1 Pseudorandom Generator

Recall that the definition of a pseudorandom generator from prior lectures:

**Definition 1** A PRG with output $l$ is a deterministic polynomial time algorithm $G$ such that:

1. $|G(1^k, s)| = l(|s|)$
2. $G(1^k, U_k)$ is pseudorandom, i.e. $\{G(1^k, U_k)\} = \{U_l(1^k)\}$.

We then saw how to construct a pseudorandom generator from a one-way permutation to get a PRG with a one-bit expansion. Now, we will first look at the pseudorandomness of several invocations of a PRG on independent seeds, and will then see how to construct a PRG with polynomial expansion.

2 PRGs on Independent Seeds

To begin this construction, we first prove a lemma on the pseudorandomness of the concatenation of invocations of a PRG $G$ on independent seeds:

**Lemma 2** If $G : \{0, 1\}^n \to \{0, 1\}^m$ is a PRG, then so is

$$\tilde{G}(\vec{s}) = (G(s_1), \ldots, G(s_p)) \forall \text{poly } p$$

**Proof:**

For contradiction, assume $\exists$ ppt. $D$ such that

$$\delta(k) = \left| Pr \left[ D(\tilde{G}(U_{np})) = 1 \right] - Pr \left[ D(U_{mp}) = 1 \right] \right|$$

is negligible in $k$. Then, for each $i$, define

$$H_k^{(i)} = \left( G(U_n^{(i)}, \ldots, G(U_n^{(i)}, U_m^{(i+1)}, \ldots, U_m^{(p)}) \right)$$

Note that $H_k^{(0)} = U_{mp}$, and $H_k^{(p)} = G(U_{np})$. Then, by the hybrid argument, we know that there exists $i$ such that:
\[ \left| Pr \left[ D(H_{k}^{(i)}) = 1 \right] - Pr \left[ D(H_{k}^{(i+1)}) = 1 \right] \right| \geq \frac{\delta(k)}{p(k)} \]

Now we construct $D'$ to distinguish between $G(U_n)$ and $U_m$.

**Algorithm 1** Distinguisher for $G(U_n)$ and $U_m$.

1: Machine $D'(y)$
2: $y_1, \ldots, y_i \xrightarrow{\$} G(U_n)$
3: $y_{i+2}, \ldots, y_{p(k)} \xrightarrow{\$} U_m$
4: $\vec{y} = (y_1, \ldots, y_i, y, y_{i+2}, \ldots, y_{p(k)})$
5: Output $D(\vec{y})$

If $y \sim G(U_n)$, we have $\vec{y} \sim H_{k}^{(i+1)}$. Else if $y \sim U_m$, we have $\vec{y} \sim H_{k}^{(i)}$.

Therefore, $D'$ distinguishes with probability $\frac{\delta(k)}{p(k)}$, which is non-negligible in $k$. □

Now, we can proceed to construct a PRG with an larger expansion factor.

### 3 Increasing the Expansion Factor

Now, we look at constructing a PRG that has a polynomial expansion factor.

**Theorem 3** Let $G$ be a PRG with $l(k) = k + 1$, i.e. one bit expansion. Then, $\forall p \exists$ PRG $\vec{G}$ with $l(k) = p(k)$.

**Proof:**

![Figure 1: Construction of $\vec{G}$](image)
In Figure 1, we see the construction of $\mathcal{G}$. Formally, we have

$$\mathcal{G}(s) = G^{(p)}(s)$$

where $G^{(i)}(s) = b|G^{(i-1)}(x)$ and $G(s) = x||b$.

Now assume for contradiction that $\mathcal{G}$ is not a PRG. Therefore, $\exists$ ppt. $D$ such that

$$\delta(k) = |Pr \left[ D(\mathcal{G}(U_k)) = 1 \right] - Pr \left[ D(U_p) = 1 \right]|$$

is non-negligible in $k$.

Then, for each $i$, we define

$$H^{(i)}_k = U_{p-i}||G^{(i)}(U_k)$$

Note that $H^{(0)}_k = U_p$ and $H^{(p)}_k = \mathcal{G}(U_k)$. Now once again by the hybrid argument, there exists a $i$ such that

$$\left| Pr \left[ D(H^{(i)}_k) = 1 \right] - Pr \left[ D(H^{(i+1)}_k) = 1 \right] \right| \geq \frac{\delta(k)}{p(k)}$$

Now, we can define a distinguisher for $G$:

**Algorithm 2:** Distinguisher for $G(U_k)$ and $U_{k+1}$.

1: Machine $D'(z)$
2: $b_1, \cdots, b_{p-i-1} \xleftarrow{\$} U_1$
3: $b_{i+2}, \cdots, b_{p(k)} \xleftarrow{\$} G^{(i)}(z)$
4: $\bar{b} = (b_1, \cdots, b_{p(k)-i-1}, b_{p(k)-i-1}, \cdots, b_p)$
5: Output $D((y))$

If $z \sim G(U_k)$, we have $\bar{b} \sim H^{(i+1)}_k$. Else if $z \sim U_{k+1}$, we have $\bar{b} \sim H^{(i)}_k$.

Therefore, $D'$ is a distinguisher for $G$ with advantage $\frac{\delta(k)}{p(k)}$, which is non-negligible in $k$. This is not possible, and hence $\mathcal{G}$ is a PRG.

□

4 Pseudorandom Functions

A pseudorandom function is called so if it cannot be distinguished from a random function by an efficient observer. More formally, we define this primitive using "Oracle Indistinguishability".

**Definition 4** A function ensemble is $\mathcal{F} = \{F_k\}_k$ where $F_k$ is a distribution over functions $f : \{0, 1\}^k \rightarrow \{0, 1\}^k$.

**Definition 5** The uniform function ensemble is $\mathcal{U} = \{U_k\}_k$ where $U_k$ is the uniform random distribution over functions $f : \{0, 1\}^k \rightarrow \{0, 1\}^k$. 

5-3
Definition 6 A function ensemble is efficiently computable if there exist ppt sampler $S$ and deterministic poly-time evaluator $E$ such that:

1. $S(1^k) = F_k$
2. $\forall f \in F_k, E(1^k, f, x) = f(x)$

Definition 7 $X$ is pseudorandom if $X \equiv \{U\}_{1(k)}$. That is, $\forall$ ppt $D$, $|Pr[D(X_k) = 1] - Pr[D(U_k)]|$ is negligible in $k$.

Definition 8 A function ensemble $F$ is pseudorandom if $\forall$ ppt $D$: $\left|Pr_{f \in F}[D^f(X_k) = 1] - Pr_{u \in U_k}[D^u(U_k) = 1]\right|$ is negligible in $k$.

Definition 9 $F$ is a PRF if it is efficient and pseudorandom.

Theorem 10 The existence of a PRG with $2 \times$ expansion implies the existence of PRFs.

Proof Intuition: Let $G$ be such a PRG. Let $G_0 = G(s)[0..k-1]$ and $G_1 = G(s)[k..2k-1]$. Now, $G(U_k) \equiv U_{2k}$ and $G_0(U_k) \equiv G_1(U_k)$. Furthermore, we have that $(G_0 \circ G_1)(U_k) \equiv U_k \equiv (G_1 \circ G_0)(U_k)$.

Now, to double once again, we have: $(G_0 \circ G_0)(U_k) \equiv G_1(U_k) \equiv U_{2k}$. To get quadruple expansion, we create $(G_0 \circ G_0)(U_k) \equiv (G_0 \circ G_1)(U_k) \equiv (G_1 \circ G_0)(U_k) \equiv (G_1 \circ G_1)(U_k) \equiv U_{4k}$. Thus we take a 2 bit seed into an exponentially larger output. This is the template for our construction.