Small Circuits for Languages Easily Reduced to Randomness

Sam Hopkins, Mentor: Professor Eric Allender

July 14, 2011
Computational (Decision) Problems

Definition by Example

\[ \text{MTN} = \{ x : x \text{ is a monotone sequence} \} \]
\[ \text{PYR-EVEN} = \{ x : x \text{ is a sequence of even length whose first and second halves are monotone} \} \]
Computational (Decision) Problems

Definition by Example

\[ \text{MTN} = \{ x : x \text{ is a monotone sequence} \} \]
\[ \text{PYR-EVEN} = \{ x : x \text{ is a sequence of even length whose first and second halves are monotone} \} \]

Decision problem: for some input \( x \), is \( x \in \text{MTN} \) (or \( \text{PYR-EVEN} \))?
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 $x \in \text{MTN}$ (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 $O(1)$. 
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 $O(1)$.
- We say “PYR-EVEN is easy with respect to MTN”.
Randomness

00000000000000000000
10010111011111000101
Randomness

Randomness is patternlessness.

00000000000000000000
10010111011111000101

Randomness is patternlessness.
Randomness

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

00000000000000000000
10010111011111000101
Randomness is patternlessness.
Patternlessness $\iff$ no short description
"$x$ is random" $\iff x$ admits no description shorter than itself.
$R = \{x : x$ is random$\}$. 

\[
\begin{array}{c}
00000000000000000000 \\
10010111011111000101 \\
\end{array}
\]
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?
{A : A 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.
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.