1 Preliminaries

Here are the notions that we need:

**Definition 1 (Half-Space).** A half-space is defined as a function $H_{w,\theta} : \{-1, 1\}^n \to \{-1, 1\}$ for some vector $w \in \mathbb{R}^n$ and some constant threshold value $\theta \in \mathbb{R}$. For any vector $x \in \mathbb{R}^n$, we define $H_{w,\theta}(x) = \text{sign}(\langle w, x \rangle - \theta)$.

I.e., we report 1 if the projection of $x$ onto $v$ is greater than $\theta$, and we report $-1$ if the projection is less than $\theta$. We assume that the length of $w$ will be 1 ($\|w\|_2 = 1$).

**Definition 2 (Regular Half-Space).** (We remind the definition of the supreme norm denoted as $\|w\|_\infty$):

$\|w\|_\infty = \max |w_i|$

A half-space is regular if $\|w\|_\infty \leq \epsilon$

**Definition 3 (Supreme distance).** We define the supreme distance denoted as $d_\infty(A, B)$: $d_\infty(A, B) \doteq \sup_{t \in \mathbb{R}} |\Pr(A < t) - \Pr(B < t)|$

**Theorem 1.** Barry-Esseen Theorem
Let $Y_1, \ldots, Y_n$ be independent random variables with the following properties:

1. $E[Y_i] = 0$
2. $\sum_i E[Y_i^2] = 1$
3. $\sum_i E[Y_i^4] \leq \epsilon^2$

Let $S_n = Y_1 + \ldots + Y_n$ and let $N(01)$ denote the normal distribution with mean 0 and variance 1. Then the supreme distance $d_\infty(S_n, N(01)) \leq \epsilon$

**Corollary 2.** Corollary of the Barry-Esseen Theorem
$d_\infty(<w, U_n>, N(01)) \leq \epsilon$
2 PRG construction attempt

Let \( Y_i = wX_i \) where \( X_i \) is uniform in -1,1. We pick \( X_i \)s from a 4-wise uniform distribution and we end up with:

\[ X_1, X_2, \ldots, X_n \]

However picking \( X_i \)s like that gives us a problem; the \( Y_i \)s will fail the third condition of the Barry-Esseen Theorem. Therefore we split them in \( t \) groups:

\[
\left( \frac{X_1, \ldots, X_n}{D^1} \right) \left( \frac{X_{n+1}, \ldots}{D^2} \right) \ldots \left( \frac{\ldots, X_n}{D^t} \right)
\]

The seed length is \( \approx t \log \frac{n}{t} \)

**Theorem 3.** \( d_\infty(S_n, N(01)) \leq \varepsilon \)

*Proof.* We use the B-E theorem:

\[
w = \left( w_1, \ldots, w_\frac{n}{t} \right) \left( w_{\frac{n}{t}+1}, \ldots \right) \ldots \left( \ldots, w_n \right)
\]

Now let:

\( Y_i \triangleq <D^i, w^i> \) then \( S_t \triangleq <w, D> \) What we have now is the following:

1. \( E[Y_i] = \sum_j w^i_j E[D^i_j] = 0 \)

2. \( \sum_i E[Y_i^2] = \sum_{i, j_1 \neq j_2} E[w^i_{j_1} D^i_{j_1}] E[w^i_{j_2} D^i_{j_2}] + \sum_i \left( w^i_j \right)^2 \sum_k w^2_k = ||w|| = 1 \)

3. \( \sum_i E[Y_i^4] \leq 3 \sum_{j_1 \neq j_2 \neq j_3} w^i_{j_1} \ldots w^i_{j_4} E[D_{j_1} \ldots D_{j_4}] \leq 3 \sum_{j_1 \neq j_2 \neq j_3} \left( w^i_j \right)^2 \left( w^i_k \right)^2 = 3 \left( \sum_j \left( w^i_j \right)^2 \right)^2 = 3 ||w^i||_2^4 \)

For the last part we require that \( \sum_{t} ||w^i||_2^4 \leq \varepsilon^2 \) for which it is sufficient that \( ||w^i||_2^4 \leq \frac{\varepsilon^2}{t} \)

For example: \( w^1 = (\varepsilon, \ldots, \varepsilon) \) will give us:

\[
||w^i||_2^4 = \left( \frac{n}{t} \right) \varepsilon^4 \leq \frac{\varepsilon^2}{t} \Leftrightarrow t \geq n^2 \varepsilon^2
\]

**Idea:** We pick the \( t \) partitions of the \( w^i \)s at random using a hash function \( h[n] \rightarrow [t] \). Now the last part becomes:

\[
\ldots \leq 3 \sum_{j,k} E_h (w^i_j)^2 (w^i_k)^2 = 3 \left( \sum_j E_h (w^i_j)^2 \right)^2 = 3 E_h ||w^i||_2^4
\]
Theorem 4. \( E_h \left[ ||w^i||^4 \right] \leq \Theta \left( \frac{\varepsilon^2}{t} \right) \)

Proof. Let \( H_j = \begin{cases} 1 & h(j) = i \\ 0 & \text{otherwise} \end{cases} \)

Then

\[
E_h \left[ ||w^i||^4 \right] = \sum_j n H_j^4 w_j^4 + \sum E \left[ H_j H_k \right] w_j^2 w_k^2 \leq \frac{\varepsilon^2}{t} + \frac{1}{t^2}
\]

and so finally:

\[
||w^i||^4 \leq \frac{\varepsilon^2}{t} + \frac{1}{t^2} = \Theta \left( \frac{\varepsilon^2}{t} \right)
\]

Now PRG \( D' = (D, h) \) satisfies

\[
d_{\infty} (\langle w, D' \rangle, N(01)) \leq \varepsilon \Rightarrow d \left( H_w, \Theta(U), H_w, \Theta(D') \right) \leq O(\varepsilon)
\]

and the seed length of \( D' \) is

\[
t \log \frac{n}{t} + \log(nt) \sim \varepsilon^2 \log \frac{1}{\varepsilon} \log n
\]