low degree tests

① Codes. $C \leq \mathbb{F}_q^m$ $\dim C = k$ $d = \min_{x \neq y \in C} d_{Hamm}(x,y) \Rightarrow [k, m, d]_q$ code

Walsh-Hadamard code $[q^m, m, q^{m-1}]_q$ code

$(\mathbb{F}_q^m)^* \longrightarrow \{\text{set maps } \mathbb{F}_q^m \to \mathbb{F}_q\}$

$WH(x) = \alpha \mapsto x(\alpha)$

$WH^{-1}(c) = (\alpha \mapsto c(\alpha+x) - c(\alpha))$, for ~~any~~ random α.

② PCP certificates.

NP-complete pb, g " $\exists$? soln of $P: \mathbb{F}_2^m \to \mathbb{F}_2^\ell$, $P(z) = \left(\langle z | M_i | z \rangle + \langle L_i | z \rangle + C_i\right)_{i=1\ldots\ell}$"

Classical certificate : z

PCP certificate : $(A = WH(z),\ B = WH(z \otimes z))$

Verifier : - test A, B linear

- test rank B $B(\alpha \otimes \beta) = A(\alpha) \cdot A(\beta)$

- test poly. choose $\gamma \in \mathbb{F}_2^\ell$ at random $p(z) = \langle P(z) | \gamma \rangle$

check $WH^{-1}(B)(M) + WH^{-1}(A)(L) + C = 0 = \langle z | M | z \rangle + \langle L | z \rangle + C$

Drawback: NUGE certificate.

(3) Reed-Muller code $\quad P_m^d = \{\text{polynomials of deg} \le d \text{ in } X_1 \dots X_m / \mathbb{F}_q\} \longrightarrow \{\text{set maps } \mathbb{F}_q^m \to \mathbb{F}_q\}$

on $\left[q^m, \binom{m+d}{d}, \left(1-\frac{d}{q}\right) q^{m-1}\right]_q$. $\quad P \longmapsto (P(\alpha))_{\alpha \in \mathbb{F}_q^m}$

"Schwartz-Zippel Lemma" (Ore)

If P polynomial $\not\equiv 0 / \mathbb{F}$ deg d, m variables: S finite $\subset \mathbb{F}$

For random UIID $r_1 \dots r_m \in S$: $\mathbb{P}_{r_i}(P = 0) < \frac{d}{|S|}$.

(Pf: induction)

$\Rightarrow \#(P^{-1}(0)) \le \frac{d}{q^{m-1}}$.

(4) Test: . Take line ℓ at random in $\mathbb{F}_q^m$
. evaluate P at $d+2$ points on ℓ
. accept iff $\exists$ poly of deg $\le d$ fitting these $d+2$ values.

Take plane Σ, evaluate at $\binom{d+2}{2} + 1$ points for $\dots$

Thm: If P comes from polynomial, accept

If $d_{rel}(P, RM) \ge \delta$, then reject with prob. $\ge \min\left(\frac{\delta}{2}, \frac{2(d+2)^2}{q}\right)$

Sketch of pf: If P (close to) ∂ RPM ✓

Assume P not well fittable: $\mathbb{P}_{\alpha,\beta}\left[\sum_{i=0}^{d+1}(-1)^i\binom{d+1}{i}P(\alpha+i\beta)=0\right] \geq 1-\rho$

ρ = rejection rate

P is polynomial on $\{\alpha+t\beta\}$

$$g(\alpha) = \underset{\beta\in\mathbb{F}^m}{\mathrm{MAJ}}\left(\sum_{i=1}^{d+1}(\quad)\right)$$

1) $d(P,g) \leq 2\rho$.

2) $\mathbb{P}_{\beta}\left[g(\alpha) = \sum_{i=1}^{d+1}(\quad)\right) \geq 1-2(d+1)\rho$.

almost maximity

3) $g \in \mathbb{P}_m^d$.

⑤ Oracle test $f: \mathbb{F}^m \to \mathbb{F}$ for being low degree

"plane oracle": $A_i\Sigma$ affine plane $\longmapsto$ fitted polynomial $\in \mathbb{P}_2^d$

"Point oracle": f x $\longmapsto$ $f(x)$.

Test: pick Σ at random, $x \in \Sigma$ at random;

accept iff $A(\Sigma)(x) = f(x)$.

(5) PCP theorem $\exists r = O(\log n)$ "random bits"

$\delta > 0$

$q = O(1)$

V verifier algo.

$\forall$ CNF φ of size n : $\exists$ "proof" π, string of $m = \text{Poly}(n)$ bits :

$V(\varphi, \pi)$: choose r random bits, compute $\{i_1, \dots i_q\} \subset \{1, \dots m\}$

$C : \{0,1\}^q \to \{0,1\}$

accept iff $C(\pi_{i_1}, \dots, \pi_{i_q}) = 1$

V must be complete : if φ then accept

if φ then $\Pr_r(C(\pi_{i_1} \dots \pi_{i_q}) = 1) \leq 1 - \delta$

$\mathbb{E}_r \, d(\pi_{i_1} \dots \pi_{i_q}, C^{-1}(1)) \geq 1 - \delta$

(7) Cube tests Given $f : \mathbb{F}^m \to \mathbb{F}$

Test if $f \equiv 0$ on $H = \{0,1\}^m$ & f polynomial of deg $\leq d$

Fact : $f_0 \equiv 0$ on H iff $f_0 = \sum_{i=1}^{m} x_i(x_i - 1) f_i$

Test : Given oracles $A : \Sigma \longmapsto (f_0, f_1, \dots, f_m)$ truth table of f_Σ

$B : x \longmapsto (f_0(x), f_1(x) \dots, f_m(x))$

Pick Σ at random, $x \in \Sigma$ at random,

accept iff $A(\Sigma)(x) = B(x)$.

Some thm: Very good test.

⑧ For PCP: Start by φ: 3CNF in n variables, $n = 2^m$: $H \leftrightarrow [n]$ $\leftrightarrow \{0,1\}^m$

$x_1, \dots, x_n$

assignment of variables $A: H \to \{0,1\} \in \mathbb{F}_q$

can be written as polynomial of degree m

φ = let $\begin{cases} H^3 \times \{0,1\}^3 \subset \mathbb{F}_q^{3m+3} \to \{0,1\} \\ (i,j,k, \alpha, \beta, \tau) \mapsto \begin{cases} 1 \text{ if } x_i^\alpha \vee x_j^\beta \vee x_k^\tau \text{ is in } \varphi \\ 0 \text{ else} \end{cases} \end{cases}$ $\leftarrow \begin{cases} x_i^0 = \bar{x}_i \\ x_i^1 = x_i \end{cases}$

$\exists$ poly. $\bar{\varphi}$ in $3m+3$ variables, degree $O(m)$, extending φ on $H^3 \times \{0,1\}^3$

Given φ, A: $f_{\varphi,A} = (\bar{A}(i) - \alpha)(\bar{A}(j) - \beta)(\bar{A}(k) - \tau)\,\bar{\varphi} \in P_{3m+3}^{O(m)}$

PCP certificate

$f \equiv 0$ on $H^3 \times \{0,1\}^3$ $\not\Leftrightarrow$ $\models \varphi$ by A.

Run lowerbound test on f.

Problem:

size of certificate	poly(n)	✓
randomness	$O(\log n)$	✓
query complexity	polylog(n)	×
q alphabet: $q \gg m$		×

(9) Constraint graphs

Fix Σ an alphabet

GAP-CG(Σ)$_{c,s}$ problem: Instance $\begin{cases} \text{graph } (V,E) \text{ (undirected)} \\ \forall e \in E \quad C_e \subset \Sigma \times \Sigma \end{cases}$

Vertex coloring $\sigma : V \to \Sigma$ with: $\forall e : u \to v : (\sigma(u), \sigma(v)) \in C_e$

Answer: yes if $\exists \sigma : V \to \Sigma$ with $\#\{e \text{ } \} \geq c \cdot \#E$

No if $\forall \sigma : V \to \Sigma$ $\#\{ \quad \} < s \cdot \#E$

whatever if other case.

Eg: 3-coloring a graph. $\Sigma = \{1,2,3\}$, $C_e = \{(i,j) : i \neq j\}$

Thm 1. PCP $\Leftrightarrow$ $\exists s_0 < 1$, Σ_0 : GAP-CG(Σ)$_{1,s_0}$ NP-hard

Thm 2. ($s_0 = 1 - 10^{-6}$, $\#\Sigma_0 = 64$.) V.

$\#$ Instance $= n = \Omega(m \cdot \log \#V + m|\Sigma|^2)$

$m = \#E$

Thm 1 $\Leftarrow$: take favourite NP problem, reduce it to $GAP\cdot CG(\Sigma)_{1,s}$.

As proof output a "good" labelling

Verifier: check a random edge for $(\pi_u, \pi_v) \in C_e$.
(a few)

$\Rightarrow$: derandomization.

take favourite NP problem, get PCP certificate $\pi = \pi_1 \ldots \pi_\ell$

construct graph w/ vertices all q-subsets of $\{1, \ldots, \ell\}$

$\Sigma = \{0,1\}^q$

$\sigma(\{i_1, \ldots i_q\}) = (\pi_{i_1}, \ldots, \pi_{i_q})$

Constraints: edges given by overlaps of subsets
check that bits agree & are verified.

Do it by exhausting the random supply.

Thm 2 Prove NP-hardness of $GAP\text{-}GC(\Sigma_0)_{1,s_0}$.

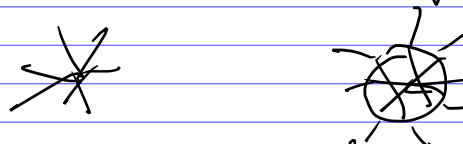
If restrict to small graphs 3-coloring is NP-hard.

$GAP\text{-}GC(\Sigma_0)_{1,1-1/m}$ NP-hard if G has $\leq m$ edges.

Start w/ $(G=(V,E), \{C_e\})$ "gap": proportion of invalid edges in optimal VX coloring

repeat $\log n$ times each at most

* degree-reduction: vertex-degree constant & small bounded



expander graph

increases size of G by const, #edges decreases gap by const.

* expanderize: add edges to make G an expander

increases #edges by const

decreases gap by const.

* replace G by G^t; namely same VX set, paths of length t become new edges,

increases #edges by a lot

IF G expander, increase gap by $\sim$ LOT $t \sim 10^6$

increases not Σ.

* Reduce alphabet. Predicates $C_\Sigma \subset \Sigma \times \Sigma$

error-correcting codes:

Want small certificate for $(\sigma, \sigma') \in C_\Sigma$ $\{0,1\}^L \times \{0,1\}^L$ or not.

PCP-subproblem: find certificate fitting in $\Sigma_0 \times \Sigma_0$, $\#\Sigma_0$ fixed (64)