| | |
|---|---|
| CS 830: Randomness and Complexity | 01/20/05 |
| Lecture 0: Reductions from weak one-way functions to strong one-way functions | |
| instructor: Jin-Yi Cai | Scribe: Anand Kumar Sinha, Vinay Choudhary |

# 1 Introduction

We begin with a proof of the lemma 5.4 of the last lecture which relates forward and reverse expansion in a bipartite graph. This is then used to construct a strong one-way function (permutation) from a weak one-way function (permutation) using some public randomness.

# 2 Forward and Reverse Expansion

Recall the definition of $(\epsilon, \delta)$-forward expanding and $(\epsilon, \delta, \gamma)$-reverse expanding bipartite graphs from the previous lecture. We stated the following lemma earlier:

Lemma 2.1. *For all $\epsilon, \delta > 0$, if the bipartite graph $(L, R, E)$ is $(\epsilon, \delta)$-forward expanding, then for all $\gamma > 0$, it is also $(\epsilon, \delta, \gamma)$-reverse expanding.*

*Proof.* We prove by contradiction. So, assume that $(L, R, E)$ is $(\epsilon, \delta)$-forward expanding, but for some $\gamma > 0$, it is not $(\epsilon, \delta, \gamma)$-reverse expanding. So, there exists $T \subseteq R$, such that $\mu(T) \geq \delta + \gamma$ and $\mu(S) < 1 - \epsilon$; where $S = \{x \in L | Pr_{y(x)}[y(x) \in T] \geq \frac{\gamma}{D_r}$.

Since $\mu(\overline{S}) \geq \epsilon$ ($\overline{S}$ is the complement of $S$ on the left, i.e. $L$ $S$), by forward expansion, we have

$$\mu(\Gamma(\overline{S})) \geq 1 - \delta$$

Hence,

$$\mu(T \cap \Gamma(\overline{S})) \geq \gamma \tag{1}$$

On the other hand, due to reverse expansion, the probability that a random neighbor of a vertex in $\overline{S}$ falls in $T$ is at most $\frac{\gamma}{D_r}$. Hence, the number of neighbors of $\overline{S}$ in $T$ can be at most

$$|\overline{S}| D_l \frac{\gamma}{D_r} \leq \frac{|L| D_l}{D_r} \gamma = |R| \gamma \tag{2}$$

This contradicts (1). ☐

# 3 Reduction from weak one-way to strong one-way function

In this section, we show how to construct a strong one-way function (call it $g(\cdot)$) from a $w(n)$-weak one-way function (call it $f(\cdot)$). Recall the definition of $g$ from the last lecture:

$$\begin{aligned} g : \{0,1\}^{n \times N} &\rightarrow \{0,1\}^{l(n) \times N} \\ (x_1, \ldots, x_N) &\mapsto (f(x_1), \ldots, f(x_N)) \end{aligned}$$

THEOREM 3.1. *If $f : \{0,1\}^n \to \{0,1\}^{l(n)}$ is a $w(n)$-weak one-way function and $N = \frac{2n}{w(n)}$, then $g$ defined above is strong one-way function.*

*Proof.* Suppose $A$ inverts $g$ with success probability $\delta(n)$ in time $T(n)$. Consider the algorithm $S^A$ below:

1. **Input**: $z \in \{0,1\}^{l(n)}$
2. **Output**: $x \in \{0,1\}^n$ s.t. $f(x) = z$
3. **Repeat** $\frac{2nN}{\delta(n)}$ times
4. Pick $i \in_u \{1, \ldots, N\}$
5. Pick independently $y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_N \in_u \{0,1\}^n$
6. Set $\alpha = \langle f(y_1), \ldots, f(y_{i-1}), f(z), f(y_{i+1}), \ldots, f(y_N)\rangle$
7. Run $A(\alpha)$ and let the $i^{th}$ component be $x'$.
8. **If** $f(x') = z$, **then output** $x'$

Now we have to prove that $S^A$ inverts $f$ with probability more than what is "allowed". We first construct a bipartite graph as follows.

- $L = \{0,1\}^n$ - the set of inputs to $f$.
- $R = \{0,1\}^{N \cdot n}$ - the set of inputs to $g$.
- $x \in L$ has an edge to $z = \langle y_1, \ldots, y_N\rangle \in R$ if $x = y_i$ for some $i$.

CLAIM 3.1.1. *For all $\epsilon > 0$, the graph $(L, R, E)$ defined above has $(\epsilon, (1-\epsilon)^N)$-forward expansion.*

*Proof.* Consider any set $S \subseteq L$ with $\mu(S) = \epsilon$. A randomly chosen element $z = \langle y_1, \ldots, y_N\rangle \in R$ is not a neighbor of any $x \in S$ iff none of the $y_i$'s lie in $S$. Clearly, this happens with probability $(1-\epsilon)^N$. This proves the claim. $\square$

Choosing $\epsilon = \frac{w(n)}{2}$, we see that the graph has $(\frac{w(n)}{2}, e^{-n})$-forward expansion. (Note that $\left(1 - \frac{w(n)}{2}\right)^N \leq e^{-n}$).

WLOG, we can assume that $\delta(n) \geq 2e^{-n}$ - it is the success probability. So, the graph has $\left(\frac{w(n)}{2}, \frac{\delta(n)}{2}\right)$-forward expansion and hence, $\left(\frac{w(n)}{2}, \frac{\delta(n)}{2}, \frac{\delta(n)}{2}\right)$-reverse expansion.

So, our parameters are $\epsilon = \frac{w(n)}{2}$, $\delta = \gamma = \frac{\delta(n)}{2}$. Let $T \subseteq R$ be the set on which $A$ succeeds on $g$. Since success probability is $\delta(n)$, $\mu(T) \geq \delta + \gamma$. So $\mu(S) \geq 1 - \epsilon = 1 - \frac{w(n)}{2}$ where $S = \{x \in L | Pr_{y(x)}[y(x) \in T] \geq \frac{\delta(n)}{2n}$.

If $x \in S$, then $S^A$ succeeds with high probability because $A$ succeeds on $g$ with high probability. In this case, $S^A$ fails to invert with probability at most $\left(1 - \frac{\delta(n)}{2N}\right)^{\frac{2nN}{\delta(n)}} < e^{-n}$.

Hence, total failure probability of $S^A$ is at most $\frac{w(n)}{2} + e^{-n} < w(n)$. This is impossible because $f$ is $w(n)$-weak one-way function. $\square$

Before moving on, we note two important properties used in the proof. These will be serve as guidelines for more involved proofs.

1. From any $f(x)$, produce $g$(a random neighbor of $x$).
2. From an inversion of $g(y(x))$, we can obtain inversion of $f(x)$.

# 4 One Way Permuations

We saw that if we have weak one-way functions then we can amplify the hardness to get strong one-way functions. The same is true for one-way permuations. In this section we will show that if there are weak one-way permuations then there are strong one-way permutations as well. The notion of weak and strong one-way permuations are analogous to the notion of weak and strong one way functions.

More formally let $f : \{0,1\}^n \rightarrow \{0,1\}^n$ be a $w(n)$ weak one-way permutation. Let $N = \frac{n}{w(n)}$, and let $\pi \in \{0,1\}^{(N-1)\times n}$ and define the one-way permutaion g as follows:

$$g(x, \pi) = \langle f(y_N), \pi \rangle$$

where $y_1 = x$ and, for all $i \in \{2, \ldots, N-1\}$, and $y_i = \pi_{i-1} \oplus f(y_{i-1})$. Note that each $\pi_i$ is $i^{th}$ block of length $n$ in $\pi$.

We will prove that $g$ is a strong one-way permutation.

THEOREM 4.1. *If $f$ is a $w(n)$ weak one-way permutaiton the permuation $g$ defined above is a strong one-way permuation.*

*Proof.* Suppose there is an algorithm, $\overline{A}$, which inverts $g$ with a non trivial success probability $\delta(n) \geq 2e^{\frac{-n}{2}}$ in time $T(n)$. Consider the procedure $A$, with oracle access to $\overline{(}A)$, below:

1. **Input**: $z \in \{0,1\}^n$.
2. **Output**: $x \in \{0,1\}^n$ s.t. $f(x) = z$.
3. **Repeat** $\frac{nN}{\delta(n)}$ times.
4. Randomly pick $i \in_u \{2, \ldots, N\}$.
5. Randomly pick $\pi \in_u \{0,1\}^{n\times(N-1)}$.
6. Set $y_i = \pi_{i-1} \oplus f(x)$.
7. Compute $y_{i+1} = f(y_i) \oplus \pi_i, \ldots, y_N = f(y_{N-1}) \oplus \pi_{N-1}$.
8. Run $\overline{A}(f(y_N), \pi)$ to get $v$, the inverse of $\langle f(y_N), \pi \rangle$.
9. Compute $v2 = f(x) \oplus \pi_1 \ldots v_{i-1} = f(v_{i-2}) \oplus \pi_{i-2}$.
10. If $f(v_{i-1}) = z$, Output $v_{i-1}$.

It remains to show that the procedure described above indeed inverts f with a sufficently high probability. The procedire described above is similar to the previous one. In principle the proof remains the same.

For this we will reconsider a similiar bipartite graph and show that it has forward expansion property. The we will show that the procedure $A$ indeed has the nice property of inducing a uniform distribution on the inverses of the ouputs of $g$ computed by it. The rest will remain same as the previous proof.

Define $G = (L, R, E)$ as follows. $L$ is the set of all inputs to $f$, namely $\{0,1\}^n$, and $R$ is the set of all inputs to $g$, namely $\{0,1\}^{n\times N}$. An $x \in L$ and a $\langle y, \pi\rangle \in R$ share an edge if there is an $i \in \{1, \ldots, N\}$ such that $y_i = x$. Here $y_i$ is the set of intermediate values we get during the computation of $g(y, \pi)$. It is easy to see that right degree of the graph is $N$. Since f is a permutation and therefore one-one, it follows that the left degree of the grah is $N2^{n\times(N-1)}$. Now we will show that the graph G is $(\frac{(w(n)}{2}, \frac{\delta(n)}{2})$ forward expanding. Consider a uniform distribution of inputs, $\langle y, \pi\rangle$ to $g$. Now consider the process of randomly and uniformly picking one of the left neighbours of $\langle y, \pi\rangle$. First note that the distribution induced by this process of first randomly and uniformly picking an input to $g$ and then randomly and uniformly picking one of its left neighbour induces a uniform distribution on inputs to $f$. To see this note that each input to $f$ occurs as a left neighbour to same number of inputs to $G$. In general, this is true for all regular bipartite graphs. Now let $F$ be a set of vertices on the left with a measure $\epsilon = \frac{w(n)}{2}$. If we randomly choose a vertex from the right than it does not have any of its neighbours in $F$ with a probabilty $(1-\epsilon)^N \leq e^{-\frac{n}{2}} \leq \frac{\delta(n)}{2}$. The forward expansion property is immediate.

Now we need to show that the procedure $A$ described above produces an ouput $\langle y_N, \pi\rangle$ of $g$ whose inverse is uniformly distributed in $adj(x)$. To see this note that for different values of $\pi$ we never get the same output. Therefore for two different values of $\pi$ the inverse of the ouput of $g$ obtained by the procedure $A$ will never be the same. Since we choose $\pi$ uniformly at random, it reamains to show that for a particular $\pi$ the random inverse of the output generated by the procedure $A$ is uniformly distributed. Here it is important to note that the only source of randomness that reamins is the random choice of $i$ such that $y_i = \pi_{i-1} \oplus f(x)$. Once we fix $\pi$ the set of all possible outputs of $g$ that can be generated by the procedure $A$ is just the multiset $S = \{\langle f(y_2), \pi\rangle, \ldots, \langle f(y_N), \pi\rangle\}$, where each $y_i$ are the intermediate values obtained during the computation of $g(x, \pi)$. Furthermore, note that there is one to one corespondence in between the choice of $i$ and the above set. For instance if $i$ is $N$ then the output is $\langle f(y_2), \pi\rangle$ and it is $\langle f(y_N), \pi\rangle$ if $i$ happens to be $N$. Therefore, the corresponding inverses will also have one to one coorsepondence with the choice of $i$. Hence the distribution is uniform in $adj(x) \cap g^{-1}(S)$. It shall be noted that S is a multiset as two different choices of $i$ may lead to the same output. However, in this case we will have two dfferent edges from $x$ coming on to the corresponding inverse. Hence the distribution remains uniform inspite of the fact that a particular vertex on the right can be the inverse of the output for more than one values of $i$. Rest of the proof is same as the previous proof. In essence it is a trivial consequence of the reverse exapnsion proerty with $\gamma(n) = \frac{\delta(n)}{2}$. □

# 5 Conclusion

In this lecture we saw a generic procedure of amplifying hardness of one-way functions and permutations. In the next lecture we will accomplish the same task with a fewer number of random bits.