Last time: two (incomparable) corr. bds for $\mathbb{F}_2$-polys.

- Any degree-$(\frac{1}{4}\sqrt{n})$ $\mathbb{F}_2$-poly p has (hi deg! :))

$$\Pr_{x \sim \mathcal{U}}[\mathrm{mod}_3(x) = p(x)] \leq 7/8.$$ (weak :( )

- Any deg-d $\mathbb{F}_2$-poly p has (low deg :( ) (non-trivial only if $d2^d \ll n$, i.e. $d \lesssim \log n$)

$$\Pr_{x \sim \mathcal{U}}[GIP_{d+1}(x) = p(x)] \leq \frac{1}{2} + 2^{-\Omega\left(\frac{n}{d2^d}\right)}$$ (strong :))

Today: • finish missing piece from 2^{-d} corr. bd:

$$\mathrm{Cor}[F, P] \leq U_{d+1}(F)^{2^{-(d+1)}} \quad \text{for } P = e(p),\ p \text{ deg } d$$

- Basic Tools for PRGs:
  - k-wise indep. RV's
  - ε-biased RV's
  - k-wise indep ε-biased RV's
  - some Fourier stuff, applications

Scribe: Akshat

Questions?

Reminder: prelim. project proposal due next Thurs March 7

To prove:

Lemma: Let $F: \mathbb{F}_2^n \to \{\pm 1\}$ any fn,

let $P = e(p)$, p a deg-d $\mathbb{F}_2$-poly.

Have $|Cor[F,P]| \le U_{d+1}(F)^{\frac{1}{2^{d+1}}}$.

Fact 1: $\forall F: \mathbb{F}_2^n \to [-1,1]$ have $U_1(F)^{\frac{1}{2}} = |\mathbb{E}[F]|$. ✓✓

Fact 2: $\forall F: \mathbb{F}_2^n \to [-1,1]$ have $U_k(F) \le U_{k+1}(F)^{\frac{1}{2}}$.

Fact 3: $\forall F: \mathbb{F}_2^n \to [-1,1]$, $\forall P = e(p)$ where $p \in OEG_d$,
have $U_{d+1}(F \cdot P) = U_{d+1}(F)$.

Pf of Lemma:

write $G(x) = F(x) \cdot P(x)$. Have

$$|Cor[F,P]| = |\mathbb{E}[G]|$$

$$\overset{F1}{=} U_1(G)^{\frac{1}{2}}$$

$$\overset{F2}{\le} U_2(G)^{1/4} \overset{F2}{\le} U_3(G)^{1/8} \cdots \overset{F2}{\le} U_{d+1}(G)^{\frac{1}{2^{d+1}}}$$

$$= U_{d+1}(F \cdot P)^{\frac{1}{2^{d+1}}} = U_{d+1}(F)^{\frac{1}{2^{d+1}}}.$$

F2: $\forall F: \mathbb{F}_2^n \to [-1,1]$, have $U_k(F) \le U_{k+1}(F)^{\frac{1}{2}}$.

Pf: $k = 1$: $y = x + h_2$

$$U_2(F) = \mathop{\mathbb{E}}_{h_1}\Big[\mathop{\mathbb{E}}_{x,h_2}\big\{F(x)F^{+h_1}(x)\underbrace{F^{+h_2}(x)F^{+h_1+h_2}(x)}_{F(y)F^{+h_1}(y),}\big\}\Big]$$

$$= \mathop{\mathbb{E}}_{h_1}\left[\mathop{\mathbb{E}}_{x}\left[F(x)F^{+h_1}(x)\right] \cdot \mathop{\mathbb{E}}_{y}\left[F(y)F^{+h_1}(y)\right]\right]$$

C-S: $\mathbb{E}[A^2] \geq \mathbb{E}[A]^2$

$$= \mathop{\mathbb{E}}_{h_1}\left[\mathop{\mathbb{E}}_{x}\left[F(x)F^{+h_1}(x)\right]^2\right]$$

$$\geq \mathop{\mathbb{E}}_{h_1,x}\left[F(x)F^{+h_1}(x)\right]^2 = U_1(F)^2.$$

General h_i: same, more subscripts.

F3: $\forall F: \mathbb{F}_2^n \to [-1,1]$, $\forall P = e(p)$ where $p \in \mathrm{OEG}_d$, have $U_{d+1}(F \cdot P) = U_{d+1}(F)$.

Pf: Recall:

$$U_{d+1}[F \cdot P] = \mathop{\mathbb{E}}_{h_1,\dots,h_{d+1},x}\left[\prod_{S \subseteq [d+1]} F^{+\sum_{j\in S} h_j}(x) \cdot P^{+\sum_{j\in S} h_j}(x)\right]$$

$(-1)^{P^{+\sum_{j\in S} h_j}(x)}$

p = deg-d poly: saw "1st deriv" $p(x)+p(x+h)$ has deg 1 less than $\deg(p)$.

So $\sum_{S\subseteq[d+1]} P^{+\sum_{j\in S} h_j}(x)$ is $(d+1)$st deriv.,

which $= 0$ b/c $\deg(d) \leq p$. So $= P^0 = 1$,

$\therefore$ hence

$$= \mathop{\mathbb{E}}_{h_1,\dots,h_{d+1},x}\left[\prod_{S \subseteq [d+1]} F^{+\sum_{j\in S} h_j}(x) \cdot 1\right] = U_{d+1}(F). \blacksquare$$

On to PRGs !!!

- k-wise indep/unif. RVs $\{0,1\}^n$
- ε-biased
- k-wise ε-biased

Applic.

---

(1) k-wise indep/uniform RV's.

"true" indep:

Def: Let $X_1, \ldots, X_n$ be RV's, each supp. on finite set A.

$(X_1, \ldots, X_n)$ is indep if $\forall (a_1, \ldots, a_n) \in A^n$, have

$$\Pr[(X_1 = a_1) \wedge \ldots \wedge (X_n = a_n)] = \prod_{j=1}^{n} \Pr[X_j = a_j]$$

Def: As before,
Let $X_1, \ldots, X_n$ be RV's, each supp. on finite set A.

$(X_1, \ldots, X_n)$ is k-wise indep. if $\forall 1 \le i_1 < i_2 < \ldots < i_k \le n$,
$\forall a_{i_1}, \ldots, a_{i_k}$, have

$$\Pr\left[(X_{i_1}=a_{i_1}) \wedge \dots \wedge (X_{i_k}=a_{i_k})\right] = \prod_{j=1}^{k} \Pr\left[X_{i_j}=a_{i_j}\right].$$

- $k=2$: "pairwise indep".
- Each X_i unif. over A: "k-wise uniform."
  ↓ indep.

Ex: $(X_1 = \dots = X_n)$ $\quad X_1 \leftarrow \$$

1-wise indep.

Ex: $X_1 = U_1$, $X_2 = U_2$, $X_3 = U_1 \oplus U_2$.

pairwise unif.

$\Pr[X_{i_1}=a, X_{i_2}=b] = 1/4$

Claim: Can generate n pairwise unif. bits using seed length $\lceil \log_2(n+1) \rceil =: k$.

Pf: Let $b_1, \dots, b_k$ be indep. unif. bits $\{0,1\}$.
For each nonempty $S \subseteq [k]$, let

$$X_S = \bigoplus_{i \in S} b_i .$$

$n = 2^k - 1$ such X_S's.

These are pairwise unif:
Fix any two nonempty $S_1 \neq S_2 \subseteq [k]$.

Consider any $(\alpha, \beta) \in \{0,1\}^2$.

WLOG $S_1 \setminus S_2 \neq \emptyset$. Have

goal: $\frac{1}{4}$ = $\frac{1}{2}$

$$\Pr_{b_1 \ldots b_k}[X_{S_1} = \alpha \wedge X_{S_2} = \beta] = \Pr\{X_{S_1} = \alpha \mid X_{S_2} = \beta\} \cdot \Pr[X_{S_2} = \beta].$$

$= \frac{1}{2}$?

$\Pr[X_{S_2} = \beta] = \frac{1}{2}$ ": fix outcomes of each b_i except last elt of S_2. ↳ j

One b_j outcome causes $X_{S_2} = 0$

" " " " " $= 1$.

For $\Pr\{X_{S_1} = \alpha \mid X_{S_2} = \beta\}$

let j' be an elt of $S_1 \setminus S_2$.

Fix all b_i, $i \in S_2$, s.t. $X_{S_2} = \beta$;

" " b_i other than $i = j'$:

one setting of j' gives $X_{S_1} = \alpha$

" " " " " $\neq \alpha$. So $= \frac{1}{2}$.

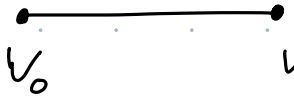
∎

Applic: Derand. simple rand approx. alg. for MAXCUT.

Maxcut: Input = $G = (V, E)$ undir. graph.

Goal: Split V into $V_0 \sqcup V_1$ s.t. (disjoint union)

edges e maximized.



NP hard.

Rand. alg. $\frac{1}{2}$-approx: v_i in $V_{\$}$ indep $i = 1, \ldots, n$.

$$\mathbb{E}\left[|E(V_0, V_1)|\right] = \sum_{e=\{u,v\} \in E} \Pr\left[\text{edge } \{u,v\} \text{ crosses cut}\right]$$

$$= \sum_{e \in E} \frac{1}{2} = \frac{1}{2} \cdot |E| \geq \frac{1}{2} (\text{size of max cut}).$$

Derand? Could use pairwise indep. dist., & analysis still works.

So could enumerate over all $2^{\lceil \log_2(n+1) \rceil} = O(n)$ strings in support of pairwise unif dist., & use the one that does best.

Let's do k-wise unif., $k > 2$.

Let $\mathbb{F}$ be finite field, $|\mathbb{F}| = n$.

Construc. of k-wise unif. RV's $(X_1, \ldots, X_n)$ over $\mathbb{F}$:

Let $c_0, \dots, c_{k-1}$ be indep. unif. $\sim \mathbb{F}$.

($k \cdot \log n$ bits of rand.)

View as coeff of univar. poly over $\mathbb{F}$:

for $\alpha \in \mathbb{F}$, let

$$X_\alpha := \sum_{i=0}^{k-1} c_i \alpha^i = p_c(\alpha) = c_0 + c_1 \alpha + c_2 \alpha^2 + \dots$$

(p_c: deg $(k-1)$ poly over $\mathbb{F}$)

This is n X_α's. k-wise unif:

Indiv. outcome: for any fixed α, X_α unif. over $\mathbb{F}$,

b/c c_0 makes it so regardless of $\alpha, c_1, \dots, c_{k-1}$.

We get k-wise indep. by Lagrange interp:

for any desired $a_1, \dots, a_k \in \mathbb{F}$,

any distinct $\alpha_1, \dots, \alpha_k \in \mathbb{F}$, there's a unique

$(c_0, \dots, c_{k-1})$ s.t. $X_{\alpha_i} = p(\alpha_i) = a_i \quad i = 1, \dots, k$:

$$X_\alpha = p_c(\alpha) = \sum_{i=1}^{k} a_i \frac{\prod_{j \neq i} (\alpha - \alpha_j)}{\prod_{j \neq i} (\alpha_i - \alpha_j)} .$$

So unif dist over $(c_0, \dots, c_{k-1})$ induces unif over $(a_1, \dots, a_k)$:

i.e.

$$\Pr\left[(X_{\alpha_1} = a_1) \wedge \dots \wedge (X_{\alpha_k} = a_k)\right] = \frac{1}{|\mathbb{F}|^k} = \prod_{i=1}^{k} \Pr[X_{\alpha_i} = a_i].$$

Got k-wise unif RV over $\mathbb{F}$, $|\mathbb{F}| = n$.

OFFICIAL HW PROBLEM:

use above (k-wise unif RV over $\mathbb{F}$, $|\mathbb{F}| = n$, $n = 2^j$)

to get n k-wise indep. RV over $\mathbb{F}$, $|\mathbb{F}| = 2$ (2^i $i \le j$).

Applic: Derand simple rand alg for MAX 3SAT

MAX 3SAT: input = a 3-CNF $C_1 \wedge \dots \wedge C_m$

$C_i = (\ell_{i_1} \vee \ell_{i_2} \vee \ell_{i_3})$ (3 dist. vars)

Goal: find asst sat max poss # clauses.

Simple rand 7/8 approx alg: pick $a \sim \{0,1\}^n$ unif.

$$\mathbb{E}[\text{sat. clauses}] = \sum_{i=1}^{m} \Pr[C_i \text{ sat. by } a] = \frac{7}{8} \cdot m \ge 7/8 \cdot \text{opt.}$$

Analysis still ok if a only 3-wise indep.

$k=3$: $2^{k \log n} = \text{poly}(n)$ time.

As before, try all $a \in \text{supp}(\text{favorite 3-wise ind dist over } \{0,1\}^n)$

+ best a sat. (# sat. clauses) $\ge \frac{7}{8} \cdot m$. ∎

PRG-type applic. of k-wise ind: juntas, DTs.

Def: a *k-junta over $\{0,1\}^n$* is a fn f s.t.

$f(x_1, \ldots, x_n) = g(x_{i_1}, \ldots, x_{i_k})$ some g, $i_1, \ldots, i_k$.

$\mathcal{J}_k$ = class of all k-juntas.

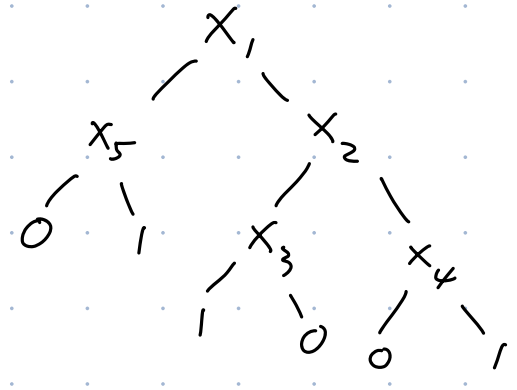
Immediate: X k-wise unif over $\{0,1\}^n \Rightarrow$

X 0-fools $\mathcal{J}_k$. ($k \log n$ seed length)

Def DT_k = all $f: \{0,1\}^n \to \{0,1\}$ computed by depth-k DT.

$k = 3$

$\mathcal{J}_k \subsetneq DT_k$:



Claim: If X 0-fools $\mathcal{J}_k$, then X 0-fools DT_k.

Pf: Let $f \in DT_k$. Have $f = \sum_{\ell \in L} f_\ell$

L = 1-leaves of the DT,

each f_ℓ is a K-junta (conj). So

$$\mathbb{E}[f(X)] = \mathbb{E}\left[\sum_{\ell \in L} f_\ell(X)\right] = \sum_\ell \mathbb{E}[f_\ell(X)]$$

$$\overset{X \text{ 0-fools } \partial_K}{=} \sum \mathbb{E}[f_\ell(U)]$$

$$= \mathbb{E}\left[\sum_\ell f_\ell(U)\right] = \mathbb{E}[f(U)].$$

Generalize to get triangle ineq:

Lemma (Δ ineq): Let $f_1, \dots, f_t : \{0,1\}^n \to \mathbb{R}$,
let $\lambda_0, \lambda_1, \dots, \lambda_t \in \mathbb{R}$,
let
$$f(x) = \lambda_0 + \sum_{i=1}^t \lambda_i f_i(x).$$

If X ε_i-fools each f_i $\quad i \in [t]$, then
X ε-fools f, where
$$\varepsilon = \sum_{i=1}^t |\lambda_i| \cdot \varepsilon_i.$$

Pf: $\left|\mathbb{E}[f(X)] - \mathbb{E}[f(U)]\right|$

$$= \left|\sum_{i=1}^t \lambda_i \mathbb{E}[f_i(X)] - \sum_{i=1}^t \lambda_i \mathbb{E}[f_i(U)]\right|$$

$$\le \sum_{i=1}^t |\lambda_i| \cdot \left|\mathbb{E}[f_i(X)]\right| - \sum_{i=1}^t |\lambda_i| \cdot \left|\mathbb{E}[f_i(U)]\right.$$

$$\leq \sum_{i=1}^{t} \lambda_i \cdot \varepsilon_i$$

Break

ε-bias dist. over $\{0,1\}^n$

Def: $PAR = \{P_S\}_{S \subseteq [n]}$ = class of all parities over $x_1, \ldots, x_n$: $\{0,1\}^n$

$$P_S = \sum_{i \in S} x_i \mod 2$$

$$= \bigoplus_{i \in S} x_i$$

Also $\chi_S(x) = (-1)^{P_S(x)} = e(P_S(x))$

"character function"

Def $X = (X_1, \ldots, X_n)$ over $\{0,1\}^n$ (RV) is ε-biased if it $(\varepsilon/2)$-fools PAR, i.e.

ε-fools all characters χ_S.

$$\left| \mathbb{E}[\chi_S(X)] - \underbrace{\mathbb{E}[\chi_S(U)]}_{\begin{array}{l} = 0 \text{ if } S \neq \emptyset \\ = 1 \text{ if } S = \emptyset. \end{array}} \right| = \varepsilon$$

i.e. for $\emptyset \neq S$, have

$$\frac{1}{2} - \frac{\varepsilon}{2} \leq \Pr[P_S(X)] \leq \frac{1}{2} + \frac{\varepsilon}{2}.$$

(we'll use ε-biased RV to fool DEG_d ...)

Construction of ε-biased RV's:

Let $bij: \mathbb{F}_{2^\ell} \to (\mathbb{F}_2)^\ell$ be a linear bijection.

(ℓ-length vector of $\mathbb{F}_2$ values.)

$bij(x+y) = bij(x) + bij(y)$

(elt is a $\deg \le (\ell-1)$ poly over $\mathbb{F}_2$, mod some fixed irred deg-ℓ poly)

(Our std constr. of $\mathbb{F}_{2^\ell}$ gives such a bij: add poly's by adding coeffs.)

$x \in \mathbb{F}_{2^\ell}$, y, $r_i \in \{0,1\}$

$(x,y) \to (r_0, \dots, r_{n-1})$

Let $\ell = \log(\frac{n}{\varepsilon})$. ε-biased gen $G: (\mathbb{F}_{2^\ell})^2 \to \{0,1\}^n$ is

seed length $= 2\ell = 2\log(n/\varepsilon)$

$G(x,y) = (r_0, \dots r_{n-1})$ where $r_i = \langle bij(y), bij(x^i) \rangle \bmod 2$.

$a, b \in (\mathbb{F}_2)^\ell$; $bij(y) \in (\mathbb{F}_2)^\ell$, $bij(x^i) \in (\mathbb{F}_2)^\ell$

$\langle a, b \rangle = a_1 b_1 + \dots + a_\ell b_\ell \bmod 2$.

Lemma: This G is an ε-biased gen:

for $U \sim \{0,1\}^{2\log(n/\varepsilon)}$, have

$G(U)$ is ε-biased RV.

Pf: To show: fool all parities.

I.e. for all nonzero $\alpha \in \{0,1\}^n$, have

$$\left| \Pr_{r \sim G(u)} \left[\sum_{i=0}^{n-1} \alpha_i r_i \equiv 1 \bmod 2 \right] - \frac{1}{2} \right| \leq \frac{\varepsilon}{2}.$$

Def of G:

$$\Pr_{r \sim G(u)} \left[\sum_{i=0}^{n-1} \alpha_i r_i \equiv 1 \right] \bmod 2$$

$$= \Pr_{x,y \sim \mathbb{F}_{2^\ell}} \left[\sum_{i=0}^{n} \alpha_i \langle b_{ij}(y), b_{ij}(x^i) \rangle \equiv 1 \bmod 2 \right]$$

lin. of b_{ij}

$$= \Pr_{x,y} \left[\langle b_{ij}(y), b_{ij}\left(\sum_{i=0}^{n-1} \alpha_i x^i \right) \rangle \equiv 1 \bmod 2 \right]$$

$$= \Pr_{x,y} \left[\langle b_{ij}(y), b_{ij}(p_\alpha(x)) \rangle \equiv 1 \bmod 2 \right],$$

(= event E)

where $p_\alpha(x) = \deg \leq (n-1)$ univ poly $\sum_{i=0}^{n-1} \alpha_i x^i$ over $\mathbb{F}_{2^\ell}$.

Case on x: $p_\alpha(x) = 0$, or $\neq 0$ (in $\mathbb{F}_{2^\ell}$).

$$\Pr_y \left[\langle b_{ij}(y), b_{ij}(p_\alpha(x)) \rangle \equiv 1 \bmod 2 \right] = \begin{cases} 0 & \text{if } p_\alpha(x) = 0 \\ \frac{1}{2} & \text{if } p_\alpha(x) \neq 0 \end{cases}$$

(event E)

(b/c nonempty parity over bits of $b_{ij}(y)$).

$$\text{(★)} = \Pr_{x,y}[E]$$

$$= \Pr_y[E \mid P_\alpha(x)=0] \cdot \Pr_x[P_\alpha(x)=0] + \Pr_y[E \mid P_\alpha(x)\neq 0] \cdot \Pr_x[P_\alpha(x)\neq 0]$$

($\Pr_y[E \mid P_\alpha(x)=0] = 0$; $\Pr_y[E \mid P_\alpha(x)\neq 0] = \frac{1}{2}$)

$$= \frac{1}{2} \cdot \Pr_x[P_\alpha(x)\neq 0] \leq \frac{1}{2}.$$

Lower bd: $P_\alpha(x)$ is a deg-$(n-1)$ poly over $\mathbb{F}_{2^\ell}$

P_α has $\leq n-1$ roots, so $\Pr_x[P_\alpha(x)\neq 0] \geq 1 - \frac{n-1}{2^\ell} \geq 1-\varepsilon$.

$2^\ell = \frac{n}{\varepsilon}$, so

so (★) $\geq \frac{1}{2}(1-\varepsilon) = \frac{1}{2} - \frac{\varepsilon}{2}$. ∎

---

k-wise ind dist, $\to$ over $\mathbb{F}_2^n$ $\to$ min. dist.

ε-biased dist over $\mathbb{F}_2^n$:

closely related to linear codes over $\mathbb{F}_2^n$. $\to$ balancedness

Coding theory motiv. to do better, for ε-biased, than our $2\log\left(\frac{n}{\varepsilon}\right)$ s.l.

Proj topic:

Conceivable: explicit $\log n + 2\log\frac{1}{\varepsilon} - \log\log\frac{1}{\varepsilon}$ s.t. ε-bias might exist. (?)

→ Ta-Shma '17:

$$\log n + 2\log\frac{1}{\varepsilon} + \tilde{O}\left(\log^{2/3}\left(\frac{1}{\varepsilon}\right)\right)$$

Best of both worlds:

Def: RV $X = (X_1, \ldots, X_n)$ over $\{0,1\}^n$ is k-wise ε-biased if it ε-fools all χ_S with $|S| \le k$.

Lemma: Explicit k-wise ε-biased $X = (X_1, \ldots, X_n) = G(U)$, seed length $O(\log k + \log\frac{1}{\varepsilon} + \log\log n)$.

Pf Let $G : \{0,1\}^s \to \{0,1\}^n$ be k-wise unif gen that's a linear transf. viewed as $(\mathbb{F}_2^s) \to (\mathbb{F}_2^n)$. $s = k\log n$

(Our k-wise unif gen. is such.)

Let Y is ε-biased dist over $\{0,1\}^s$

Overall X is $X = G(Y)$. Outputs n bits.

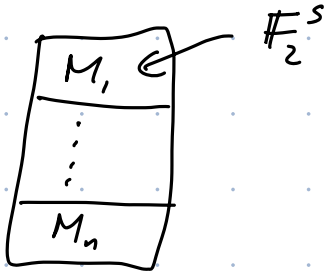
s.l. is $2\log(s/\varepsilon) = O(\log k + \log\frac{1}{\varepsilon} + \log\log n)$.

To show: $G(Y)$ ε-fools par's of size $\le k$.

Let $S \subset [n]$, $|S| \le k$.

$P_S(x) = \sum_{i \in S} x_i \qquad x \in (\mathbb{F}_2)^n$. parity to fool.

Let $M \in \mathbb{F}_2^{n \times s}$ matrix for lin transf G

rows 

so

$$G(Y) = \left(\langle M_1, Y \rangle, \dots \langle M_n, Y \rangle \right) \in \mathbb{F}_2^n.$$

For $y \in \mathbb{F}_2^s$, have

$$P_S(G(Y)) = \sum_{i \in S} \langle M_i, Y \rangle = \sum_{i \in S} \sum_{j=1}^{s} M_{ij} Y_j$$

$$= \sum_{j=1}^{s} \left(\sum_{i \in S} M_{ij} \right) Y_j .$$

This is some PAR over $Y_1, \dots, Y_s$

Since $Y = (Y_1, \dots, Y_s)$ is ε-biased,

$$\left| \mathbb{E}[P_S(G(Y))] - \mathbb{E}[P_S(G(U))] \right| \le \frac{\varepsilon}{2}.$$

Since P_S is k-junta + G k-wise unif, have

$$\mathbb{E}\{p_s(G(U))\} = \mathbb{E}\{p_s(U_n)\}.$$

So $\left|\mathbb{E}\{p_s(G(Y))\} - \mathbb{E}\{p_s(U_n)\}\right| \le \varepsilon/2$,

i.e. Y $(\varepsilon/2)$-fools p_s. ▨

Next time: Fourier, applic. of today (easy & non-easy)