Proof of weak PCP thm: $PCP(poly(n), O(1)) \supseteq NP$

def Walsh-Hadamard code. $WH : \{0,1\}^n \to \{0,1\}^{2^n}$
$WH(u)(x) = \langle u,x \rangle \pmod 2$.
can think of $WH(u)$ as tt of function $\langle u, \cdot \rangle$.

claim: $u \neq v \Rightarrow dist(WH(u), WH(v)) \geq 1/2 \cdot 2^n$. $\rightsquigarrow$ why?

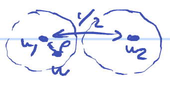
given u, $\{v : \langle u,v \rangle = 0\}$ is linear space of dim $n-1$, and size 2^{n-1}.
hence $\{x : HW(u) = HW(v)\} =$
$= \{x : \langle u-v, x \rangle = 0\}$ has size $\frac{1}{2} \cdot 2^{n-1}$.

we will use this extensively.

How to know if w is a valid codeword? Obs $WH(\{0,1\}^n)$ is set of all linear functions, hence enough to test if f is linear.

def. Linearity Testing.
f, g ρ-close if $\Pr[f(x) = g(x)] \geq \rho$.
f close to linear if $\exists$ g linear, f, g ρ-close.

th: if $\Pr_{x,y}[f(x+y) = f(x) + f(y)] \geq \rho$, then f ρ-close to linear.

From now on, can assume we're $1-\delta$-close to linear.
Can we recover real codeword $\tilde{w}$ from w?
Yes:  . But locally & efficiently?

Also yes. Want $\tilde{w}[x]$.
Sample x'; set $x'' = x' + x$.
Query $y' = w[x']$, $y'' = w[x'']$.
Answer $y = y' + y''$.

obs $\left.\begin{array}{l}\Pr[y' = \tilde{w}[x']] \geq 1-\delta \\ \Pr[y'' = \tilde{w}[x'']] \geq 1-\delta\end{array}\right] \Pr[y = \tilde{w}[x]] \geq 1 - 2\delta$.

We'll build a PCP for problem QuadEq.
ie: find if system of quadratic eqs over $\mathbb{F}_2$ has solution.
claim: QuadEq is NP-complete.
assume wlog no terms of deg 1 (replace x_i by x_i^2).
reinterpret problem as $AU = b$,
where A is an $m \times n^2$ matrix and $U = u \otimes u = uu^T$.

π is $WH(u)\, WH(uu^T)$.
need to check: 1. $\pi = fg$ is concatenation of two WH codes.
2. $U = uu^T$.
3. $AU = b$.

correctness Ok.
soundness of 1: OK by linearity testing.
for 2 and 3 we'll assume that all queries done using local decoding protocol.

to test 2, let $u = WH^{-1}(f)$, $w = WH^{-1}(g)$; we test if

$$\underbrace{\langle (u \otimes u), r \otimes r' \rangle}_{\substack{= \langle u,r \rangle \cdot \langle u,r' \rangle \\ = f(r) \cdot f(r')}} = \langle w, r \otimes r' \rangle = \underbrace{g(r \otimes r')}_{\text{obs can read directly from } \pi} \quad \text{for random } r, r'.$$

claim: if $w \neq u \otimes u$, then $\Pr_{r,r'}[f(r) \cdot f(r') \neq g(r \otimes r')] \geq 1/4$.

(apply $A \neq B \Rightarrow \Pr_x[A_x \neq B_x] \geq 1/2$ twice).

to test 3, we'd like to test if $A_i U = b_i$ $\forall i$

instead we'll check if $\sum_{i \in J} A_i U = b_i$ for random J.

iow: $\langle 1_J, A_i U \rangle = \langle 1_J, b_i \rangle$.
$\qquad = \langle 1_J^T A_i, U \rangle$
can read directly from π.

this finishes proof of PCP thm.
Now let us see linearity test.
We'll represent functions in Fourier basis. $f : \{\pm 1\}^n \to \{\pm 1\}$.
i.e. usually we write $f = \sum f_x e_x$ $\quad x \in \{-1,1\}^n$
instead we'll write $f = \sum \hat{f}_S \chi_S$ $\quad S \subseteq [n]$.
obs $x+y$ in $\{0,1\}^n$ $\equiv$ $x \cdot y$ in $\{\pm 1\}^n$
linear functions over $\{0,1\}^n$ are characters χ_S in $\{\pm 1\}^n$.

$\langle f, g \rangle = \sum_x f(x) g(x) / 2^n$
$\hat{f}_S = \langle f, \chi_S \rangle = (\#x : f = g - \#x : f \neq g)/2^n \Rightarrow f$ $\frac{1}{2} + \varepsilon$-close to χ_S iff $\hat{f}_S = 2\varepsilon$.

linear test thm is:

$\Pr[f(xy) = f(x) f(y)] \geq \frac{1}{2} + \varepsilon \Rightarrow \exists S$ st $\hat{f}_S \geq 2\varepsilon$.

proof: obs $E[f(xy) f(x) f(y)] = \Pr[=] - \Pr[\neq] \geq 2\varepsilon$.
$=$
$E\left[\left(\sum \hat{f}_S \underbrace{\chi_S(xy)}_{= \chi_S(x)\chi_S(y)}\right) \cdot \left(\sum \hat{f}_S \chi_S(x)\right) \cdot \left(\sum \hat{f}_S \chi_S(y)\right)\right] =$

$= E\left[\sum \hat{f}_S \hat{f}_{S'} \hat{f}_{S''} \chi_S(x) \chi_S(y) \chi_{S'}(x) \chi_{S''}(y)\right] = \sum \hat{f}\hat{f}\hat{f}\, E =$

$= \sum \hat{f}\hat{f}\hat{f} \underbrace{E\, \chi_S(x) \chi_{S'}(x)}_{\substack{\langle \chi_S, \chi_{S'} \rangle \\ = \delta_{S,S'}}} \underbrace{E\, \chi_S(y) \chi_{S''}(y)}_{\substack{\langle \chi_S, \chi_{S''} \rangle \\ = \delta_{S,S''}}} = \sum \hat{f}_S^3 \leq$
x, y indep

$\leq \max_S \hat{f}_S \cdot \underbrace{\sum \hat{f}_S^2}_{=1 \text{ (Parseval)}}$.