• How well does C' predict?

$$\Pr_{y \in NW(U_\ell),\, \bar{z} \in U_m} \left[C'(y_1, \dots, y_{i_0-1}) = y_{i_0} \right] =$$

$$\Pr[z_{i_0} = y_{i_0}] \cdot \Pr[C(y_1, \dots, y_{i_0-1}, z_{i_0}, \dots, z_m) = 1 \,|\, z_{i_0} = y_{i_0}]$$
$$+ \Pr[z_{i_0} \neq y_{i_0}] \cdot \Pr[\qquad " \qquad \neq 1 \,|\, z_{i_0} \neq y_{i_0}]$$

$$= \frac{1}{2} \cdot \Pr[C(D_{i_0}) = 1] + \frac{1}{2} \cdot \left(1 - \Pr[C(y_1, \dots, y_{i_0-1}, \bar{y}_{i_0}, z_{i_0+1}, \dots) = 1]\right)$$
$$= p_{i_0} + \frac{1}{2} - \frac{1}{2}\left(p_{i_0} + \Pr[C(y_1, \dots, y_{i_0-1}, \bar{y}_{i_0}, z_{i_0+1}, \dots) = 1] \right)$$

union bound

$$= p_{i_0} + \frac{1}{2} - \frac{1}{2} \cdot (2 p_{i_0-1}) \geq \left(\frac{1}{2} + \frac{0.1}{m} \right).$$

• To make C' deterministic, we could fix $z_{i_0}, \dots, z_{i_m}$ & get a circuit C'' s.t.

$$\Pr_{y \in NW(U_\ell)} \left[C''(y_1, \dots, y_{i_0-1}) = y_{i_0} \right] \geq \left(\frac{1}{2} + \frac{0.1}{m} \right).$$

• Clearly, $\text{size}(C'') < 2 \cdot \text{size}(C) \leq S/5$.

• Now we plug the definition of NW_ℓ^f, to get:

$$\Pr_{Z \in U_\ell}\left[C''(f(Z_{I_1}), \ldots, f(Z_{I_{i_0-1}})) = f(Z_{I_{i_0}})\right] \geq \left(\frac{1}{2} + \frac{0.1}{m}\right)$$

- Let us fix $Z_{[\ell] \setminus I_{i_0}}$ s.t. the above probability advantage is retained.

- Note that this leaves only $|I_j \cap I_{i_0}|$ many variables free in Z_{I_j}, $j \in [i_0 - 1]$.

$\Rightarrow f(Z_{I_1}), \ldots, f(Z_{I_{i_0-1}})$ are d-variate.

$\Rightarrow$ " " can be computed (trivially) by circuits of size $O(d \cdot 2^d)$.

$\Rightarrow \exists$ a circuit B of size $< \frac{S}{5} + O(d 2^d) \cdot m$
$= S/5 + O(d\, 2^{d + d/10}) < S$ ($\because S > 2^{2d}$) s.t.

$$\Pr_{Z_{I_{i_0}} \in U_n}\left[B(Z_{I_{i_0}}) = f(Z_{I_{i_0}})\right] \geq \frac{1}{2} + \frac{0.1}{m} > \frac{1}{2} + \frac{1}{S}.$$

- This contradicts the assumption that $H_{avg}(f) = S$.

$\Rightarrow NW_{\mathcal{I}}^{f}(U_\ell)$ is $(S/10, 0.1)$-pseudorandom. $\square$

<u>Proof</u> (NW theorem):

- Let $f \in \mathrm{Dtime}(2^{O(n)})$ s.t. $H_{avg}(f) \geq S(n)$.
- We will define an $S'(\ell)$-prg G:

  On input $z \in \{0,1\}^\ell$,

1) Pick n s.t. $\frac{100n^2}{\lg S(n)} < \ell \leq \frac{100(n+1)^2}{\lg S(n+1)} \leq \frac{200n^2}{\lg S(n)}$.
2) Set $d = \lg S(n)/10$.
3) Compute an (ℓ, n, d)-design $\mathcal{I} = \{I_1, \dots, I_m\}$ with $m = 2^{d/10}$.
4) Output $NW_{\mathcal{I}}^f(z)$.

- This takes time: $2^{O(\ell)} + 2^{O(n)} \cdot 2^{d/10} = 2^{O(\ell)}$.
- Since $H_{avg}(f) \geq S(n) = 2^{10d}$, by Lemma 2 we get: $NW_{\mathcal{I}}^f(U_\ell)$ is $(S(n)/10, 0.1)$-pseudorandom.

- Finally, the stretch is $2^{d/10} = S(n)^{1/100} =: S'(\ell)$.
- Clearly, G is an $S'(\ell)$-prg. $\square$