# Notes on lower bounding formulas

October 14, 2015

## 1 Main Goal

**Theorem 1.1.** *For any formula $f$ on $k$ bits and PRG $G$ whose input is $T$ bits and output is $k$ bits, if $f(G(x|_\rho)) = f(U_k)$, then we have $L(f(G)) \geq (T/k)^2 L(f)$.*

However, if $L(f) = k^d$, then we can only get $L(f(G)) \geq T^2 k^{d-2} = O(T^d)$. That is, this method cannot improve our conclusion. But it sheds light on how to composite functions to increase the formula complexity. Furthermore, the Andreev function is the special case when $k = \log n$ and $T = n$ where $L(f) = \log n$.

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.*

Our first theorem shows that,

**Theorem 1.3.** *For any formula $F$ with $k$ variables and formula $G$ with $T$ variables, if $F \circ G(x|_\rho) = F(U_k)$ and $L(G) \leq T^2$, then the KRW conjecture is true.*

**Question 1.4.**

1. *How about $L(G) \geq T^2$? Can we develop new technique to prove it, instead of using the Hastad's shrinkage argument?*
2. *Maybe the PRG can have more property, rather than only fixing the bit-fixing source.*
3. *Also, $F$ could have more properties, e.g. $F \in AC^0$. Then, this could significantly decrease the of size input(seed) by using a poly$\log n$ independence. This part is covered in Section 3*
4. *What can be revealed for the formula from the random formula restriction?*

### 1.1 Related work

In the paper [2], 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.

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 $p^2 L$ and has a high upper concentration result. We proceed to ask what about $Var[L(\phi|_\rho)]$

## 3 Assuming $F$ is AC0 and has average-case hardness

By [3], 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 [1],

**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 $\mu$ 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 $\epsilon$-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 $\epsilon, \delta$ could be both exponentially small. Then we hope to prove the following theorem, and we could get a much better lower bound than $\Omega(n^3)$.

Then, by the paper [4], we want to show the indistinguishability can imply a good approximation for each $f$.

**Theorem 3.4** (Main theorem to prove)**.** *If there are two functions $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$ such that $f$ approximates $g$ within $1/2 + \epsilon$, and for any $s$-sized formula $\Phi$,*

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

*then we know*

$$L(f) \leq L(g) + poly(\log 1/\epsilon)$$

*Proof.* Assume by contradiction, there is a $s$-sized formula $\Phi$ computing $g$. Then based on $\Phi$, we can construct a formula $\Psi$ 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.

By the above those things, we can get our desired conclusion. □

# References


[1] Mark Braverman. Polylogarithmic independence fools ac 0 circuits. *Journal of the ACM (JACM)*, 57(5):28, 2010.

[2] Dmitry Gavinsky, Or Meir, Omri Weinstein, and Avi Wigderson. Toward better formula lower bounds: An information complexity approach to the krw composition conjecture. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 213–222. ACM, 2014.

[3] Ilan Komargodski, Ran Raz, and Avishay Tal. Improved average-case lower bounds for demorgan formula size. In *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, pages 588–597. IEEE, 2013.

[4] Luca Trevisan, Madhur Tulsiani, and Salil Vadhan. Regularity, boosting, and efficiently simulating every high-entropy distribution. In *Computational Complexity, 2009. CCC'09. 24th Annual IEEE Conference on*, pages 126–136. IEEE, 2009.