On the Range Avoidance Problem for Circuits

Hanlin Ren — University of Oxford
Rahul Santhanam — University of Oxford
Zhikun Wang — Xi'an Jiaotong University

https://eccc.weizmann.ac.il/report/2022/048/

Range Avoidance Problem (Avoid)

- **Input:** a circuit $C: \{0,1\}^n \to \{0,1\}^\ell$, where $\ell > n$
- **Output:** any string $y \in \{0,1\}^\ell$ not in $\text{range}(C)$
  - That is, for any $x \in \{0,1\}^n$, $C(x) \neq y$
- "Dual Weak Pigeonhole Principle": if you throw 2^n pigeons into 2^ℓ holes, then there is an empty hole
- The problem is easy for randomised algorithms, so the point is to design **deterministic** algorithms

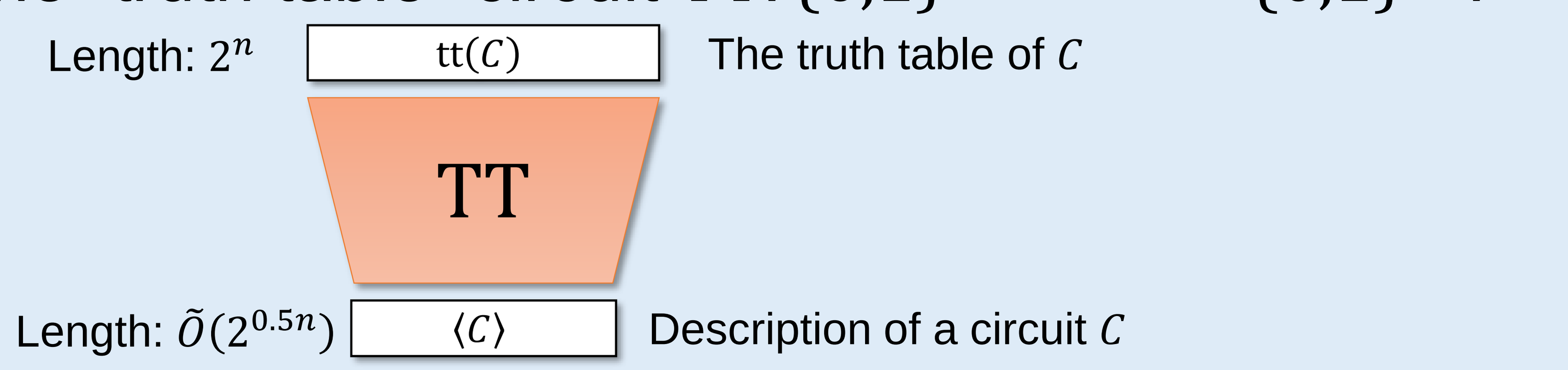
Background: Explicit constructions

"How difficult could it be to find a hay in a haystack?"
------ Howard Karloff

- Deterministic constructions of pseudorandom objects: Ramsey graphs, rigid matrices, extractors, hard truth tables
  - Existence (abundance) proven by the probabilistic method
  - Explicit construction: big open problems!
  - For many problems, even $\mathbf{FP}^{\mathbf{NP}}$-explicit constructions are notoriously open.
- [Korten'21]: Avoid captures explicit constructions (whose existences are proven by the probabilistic method)

Example: Circuit Lower Bounds

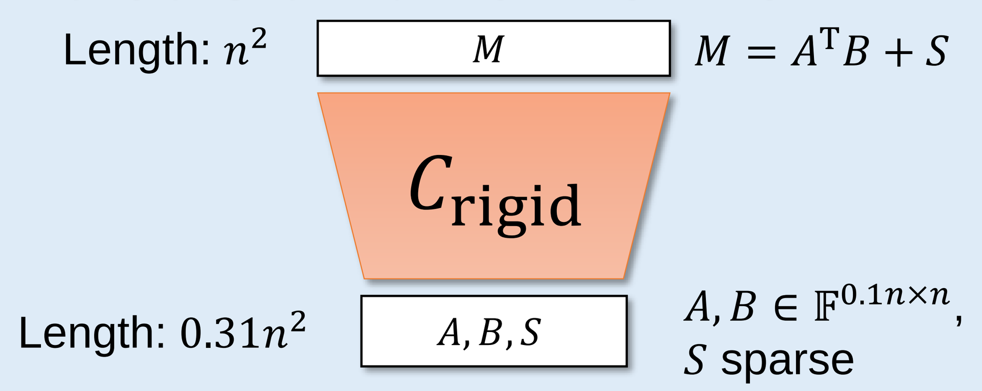
- **Problem:** find the truth table of a function $f: \{0,1\}^n \to \{0,1\}$ that cannot be computed by size-$2^{0.5n}$ circuits
- Consider the "truth table" circuit $\text{TT}: \{0,1\}^{\tilde{O}(2^{0.5n})} \to \{0,1\}^{2^n}$:



- Solving Avoid for TT deterministically implies circuit LBs!

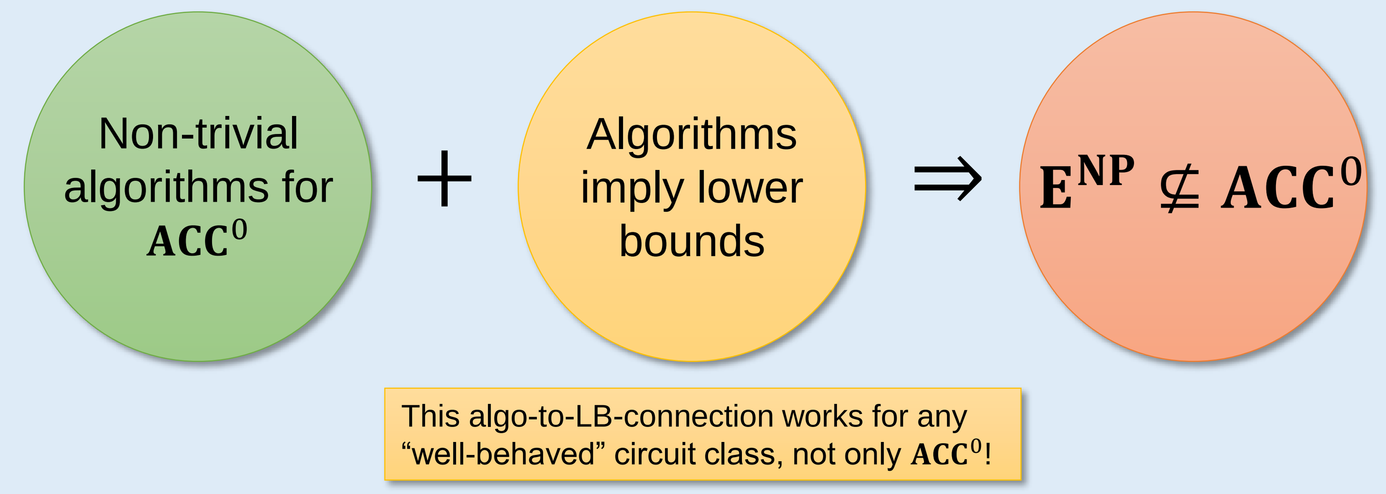
Example: Rigid Matrices

- **Problem:** find an $n \times n$ matrix that is $0.1n^2$-far from rank-$0.1n$ matrices (over $\mathbb{F}_2$)
- Solving Avoid for C_{rigid} deterministically implies rigid matrix construction!



The Algorithmic Method

[Williams'11]: $\mathbf{E}^{\mathbf{NP}} \not\subseteq \mathbf{ACC}^0$.
Ideas: (1) Design non-trivial ($2^n/n^{\omega(1)}$-time) derandomisation algorithms for $\mathbf{ACC}^0$
(2) Prove such algorithms imply lower bounds



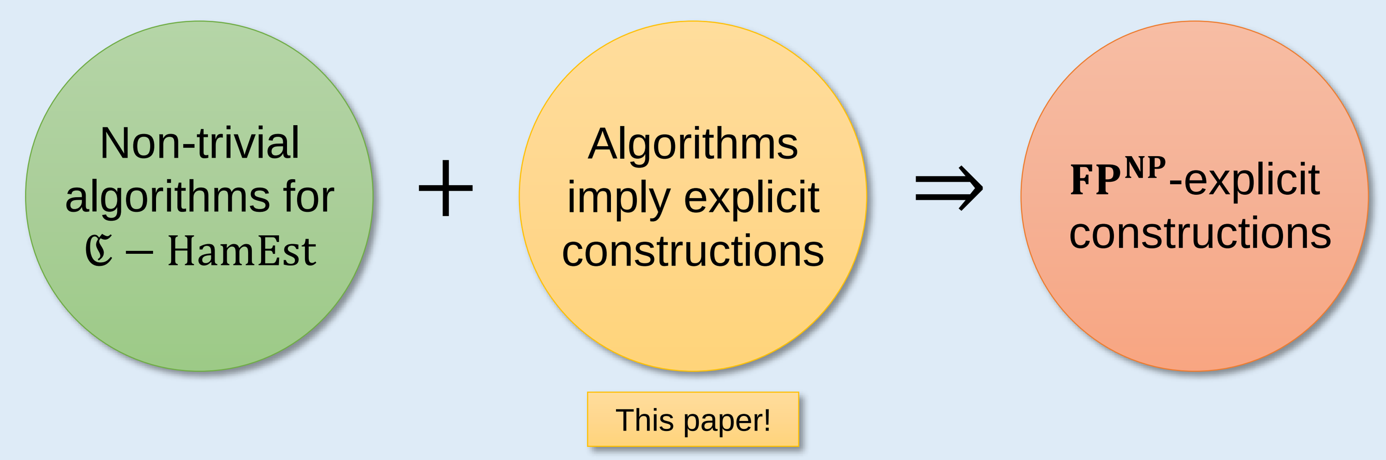
[Alman-Chen'19]: $\mathbf{FP}^{\mathbf{NP}}$-explicit construction of rigid matrices using this method!

- Treat low-rank matrices as a special type of circuit class, then prove avg-case LB against them

Can we apply the Algorithmic Method to more explicit construction problems?

Our Result 1: An Algorithmic Method for Avoid

Theorem: non-trivial data structures for HamEst imply $\mathbf{FP}^{\mathbf{NP}}$ algorithms for Avoid



HamEst: Hamming Weight Estimation

Preprocessing: Given a multi-output circuit $C: \{0,1\}^n \to \{0,1\}^\ell$, runs in $\mathbf{DTIME}[\text{poly}(\ell)]^{\mathbf{NP}}$, produces a data structure $DS \in \{0,1\}^{\text{poly}(\ell)}$

Query: Given $x \in \{0,1\}^n$, estimate the Hamming weight of $C(x)$ in deterministic non-trivial $(\ell/\log^{\omega(1)} \ell)$ time, with random access to DS

Our Result 2: Characterisation of Circuit Lower Bounds for $\mathbf{E}^{\mathbf{NP}}$

Theorem: the following are equivalent:

- $\mathbf{E}^{\mathbf{NP}} \not\subseteq \mathbf{TC}^0$
- $\mathbf{E}^{\mathbf{NP}}$ is avg-case hard for $\mathbf{TC}^0$
- Non-trivial derandomisation for $\mathbf{TC}^0$ with $\mathbf{E}^{\mathbf{NP}}$ preprocessing
- Subexponential-time derandomisation for $\mathbf{TC}^0$ with $\mathbf{E}^{\mathbf{NP}}$ preprocessing
- $\mathbf{E}^{\mathbf{NP}}$-computable PRG fooling $\mathbf{TC}^0$

Results extend to larger (2^{n^ϵ}) size bounds and smaller circuit classes ($\mathbf{ACC}^0$)…

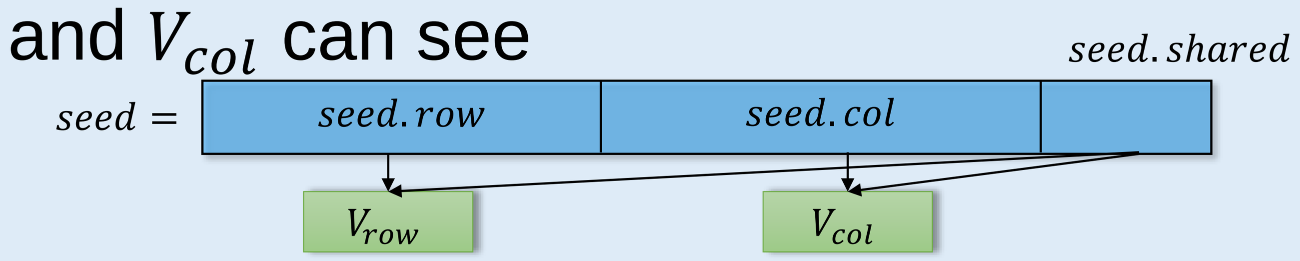
Technique: Rectangular PCPP

Rectangular PCP [BHPT'20]: query patterns are in a "rectangular" fashion

- Proof is an $H \times W$ matrix
- $seed = (seed.row, seed.col)$ (randomness of the verifier)
- $(irow[1], \dots, irow[q]) \leftarrow V_{row}(seed.row)$
- $(icol[1], \dots, icol[q]) \leftarrow V_{col}(seed.col)$
- Query indices are $\{(irow[i], icol[i])\}_{i=1}^q$

Rectangular PCPP (PCP of Proximity): Both proof and input are matrices, queries to both are in a "rectangular" fashion

Almost rectangular PCPP: there is also a short portion $seed.shared$ which both V_{row} and V_{col} can see



Technical ingredient: an almost rectangular PCPP with short proof length!

Conceptual Message

$\mathbf{FP}^{\mathbf{NP}}$-explicit constructions are worth studying!

- Potentially easier than $\mathbf{FP}$-explicit constructions
- Still open for many important cases
- We have a clearer understanding ([Korten'21]) and more tools (this paper)