PCPs.

Non-interactive version of IP.

def $(r(n), q(n))$-PCP. Have input x, $|x|=n$, proof π,
Verifier uses r coins and queries q positions of π.
Then: $x \in L \Rightarrow \exists \pi$ $V(x,\pi)$ accepts w/ pr 1
$x \notin L \Rightarrow \forall \pi$ $V(x,\pi)$ — $\leq 1/2$.

th[1] $NP = PCP(O(\log n), O(1))$. // in fact $q=3$ enough
th $NEXP = PCP(poly, O(1)) = MIP$

MIP : multi-prover IP, where provers do not communicate

remarks about PCP thm.
- → can assume wlog $|\pi| \leq q \cdot 2^r$; o/w cannot query some part of the string.
- → $1/2$ not important.
- → $PCP(r,q) \subseteq NTIME(2^r \cdot q)$

Example: PCP for GNI.
π indexed by graphs. $\pi[G] = i$ if $G \cong G_i$; whatever o/w.
V samples σ and i ; checks $\pi[\sigma(G_i)] = i$.

PCP $\equiv$ inapproximability.

given a function $f: \mathbb{N} \to \mathbb{N}$, a TM is a ρ-approx of f if $TM(x)$ within a factor ρ of $f(x)$ $\forall x$.

For NP-optimization problems we also want a witness.

eg. MaxSAT : $val(F) = \max_\alpha |C \in F : F(\alpha)=1|$. / $|F|$.
ρ-approx is α st $val(F,\alpha) \geq \rho \cdot val(F)$.

obs F sat iff $val(F)=1$.
obs 1-sided error is enough.

th[2] $\exists \rho<1$ st $\forall L \in NP$ $\exists f$ poly-time st
$x \in L \Rightarrow val(f(x)) = 1$
$x \notin L \Rightarrow val(f(x)) < \rho$.

we have th[1] $\Leftrightarrow$ th[2].

def CSP: $\varphi = \{\varphi_i\}$; $\varphi_i : \{0,1\}^{I_i} \to \{0,1\}$.
$val(\varphi) = \max_\alpha |i : \varphi_i(\alpha) = 1|$.
e.g. when $\varphi_i = \bigvee_{j \in I} x_j$, we have SAT.
when $|I_i| \leq q$ $\forall i$, we say φ is q-CSP.

def gap CSP: given φ, ρ, determine $val(\varphi)=1$ or $\leq \rho$.
(if $\rho < val\, \varphi < 1$, can answer whatever).

th[3] ρ-Gap-q-CSP is NP-hard (in the th[2] sense)

claim: th[1] $\equiv$ th[3].

1⇒3) Assume $NP = PCP(O(\log n), q)$.
We show $1/2$-Gap-q-PCP NP-hard. L SAT. By assumption $\exists$ verifier that makes q queries using $c \log n$ random bits.
so $m = n^c$ possible queries.
let $\varphi_i(\pi) = 1$ iff V accepts w. randomness i ; $\varphi = \{\varphi_i\}$.
then x SAT $\Rightarrow val(\varphi)=1$
x UNSAT $\Rightarrow val(\varphi) \leq 1/2$.

3⇒1) Assume $1/2$-Gap-q-PCP NP-hard. $L \in NP$. By assumption $\exists f$ st $x \in L \Rightarrow val(f(x))=1$
$x \notin L \Rightarrow val(f(x)) \leq 1/2$.
Verifier: choose $i \in f(x)$; check if π satisfies.
$x \in L \Rightarrow \varphi$ sat; can take π as asgn.
$x \notin L \Rightarrow val(f(x)) \leq 1/2$; ——

2⇒3) Trivial
3⇒2) Build reduction.

We'll prove weak PCP theorem: $NP \subseteq PCP(poly, O(1))$.

Need robust way to encode strings, so they are resilient to errors : locally decodable error-correcting codes.

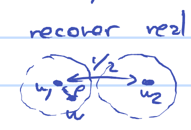
def Walsh-Hadamard code. $WH : \{0,1\}^n \to \{0,1\}^{2^n}$
$WH(u)(x) = \langle u,x \rangle \pmod 2$.
can think of $WH(u)$ as tt of function $\langle u, \cdot \rangle$.

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

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