Small Circuits for Languages Easily Reduced to Randomness

Sam Hopkins, Mentor: Professor Eric Allender

July 14, 2011

Computational (Decision) Problems

- Definition by Example

$$\begin{aligned} \text{MTN} &= \{x : x \text{ is a monotone sequence } \} \\ \text{PYR-EVEN} &= \{x : x \text{ is a sequence of even length} \\ &\qquad \text{whose first and second halves} \\ &\qquad \text{are monotone}\} \end{aligned}$$

Computational (Decision) Problems

- Definition by Example

$$\begin{aligned} \text{MTN} &= \{x : x \text{ is a monotone sequence } \} \\ \text{PYR-EVEN} &= \{x : x \text{ is a sequence of even length} \\ &\qquad \text{whose first and second halves} \\ &\qquad \text{are monotone}\} \end{aligned}$$

- Decision problem: for some input x, is $x \in$ MTN (or PYR-EVEN)?

Difficulty of Decision Problem

- How hard is it to (algorithmically) decide if $x \in$ MTN (or PYR-EVEN)?

Difficulty of Decision Problem

- How hard is it to (algorithmically) decide if $x \in$ MTN (or PYR-EVEN)?
- MTN, PYR-EVEN $\in \mathcal{O}(n)$.

Relative Difficulty of Decision Problems

- If I already have answers to MTN, how easily can I decide PYR-EVEN?

Relative Difficulty of Decision Problems

- If I already have answers to MTN, how easily can I decide PYR-EVEN?
- With answers to MTN, PYR-EVEN becomes $\mathcal{O}(1)$.

Relative Difficulty of Decision Problems

- If I already have answers to MTN, how easily can I decide PYR-EVEN?
- With answers to MTN, PYR-EVEN becomes $\mathcal{O}(1)$.
- We say "PYR-EVEN is easy with respect to MTN".

Randomness

00000000000000000000

10010111011111000101

Randomness

00000000000000000000

10010111011111000101

- Randomness is patternlessness.

Randomness

00000000000000000000

10010111011111000101

- Randomness is patternlessness.
- Patternlessness $\Leftrightarrow$ no short description

Randomness

00000000000000000000

10010111011111000101

- Randomness is patternlessness.
- Patternlessness $\Leftrightarrow$ no short description
- "x is random" $\Leftrightarrow$ x admits no description shorter than itself.
- $R = \{x : x \text{ is random}\}$.

Conjecture

- $\{A : A \text{ is easy with respect to } R\}$

Conjecture

- $\{A : A \text{ is easy with respect to } R\}$
- How does having access to R help in solving a decision problem?

Conjecture

- $\{A : A \text{ is easy with respect to } R\}$
- How does having access to R help in solving a decision problem?
- Conjecture:

$$\{A : A \text{ is easy w.r.t } R\} \subseteq \{A : A \text{ is easy}\}$$

Proof Technique

- Let algorithm ALG solve decision problem A given R (the set of random strings).
- How much information is ALG getting from R?

Proof Technique

- Let algorithm ALG solve decision problem A given R (the set of random strings).
- How much information is ALG getting from R?
- Feed ALG garbage answers to its queries into R.
- If ALG still decides A properly, then it wasn't using R for very much information.

My Progress

- At beginning of summer, knew that for long-enough x there are garbage answers that work.

My Progress

- At beginning of summer, knew that for long-enough x there are garbage answers that work.
- Showed that there are *lots* of garbage answers that work.
- For arbitrary $n \in \mathbb{N}$ there is some input x such that there are n unique sets of garbage answers such that ALG still decides whether $x \in A$ or not.