1 Definition and preliminaries

A function $g : \{0, 1\}^* \rightarrow \{0, 1\}^*$ is called a pseudorandom generator (PRG) if it satisfies the following conditions:

1. **Efficiency**: $g$ is PPT computable
2. **Expanding**: $|g(x)| = l(|x|)$, where $l(k) > k$
3. **Pseudorandomness**: $\{x \leftarrow \{0, 1\}^n : g(x)\}$ is pseudorandom.

A first attempt at constructing a PRG was made by Shamir, as follows:

Let $f$ be a OWP. Then construct $g(s) = f^m(s)||f^{m-1}(s)||\ldots||f(s)||s$.

It is easy to see that this function fails the pseudorandomness property, by considering the distinguisher $D$ that, on input $(1^n, y)$, considers the last block of $n$ bits $x$, computes $f(x), f^2(x), \ldots, f^m(x)$, and then compares $y$ to $f^m(x)||f^{m-1}(x)||\ldots||f(s)||x$. If they are equal, it outputs 1, otherwise 0. Then clearly $D$ distinguishes $\{x \leftarrow \{0, 1\}^n : g(x)\}$ from $U_{l(n)}$.

However, Shamir was able argue that given any prefix of the output $g$, of the form $f^m(s)||\ldots||f^k(s)$, it is impossible to guess the next block, because doing so would involve inverting $f$. In a modern approach, though, we require a stronger property: that given any prefix of $k$ bits, we be unable to predict the next bit. By Yao’s theorem, this would be equivalent to pseudorandomness of the output. In the next section, we consider an attempt at constructing such PRGs.

2 PRGs with 1-bit expansion

**Theorem 1** Let $f$ be a OWP, $b$ a hardcore predicate for $f$. Then $g(s) = f(s)||b(s)$ is a PRG.

This theorem has the following corollary:

**Corollary 1** If there exists a one-way-permutation, then there exists a PRG with 1-bit expansion.
Proof. Let $f$ be a OWP. Then $f'(x||r) = f(x)||r, |x| = |r|$ is also a OWP, and $b(x||r) = <x,r>$ is a hardcore predicate for it. Using the theorem, it follows that $g(x) = f'(x)||b(x)$ is a PRG.

Proof of Theorem 1. By Yao’s theorem, if $g$ is not pseudorandom, then $\exists i$ such that $\exists$ n.u.P.P.T. $D$, a distinguisher, such that for some polynomial $p(\cdot)$, for infinitely many $n$,

$$\Pr[x \leftarrow \{0,1\}^n; g(x) = y_1 y_2 \ldots y_{n+1} : D(1^n, y_1 y_2 \ldots y_i) = y_{i+1}] \geq \frac{1}{2} + \frac{1}{p(n)}$$

Notice that since $f$ is a permutation, the first $n$ bits of $g(s)$ are distributed as the uniform distribution, with each bit uniformly random and independent. Thus, if $i < n$, even an unbounded adversary cannot guess the $i + 1$th bit with probability $> 1/2$. It must then be the case that $i = n$. But then, for infinitely many $n$, $D$ can guess $b(s)$ given $f(s)$ with probability $\geq \frac{1}{2} + \frac{1}{p(n)}$, contradicting the fact that $b$ is a hardcore predicate for $f$.

Hence such a $D$, cannot exist, and $g$ must be a PRG.

We will now show that PRGs with a single-bit expansion can be used to obtain PRGs with polynomial expansion.

3 PRGs with polynomial expansion

Theorem 2 The existence of PRGs with 1-bit expansion implies the existence of PRGs with polynomial expansion.

The theorem follows directly from the following lemma, which shows how to construct a PRG with polynomial expansion from a PRG with single-bit expansion.

Lemma 3 Let $g : \{0,1\}^n \rightarrow \{0,1\}^{n+1}$ be a PRG with 1-bit expansion. Let $m = m(n)$ be a polynomial. Then $g'(x_0) = b_1 b_2 \ldots b_m$, where $x_{i+1} || b_{i+1} = g(x_i)$, is a PRG with $m$-bit expansion.

Proof. We define $g'$ recursively, as follows:

$g'_0(s) = \text{empty}$

$g'_k(s) = \text{run } g(s) \text{ to obtain } x || b$. Output $b || g'_{k-1}(x)$

Then $g' = g'_m$. We will now prove that $g'$ is a PRG.

Assume $\exists$ n.u.P.P.T. $D$ and poly $p(\cdot)$ such that for infinitely many $n \in \mathcal{N}$, $D$ distinguishes $U_m$ and $g'(U_n)$ with probability at least $\frac{1}{p(n)}$. We define $m$ hybrids as follows:
\( H_i = U_m | | g_i'(U_n) \)

Then,

\[ H_0 = U_m \\
H_m = g_m(U_n) = g'(U_n) \]

By the Hybrid Lemma, \( \exists i \) such that \( \mathcal{D} \) distinguishes \( H_i \) and \( H_{i+1} \) with probability \( \geq \frac{1}{m(n)p(n)} \). Note that:

\[ H_i = U_m | | g_i'(U_n) = \{ l \leftarrow U_{m-i-1}; b \leftarrow U_1; r \leftarrow g_i'(U_n) : l || b || r \} \]

\[ H_{i+1} = U_m | | g_{i+1}'(U_n) = \{ l \leftarrow U_{m-i-1}; x || b \leftarrow g(U_n); r \leftarrow g_i'(x) : l || b || r \} \]

Then consider the PPT machine \( M \) that acts as follows:

On input \( y = x || b \):
- sample \( l \leftarrow U_{m-i-1} \), \( r \leftarrow g_i'(x) \)
- output \( l || b || r \).

Observe that:

\[ M(U_n) = H_i \]
\[ M(g(U_n)) = H_{i+1} \]

Since \( g \) is a PRG, \( U_n \) and \( g(U_n) \) are indistinguishable, and by closure under efficient operations, \( M(U_n) = H_i \) and \( M(g(U_n)) = H_{i+1} \) are also indistinguishable. But \( \mathcal{D} \) distinguishes them with probability \( \geq \frac{1}{m(n)p(n)} \), a contradiction. Hence such a \( \mathcal{D} \) cannot exist, and \( g' \) must be a PRG.

Combining the two theorems, we get the following corollary:

**Corollary 2** Let \( f \) be a OWP, \( h_f \) a hardcore predicate for \( f \). Then \( g(x) = h_f(x) || h_{f^2}(x) || \ldots || h_{f^m}(x) \) is a PRG.

We can also use an analogous construction for \( \text{collections} \) of OWP, by defining \( g(r_1, r_2) = h_f(x) || h_{f^2}(x) || \ldots || h_{f^m}(x) \), where \( r_1 \) is used to sample \( f \), and \( r_2 \) is used to sample \( x \).

## 4 PRGs from standard assumptions

We can use the above constructions to generate PRGs from familiar collections of OWPs, using random seeds.
**DDH**: Use the seed to generate $p$, a prime, $g$, a generator for $\mathbb{Z}_p^*$, $x$, a random element of $\mathbb{Z}_p^*$. Then, under the Discrete Log assumption, the following function is a PRG:

$$half_{p-1}(x) || half_{p-1}(g^x) || half_{p-1}(g^{9^x}) \ldots$$

**RSA**: Use the seed to generate $p, q$, k-bit primes, $N = pq$, $e$, a random element of $\mathbb{Z}_N^*$. Then, under the RSA assumption, the following function is a PRG:

$$\text{lsb}(x) || \text{lsb}(x^e) || \text{lsb}(x^{e^2}) || \ldots$$