Circuit Complexity Notes

Bob Chen

Fall 2013

1 November 27 - Constant Depth Circuits for approximate counting (aka BPP is in the Polynomial Hierarchy)

Definition 1.1. $ApxMaj_{1/3}(\vec{x})$ outputs $i \in \{0,1\}$ if more than $2/3$ of the input are equal to i, else it outputs whatever.

Note that $\frac{1}{3}, \frac{2}{3}$ can be replaced by any $\epsilon, 1-\epsilon$ or even $\frac{1}{\log n}, 1-\frac{1}{\log n}$.

Theorem 1.2. *(Sipser, Gacs, Lautemann.) There are quasipolynomial size, depth 3 unbounded fan $\bigvee, \bigwedge, x_i, \overline{x_i}$ circuits for $ApxMaj_{1/3}$. In fact, we can achieve depth $2\frac{1}{2}$.*

Definition 1.3. Quasipolynomial size means we have $n^{\log n^{O(1)}}$ or $2^{\log n^{O(1)}}$. Of course, note that $n^{\log n^c} = 2^{\log n^{c+1}}$.

Note that quasipolynomial is much closer to polynomial ($2^{O(\log n)}$) than exponential ($2^{O(n)}$ or $2^{n^{O(1)}}$).

Recall 1.4. (Chernoff Bound.) Let X_i be 0-1 random variables. Let $E(\frac{1}{m}\sum X_i) = \mu$ (for instance if $E(X_i) = \mu$ for all i). Let $c > 0$.

Then

$$P\left[\left|\frac{1}{m}\sum X_i - \mu\right| > c\mu\right] \leq 2e^{-\mu m \min\{c^2/4, c/2\}}.$$

That is, there exists $\delta = \delta(c,\mu)$ such that

$$P\left[\left|\frac{1}{m}\sum X_i - \mu\right| > c\mu\right] \leq 2^{-\delta\mu}.$$

Remark 1.5. Here's the idea of the proof. Pick m many inputs at random (with replacement).

Then if $\sum x_i < \frac{1}{3}n$, the probability that the majority of the selected inputs is 0 is at least $1 - 2^{-\delta m}$, and vice versa.

Proof. (of Theorem 1.2.) Let $c = \frac{1}{2}, \mu = \frac{2}{3}$. Set $\delta = \delta(c,\mu)$. Without loss of generality, let n be a power of 2 with $n = 2^l$. Let $\alpha = \lceil \delta^{-1} \rceil$, and let $m = \alpha \log n = \alpha l$

Consider all n^m many sequences of the inputs $x_{\vec{\imath}} = x_{i_1}, \ldots, x_{i_m}$. Compute $Maj(x_{\vec{\imath}})$ for each sequence. Call these values $y_{\vec{\imath}}$. Note that it depends on $m = \alpha \log n = \alpha l$ different variables, so it has a DNF of size at most $2^{\alpha \log n} = n^\alpha$. There are $n^m = 2^{\alpha (\log n)^2}$ many such sequences (quasipolynomially many).

If $\sum x_i < \frac{1}{3}n$, then the number of values $y_{\vec{\imath}} = 1$ is at most

$$\begin{aligned} 2^{-\delta m}(n^m) &= 2^{-\delta \alpha \log n}(n^m) \\ &= m^{-\delta\alpha} n^m \\ &\leq \frac{1}{n} n^m \\ &= 2^{-l} n^m. \end{aligned}$$

So $y_{\vec{\imath}} = 0$ for at least $(1 - 2^{-l})n^m$ many choices of $\vec{\imath}$. Same is true of the dual situation: when $\sum x_i \geq \frac{2}{3}n$, most of the $y_{\vec{\imath}}$s are 1.

Now, $n^m = 2^{\alpha l^2}$. Let $L = \alpha l^2$. There are 2^L many sequences of length m. A sequence is specified by L many bits; that is, l bits for each of its m members. We want a function f such that

$$f(\vec{y}) = \begin{cases} 1 & \text{if the number of } y_{\vec{\imath}} = 1 \text{ is at least } (1 - 2^{-l})2^L, \\ 0 & \text{if the number of } y_{\vec{\imath}} = 0 \text{ is at least } (1 - 2^{-l})2^L, \end{cases}$$

and is arbitrary otherwise. f has 2^L many inputs, and we want a constant depth circuit for f.

Identify sequences of length m with binary strings in $\omega \in \{0,1\}^L$. If $u, v \in 2^L$ define $u \oplus v$ as the bitwise XOR of u, v. We have the following facts.

(1) $(u \oplus v) \oplus u = v$.

(2) $u \in S \oplus v$ if and only if $u \oplus v \in S$.

(3) $|S \oplus v| = |S|$.

(4) If $w \in 2^L$ and u is chosen at random, then

$$P\left[w \in S \oplus u\right] = \frac{|S|}{2^L}.$$

Looking ahead: S will be the set of $\vec{\imath}$ for which $y_{\vec{\imath}} = 1$, and we'll have

$$\frac{|S|}{2^L} \geq 1 - 2^{-l} \text{ or } \leq 2^{-l}.$$

Note that if $|S| \leq 2^{-l}2^L$, then

$$P[w \in S \oplus u] \leq 2^{-l}.$$

If $|S| \geq (1 - 2^{-l})2^L$, then

$$P[w \notin S \oplus u] \leq 2^{-l}.$$

Let $k = \lceil \frac{L+1}{l} \rceil \approx \alpha l$. If $|S| \geq (1 - 2^{-l})2^L$, we claim there exists $u_1, \ldots, u_k \in 2^L$ so that

$$\bigcup (S \oplus u_i) = 2^L.$$

That is, we can cover all strings with k (XOR) translations of S. We'll prove this now.

Consider any fixed $w \in 2^L$. $P(w \notin S \oplus u_i) \leq 2^{-l}$. Thus, the probability that w is not in any of $S \oplus u_i$ is at most $(2^-l)^k \leq 2^{-(L+1)}$. So, the probability that some w is not in $\bigcup S \oplus u_i$ is at most $\frac{1}{2}$ by the union bound. Hence there exists some selection of u_is so that the union covers all strings.

Inversely, if $|S| \leq 2^{-l}2^L$, then no choice of k u_is will be able to cover the whole space, since

$$\left| \bigcup S \oplus u_i \right| \leq k|S| \leq \alpha l 2^{-l} 2^L \ll 2^L.$$

Now we're ready to write down f! It's simply

$$\bigvee_{u_1,\ldots,u_k \in 2^L} \bigwedge_{w \in 2^L} \bigvee_{i=1}^{k} w \in S \oplus u_i.$$

Since S is the set of $\vec{\imath}$ for which $y_{\vec{\imath}} = 1$, we can rewrite this as

$$\bigvee_{u_1,\ldots,u_k \in 2^L} \bigwedge_{w \in 2^L} \bigvee_{i=1}^{k} y_{w \oplus u_i}.$$

Using the distributive law, we can write $\bigvee_{i=1}^{k} y_{w \oplus u_i}$ as a big $\bigwedge$ of small $\bigvee$s (small in the sense that their fan in is $O((\log n)^2)$). This reduces the formula to depth 3; even to depth $2\frac{1}{2}$ if one counts the small fan-in gates as only half a level.

Let's check the size of this monstrosity. The outermost $\bigvee$ has how many disjuncts? The number of chocies of u_i is at most $(2^L)^k \approx 2^{(\log n)^{O(1)}}$. The next level of $\bigwedge$: there are $2^L = 2^{(\log n)^{O(1)}}$ many choices of w. The $\bigwedge$s from the distribution law are also $2^{(\log n)^{O(1)}}$. Finally, the bottom level of $\bigvee$s are $2^{O((\log n)^3)} = 2^{(\log n)^{O(1)}}$. So we're done! $\square$

Definition 1.6. Let Q be a language, i.e. a subset of 2^L. Q is in BPP if there exists a polytime computable $R(x, y)$ and a polynomial $p(m)$ so that for all $|x| = m$, $x \in Q$ implies

$$P_{z \in \{0,1\}^{p(m)}} [R(x, z) = 1] \geq \frac{2}{3},$$

and if $x \notin Q$ then

$$P_{z \in \{0,1\}^{p(m)}} [R(x, z) = 1] \leq \frac{1}{3}.$$

Remark 1.7. The above proof applied to this setting shows that $Q \in \Sigma_2^P$, the second level of the polynomial hierarchy.

Here is a sketch of the proof. Let $n = 2^{p(m)}$, so $l = p(m)$, and set $x_i = R(x, i)$ with $i \in 2^{p(m)}$. Existentially guess $u_1, \ldots, u_k \in 2^L$, universally guess $w \in 2^L$, and for $i = 1, \ldots, k$, check if $Majority\{R(x, \pi_j(w \oplus u_i)) \mid j = 1 \ldots \alpha l\} = 1$. Here π_j picks out the jth substring. If this holds for some i, accept; otherwise reject.