# 15-251: Great Theoretical Ideas In Computer Science

## Recitation 14

- Remember to fill out the FCEs!
- Our final is next Friday from 1:00-4:00 in Rashid (GHC 4401). Look for practice problems and review sessions to be posted soon.

## All The Stuff From September You Forgot About

(a) Apoorva is a former ECE major, so he likes circuits. He comes up with the following language: APOORVA $= \{(\langle M \rangle, n, s) |$ $M$ is a TM with tape alphabet $\{0, 1\}, n, s \in \mathbb{N}$, and there exists a circuit of size at most $s$ which accepts the same inputs of length $n$ as $M\}$. Prove that APOORVA is undecidable.

(b) Josh is a current ECE major, so he also like circuits. He decides to come up with his own language: JOSH-KORN $= \{(\langle D \rangle, n, s) |$ $D$ is a DFA with alphabet $\{0, 1\}, n, s \in \mathbb{N}$, and there exists a circuit of size at most $s$ which accepts the same inputs of length $n$ as $D\}$. Prove that JOSH-KORN is decidable.

(c) Woo has never been an ECE major, but also wants to get in on the circuit-related language fun. He comes up with a language simmilar to the other two: WOO $= \{(\langle C \rangle, n, k) |$ $C$ is a Boolean Circuit with $n$ inputs, $n, k \in \mathbb{N}$, and $C$ accepts at least $k$ inputs $\}$. Prove that WOO is countable.

(d) Newton thinks that WOO is in NP, and offers the following proof: "Let the certificate for $(\langle C \rangle, n, k)$ be a list of $k$ inputs which $C$ accepts. Our verifier is as follows: Given as input $(x, c)$,

- Check that $x$ is an encoding of a triple $(y, n, k)$. If not, reject.
- Check that $n$ and $k$ are integers with $0 < k \leq n$. If not, reject.
- Check that $y$ is the encoding of a circuit $C$ with $n$ inputs. If not, reject.
- Check that $c$ is a list of $k$ binary strings. If not, reject.
- For each $s$ in $c$, check that $s$ is of length $n$ and $C(s)$ returns true and $s$ is distinct from every previous string in $c$. If not, reject.
- Accept

Runtime is $O(k|C| + k^2 n)$, which is polynomial. We have to check $C(s)$ each of $k$ inputs, and the time to check an input is proportional to the number of gates in the circuit. We also need to check that the inputs are distinct, which involves $O(k^2)$ comparisons between $n$ bit strings. Certificate length is $O(nk)$, which is poly, since we have $k$ $n$-bit strings. If this verifier accepts $(x, c)$, $c$ is a list of $k$ distinct inputs satisfying $C$, so there are $k$ such inputs. If $x$ has $k$ satisfying assignments, we can give those as the certificate. Thus, if $x \in$ WOO, there is a certificate that makes this verifier accept, and if the verifier accepts $(x, c)$, $x \in$ WOO."

Is Newton's proof correct? Find the key flaw in the proof.

(e) Raunak isn't interested in circuits, but makes up a language anyway: RAUNAK $= \{s | s = xy$, where $x$ and $y$ are binary strings of the same length and $x$ corresponds to a larger binary value than $y\}$. Prove that RAUNAK is not regular.

(f) Ji An isn't interested in circuits either, he just wants a big language: JI-AN $= \{s | s \in \{0, 1\}^\infty$ and for every $i \in \mathbb{N}$, if $x$ is the number whose binary representation is $s_0 s_1 s_2 \ldots s_{i-1}$ (the first $i$ characters of $s$), then $s_x = 1$. $\}$. Prove that JI-AN is uncountable.

## Ramsey Theory

Carolyn's cat and Calvin's dog are playing a game with graphs. They start with an empty graph on $n$ vertices (one with no edges). On the cat's turn, she adds a red edge to the graph. On the dog's turn, he adds a blue edge to the graph (a single pair of vertices cannot be joined by both a red and a blue edge). The cat wins if she creates a red clique of size $k$ in the graph. The dog wins if he creates a blue clique of size $k$ in the graph. The game is a draw if the graph is complete (all possible edges have been added) and it has neither a red clique nor a blue clique of size $k$. Prove that if $n$ is large enough, this game cannot end in a draw (no matter how poorly the pets play). First show the following stronger claim:

For every $i, k \in \mathbb{N}$, $\exists\, n \in \mathbb{N}$ such that every graph on $n$ vertices contains either an independent set of size $i$ or a clique of size $k$.

(HINT: Prove this by induction. Consider choosing an aribitrary vertex $v$ and separating the other vertices into two sets based on whether or not they are adjacent to $v$)

## Chernoff Bounds

Chris and Anna are playing a series of high stakes poker games. The loser of each game must pay the winner \$100. Chris has been practicing Poker all semester, so he has a $\frac{2}{3}$ chance of winning each game. He reasons that he can't lose money as long as he plays enough games. Prove that the chance that Chris loses money overall decreases exponentially in the number of games $n$ that the head TAs play.

Here are some steps to help:

(a) Let $A$ be the number of games won by Anna. Using Markov's inequality, show that for every $t \in \mathbb{R}^+$, $\Pr\{A > \frac{n}{2}\} \leq \frac{\mathbf{E}[e^{tA}]}{e^{0.5tn}}$

(b) Show that $\mathbf{E}[e^{tA}] \leq e^{\frac{n}{3}(e^t - 1)}$ (You'll want to write $A$ as a sum of Bernoulli random variables, and you'll need to use the "useful inequality" from the randomized algorithms lecture)

(c) Let $t = \ln(\frac{3}{2})$ (found using the magic of calculus). Show that $\Pr\{A > \frac{n}{2}\} \leq e^{-\frac{n}{30}}$ (You may use the fact that $\ln(\frac{3}{2}) > \frac{2}{5}$)

## Stone Triangles

Annie and Corwin are playing a game on an $n$ by $n$ grid. On a player's turn, they must place a stone on the bottommost empty space in some column. They may play in the $i$th column from the left only if it has fewer than $i$ stones. They also place a stone in every empty square to the left of the first stone they placed. A player who is unable to make a move loses. Prove that if Annie goes first, she has a winning strategy for every board size.