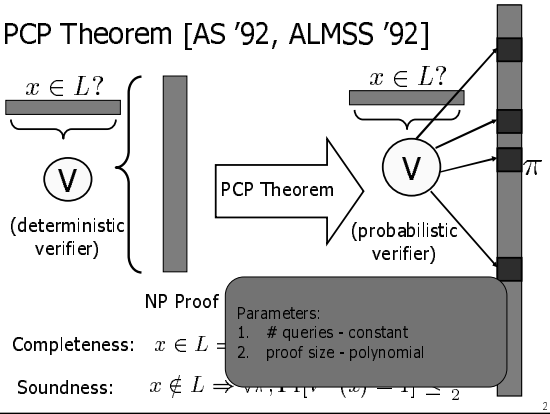
PCP Theorem [AS '92, ALMSS '92]



2

Robust PCPs of Proximity

(Shorter PCPs, applications to Coding)

Eli Ben-Sasson (Radcliffe)

Oded Goldreich (Weizmann & Radcliffe)

Prahladh Harsha (MIT)

Madhu Sudan (MIT & Radcliffe)

Salil Vadhan (Harvard & Radcliffe)

1

Short PCPs vs Query Complexity

	queries	Blowup in proof size |PCP proof|/|NP proof|
[PS '94]	$O(\frac{1}{\epsilon})$	n^{ϵ}
[GS '02, BSVW '03]	$O(1)$	$2^{\sqrt{\log n}}$
This paper	$O(\frac{1}{\epsilon})$	$2^{(\log n)^{\epsilon}}$
This paper	$o(\log \log n)$	quasi $\operatorname{poly} \log n$

Previous PCPs required blowup factor of $2^{\sqrt{\log n}}$ even when reading ϵ bit-locations

4

Short PCPs?

How long is the new PCP?

- Old NP proof – n ; New PCP - *?*

3

Proof Techniques

6

Why Short PCPs?

- Negative Consequences
  - Tightness of inapproximability results with respect to running time
- Positive Consequences
  - Future "practical implementations" of proof-verification
  - Coding Theory
    - Locally testable codes [GS '02, BSVW '03, this paper]
    - "Relaxed Locally Decodable Codes" [this paper]
  - Cryptography
    - e.g.: non-blackbox techniques

5

Robust PCP of Proximity
and
Composition Theorem

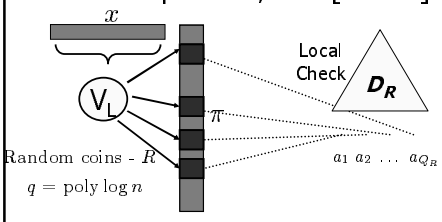
8

Proof Overview

- New Definition: Robust PCP of Proximity
  New Composition Theorem
  - Simple, modular
  - Avoid overhead present in earlier compositions
- Building Block

7

Proof Composition, a la [AS '92]



Completeness: $x \in L \Rightarrow \exists \pi, \Pr[V_R^{x,\pi}(a_1, \ldots, a_{Q_R}) = 1] = 1$

Soundness: $x \notin L \Rightarrow \forall \pi, \Pr[V_R^{x,\pi}(a_1, \ldots, a_{Q_R}) = 1] \leq \frac{1}{2}$

Need to verify that $a_1\ a_2\ \ldots\ a_{Q_R}$ satisfy local check D_R

Idea : Use a PCP verifier to check !

10

Why Composition?

- Don't know to build PCPs with $q = O(1)$ and size = poly(n) directly
- However,

[BFLS '91] type of PCP:
size = poly(n)
q = poly log n
} Verifier V

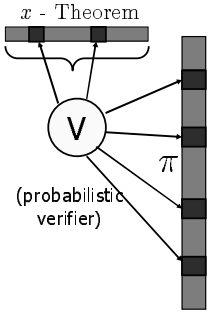
[AS '92, ALMSS '92] "magically compose" verifier V with itself to obtain new verifier $V \oplus V$ with following parameters

size = poly(n)
q = poly log log n
} $V \oplus V$

9

PCP of Proximity (PCPP) New!

(aka, Assignment testers [DR '03])



Completeness:

$x \in L \Rightarrow \exists \pi, \Pr[V^{x,\pi}() = 1] = 1$

Soundness:

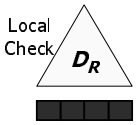
x is far from $L \Rightarrow$
$\forall \pi, \Pr[V^{x,\pi}() = 1] \leq \frac{1}{2}$

Important:
- # queries = sum of queries into theorem + proof
- Theorem is not encoded in any error correcting code

Specialization of "PCP spot checkers" [EKR '99]

12

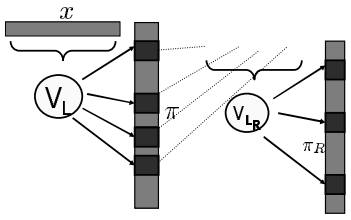
Proof Composition, Contd



Create language

$L_R = \{(a_1, \ldots, a_{Q_R}) | D_R \text{ accepts } (a_1, \ldots, a_{Q_R})\}$

Check if $(a_1, \ldots, a_{Q_R}) \in L_R$ using a PCP verifier

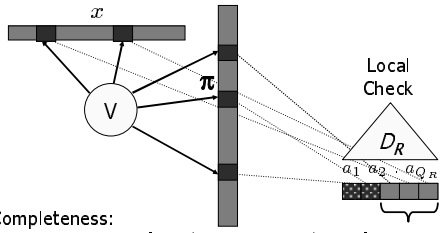


Problem: PCP verifier V_{L_R} needs to read all of theorem (input)

Idea: Define a new Verifier that "barely reads" the theorem

11

Robust PCP of Proximity (Robust-PCPP) New!



Completeness:

$x \in L \Rightarrow \exists \pi, \Pr[D_R(a_1, \ldots, a_{Q_R}) = 1] = 1$

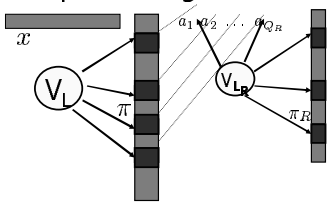
Robustness:

x is far from $L \Rightarrow \forall \pi, \Pr[D_R(a_1, \ldots, a_{Q_R}) = 0] > \frac{1}{2}$

$\forall \pi, \Pr[(a_1, \ldots, a_{Q_R}) \text{ is far from } L_R] > \frac{1}{2}$

14

Composition again



Completeness: $x \in L \Rightarrow \exists \pi, \Pr[(a_1, \ldots, a_{Q_R}) \in L_R] = 1$

Soundness: $x \notin L \Rightarrow \forall \pi, \Pr[(a_1, \ldots, a_{Q_R}) \notin L_R] > \frac{1}{2}$

Problem:

Need to distinguish between $(a_1, \ldots, a_{Q_R}) \in L_R$ & $(a_1, \ldots, a_{Q_R}) \notin L_R$

PCPP distinguishes between $(a_1, \ldots, a_{Q_R}) \in L_R$ & far from L_R

Strengthen soundness condition of verifier V_L

13

Summarizing...

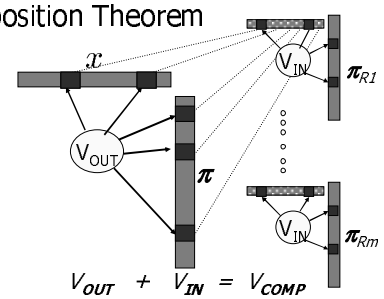
- Defined Robust-PCPs of Proximity
- Proved a natural composition theorem for robust-PCPPs
- Simpler and shorter constructions of PCPs

Open Questions:

- Constant query PCPs of size $n \cdot \text{poly} \log n$?

16

Composition Theorem



V_{OUT} + V_{IN} = V_{COMP}

- Req. of Inner Verifier: proximity of inner< robustness of outer

Randomness: $r_{COMP} = r_{OUT} + r_{IN}$ Queries: $q_{COMP} = q_{IN}$

Proximity: $\delta_{COMP} = \delta_{OUT}$ Robustness: $\rho_{COMP} = \rho_{IN}$

New PCPP Proof for $V_{COMP} = (\pi, \pi_{R1}, \ldots, \pi_{Rm})$

15

The End

17