Notes on lower bounding formulas

October 13, 2015

1 Main Goal

Theorem 1.1. *For any formulae F with k variables and random formulas $f_1, \ldots, f_k$ depending on distinct t variables, if*

$$F(f_1|_\rho, \ldots, f_k|_\rho) = F(U_k)$$

, then $L(F(f_1, \ldots, f_k)) \geq L(F) \cdot \min_i L(f_i)$.

Note that, the Andreev function is the special case when $k = \log n$ and $f_j = \oplus_{i=1}^{n/\log n} x_{ji}$ where $j \in [k]$.

Actually, there has been a similar conjecture:

Conjecture 1.2 (KRW conjecture)**.** *Let $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^m \to \{0,1\}$ be non-constant functions. Then*

$$D(g \circ f) \simeq D(g) + D(f),$$

where $D(f)$ denotes the depth of f and $g \circ f$ represents the composition of functions, i.e. $g \circ f = g(f(\overline{x_1}), \ldots, f(\overline{x_m}))$, in which $\overline{x_i}$ is the vector of n distinct variables.

In the paper [**?**], Gavinsky, Meir, Weinstein and Avi Wigderson tried to use information-theoretic approach to prove it.

They have observed the Andreev functions is just $L(g \circ \oplus_m) = \Omega(L(g) \cdot L(\oplus_m))$. Thus, the $F(f_1, \ldots, f_n) = t^{d+1}/polylog(t)$ where $t = n \log n$

And they made a new conjecture about $\oplus_m \circ f$, However, this is a significant difference: when the parity function is at the bottom , one can easily apply random restrictions to the function, but it is not clear how to do it when the parity function is at the top.

Question 1.3. *1. How to let PRG be involved?*

2. what can be revealed for the formula from the random formula restriction?

Proof. First of all, we need th following property:

1. $F(f_1|_\rho, \ldots, f_n|_\rho) = F(x_1, \ldots, x_n)$

That is

$$p^2 L(F^*) \geq s(n)$$

If $p = \log n/n$, then we know $L(F^*) \geq n$ □

In Andreev function, we only need $\log n$ variables left but now we need n.

2 Another Way– bound the variance of shrinkage

First of all, we know the shrinkage size $L(\phi|_\rho)$ is a random variable with expected size p^2L and has a high upper concentration result. We proceed to ask what about $Var[L(\phi|_\rho)]$

3 Using average-case hardness

By [**?**], we know

Theorem 3.1. *There is an explicit Boolean function $h : \{0,1\}^n \to \{0,1\}$ and a constant $c \geq 8$ and a constant $c \geq 8$ such that for any parameter r such that $c\log(n) \leq r \leq n^{1/3}$, any formula of size $\frac{n^3-o(1)}{r^2}$ computes h correctly on a fraction of at most $1/2 + 2^{-\Omega(r)}$ of the inputs.*

Furthermore, by the [**?**],

Theorem 3.2. *Let $s \geq \log m$ be any parameter. Let F be a Boolean function computed by a circuit of depth d and size m. Let μ be an r-independent distribution where*

$$r \geq r(s,d) = 3 \cdot 60d + 3 \cdot (\log m)$$

then

$$|Pr_{x\sim U_{poly\log n}}[f(x=1)] - Pr_{x\sim U_n}[f(x)=1]| = |E_\mu[F] - E[F]| < \epsilon(s,d),$$

where $\epsilon(s,d) = 0.82s \cdot (10m)$.

Theorem 3.3. *$r(m,d,\epsilon)$-independence ϵ-fools depth-d AC0 circuits of size m, where*

$$r(m,d,) = \log(\frac{m}{\epsilon}))^{O(d^2)}$$

.

Now, we consider the following composition $f \circ G$ on polylog many bits, where G is puesudorandom generator to generate polylog-wise independent distribution from $poly\log n$ inputs. That is,

$$\left|Pr_{x\sim U_{poly\log n}}[f(x)=1] - Pr_{y\in\{0,1\}^{poly\log n}}[f(G(y))=1]\right| \leq \delta$$

Note that instead of fooling the formula on uniform random distribution, what we want to fool here is the formula over $poly\log n$-wise independent distribution. This should give a exponentially error bound, rather than the polynomially small compared with the uniform distribution case.

Concluding with the above two theorems, we get

$$|Pr_{x\sim U_n}[f(x)=1] - Pr_{y\in\{0,1\}^{poly\log n}}[f(G(y))=1]| \leq \delta + \epsilon.$$

where ϵ, δ could be both exponentially small. Then we hope to prove the following theorem, and we could get a much better lower bound than $\Omega(n^3)$.

Theorem 3.4 (Main theorem to prove)**.** *If there are two functions* $f : \{0,1\}^n \to \{0,1\}$ *and* $g : \{0,1\}^{poly \log n} \to \{0,1\}$ *such that*

$$|E[f(x)] - E[g(x)]| \leq 2^{-\Omega(r)},$$

and we know for any s*-sized formula* Φ*,*

$$Pr_x[f(x) = \Phi(x)] \leq 1/2 + 2^{\Omega(r)};$$

then we know

$$Pr_x[g(x) = \Phi(x)] \leq 1 - 2^{\Omega(r)},$$

which means $L(g) \geq s$*.*

Proof. Assume by contradiction, there is a s-sized formula Φ computing g. Then based on Φ, we can construct a formula Ψ in the same size computing f.

That is, first of all, divided the input into two parts: $S_1 = \{x|\Phi(x) = f(x)\}$ and $S_2 = \{x|\Phi(x) \neq f(x)\}$. If there exists a large subset $S^* \subset S_2$ which can be efficiently computed by formula such that $|S_1| + |S^*| > 2^n(1/2 + 2^{-Omega(r)})$, then it is contradicting with the average-case hardness of f.

First of all, we bound the size of $|S_1|$ by using the first equation.

Second, we show how to compute the majority of given set efficiently. □