<u>Theorem</u> (Nisan, Wigderson, 1988): If $\exists$ $f \in E$ with $H_{avg}(f) \geq S(n)$ then $\exists$ an $S'(\ell)$-prg where

$S' \approx S$ $\left\{ \quad S'(\ell) := S(n)^{0.01} \text{ for } \frac{100n^2}{\log S(n)} < \ell \leq \frac{100(n+1)^2}{\log S(n+1)}. \right.$

<u>Proof</u>:

- Idea — We stretch a seed $z \in \{0,1\}^\ell$ to $\{0,1\}^{S'(\ell)}$ by choosing n-sized subsets

little overlap → $I_1, \ldots, I_m \subseteq [\ell]$ & considering

hard to guess the next bit → $f(z_{I_1}) \circ f(z_{I_2}) \circ \cdots \circ f(z_{I_m})$.

- <u>Definition</u>: Let $\mathcal{I} := \{I_1, \ldots, I_m\}$ be a family of n-sized subsets of $[\ell]$ & let $f: \{0,1\}^n \to \{0,1\}$.

  The <u>$(\mathcal{I}, f)$-NW generator</u> is the function $NW_{\mathcal{I}}^f : \{0,1\}^\ell \to \{0,1\}^m$ s.t. $\forall z \in \{0,1\}^\ell$,

$$NW_{\mathcal{I}}^f(z) := f(z_{I_1}) \circ \cdots \circ f(z_{I_m})$$

where z_I is the restriction to the coordinates I.

- For an $(\mathcal{I}, f)$-NW generator to be pseudo-random, we will show that, f should be hard & $\mathcal{I}$ should be a certain <u>design</u>:

<u>Definition</u>: Let $\ell > n > d$. A collection $\mathcal{I} = \{I_1, \dots, I_m\}$ of n-sized subsets of $[\ell]$ is an <u>(ℓ, n, d)-design</u> if $|I_j \cap I_k| \leq d$ for all $j \neq k \in [m]$.

<u>Lemma 1</u> (designs): $\exists$ algorithm A that on input (ℓ, n, d), where $\ell > 10n^2/d$, outputs an (ℓ, n, d)-design $\mathcal{I}$ having $m \geq 2^{d/10}$ subsets, in time $2^{O(\ell)}$.

<u>Proof</u>:

- Idea - Greedily build $\mathcal{I}$.
- Initialize $\mathcal{I} = \phi$.

(1) Say, $\mathcal{I} = \{I_1, \dots, I_m\}$ with $m < 2^{d/10}$.
Find an $I \in \binom{[\ell]}{n}$ s.t. $\forall j \in [m]$, $|I \cap I_j| \leq d$.

(2) $\mathcal{I} \leftarrow \mathcal{I} \cup \{I\}$ & goto (1).

- Clearly this takes time $< (2^{d/10})^2 \times 2^{\ell} \cdot n = 2^{O(\ell)}$.

- Can it get stuck at $m < 2^{d/10}$?

  We show the existence of I by the probabilistic method.

- Build I by picking each $x \in [\ell]$ with probability $2n/\ell$.

$\Rightarrow$

$$E[\#I] = \sum_{x \in [\ell]} \frac{2n}{\ell} = 2n.$$

& $\forall j \in [m]$, $E[|I \cap I_j|] = \sum_{x \in I_j} \frac{2n}{\ell} = \frac{2n^2}{\ell} < \frac{d}{5}$.

- Thus, by Chernoff bounds:

$$\Pr_I[|I| < n] < 2 \cdot e^{-n/8}$$

$\left\{ \Pr[|\sum X_i - \mu| \geq c\mu] \leq 2 \cdot \exp(-\mu \cdot \min(\frac{c}{2}, \frac{c^2}{4})) \right.$.

& $\forall j$, $\Pr_I[|I \cap I_j| > d] < 2 \cdot e^{-2d/5}$.

$\Rightarrow \Pr[|I| < n \vee \exists j, |I \cap I_j| > d]$

$< 2e^{-n/8} + 2e^{-4d/10 + d/10} < 1$

$\Rightarrow \Pr_I[|I| \geq n \wedge \forall j, |I \cap I_j| \leq d] > 0$.

$\Rightarrow$ There exists an I in Step-(1).
(If it is larger than n then we can drop the extra elements.) $\square$

- Let us use this design now.

<u>Lemma 2</u> (NW-generator): If $\mathcal{I}$ is an (ℓ, n, d)-design with $|\mathcal{I}| = 2^{d/10} =: m$, $f:\{0,1\}^n \to \{0,1\}$ & $H_{avg}(f) > 2^{2d}$, then

$$NW_{\mathcal{I}}^{f}(U_\ell) \text{ is } (H_{avg}(f)/10, 0.1)-$$

pseudorandom.

<u>Proof</u>:

- Let $S := H_{avg}(f)$.
- Suppose $\exists$ a circuit C of size $\leq S/10$ s.t.

I.e. $NW_{\mathcal{I}}^{f}$ is not pseudornd

$$\left|\Pr[C(NW_{\mathcal{I}}^{f}(U_\ell))=1] - \Pr[C(U_m)=1]\right| \geq 0.1.$$

- Wlog assume,

$$\Pr[C(NW_{\mathcal{I}}^{f}(U_\ell))=1] - \Pr[C(U_m)=1] \geq 0.1.$$

- We will now devise a <u>bit-predictor</u> for $NW_{\mathcal{I}}^{f}$.

- For that let us define distributions $\mathcal{D}_0, \dots, \mathcal{D}_m$ over $\{0,1\}^m$ s.t. $\forall i$,

  $\underline{\mathcal{D}_i}$: choose $x \in_R \{0,1\}^\ell$; $z_{i+1}, \dots, z_m \in_R \{0,1\}$,
  compute $y = NW_g^f(x)$
  output $\langle y_1, \dots, y_i, z_{i+1}, \dots, z_m \rangle$.

hybrid distribution

$\triangleright$ $\mathcal{D}_0 \cong \mathcal{U}_m$ & $\mathcal{D}_m \cong NW_g^f(\mathcal{U}_\ell)$.

- Define $p_i := \Pr[C(\mathcal{D}_i) = 1]$.
- Since $p_m - p_0 \geq 0.1$, averaging gives us: $\exists i_0 \in [m]$, $p_{i_0} - p_{i_0-1} \geq 0.1/m$

- We will use this advantage to predict the i_0-th bit of $NW_g^f(\mathcal{U}_\ell)$ given the preceding (i_0-1) bits.

- Define circuit $\underline{C'}$: on input $y_1, \dots, y_{i_0-1}$,
  pick $z_{i_0}, \dots, z_m \in_R \{0,1\}$,
  output $\begin{cases} z_{i_0}, & \text{if } C(y_1, \dots, y_{i_0-1}, z_{i_0}, \dots, z_m) = 1 \\ 1 - z_{i_0}, & \text{else.} \end{cases}$