def Pseudorandom Generator. R distr. over $\{0,1\}^m$.
is (S,ε)- pseudor. if $\forall$ ckt C, $|C| \le S$,

$$\left| \Pr_{r \sim R}[C(r)=1] - \Pr_{r \sim U_m}[C(r)=1] \right| < \varepsilon.$$

$G: \{0,1\}^* \to \{0,1\}^*$ exp-time computable is $S(n)$-PRG if $|G(z)| = S(|z|)$ for every seed z and $\ell \in \mathbb{N}$ $G(U_\ell)$ is $(S(\ell)^3, 1/10)$- pseudor.

def. Unpredictable Function. R distr. over $\{0,1\}^m$
is (S,ε)-unpred. if $\forall$ ckt C, $|C| \le S$, $\forall i \in [m]$

$$\Pr_{r \sim R}[C(r_1 \dots r_{i-1}) = r_i] \le \frac{1}{2} + \frac{\varepsilon}{m}.$$

obs R pseud. $\Rightarrow$ unpred. (just rm same C).

th R $(2S,\varepsilon)$- unpred $\Rightarrow$ R (S,ε) pseud. [Gol09 ex 8.20]

proof. assume R not pseudor. assume wlog

$$\Pr_R[\ ] - \Pr_U[\ ] > \varepsilon \text{ for some ckt } C.$$

consider "hybrid distributions" R_i, where we pick first i bits from R and last $m-i$ from U.

then we must have some i s.t

$$\Pr_{R_i}[\ ] - \Pr_{R_{i-1}}[\ ] > \varepsilon/m.$$

i.e. $\Pr[C(r_1 \dots r_i, u_{i+1} \dots u_m)] - \Pr[C(r_1 \dots r_{i-1}, u_i \dots u_m)] > \varepsilon/m$.

fix $a_{i+1} \dots a_m$ s.t this happens.
on input $r_1 \dots r_{i-1}$, have D eval $C(\dots 0)$ and $C(\dots 1)$.
output whichever makes C larger.

How to build PRGs?
Can do from avg-hard functions.

def $f: \{0,1\}^n \to \{0,1\}$. $\rho \in [0,1]$.

$$H^\rho_{avg}(f) = \max_S \text{ s.t } \forall C \text{ ckt}, |C| \le S, \Pr_x[f(x)=C(x)] < \rho.$$

$$H_{avg}(f) = \max_S \text{ s.t } H^{1/2+1/S}_{avg}(f) \ge S.$$

iow: $H_{avg} = \max_S$ s.t $\forall C, |C| \le S, \Pr_x[f(x)=C(x)] \le 1/2 + 1/S$

def looks a bit weird, it's crafted so that it works with PRGs.
it is possible to transform a worst-case hard function into an avg-case hard function. ↓ $\Pr[f=C] < 1$

th (avg-hard $\Rightarrow$ PRG).

If $\exists f_n \in DTIME(2^{O(n)})$ s.t $H_{avg}(f_n) \ge S_n$ $\forall n$
Then a $S(\delta\ell)^\delta$ PRG exists for some $\delta > 0$.

we'll prove weaker version $S(n)^\delta$ where $n \ge \delta \cdot \sqrt{\ell \cdot \log S(n)}$.

First of all let us see how to obtain 1 extra bit.

prop. If $\exists f_n \in E$ s.t $H_{avg}(f_n) \ge n^4$
then a $\ell+1$ PRG exists.

proof. Enough to build unpredictable function.

We'll do $G(z) = z \cdot f(z)$.
Bits $1 \dots \ell$ unif random $\Rightarrow$ unpredictable.
Assume last bit predictable, i.e.
$\exists C, |C| < 2^{n^3}$ s.t $\Pr[C(z) = f(z)] > \frac{1}{2} + \frac{1}{10(\ell+1)}$

This contradicts $H_{avg}(f_n) \ge n^4$.

Let us now do 2 extra bits.

prop. If $\exists f_n \in E$ s.t $H_{avg}(f_n) \ge n^4$
then a $\ell+2$ PRG exists.

proof. $G(z) = z \cdot f(z_1 \dots z_{n/2}) \cdot f(z_{n/2+1} \dots z_n)$.

Bits $1 \dots \ell+1$ ok.
Bit $\ell+1$ a bit tricky: C receives as input some info that it could not compute on its own. Could that help?
Intuitively no: info gained from $\ell+1$-th bit only applies to first half of z, while $\ell+2$-th bit depends on second half, which is indep.

To do more bits we'll have to deal with bits for which we know partial information.

We will do $G(z) = f(z_{I_1}) \cdot f(z_{I_2}) \cdots f(z_{I_m})$
where $\{I_i\}$ family of subsets of $[\ell]$, $|I_i| = n$, and $|I_i \cap I_j| \le d$ (for some d).
Such families are called (ℓ, n, d)-designs, and can be constructed efficiently.

lemma: if $n \ge d$, $\ell > 10n^2/d$, then can build a design of size $2^{d/10}$ in time $2^{O(\ell)}$.

Assuming lemma we prove G is a PRG.

lemma: if $\{I_i\}$ (ℓ, n, d)-design, $|I_i| = 2^{d/10}$,
and $f: \{0,1\}^n \to \{0,1\}$ is 2^{2d}-avg-hard then
$G(z)$ is $(2^{2d}/10, 1/10)$-pseudorandom.

proof. as usual slow any ckt of size $2^{2d}/10$ cannot guess ith-bit with more than $\frac{1}{10 \cdot 2^{d/10}}$ advantage.

proof by contradiction.

assume $\Pr_z[C(f(z_{I_1}) \dots f(z_{I_{i-1}})) = f(z_{I_i})] \ge \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}$.

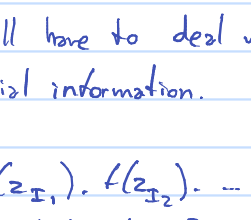
problem: z_{I_i} are not indep. random vars.
sample z as two indep. random vars: $z_+ = z_{I_i}$, $z_- = z_{\bar{I}_i}$.

$$\Pr_{z_+, z_-}[\ w(z_+, z_-) = f(z_+)\ ] \ge \frac{\quad}{\quad}.$$

by averaging, $\exists z^*$ evaluation of z_- s.t

$$\Pr_{z_+}[\ z_- = z^*\ ] \ge \Pr_{z_+, z_-}[\ \ ].$$

now because $|z_{I_j} \cap z_{I_i}| \le d$, we have that after fixing z^* all of the $f(z_{I_j})$ have at most d vars left.
Hence can compute $f(z_{I_j})$ with a ckt of sz 2^d.
and we got a ckt



of sz $< 2^{2d}$

that guesses $f(z_+)$ w/pr $\ge \frac{1}{2} + \frac{1}{10 \cdot 2^{d/10}}$!! //.

Pick appropriate values to finish proof of thm.

Finally, prove design lemma.
lemma: if $n \ge d$, $\ell > 10n^2/d$, then can build a design of size $2^{d/10}$ in time $2^{O(\ell)}$.

proof: greedy algorithm. pick first subset of $[\ell]$ of sz n s.t $|I_i \cap I_j| < d$. $\forall j$. picked so far.

time $poly(m) \cdot 2^d$ ok.