Summary of Algebraic Proof

Result $NP \subseteq PCP[O(\log n), O(1)]_{\{0,1\}^{\text{polylog } n}}$

Toolbox "The low deg poly toolbox"

(1) Low degree extension - work with low deg poly instead of arbitrary strings.

Low deg poly = good code ("Reed-Muller code")

Advantages:
- (i) good rate (= encoding doesn't increase the length too much)
- (ii) good distance (= two codewords differ almost everywhere)
- (iii) (2) Self-correction
- (iv) (3) Local testing

(4) recursive structure (used for sum-check and ldt)

(5) expressibility
zero checking

Disadvantages:

(i) large alphabet $\mathbb{F}$ which is large $|\mathbb{F}| = \text{polylog} n$

Note the alphabet of PCP construction is $\{0,1\}^{\text{polylog} n}$, not $[\text{polylog} n]$ (which is not $O(1)$, but not that bad either).

The reason is (ii):

(ii) large locality & ~~test~~ correction locality are $|\mathbb{F}|$ (or $\text{poly}|\mathbb{F}|$) points (corr. to line or plane inside $\mathbb{F}^m$).

(ii) non-optimal rate length of encoding is polynomial rather than linear in length of encoded message.

Choosing $|\mathbb{F}|$ and m differently can make almost linear.

Proof Outline

Want to decide whether φ is sat.

① Sum-Check

Comp

φ is sat $\Rightarrow \exists$ proof that consists of poly that we always accept.

Sound

φ is not sat $\Rightarrow \forall$ proof that consists of poly we accept with probability $\leq \frac{1}{2}$.

② New proof consists of:

I Proof from sum-check.

II Proof needed for self-correction (restrictions to lines)

III proof needed for low deg testing (restrictions to planes)

③ New verification

Simulate sum-check verifier. Replace each query to poly by:

I Low degree test.

II Self correction to answer query.

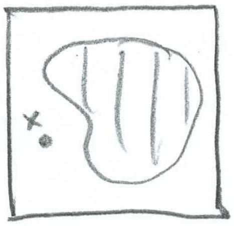
③ The argument   Completeness is easy. Assume φ is not sat.

Three BAD things can happen:

I For some poly, the prover in fact gives a table of a func. that is far from poly.

→ Will catch with const. prob.

II For some poly, the prover gives a table of a func. that is close to poly, but on some query it gives a value which is not consistent with the close poly.



→ Will catch with const. prob.

III For all poly, the prover gives to all queries values that are consis. with the close low deg poly.

→ The Sum-Check verifier on the proof that contains for every poly, the low deg poly that is close to the given func., Should reject with const. prob.

<u>Next</u> Decrease alphabet from $\{0,1\}^{\text{polylog}\, n}$ to $O(1)$. — Via composition.