Summary paragraph

1 Lower Bound For Perfect Extraction

Last time we stated that for a perfect \( (\ell, n, k) \) Resilient Function, \( \{0,1\}^n \rightarrow \{0,1\}^k \), the lower bound for \( \ell \) is \( \ell \geq \frac{n}{2} + \left(1 - \frac{n}{2(2^k-1)}\right) \). We now give a general proof of the lower bound.

**Theorem 1** All AONTs from \( k \rightarrow n \) bits which is \( \ell \)-secure must satisfy the lower bound.

Consider \( k = 1, n = 3 \).

Drawing of cube colored with parity here
\( f(b) = \text{random } y_1, y_2, y_3 \text{ s.t. } y_1 \oplus y_2 \oplus y_3 = \ell \).

Let \( c = 2^k \) be the number of colors. Then AONT is equivalent to weighted coloring of \( \{0,1\}^n \) into \( c \) colors. Define \( \chi_i(z) = \text{prob}(T(i) = z) \). If \( \chi_i(z) > 0 \) then \( \chi_i(z) = 0, \forall z \neq i \).
\( \forall i, \sum z \chi_i(z) = 1 \). \( \ell \)-AONT means \( \forall i, j \), for any \( \ell \)-dimensional subcube we have \( \sum_H \chi_i = \sum_H \chi_j \).

A-adjacency matrix of hypercube \( \{0,1\}^n \) is \( 2^n \times 2^n \) symmetric, so it has \( 2^n \) eigenvectors \( v_z \), with \( Av_z = \lambda_z v_z \) where \( \lambda_z \) is the eigenvalue. For a hypercube, \( \{v_z|z \in \{0,1\}^n\} \) is known. \( v_z(x) = \frac{1}{\sqrt{2^n}}(-1)^{x \cdot z} \). This means that \( v_z \) are all orthonormal, \( ||v_z|| = 1, <v_z, v_y> = 0, \forall z \neq y \).

**Key Claim:** If the weight of \( z \) is \( \leq n - \ell \) then \( <v_z, \chi_i - \chi_j> = 0 \).

We can decompose this inner product into collections of smaller hypercubes. As a trivial example, suppose weight of \( z \) is \( 0^n \). Then \( v_z = \frac{1}{\sqrt{2^n}} 1^n \). Now \( <v_z, \chi_i - \chi_j> = \sum x_i - \sum x_j = \sum (1 - 1) = 0 \). Generally, break down into lower hypercubes and \( x_i \)'s and \( x_j \)'s cancel out.

Given \( z = \alpha H_\alpha \), where \( \alpha = 1^p \), \( H_\alpha = 0^{n-p} \), \( p \leq n-\ell \), \( \forall x \in H_\alpha \), \( x \cdot z = c \), \( c \) constant.

**Claim:** For any \( i, j \), \( (\chi_i - \chi_j)^\perp A(\chi_i - \chi_j) \leq (2\ell - n - 2)||\chi_i - \chi_j|| \).

**Courant-Fischer theorem** If \( \lambda_1 \geq \lambda_2 \geq \ldots \lambda_{2^n} \) are eigenvalues with \( v_i \) corresponding to \( \lambda_i \), if \( u \) is orthogonal to \( v_1, \ldots, v_i \), then \( u^\perp Au \leq \lambda_{i+1}||u||^2 \).

This corollary follows from previous lemma.
\[ \Delta = \sum_{i,j} (\chi_i - \chi_j)^\perp A(\chi_i - \chi_j) \leq (2\ell - n - 2)\sum_{i,j} ||\chi_i - \chi_j||^2 = 2(2\ell - n - 2)(c - 1)\sum_{i} ||\chi_i||^2, \]
\[ \text{LHS} = \sum_{i,j} (\chi_i^\perp A\chi_i + \chi_j^\perp A\chi_j - 2\chi_i^\perp A\chi_j) = 2c \sum_i \chi_i^\perp A\chi_i - 2(\sum_i \chi_i^\perp A(\sum_j \chi_j) \geq 2n||\sum \chi_i||^2 \forall u, u^\perp Au \leq n||u||^2, \]
\[ 2(2\ell - n - 2)(c - 1) \geq -2n \Rightarrow \ell \geq \frac{n}{2} + \left(1 - \frac{n}{2(2^k-1)}\right) \text{. Q.E.D.} \]

Now we examine whether we can relax the perfect security in order to beat this bound.

Consider a Von Neumann coin. Suppose I flip the coin 75 times, with heads as 0, tails as 1, and suppose we just xor the results. It's not perfect, but maybe it's almost as good.
The probability of heads is \( \sum_{i=0}^{n/2} \binom{n}{2i} p^{2i}(1-p)^{n-2i} = \frac{1}{2} - \frac{1}{2} (1-2p)^n \).

To get error \( \epsilon \), we need \( (1-2p)^n \leq \epsilon \), so \( n \log(1-2p) = \log \epsilon \), so \( n = \log(1/\epsilon)/(2p) \).

**Definition:** Given distributions \( x, y \), define the statistical distance \( SD(x, y) = \frac{1}{2} \sum_z \Pr(x = z) - \Pr(y = z) \).

So there are two regions: one where \( x < y \), the other where \( y < x \).

\[ SD(x, y) = \max_S(\Pr(x \in S) - \Pr(y \in S)) = \max_S(\Pr(y \in S) - \Pr(x \in S)) \]

**Lemma:** \( \forall \) algorithms \( A \), if \( SD(x, y) < \epsilon \), then \( SD(A(x), A(y)) \leq \epsilon \).

## 2 Bit-Fixing Sources

\( (n - \ell) \) bits of \( X \) are fixed and \( \ell \) bits are random. We want to construct \( f(X) \) “close” to \( U_k \).

- (a) \( f(X) \equiv U_k \) (if \( k > \log_2 n \Rightarrow \ell \geq n/2 \)).
- (b) \( \epsilon \)-resilient functions, such that \( SD(f(X), U_k) \leq \epsilon \).
- (c) \( \epsilon \)-APRF (almost perfect resilient function): \( \forall y \in \{0,1\}^k \), \( \forall \) bit-fixing \( X \), \( (1 - \epsilon)^{\frac{1}{2\ell}} \leq \Pr(f(x) = y) \leq (1 + \epsilon)^{\frac{1}{2\ell}} \). \( SD(f(X), U_k) \leq \frac{1}{2} \sum_y \Pr(f(X) = y) - \frac{1}{2\ell} \leq \frac{1}{2} \sum_y \frac{1}{2\ell} \leq \frac{1}{2} \).

**Idea:** Pick random function \( f : \{0,1\}^n \rightarrow \{0,1\}^k \). We show that \( \Pr(f \epsilon - APRF) \approx 1 \).

\[ \Pr_x(f(x) = y) \notin (1 \pm \epsilon)^{\frac{1}{2\ell}}. \]

We could compute this using Chernoff bounds. **Idea:** throw \( 2^\ell \) balls into \( 2^n \) bins. What is the probability that we are close to the expectation? Chernoff.

\[ \Pr(bin y \ is \ bad) \leq 2^{-c(\epsilon^2)2^{4\ell-k}} \]

Sum over all \( y \), and we get that the probability is less than 1.

\[ \Pr(\exists \ source \ X \ s.t. \ f \ is \ bad) \leq (\binom{n}{\ell})^{2^{n-\ell}} 2^{-O(\epsilon^22^\ell-k)} \leq 2^{2n-O(\epsilon^22^\ell-k)}. \]

This is significantly less than 1 if \( k \leq \ell - 2 \log(1/\epsilon) - O(\log n) \). Then \( \epsilon \)-APRF’s exist, and a random function will be one with high probability.

**Application (and open problem):** Define \( T_f(y) = \text{random} \ x \in f^{-1}(y) \).

**Lemma:** If \( f \) is \( \epsilon \)-APRF then \( T_f \) is \( \epsilon \)-AONT, i.e. \( \forall y_0, y_1, \forall L \in \binom{n}{\ell}, \alpha \in \{0,1\}^{n-\ell}, SD(T_{y_0}, T_{y_1}) \leq \epsilon \).

For proof, refer to paper. There is a factor of 2 lost.

First result: partial derandomization. Don’t have to choose entire \( f \) at random. Can choose \( F = \{ f : \{0,1\}^n \rightarrow \{0,1\}^k \} \) is \( t \)-wise independent if \( \forall x_1, \ldots, x_t \) distinct, \( < f(x_1), \ldots, f(x_t) > \equiv \{ U_k, \ldots, U_k > \).

If \( k \leq n \), can construct such \( F \) with “complexity” \( tn \), efficiency of \( f \) polynomial in \( nt \).

Random \( \frac{n}{\log n} \)-wise independent \( f : \{0,1\}^n \rightarrow \{0,1\}^k \) is \( \epsilon \)-APRF with probability \( \geq 1 - 2^{-n} \) provided \( k \) is as above.

It is open how to totally derandomize this but there is some partial progress. Idea: do random walks on expander graphs.

Consider an expander graph on \( 2^k \) vertices, degree \( d \) and a property that a random walk of length \( \ell \) is \( \epsilon \)-close to \( U_k \).
$G$ has eigenvalues $\lambda_1 \geq \lambda_2 \ldots \lambda_k$ with $\lambda_1 = d$. The key thing is how large the second eigenvalue is: $\lambda_1 = d$, what is $\frac{\lambda_2}{\lambda_1}$. If it is less than $1$, then given $\pi_1, \ldots, \pi_i = U_k + \Omega_i$, then $||A\rho_i||_2 \leq \frac{\lambda_2}{\lambda_1}||\rho||_2$.

Campbell-Zuckerman achieve this. Optimal $\frac{\lambda_2}{\lambda_1} \approx \frac{\sqrt{2}}{\sqrt{d}}$. So $\ell \geq n^{\frac{1}{2}+\gamma}$. 