Restricted Non-interactive Zero Knowledge Proofs

Jacob Gray[1] Saachi Mutreja[2] Pengxiang Wang[3]

[1]University of Massachusetts Amherst

[2]University of California, Berkeley

[3]University of Michigan

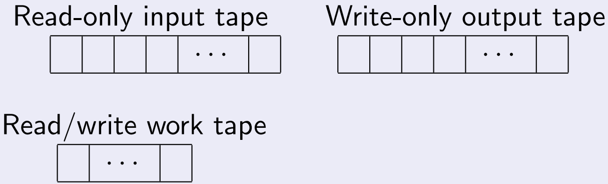
July 21, 2022

Outline

Log-space computation

Definition

Figure 1: Log-space transducer



Has only logarithmic work space, but still relatively powerful

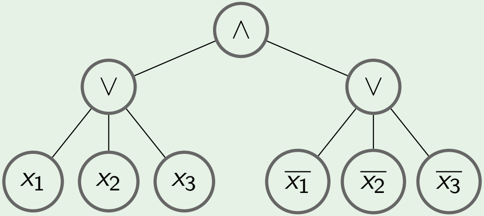
- Closed under function composition
- Closed under complement
- Can run for (at most) polynomial time

L is the class of problems computable by some log-space transducer

Circuit complexity

Example

Figure 2: Output node is 1 iff input has at least one 0 and one 1



Circuit (family) classes:

- NC^0: Fan-in 2, constant depth, poly-size
- AC^0: Unbounded fan-in, constant depth, poly-size
- Projection: no gates, only wires from input to output (possibly negated)

(NISZK) Non-interactive, statistical zero knowledge proof

Intuition: prover wants to prove input x has some property to the verifier without revealing additional information

Definition

An NISZK proof system consists of four main parts:

- Prover: very powerful machine, outputs some distribution of proofs given (x, σ).
- Verifier: randomized, limited machine which almost always accepts if correct proof is provided for (x, σ) (completeness), and almost always rejects on a fake or insufficient proof (soundness)
- Simulator: used to guarantee zero knowledge. Should output a distribution of proofs statistically similar to the prover's distribution
- Reference string σ: uniformly random string provided to verifier and prover to use during the proof - "shared randomness"

Known results

$\mathsf{NISZK_L}$

NISZK, but with log-space verifier and simulator. Introduced in 2020 paper by Allender and REU students [All+21].

Was shown to have two complete problems - SDU_{NC^0} and EA_{NC^0} - which are modified versions of complete problems for NISZK.

Definition

Promise-$\mathsf{EA}_{\mathsf{NC}^0}$: a promise problem over pairs (C, k), where C is an NC^0_4 circuit and k an integer.

$$(C, k) \in \mathsf{EA}_{YES} \text{ if the Shannon entropy of } C \text{ is } \geq k + 1$$
$$(C, k) \in \mathsf{EA}_{NO} \text{ if the Shannon entropy of } C \text{ is } \leq k - 1.$$

Not much else was known about this class outside of this paper.

Perfect randomized encodings

Introduced in [AIK06] to show that NC^0 had OWFs iff more powerful classes like NL did.

Definition

Adapted from [AII+21, Definition 27] (perfect randomized encoding):

Let $f : \{0,1\}^n \to \{0,1\}^{l(n)}$ be a function. We say that $\hat{f} : \{0,1\}^n \times \{0,1\}^m \to \{0,1\}^s$ is a perfect uniform randomized encoding of f with blowup b if it is:

- **Input Independent:** for every $x, x' \in \{0,1\}^n$ such that $f(x) = f(x')$, $\hat{f}(x, U_m)$ and $\hat{f}(x', U_m)$ are identically distributed.
- **Output Disjoint:** for every $x, x' \in \{0,1\}^n$ such that $f(x) \neq f(x')$, $\operatorname{supp} \hat{f}(x, U_m) \cap \operatorname{supp} \hat{f}(x', U_m) = \emptyset$.
- **Uniform:** for every $x \in \{0,1\}^n$ the random variable $\hat{f}(x, U_m)$ is uniform over $\operatorname{supp} \hat{f}(x, U_m)$.
- **Balanced:** for every $x, x' \in \{0,1\}^n$ $|\operatorname{supp} \hat{f}(x, U_m)| = |\operatorname{supp} \hat{f}(x', U_m)| = b$.

New results

$\mathsf{NISZK_L} = \mathsf{NISZK_{AC_0}}$

Since $\mathsf{AC_0} \in \mathsf{L}$, it is clear that $\mathsf{NISZK_{AC_0}} \in \mathsf{NISZK_L}$.
To prove: $\mathsf{NISZK_L} \in \mathsf{NISZK_{AC_0}}$ The Entropy Approximation Problem in $\mathsf{NC_0}$, denoted $EA_{\mathsf{NC_0}}$, is a complete problem for $\mathsf{NISZK_L}$.
We will show that $EA_{\mathsf{NC_0}} \in \mathsf{NISZK_{AC_0}}$.

Proving $EA \in$ NISZK

Transform an instance (C, k) of EA of length s into a distribution Z by

- Taking poly(s) copies of X
- hashing
- repeat items 1 and 2

The Problem: AC_0 circuits cannot compute hash functions. They can be computed in logspace.

Solution

Theorem

There exists a constant c such that, for every $k(n) > n/\operatorname{poly}(\log n)$, and every $r(n) \in [\Omega(\log n), k(n)/c]$, extraction of $(1+c)\cdot r(n)$ bits that are $\epsilon(n) = \frac{1}{n^3}$ close to $\{0,1\}^{(1+c)\cdot r(n)}$ in total variation distance is possible in uniform AC_0 using a seed of length $r(n)$.

Theorem

There is a polynomial time computable function that takes an instance $(X, m-a)$ of EA_{NC_0} and a parameter s, and produces a distribution Z on $\{0,1\}^l$ such that:

1. *If $H(X) > m-a+1$, then Z has statistical difference at most $1/\operatorname{poly}(s)$ from the uniform distribution on $\{0,1\}^l$.*
2. *If $H(X) < m-a-1$, then the support of Z is at most a 2^{-s} fraction of $\{0,1\}^l$.*

Non Interactive Proof System

1. Let Z be the distribution on $\{0,1\}^l$ obtained from $(X, m-a)$ taking s to be the total description length of $(X, m-a)$ in bits. Let $\sigma_1, \sigma_2, \ldots, \sigma_{s/\log s} \in \{0,1\}^l$ be the reference strings. The verifier sends $\sigma_1, \sigma_2, \ldots, \sigma_{s/\log s}$ to the prover.
2. The prover picks an i at random from $i \in \{0, 1, \ldots, s/\log(s)\}$ such that $|\{r_i | Z(r_i) = \sigma_i\}| \neq \phi$. Then, after fixing i,it picks a random r_i from $\{r_i | Z(r_i) = \sigma_i\}$. It sends r_i to the verifier.
3. V accepts if $Z(r_i) = \sigma_i$.

Simulator

1. Let Z be obtained from $(X, m-a)$ as in the proof system.
2. Sample an i uniformly at random from $\{1, 2, \ldots, s/\log s\}$.
3. For this index i,sample r_i at random, and compute $Z(r_i) = \sigma_i$.
4. For all $j \in \{1, 2, \ldots, i-1, i+1, \ldots, s/\log(s)\}$, sample σ_j uniformly at random.
5. Output $(r_i, \sigma_1, \ldots \sigma_i = Z(r_i), \ldots \sigma_{s/\log(s)})$

Completeness

Claim

If $H(X) > m - a + 1$, then the verifier accepts with probability $\geq 1 - \frac{1}{2^s}$.

Proof.

If $H(X) > m - a + 1$, then $TV(Z, U_{\{0,1\}^l}) \leq \frac{1}{\text{poly}(s)}$. Thus, for a given i

$$
\begin{aligned}
P(\exists r_i | Z(r_i) = \sigma_i) &\geq 1 - P(\nexists r_i | Z(r_i) = \sigma_i) \\
&\geq 1 - \prod_{i=1}^{s/\log(S)} \frac{1}{\text{poly}(s)} \\
&\geq 1 - \frac{1}{\text{poly}(s)^{s/\log s}} \\
&\geq 1 - \frac{1}{2^s}
\end{aligned}
$$

□

Soundness

Claim

If $H(X) < m - a - 1$, then the verifier accepts with probability $\leq \frac{1}{2^s}$.

Proof.

If $H(X) < m - a - 1$, then, by Lemma 0.2, the support of Z is at most a 2^{-s} fraction of $\{0,1\}^l$. Thus,

$$\begin{aligned} P(\textit{verifier accepts}) &= P(\exists i | Z(r_i) = \sigma_i) \\ &\leq \sum_{i=1}^{s/\log s} \frac{1}{2^s} \\ &\leq \frac{s}{\log s} \cdot \frac{1}{2^s} \\ &\approx \frac{1}{2^s} \end{aligned}$$

□

Construction of Distribution Z by AC_0 Circuits

We let $s \approx m$ be the length of the description of an instance of (X, k) of EA.

Let the threshold for the EA problem be $k = m - a$, where a is a small constant $\in (0, 1)$.

STEP 1: Many copies of distribution X

Let m (resp. n) be the number input (resp. output) gates to X. We take $q = 4sm^2$ independent copies of X to create distribution X'. Observe that $H(X') = q \cdot H(X)$. For every $x, P(X = x) \geq \frac{1}{2^m}$. So the flattening lemma implies that X' is $\delta = \sqrt{q} \cdot m = 2\sqrt{s} \cdot m^2$ flat.
Thus,

1. if $H(X) > k + 1$, then $H(X') > q \cdot k + q > qk$.
2. If $H(X) < k - 1$, then $H(X') < q \cdot k - q$.

STEP 2: Using AC_0 Randomness Extractor on X'

Randomness source: $r \in \{0,1\}^{qk/c}$, where c is the constant mentioned in theorem 1. Consider distribution Y on $E(x', r) : \{0,1\}^{qm} \times \{0,1\}^{qk/c} \to \{0,1\}^{qk+qk/c}$.

1. If $H(X) > k + 1$, then the statistical difference of Y from the uniform distribution over $\{0,1\}^{qk+qk/c}$ is at most $1/(qm)^3$.
2. If $H(X) < qk - 1$, then $H(Y) < q \cdot k - q + qk/c$.

STEP 3: Many copies of distribution Y

1. If $H(X) > k+1$, then Y' has statistical difference at most $q' \cdot \frac{1}{(qm)^3} = (4s(qm)^2) \cdot \frac{1}{(qm)^3} = \frac{4s}{qm} = \frac{1}{m^3} = \mathcal{O}\frac{1}{\text{poly}(s)}$.
2. If $H(X) < k-1$, then $H(Y') < q' \cdot H(Y) < q' \cdot q \cdot k \cdot (\frac{c+1}{c}) - q' \cdot q$.

STEP 4: Using AC_0 randomness extractor on Y'.

Let Z be the resulting distribution.
$Z(r') = (Y'(r'), E(r', r))$
If $H(X) > k + 1$,the statistical distance of Z from uniform is $\approx 1/\operatorname{poly}(s)$.
If $H(X) < k - 1$,
$S1 : \{(Y'(r'), E(r', r)) | P(Y'(r') = y') \leq 2^{-N-2M}\}$
$S2 : \{(Y'(r'), E(r', r)) | 2^{-N-2M} \leq P(Y'(r') = y') \leq 2^{-N}\}$
$S3 : \{(Y'(r'), E(r', r)) | P(Y'(r') = y') \geq 2^{-N}\}$
For $i \in \{1, 2, 3\}, |S_i|/|D| = \frac{1}{2^s}$, where D is the uniform distribution.
Thus, $Z = S1 \cup S2 \cup S3$
$|Z|/|D| = \frac{1}{2^s}$

$\mathsf{NISZK}_\mathsf{L} = \mathsf{NISZK}_\mathsf{NL}$

For an arbitary problem $\Pi \in \mathsf{NISZK}_\mathsf{NL}$, let (S, P, V) be its protocol. Then, we will run the following:

Algorithm 1: $M_x(s)$

Data: $x \in \Pi \cup \bar{\Pi}, s$ coin flips, (S, V) the simulator and verifier
$(\sigma, p) \leftarrow S(x)$ `// under coin flip` s
if $V(\sigma, p) = 1$ **then**
  return σ;
else
  return $0^{|\sigma|}$;

(Convince yourself that $M_x(s)$ is NL-computable). Now, on $x \in \Pi$, w.h.p. $M_x(s)$ is uniform over its support, and on $x \notin \Pi$ w.h.p. $M_x(s)$ has small support. We want to find an encoding of $M_x(s)$ in NC^0 with similar entropy.

$\mathsf{NISZK_L} = \mathsf{NISZK_{NL}}$

Idea: [RA97] shows that for any instance of

$$\mathsf{PATH} := \{\langle G, s, t\rangle : s \rightsquigarrow t\}$$

there is a random weight assignment $W = \{w_i : i \in [n^2]\}, w_i : E(G) \to [4n^2]$ such that with probability exponentially close to 1: $\exists i$ minimal such that (G, w_i) has a unique minimum path from s to t.
This reduces any NL problem to a UL problem, where UL is a class already known to have perfect randomized encodings in NC^0. This completes the high level idea of our proof.
We also proved that $\mathsf{NISZK_L} = \mathsf{NISZK_{PM}}$ using a similar proof, but due to time constraints it won't be explained here.

Summary

Presented results:

- $\mathsf{NISZK}_{\mathsf{AC}^0} = \mathsf{NISZK}_{\mathsf{L}} = \mathsf{NISZK}_{\mathsf{NL}}$

Going forward:

- $\mathsf{NISZK}_{\mathsf{L}} \stackrel{?}{=} \mathsf{NISZK}_{\mathsf{DET}}$
- $\mathsf{OWFs} \in \mathsf{NC}^0 \stackrel{?}{\leftrightarrow} \mathsf{OWFs} \in DET$

Acknowledgements

We would like to thank our advisor, Eric Allender, his graduate student, Harsha Tirumala, and the DIMACS REU 2022 program, which this research is being conducted as part of.

We would also like to thank the NSF, with this research being supported by NSF grant CCF-185221.

Bibliography

[RA97] K. Reinhardt and E. Allender. “Making nondeterminism unambiguous”. In: *Proceedings 38th Annual Symposium on Foundations of Computer Science*. 1997, pp. 244–253. DOI: 10.1109/SFCS.1997.646113.

[AIK06] Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. “Cryptography in NC^0”. In: *SIAM Journal on Computing* 36.4 (2006), pp. 845–888. DOI: 10.1137/S0097539705446950.

[All+21] Eric Allender et al. “Cryptographic Hardness Under Projections for Time-Bounded Kolmogorov Complexity”. In: LIPIcs 212 (2021). Ed. by Hee-Kap Ahn and Kunihiko Sadakane, 54:1–54:17. DOI: 10.4230/LIPIcs.ISAAC.2021.54.