On the Range Avoidance Problem for Circuits

Hanlin Ren
University of Oxford

Rahul Santhanam
University of Oxford

Zhikun Wang
Xi’an Jiaotong University

Range Avoidance Problem (Avoid)

- **Input**: a circuit $C : \{0,1\}^n \rightarrow \{0,1\}^\ell$, where $\ell > n$
- **Output**: any string $y \in \{0,1\}^\ell$ not in 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 $2^\ell$ 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: open big problems!
  - For many problems, even $\text{FP}^\text{NP}$-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 $f : \{0,1\}^n \rightarrow \{0,1\}$ that cannot be computed by size-$2^{0.5n}$ circuits
- Consider the “truth table” circuit $\text{TT} : \{0,1\}^{\tilde{O}(2^{0.5n})} \rightarrow \{0,1\}^{2^n}$:
  
  Length: $2^n$
  
  The truth table of $C$
  
  $\tilde{O}(2^{0.5n})$
  
  $\tilde{O}^{-1}$
  
  Description of a circuit $C$

- 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 $F_2$)
- Solving Avoid for $C_{\text{rigid}}$ deterministically implies rigid matrix construction!

The Algorithmic Method

[Williams'11]: $\text{E}^\text{NP} \not\subseteq \text{ACC}^0$.

Ideas: (1) Design non-trivial $(2^n/n^{o(1)})$-time derandomisation algorithms for $\text{ACC}^0$

(2) Prove such algorithms imply lower bounds

$\text{Non-trivial algorithms for } \text{ACC}^0 + \text{Algorithms imply lower bounds} \Rightarrow \text{E}^\text{NP} \not\subseteq \text{ACC}^0$

[Alman-Chen’19]: $\text{FP}^\text{NP}$-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 $\text{FP}^\text{NP}$ algorithms for Avoid

*New construction, improves the current best $\tilde{O}(n^{0.75})$

HamEst: Hamming Weight Estimation

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

**Query**: Given $x \in \{0,1\}^n$, estimate the Hamming weight of $C(x)$ in deterministic non-trivial $(\ell/\log^2(1) \ell)$ time, with random access to $D_S$

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

**Theorem**: the following are equivalent:

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

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

Technique: Rectangular PCPP

Rectangular PCP [BHPT’20]: query patterns are in a “rectangular” fashion

- Proof is an $H \times W$ matrix
- $\text{seed} = (\text{seed}.\text{row}, \text{seed}.\text{col})$
- $(\text{row}[1],...,\text{row}[q]) \leftarrow V_{\text{row}}(\text{seed}.\text{row})$
- $(\text{col}[1],...,\text{col}[q]) \leftarrow V_{\text{col}}(\text{seed}.\text{col})$
- Query indices are $\langle \text{row}[i], \text{col}[i] \rangle_{i=1}^q$

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 $\text{seed}$.shared which both $V_{\text{row}}$ and $V_{\text{col}}$ can see

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

Conceptual Message

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

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