since } P_1 - P_2 \text{ has } 2q \text{ zeros, but } \frac{2q}{100} > \sqrt{q}, \text{ so } P_1 = P_2. \]

\[ \text{[Th]} \quad \text{(Berlekamp-Welch 1986)} \text{ One can recover } P \text{ from } F \text{ in poly-time.} \]

\[ \checkmark \text{ Method seems blocked by 50\% since one needs common agreement, but} \]

\[ \text{the very surprising result holds:} \]

\[ \text{[Th]} \quad \text{(Sudan '97)} \text{ Let } F \text{ be a field of size } q. \text{ Given } f: F \rightarrow F, \text{ there is an} \]
efficient algo retrieving all $P$ with degree $\leq \frac{\sqrt{q}}{200}$ with 1% agreement with $f$.\]
Given a needle at the plane, what is the minimum area needed to return it? Review: Besicovitch showed measure 0. However, such a Besicovitch set (subset of the plane containing all unit segments with allowance) has dimension 2 (for various definition). The Kakeya conjecture asserts that in $\mathbb{R}^n$, a B-set has dimension 0. (Big open problem.) Wolff proposed the following version in finite fields $\mathbb{F}_p$.

A B-set $B \subseteq \mathbb{F}_p^n$ is a set containing all lines, i.e., $\forall x \in \mathbb{F}_p^d \exists b \in B$ s.t. $b + bx$ is in $B$.

**Wolff (99)**: A constant $C_n$ depends only on $n$, s.t. $\forall x \in \mathbb{F}_p$ finite, and for every B-set $B \subseteq \mathbb{F}_p$, we have $|B| > C_n |\mathbb{F}_p|^n$.

\[\exists \in \text{In other words, every B-set in dimension } n \text{ must occupy a positive fraction of the space.}\]

**Theorem (Dvir, ‘09)**: $C_n$ exists $\forall n$.

We need two tools: “Interpolation with low degree.”

**Lemma 1:** Let $S \subseteq \mathbb{F}_p^n$ be a finite set and $d$ integer such that $|S| < (\binom{n+d}{n})$, then there exists $P \in \mathbb{F}_p[\prod_{i=0}^n x_i]$ with degree non-zero at most $d$ which vanishes on $S$.

**Proof:** The set of all $P \in \mathbb{F}_p[\prod_{i=0}^n x_i]$ with $d^0 \leq d$ is an $\mathbb{F}_p$-vector space with dimension $(n+d)$. (A basis is provided by monomials.)

Rem.: $d^0 \leq 7$: $x_0, x_2, x_3$ gives big set:

- $x_1^2 x_2^2 x_3^2 \rightarrow 001001001$
- $x_2^3 x_3^3 \rightarrow 100000$

01 words of $1^0 n+d$ with $n^0 0^4$.

We now turn to another application of poly method: How to prove statements 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 from $\mathbb{F}^n(x_1, \ldots, x_n) \rightarrow \mathbb{F}^s$

$$P \mapsto (P(a_{i,j})_{i,j \in S})$$

$\dim(w) > \dim(\mathbb{F}^s) = 1$, thus $\ker(\delta) \neq \{0\}$. So there is $P \in W$ s.t. $P(\mathbb{F})$ vanishes on $S$.

Remark: 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 poly do not vanish too much.”

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

Pr Induction on $n$. Exercise in Schwartz-Zippel.

Pr Proof of Finite Field Vakilera: Let $B \subseteq \mathbb{F}^n$ be a $B$-set. Let us show first that a polynomial $P \in \mathbb{F}[x_1, \ldots, x_n]$ with degree $\leq 1|\mathbb{F}|$ 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, if $a \in \mathbb{F}^n$ 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.

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

and note that $\deg Q < 1|\mathbb{F}|$. 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 $\mathbb{F}^* \mathbb{F}$, thus by Alon-Tarsi, vanishes on is 0, contradiction.

Now, why can exist? Consider $a$ fixed and $q := |\mathbb{F}|$ arbitrarily large.
If \( C_n \cdot q^n < \binom{n+q-1}{n} \), there is a \( P \in \mathbf{F}(x_1, \ldots, x_n) \) of degree \( q-1 \) and non-trivial which vanishes on any given set of size \( C_n \cdot q^n \).

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

Let \( q_0 \) s.t. \( \forall q > q_0 \), \( \binom{n+q-1}{n} > \frac{q^n}{\epsilon \cdot n!} \).

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

4 Additive Number Theory - Cauchy-Davenport

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

**Theorem (Cauchy-Davenport)** If \( p \) is a prime and \( A, B \subseteq \mathbb{Z}_p \), then \( |A+B| \geq \min \left( p, |A|+|B|-1 \right) \)

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

**Rough**

- \( p \) is necessary since we could have \( A=B=\mathbb{Z}_p \) for instance.
- When \( A=\{0, \ldots, k-1\} = B \) we have \( A+B=\{2, \ldots, 2k-2\} \) (sharp).

A much more complicated 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:

**Theorem (Alon's combinatorial Nullstellensatz)** Given \( S_1, \ldots, S_n \subseteq \mathbf{F} \) and \( P \in \mathbf{F}[x_1, \ldots, x_n] \) such that the coefficient of \( x_1^{d_1} \cdots x_n^{d_n} \) is non-zero and \( P \) has total degree \( d = d_1 + \cdots + d_n \). IF \( |S_i| > d_i \) for all \( i \), then \( P \) cannot vanish on all \( S_1 \times \cdots \times S_n \).

**Proof**

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 \( S_1 \times \cdots \times S_n \). Wlog we can assume \( d_i > 0 \). Take \( a \in S_1 \)

\[ P = (x_1-a)Q + R \] where \( Q \in \mathbf{F}[x_1, \ldots, x_n] \) & \( R \in \mathbf{F}[x_1, \ldots, x_n] \).
Since $P$ vanishes on $x_1 + x_2 + \ldots + x_n$, $R$ vanishes on $x_2 x - x S_n$.

Since both $P$ and $R$ vanish on $(x_1 x a) x_2 x - x S_n$, so does $Q$.

Note that $Q$ is non-zero, the coefficient of $x_1^{d_1} x_2^{d_2} \ldots x_n^{d_n}$ in $Q$ is non-zero.

and $Q$ has total degree $d - 1$. Thus by induction, there exists

$a_1 \in S_n \backslash \set{a}; a_2 \in S_2, \ldots, a_n \in S_n$ s.t. $Q(a_1) \neq 0$. But then

$s_1, \ldots, s_n = (s_1 - a_1) Q(s_1, \ldots, s_n) + R(s_1, \ldots, s_n)$ is contradicted.

**Proof of CD (by Alon, Nathanson, Ruzsa)**

Let $A, B \subseteq \mathbb{Z}_p$. We assume $|A| + |B| < p$ since if $|A| + |B| \geq p$, we have always $A \cap (B - a) \neq \emptyset$, and thus $x \in A + B$, hence $A + B = \mathbb{Z}_p$.

Suppose for contradiction that $|A| + |B| < 1 + |A| + |B| - 2$. Let $E \subseteq \mathbb{Z}_p$ s.t.

$A + B \subseteq E$ & $|E| = |A| + |B| - 2$. Consider the bivariate polynomial

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

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 $(d_1 + d_2)$ which is non-zero mod $p$ since $d_1 + d_2 < p - 2 < p$.

$\Rightarrow$ contradiction via Nullstellensatz.

**5. Graph Theory - Olsen lemma.**

Recall that a graph $G = (V, E)$ with at least $|V|$ edges always contain a cycle. (E.g.: 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.

Remarkably, a generalization exist for all $d$ such that primes:

If $p$ is a prime, and $|E| \geq (p - 1)|V| + 1$

then $G$ has a non-trivial subgraph $H$ which all degrees are

$O(1)$. 

**
Sharp for \( p \leq 3 \) for instance \( |E| = 2|V| \) no subgraph \( O[3] \)

- 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:

\[ P \in \mathbb{F}_p[x_1, \ldots, x_n] \]

where each \( x_i \) corresponds to a vertex \( v \) of \( V \):

\[ P = \prod_{i \in E} (1 - x_i x_j) \]

We moreover quotient \( P \) by the polynomials \( x_i^p - 1 \), for all \( i = 1 \to n \). (This amounts to reduce every degree \( d \) mod \( p \)). We denote this quotient by \( \tilde{P} \).

**Fact:** \( \tilde{P} = 0 \)

**Proof** Rewrite \( P = \prod_{i \in E} (1 - x_i x_j + x_i - x_i x_j) \)

\[ = \prod_{i \in E} \left( (1 - x_i) + x_i (1 - x_j) \right) \]

Now develop the product wrt each of the two terms. We obtain that

\[ P = \sum_{d \in \mathbb{Z}_{\leq n}} \alpha_d (1 - x_1)^d (1 - x_2)^d \cdots (1 - x_n)^d \]

where \( \sum_{d} \alpha_d = |E| \). Since \( |E| \geq (p-1)|V| + 1 \), one of the \( x_i \) 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 \( \tilde{P} = 0 \).

But \( P \) has the constant term \( 1 \) which most then be cancelled by some other monomial of \( \prod (1 - x_i x_j) \). Such a monomial precisely corresponds to a subgraph of \( G \) where all degrees are \( O[p] \).

**5) AI - Perceptrons**

In 1969, Minsky & Papert were studying the computational
A K-perception is a boolean function \( f: \mathbb{B}^n \rightarrow \mathbb{B} \) which can be expressed as a threshold of a sum of simpler functions, i.e., defined on only \( K \) variables.

Precisely: \( \exists S_1, \ldots, S_m \), each \( S_i \subseteq [n] \) \& \( |S_i| = K \) and functions \( f_i: \mathbb{B}^{S_i} \rightarrow \mathbb{B} \) such that

\[
f(x) = 1 \iff \sum_{i=0}^{m} f_i(x_{|S_i|}) \geq 0
\]

\( \square \) (Plunkett-Plant 59) The PARITY function \( \chi_n \oplus \ldots \oplus \chi_n \)

is not a K-perception, when \( K < n \).

Proof: \( \circ \) First observe that there exists for each \( i \), a polynomial \( P_i \in \mathbb{R}^{S_i} \) which satisfies \( P_i = f_i \) on \( \mathbb{B}^{S_i} \), and is expressed as \( P_i = \bigwedge_{j} P_j \), where

\[P_i = \bigwedge_{j} P_j \]

\( \quad P_i \subseteq \bigwedge_{j} P_j \)

We exists since \( \bigwedge_{j} P_j \)

\[\square \]

\( \square \) Next, we can take \( P_i \) with degree \( K \), since reducing 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:

\[P_i \text{ has degree } \leq K\]

Now \( f(x) = 1 \iff \sum_{i=0}^{m} P_i(x_{|S_i|}) \geq 0 \)

\( p(x) = \sum_{S_i \subseteq [n]} \mathbb{P}(x_{|S_i|} \geq 0) \quad \text{poly of degree } K. \)

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

\[Q(x) := \mathbb{E}(P(x_1, \ldots, x_n) \mid x_1 + \ldots + x_n = 0 \& x \in \mathbb{B}^n)\]

\( \sum_{S_i \subseteq [n]} \mathbb{E}(\prod_{i \in S_i} x_i) \bigwedge_{\text{sym}} \)
\[
\begin{align*}
Q(t) &= \sum_{i=0}^{\infty} \frac{(n-1)_i}{(e-1)_i} i^t t! \\
&= \frac{(n-1)!}{(e-1)!} \sum_{i=0}^{\infty} \frac{t^i}{i!} \\
&= \frac{(n-1)!}{(e-1)!} \left( e^t - \frac{t^{e-1}}{(e-1)!} \right) \\
&= \frac{(n-1)!}{e^t} \left( e^{t-1} - \frac{t^{e-1}}{(e-1)!} \right)
\end{align*}
\]

- \( Q(t) \) has degree \( \leq k \).
- But \( Q(0) < 0, Q(1) \geq 0, Q(2) < 0, \ldots, Q(k) > 0 \), thus \( Q \) has \( n \) roots, so \( k \geq n \).

- \( H^* \) for percepts.

Later, (P&P) found two \( n \)-percepts \( f_1, f_2 \) s.t.
- \( f_1 \neq f_2 \) was not \( O(1) \) perception.

\( \text{Error Correcting Codes - Berlekamp-Welch} \)

Assume that you have a heavily noisy channel (e.g., 90% error)
- a large alphabet of size \( q \) (power of \( p \), \( p = m + c \)).

How to transmit information? i.e., sequence of letters \( a_0, \ldots, a_{q-1} \)?

\( \rightarrow \) Idea is to consider \( P \in F_q[x] \), \( P = a_0 + a_1 x + \ldots + a_{q-1} x^{q-1} + a_q x^q \).

\& send all: \( P(t) : t \in F_q \).

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

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

If \( P \in F_q[x] \) has degree \( \leq \frac{q}{100} \) and we are given a function \( F : F_q^* \rightarrow \) such that \( \forall e : P(e) = F(e) \) has size at least \( \frac{5q^2}{100} \), then we can compute in \( poly(t) \) the polynomial \( P_o \) \( \forall e : F(e) \land P(e) \).

\( G \in F_q^* \).

Remark: Observe that in particular, there is a unique solution. This is true
- clear since if \( P \& Q \) are solutions, they coincide on \( \frac{2q}{100} \) entries.
Thus P-Q is identically 0.

Given F, how to retrieve P?
Poly method: Define poly low degree
- Show that if \( f(x) = 0 \)

Input is function \((x, F(x))\)
Define \( R(x, y) \) which vanishes on \((x, F(x))\) \((\text{size } q)\)
Choose \( R \) of the form \( R_0(x) + y R_1(x) \) where \( d_0(R_0) \leq \frac{q}{2}, d_0(R_1) \leq \frac{q}{2} \)
The dimension of this space is \( \left\lfloor \frac{q}{2} \right\rfloor + 1 + \left\lfloor \frac{q}{2} \right\rfloor + 1 > q \)
so such an \( R \) exists.

Lemma: \( R \) is the 0 polynomial \( R(x, P(x)) \) is the 0 polynomial.

On \( 50q \) entries, we have \( R(x, P(x)) = 0 \). But the degree of \( R(x, P(x)) \) is \( \leq \frac{q}{2} + \frac{q}{100} \).
Thus \( R_0(x) + P(x) R_1(x) = 0 \) and then \( P(x) = \frac{-R_0(x)}{R_1(x)} \).

Can we say more about \( R \)?

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

Thus \( R(e, f) \) vs \( e \in \mathbb{F}_p[y] \) & \( d^0 y = 1 \). But \( R(e, F(e)) = R(e, P(e)) = 0 \).

Moreover, if \( R \) is chosen with minimum degree, we have that
\[ R(x, y) = \sum \frac{c}{e} (y-P(e)) (x-e) \]
where \( E = \{ e : R(e) \neq F(e) \} \).

Given \( R \), to test if only error \( e \in E \),
\[ R(e, F(e)+1) \neq 0 \text{ erroneous} \]

\( \cup \neq 0 F(e) = P(e) \)

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