→ <u>Boolean Functions</u>

$$f : \{0,1\}^n \longrightarrow \{0,1\}$$

Q: How complex is it?
(How hard is it to compute f)

A: It depends on our model of computation (TMs, Circuits, Dec. Trees)

But our model is Polynomials.

$$\forall \vec{x} \in \{0,1\}^n \qquad p(\vec{x}) = f(\vec{x})$$

Measure of complexity is $\boxed{\deg(f)}$.

<u>Fact 1</u>: Given $f : \{0,1\}^n \rightarrow \{0,1\}$ $\exists$ a unique multilinear polynomial $h : \mathbb{R}^n \rightarrow \mathbb{R}^n$ that agrees with f on hypercube & deg $\leq n$.

Proof: We can write an indicator func for $\vec{a} = (a_1, a_2, \ldots, a_n) \in \{0,1\}^n$

$$\mathbb{1}_{\{a\}}(x) = (1 + a_1 + x_1)(1 + a_2 + x_2) \cdots (1 + a_n + x_n)$$

Then by Lagrange's Poly.

$$f(x) = \sum_{a \in \{0,1\}^n} f(a)\, \mathbb{1}_{\{a\}}(x)$$

Eg: Max_2:

0	0	0
0	1	1
1	0	1
1	1	1

$$f(x) = 0(1+x_1)(1+x_2) + (1)(1+x_1)(x_2) + (1)x_1(1+x_2) + x_1 x_2$$

$$= x_1 x_2 + x_2(1+x_1) + x_1(1+x_2)$$

It's called Representing Polynomial of the Boolean func.

Symmetric Boolean funcs

Funcs whose value depend on no. of 1's.

Think of it as a univariate func of weight

$$f\left(\sum x_i\right) = f(\vec{x})$$

From now on, $f_{symm} = f(x)$

Eg: $OR(x)$, $AND(x)$, $PARITY(x)$, $MAJORITY(x)$

Q: Understanding the degree of symm bool funcs?

DETOUR: Learning symmetric juntas

Given $f(\vec{x}_n)$

which depends on only k ($\omega(n)$) variables. $x = (x_{i_1}, \ldots x_{i_k})$

Junta

$$f(\vec{x}_n) = g(\vec{x}_k)$$

hidden func

→ Goal is to identify "k" relevant vars.

→ Trivially $O(n^k)$ algo. (Try all k-size subsets)

→ Now the genral case is HARD! (exp!)

→ But still the symmetric case is natural to solve.

→ Mossel, O'Donnell & Servedio proved first non-trivial lower bound of $(n^k)^{\omega/\omega+1} = n^{2k/3}$ where ω is mat-mul exponent.
<2.376

→ For balanced funcs (1 on half of the inputs) using "von zur Gathen & Roche" given an algo $O(n^{.548})$.

→ Generally any improvement on lower bound $\longrightarrow$ ↑ in upper bound of learning symmetric juntas

→ Previous Results

Claim: $\deg f \geq n/2$

Proof: Consider roots of either f or $1-f$.

Claim: (Nisan & Szegedy): For general Boolean funcs f on n vars.

$$\boxed{\deg f \geq \log_2 n - O(\log \log n)}$$

Proof ideas:

→ Fourier rep^n. $f = \sum_S \alpha_S \chi_S$.

→ Parseval's Eq: $\sum_S \alpha_S^2 = 1$

$\Pr(\ldots, T, \ldots) \neq \Pr(\ldots, F, \ldots)$

→ Using influence, $\sum_{i=1} \mathrm{Inf}_i(f) = \sum_S |S|\alpha_S^2$.

→ $\sum_{i=1}^{n} \mathrm{Inf}_i(f) \le \deg f$.

Let $p(x_1, \dots, x_n)$ multilinear d

→ Lemma (Schwartz): $\Pr[p(x_1, \dots, x_n) \neq 0] \ge 2^{-d}$

Choose $x_1, \dots, x_n$ $\Pr(p(x \dots) \neq 0) \ge 2^{-d}$ →

$\mathrm{Inf}_i(f) \ge 2^{-d}$ (Define $f(x_1, \dots -1, \dots) - f(x_1, \dots 1, \dots)$)

→ Now $\frac{n}{2^d} \le \sum \mathrm{Inf}_i \le d$

→ $n \le d \cdot 2^d$

⇒ $\boxed{d \ge \log_2 n - O(\log \log n)}$

Claim (von zur Gathen & Roche):

$$\boxed{\deg f \ge n - O(n^{.548})}$$

Also: → for $n \le 128$, conjectured $\deg f \ge n-3$

Proof idea:

→ For $n = p - 1$ (prime p) : then $\deg f = n$

→ Applying Mozzochi's thm. on gap b/w consecutive primes one gets

$$\boxed{\deg f \geq n - O(n^{.548})}$$

Slight Improvement (Baker, Harman, Pintz)

$$\boxed{\deg f \geq n - O(n^{.525})}$$

→ Gill Cohen's work:

Consider,

$$f : \{0, 1, \ldots, n\} \longrightarrow \{0, 1, 2, \ldots c\}$$

$\deg f = ?$

1) if $c = 1$ $\deg f = n - o(n)$

2) $c = n$ $f(k) = k$ has $\deg = 1$.

VZGR noted, $\deg f \geq \frac{n+1}{c+1}$

→ Relative degree

$$D_c(n) = \frac{1}{n} \min \{ \deg f \}$$

- $D_c(n)$ is monotone dec. in c.
  $\left(> \frac{1}{n+1} \right)$

Main thm 1: Let f be non-constant

$f: \{0, 1, \ldots, n\} \rightarrow \{0, 1, \ldots, n-1\}$

$$\boxed{\deg f \geq \frac{9}{22} n - O(n^{.525})}$$

Observe threshold behaviour at $c = n$.

Proof Strategy

L1: For any n $\exists$ p s.t.

$=$ ' ' Γ

$$n - o(n) < 2p < n \quad \&$$

$$D_{n-1}(n) > \frac{1}{2} D_4(p) - o(1)$$

(Trivially $D_4(p) > \frac{1}{5}$ & $D_{n-1}(n) > \frac{1}{10} - o(1)$)

L2

For every n, m, n s.t. $n > m$

$$D_c(n) > \frac{m}{m+1} D_c(m) - o(1)$$

By. Computer Search $D_4(21) = 6/7$.

So, $$D_4(n) > \frac{21}{22} \cdot \frac{6}{7} - o(1)$$

By L1

$$D_{n-1}(n) > \frac{1}{2} D_4(p) - o(1)$$

$$> \frac{9}{22} - o(1)$$

Periodicity & Degree

Thm2: $f : \{0, 1, \ldots n\} \to \{0, \ldots c\}$

$\deg f = d$. Let $d < p \le n$.

Then for $0 \le j \le d$ s.t. $p+j \le n$

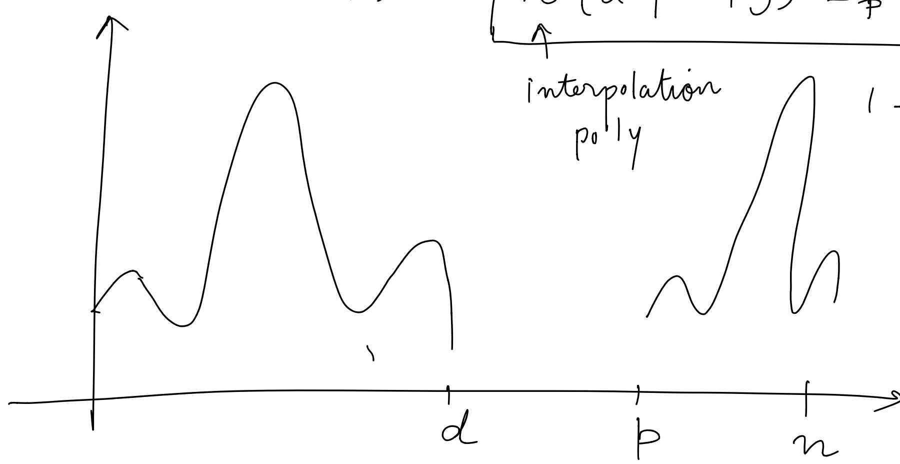
$$\boxed{f(p+j) \equiv_p f(j)}$$

also $\boxed{h(a \cdot p^m + j) \equiv_p f(j)}$

interpolation poly

$1 \le a < p$

$n < p^m$



Def: $f: \{0, 1, .. n\} \to \{0, \dots, c\}$ & $T \ge 1$, $\Delta \ge 0$

$$P_T^{\Delta}(f) = \{0 \le k \le n-T : f(k) + \Delta = f(k+T)\}$$

L4: If $\Delta = 0$ $\quad d \ge |P_T^{\Delta}(f)|$

$\Delta \ne 0$ $\quad d \ge |P_T^{\Delta}(f)|$ or 1

Pf 1: Use Lucas theorem

Defⁿ: Given $f \in \mathcal{F}_c(n)$

$$\boxed{\gamma(f) = n - \deg f}$$

gap of f.

Defⁿ: $\Gamma_c(n) = \max_{f \in \mathcal{F}_c(n)} \gamma(f)$

gap of (n,c) funcs.

Easily, $\boxed{\Gamma_c(n) = n(1 - D_c(n))}$

Thm: p be odd prime & $n = p^m - 1$ and $p \nmid w(f)$.

$\deg f \geq p^m - p \geq n - \sqrt{n}$.

→ <u>Special case</u> $n = p^2 - 1$

<u>Composite case</u>:

<u>Thm</u>: Let p, q be add primes s.t. $q \le \log_2 p$. $n = pq - 1$

$$\deg f \ge p(q-1) - 1$$
$$= \Omega\left(\left(1 - \frac{1}{\log n}\right) n\right)$$

at $q = \log p$.

→ <u>Another type lower bound</u>

Based on parity of distances b/w cons 1's of f.

<u>Def^n</u>: Let f be symm bool func

$$f^{-1}(1) = \{ a_1, \ldots\ldots a_m \} \qquad a_i < a_j \quad i < j$$

$$\Theta(f) = \{ i \in [m-1] : 2 \mid (a_{i+1} - a_i) \}$$

$= $ No of cons 1's separated by odd no. of zeros

Thm: $\boxed{\deg f \geq n - w(f) + \theta(f)}$

Thus any f with odd zeros b/w cons 1's has deg n. Eg PARITY.

Research Sub Goals:

Main goal: Tight lower bound on symm. bool f.

1. Find families with $\deg = n$
If such families will be dense enough to ensure small gaps b/w cons. number.
2. For $n = p^m - 1$, find lower bounds.
3. Try $n > 128$ computationally.
4. Behaviour of $D_c(n)$ asymptotically
Does $D_{n-1}(n) \sim 1/2$?
5. Does $T_1(n) = O(1)$?

⑥ Natural generalization:

$f : \{0,1,\dots,n\}^m \to \{0,1,\dots,c\}$

deg of such func?

Appendix:

Corr: $g(x) = f(x+n) - f(x)$

Consider $x = 1, 2, \dots, n$ thus n-roots

so deg $= n$.

Lucas' thm: Let $a, b \in \mathbb{N} \setminus \{0\}$ & let p be prime,

$$a = a_0 + a_1 p + a_2 p^2 + \cdots + a_k p^k$$

$$b = b_0 + \cdots + b_k p^k$$

$$\binom{a}{b} \equiv_p \prod_{i=0}^{k} \binom{a_i}{b_i}$$

Prime Gap: $n \in \mathbb{N}$ $\exists$ p

$$\boxed{n - O(n^{.525}) < p < n}$$

Proof Ideas

① Low deg $\longrightarrow$ S.P.S

Apply Lucas' thm to interpolation polynomial.

$\rightarrow$ Lower d implies more primes $[d, n]$ more layers.

② S.P.S $\longrightarrow$ High deg

③ $n = p^m - p^{m-1} - 1$

④ Simplified proof of [VZGR]

Claim: Any p $D_1(p-1) = 1$

Consider over $\mathbb{F}_p$

$$h(x) = \sum \left(1 - (x-b)^{p-1}\right)$$

$$\sum_{k:\, f(k)=1} \left(1 - (x-k) \qquad\right)$$

$$\Rightarrow \quad \deg h = p - 1$$

Now

$$h_f = \sum_{k:\, f(k)=1} \prod_{\substack{j=0 \\ j \neq k}}^{p-1} \frac{x-j}{k-j}$$

Since none of the denominators is multiple of p so h_f as a poly over $\mathbb{F}_p$.

$$h_f^{(p)}(x) = \sum_{k:\, f(k)=1} \prod_{\substack{j=0 \\ j \neq k}}^{p-1} (x-j)(k-j)^{-1}$$

$$\Rightarrow \quad \deg h_f^{p}(x) \leq \deg h_f \leq p-1$$

From uniqueness of interpolating polynomial over $\mathbb{F}_p$. $h_f^{(p)} = h$ & $\deg h_f^{(p)} = p-1$

$$\Rightarrow \quad \boxed{\deg h_f = p-1} = n$$

(1) Concrete Math : Knuth

(2) [illegible] Newton's series