Logic and Computation Seminar

Bob Chen

Fall 2011

1 11/30/11

Recall 1.1. Let \( m > k, l > 10m^2/k \), and \( n \leq 2^{\frac{k}{r}} \). We will be working over a \((k, m, l, n)\)-design.

Lemma 1.2. Let \( d \) be a \((k, m, l, n)\)-design with hyperedges \( I_j \). Let \( f \) be as above, and let \( S(n) \geq n^{12} \). Then \( G : \{0, 1\}^l \rightarrow \{0, 1\}^n \) defined by

\[
G(z) = (f_1(z), \ldots, f_n(z))
\]

where \( f_j(z) = f(z \cap I_j) \) is \((S(n)/10, \frac{1}{10})\)-pseudorandom.

Proof. By a previous lemma, it suffices to show that there does NOT exist a circuit \( C \) of size less than \( \frac{2}{r} \) such that

\[
P[C(f_1(z), \ldots, f_i(z)) = f_{i+1}(z)] > \frac{1}{2} + \frac{1}{10n} = \frac{1}{2} + \frac{1}{10 \cdot 2^{\frac{r}{m}}}.
\]

Suppose to the contrary that this DOES happen. We will show that this contradicts the hardness of \( f \).

Split \( z \) into 2 parts: \( \tilde{z}_1 = z \cap I_{i+1} \) and \( \tilde{z}_2 \) is everything else. Note that \( \tilde{v}_1 \) has \( m \) bits and \( \tilde{v}_2 \) has \( l - m \) bits. Then \( f_1(z) = f_1(\tilde{z}_1, \tilde{z}_2) = f(\tilde{z}_1 \cap I_1, \tilde{z}_2 \cap I_1) \). Of course, \( |\tilde{v}_1 \cap I_1| \leq k \). Now, let’s pick and fix \( \tilde{z}_2 \) to maximize our probability of guessing correctly. But \( f_1(z) \) is now a function of at most \( k \) bits, so we can just hardwire in a table lookup of \( f(z) \) using CNF representation. This has size \( 2^{k}k^{-1}(1 + o(1)) \) by Shannon-Lupanov.

Call this new circuit \( C^* \) (it’s \( C \) except with the \( f_i \)’s hardwired in by the lookup tables). Then the size of \( C^* \) is

\[
|C^*| = |C| + n2k2^k \leq 2^m 2^k = 2^{11k} < 2^{12k} = n^{12},
\]

which is a contradiction. \( \square \)

Theorem 1.3. (NW.) Suppose \( f \in E \) is exponential and has average case hardness \( H_{avg} \geq S(m) < 2^{n} \). Define \( S'(l) \) by \( S'(l) = S(m)^{\delta} \) where \( m \) is the least value such that

\[
\frac{m^2}{\log(S(m))} \geq \delta^2 l
\]

(\( \text{here we’re taking } \delta = 100^{-1} \)). Then there exists \( S'(l) \)-pseudorandom generator (an exponential time function which takes \( l \) bits and spits out a \( S'(l) \) bit string on which no circuit of size \( S'(l)^3 \) size can be right more than \( \frac{r}{100} \) of the time).

Proof. We’re taking

\[
m = \sqrt{\log(S(m))}/100.
\]

Note that \( S(m) = 2^{O(m)} \) and in fact \( 2^{en} \), since \( m < l \). Let \( m > k, l > \frac{10m^2}{k} \), and set \( n = 2^{\frac{k}{r}} \). By a lemma, there exists a \((k, m, l, n)\)-design. Then consider

\[
G : z \mapsto f_1(z), \ldots, f_n(z)
\]

\( G \) is exponential time.

It takes \( 2^{O(l)} \) time to construct \( d \) and \( n2^{O(n)} = 2^{O(l)} \) to evaluate the \( f_i \)’s, so everything takes \( 2^{O(l)} \).

Second, note that \( S(n) > (S'(l))^{\frac{m}{10}} \) (because \( l < n \)). This proves the theorem. \( \square \)
Remark 1.4. NW showed that if there exists $f \in E$ with $H_{avg} \geq 2^{en}$, then PromiseBPP = P.

Theorem 1.5. If $g \in E$ has worst case hardness at least $2^{en}$ then there exists an $n$ with average case hardness at least $2^{en}$.

Corollary 1.6. If $f \in E$ exists with $H_{wrs}(f) > 2^{en}$ then PromiseBPP = P.

Remark 1.7. The Shannon-Lyapunov correspondence between runtime and circuit size breaks down above $2^n$ (say, at $2^{n^2}$) time.