AICR · OPEN PROBLEM

Circuit Satisfiability Resists Small Space with Preprocessing

A space-time hypothesis whose consequence is a limitation on succinct interactive oracle proofs

Status. Statement: AI-written from Shafik Nassar and Ron D. Rothblum, *Succinct Interactive Oracle Proofs: Applications and Limitations*, IACR ePrint 2022/281. Not yet checked by a human. This is their Conjecture 1.2, a parameterized family rather than a single claim; the source's Corollary 1.3 turns each parameter setting into a limitation on succinct IOPs, and it is careful that the strongest setting is only "(arguably) unlikely" to be false rather than confidently believed.

Category. *Proof Systems.*

Conjecture (informal). *Interactive oracle proofs let a verifier be convinced by reading a few bits of the prover's messages, and* succinct *ones keep the communication close to the size of the witness rather than the size of the computation. Strong impossibility results are known for succinct PCPs; for IOPs the picture is better, since relations decidable in small space do have them. What is the limit? The source turns the question into one about circuit satisfiability with two resources: how much space, and how much time in a preprocessing phase that does not yet see the instance. Its conjecture is that a circuit's satisfiability cannot be decided in space polynomial in the number of* inputs *— which may be far fewer than the number of gates — however much preprocessing time is allowed within a stated budget.*

1 The setting

An interactive oracle proof combines interactive proofs and PCPs: the verifier interacts with an untrusted prover while reading only a few bits of each message. A *succinct* IOP is one whose communication complexity is polynomial — or even linear — in the original witness, rather than in the size of the computation verifying it. Succinct PCPs, whose length is polynomial in the witness, are subject to strong

impossibility results; succinct IOPs are known to exist for the rich class of NP relations decidable in small space, which is why the boundary is worth locating.

The source's route to a limitation runs through a space-time question about circuit satisfiability. Write CSAT for satisfiability of a circuit of size n over m input bits, and note the asymmetry that makes the question interesting: m can be much smaller than n, so $\mathrm{poly}(m)$ space can be far less than the circuit itself.

The source is explicit about how much confidence to attach: it conjectures "that even probabilistic quasi-polynomial time preprocessing would not be sufficient, and taking things to an extreme, it is (arguably) unlikely that $(2^{o(m)} \cdot \mathrm{poly}(n))$-time preprocessing is sufficient." Those are three different levels of confidence and the conjecture is parameterized accordingly.

2 Notation and parameters

- n is the circuit size and m the number of input bits; the regime of interest has $m \ll n$.
- T is a class of functions $t(n, m)$ bounding the preprocessing time. Larger T makes the conjecture stronger and the resulting IOP bound stronger.
- Preprocessing is *probabilistic* and happens before the instance-dependent phase; the space bound $\mathrm{poly}(m)$ applies to the algorithm.
- $\mathcal{R}_{\mathrm{CSAT}}$ is the circuit-satisfiability relation the IOP consequences are stated for.

3 The conjecture

Conjecture 1 ([NR22, Conjecture 1.2]). *For a function class T:* CSAT *for circuits of size n over m input bits cannot be solved by an algorithm that uses* $\mathrm{poly}(m)$ *space and $t(n, m)$-time probabilistic preprocessing, for any $t \in T$.*

Theorem 1 (What it buys, [NR22, Corollary 1.3]). *Assuming Conjecture 1:*

- *with $t(n, m) = \mathrm{poly}(n)$, there is no succinct IOP for $\mathcal{R}_{\mathrm{CSAT}}$ with a constant number of rounds and $O(\log n)$ query complexity;*

- *with* $t(n,m) = 2^{\text{polylog}(m)} \cdot \text{poly}(n)$*, there is no succinct IOP for* $\mathcal{R}_{\text{CSAT}}$ *with* $\text{polylog}(m)$ *rounds and* $\text{polylog}(m) + O(\log n)$ *query complexity;*
- *with* $t(n,m) = 2^{o(m)} \cdot \text{poly}(n)$*, there is no succinct IOP for* $\mathcal{R}_{\text{CSAT}}$ *with* $o(m/\log m)$ *rounds and* $o(m) + O(\log n)$ *query complexity.*

Remark 1 (It is a family, and the members are not equally safe). Conjecture 1 is stated relative to a function class T, so it is really a scale of hypotheses. The source orders the three consequences "from the weakest bound" and attaches decreasing confidence as T grows, describing the largest setting only as "(arguably) unlikely" to be false. A resolution — in either direction — must name its T. Refuting the strongest setting would say nothing about the weakest, and proving the weakest would leave the interesting IOP bounds untouched.

Remark 2 (Why small space for CSAT is not already known). The source's Appendix A gives the calibration. The circuit value problem CVAL is P-complete under log-space reductions, so under the widely believed $\mathsf{P} \not\subseteq \text{Space}(\log)$ it cannot be solved in logarithmic space. But little is known even in sub-linear space: the most space-efficient algorithm known follows the pebbling approach and yields $O(n/\log n)$ space, and it was later proved that for general circuits pebbling cannot do much better — a space lower bound of $\Omega(n/\log n)$ for that technique. Since m can be far smaller than n, $\text{poly}(m)$ space is a genuinely different regime, and this is why the conjecture is not simply a restatement of a known separation.

Remark 3 (What a refutation would mean). The source spells this out, and it is the best argument for the conjecture. If a circuit of size n over m variables could be solved in $\text{poly}(m)$ space with non-trivial probabilistic preprocessing, then "either it can be solved in a single phase; in $\text{poly}(m)$ space or non-trivial time, or it would imply a surprising interplay between space and time complexities and in particular, yield an interesting space-time trade-off for CSAT." So a refutation is not merely a counterexample: it is forced to be a genuine space-time result.

Remark 4 (The direction the source's other results run). The same paper's positive contribution runs the opposite way: using one-way functions it compiles IOPs into zero-knowledge proofs while

nearly preserving proof length, complementing the line initiated by Ben Sasson et al. that compiles IOPs into super-succinct zero-knowledge arguments. That is not this statement, and a resolution of Conjecture 1 does not bear on it.

Remark 5 (Query complexity is measured in a specific way). Each item of Theorem 1 bounds rounds and query complexity together, and the query bounds carry an additive $O(\log n)$ throughout. A claimed succinct IOP that beats one of these bounds should be checked against the exact pairing of round count and query complexity, since loosening either alone does not contradict the corollary.

4 Bibliography

[NR22] Shafik Nassar and Ron D. Rothblum. *Succinct interactive oracle proofs: applications and limitations.* IACR ePrint 2022/281. The source. Conjecture 1.2 and Corollary 1.3 are on page 5; the extended discussion of the conjecture, including the CVAL calibration, is Appendix A on page 33.

[HPV77] John Hopcroft, Wolfgang Paul and Leslie Valiant. *On time versus space.* Journal of the ACM, 1977. The pebbling approach giving the $O(n/\log n)$-space algorithm the source quotes as the state of the art for CVAL.

[PTC77] Wolfgang Paul, Robert Tarjan and James Celoni. *Space bounds for a game on graphs.* Mathematical Systems Theory, 1977. The $\Omega(n/\log n)$ lower bound showing pebbling cannot do much better.

[GVW02] Oded Goldreich, Salil Vadhan and Avi Wigderson. *On interactive proofs with a laconic prover.* Computational Complexity, 2002. Limits on the communication complexity of interactive proofs, which the source positions its IOP limitations against.

[RR20] Noga Ron-Zewi and Ron D. Rothblum. *Local proofs approaching the witness length.* FOCS 2020. The state-of-the-art succinct IOP whose compactness the source verifies in its Appendix B. [UNVERIFIED] — cited in the source as [RR20]; the bibliographic detail here is inferred.