Applications of Expanders "in the Wild" II

50s, 60s: Numerical Integration: $f : [0,1]^2 \to \mathbb{R}$

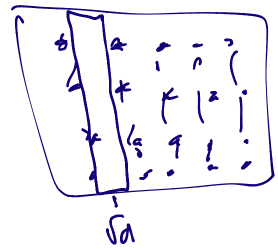
Koksma-Hlawka: $$\left| \int_0^1\!\!\int_0^1 f - \frac{1}{d}\sum_{j=1}^{d} f(z_j) \right| \le V(f)\cdot \mathrm{Discr}(\{z_j\})$$

$$\mathrm{Discr}(\{z_j\}_{j=1}^d) := \sup_R \left| \frac{\#\{z_j\}\cap R}{d} - \frac{\mathrm{Area}(R)}{1} \right|$$

1st variation $V(f) = \iint |f| + |f_x| + |f_y| + |f_{xy}|$
Sobolev norm

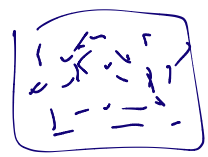
Problem: Minimize discrepancy.

$\ll \iff O()$
$\to 0 \iff o()$



Ex 1: $\mathrm{Discr}(\{z_j\}_{j=1}^d) \ge \frac{1}{d}$.

Ex 2: $\mathrm{Discr}(\{\sqrt{d}\times\sqrt{d} \text{ grid}\}) \gg \frac{1}{\sqrt{d}} = \frac{\sqrt{d}}{d}$.



Ex 3 **: $\mathrm{Discr}(\text{uniformly sampled}) \approx d^{-\frac{1}{2}+o(1)}$.

Thm: (Schmidt '70s): Any $\{z_j\}_{j=1}^d$ has $\mathrm{Discr}(\{z_j\}) > \frac{1}{100}\frac{\log d}{d}$.

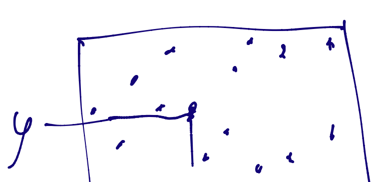
Quasi-Monte Carlo integration: Don't sample at random, try to minimize Discr

---

70s: pseudorandom Number Generators. Deterministic functions that "behave" like random ones.

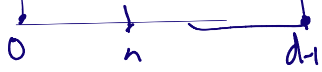
Linear Congruential PNG: $x \mapsto \overset{\text{multiplier}}{b}x + \overset{\text{shift}}{c} \ (\mathrm{mod}\ \overset{\text{modulus}}{d})$.

Eg: $x_0 = 1,\ c = 0,\ x_n = b^n \ (\mathrm{mod}\ d)$.



If ...

If d = prime & b = root mod d



$n \mapsto b^n \bmod d$

$b^{d-1} \equiv 1 \pmod d$.

"Randomness" of this graph $\longleftrightarrow$ $\forall y\ \exists n$ s.t. $y \equiv b^n \pmod d$. Which n??

Discrete log "HARD".

Get to see $x_0, x_1, x_2, x_3, \dots$ Can we "guess" value of x_{n+1}

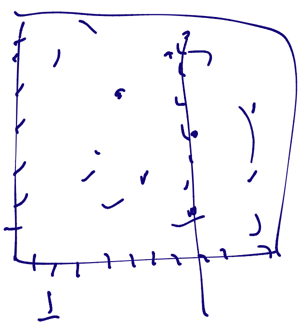
Knowing values of $x_0, \dots, x_n$?

Statistical test: Serial correlation of pairs $(\overset{b^0}{x_0}, \overset{b^1}{x_1}), (x_1, x_2), (\overset{b^2}{x_2}, \overset{b^3}{x_3}), \dots$

Same as $\{(y, by) \mid y \in \mathbb{Z}/d\}$.

Ex5: plot ↗ for $d = 10037$ (prime), $b = 4217$ (Ex4: is a root mod)

$\frac{1}{d}$

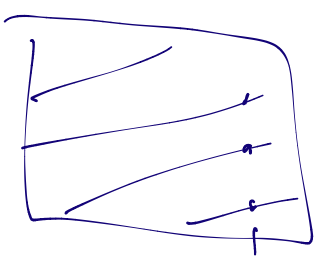


$\frac{1}{d}$

d^2 choices of dots, place only d points.

Very well distributed. ← Discr log!

Ex6: same for $d = 10037$ & $b = 4015$.



x_n

Knowing x_n gives a $1:4$ chance of where x_{n+1} will be!!

Problem 1: Find good $(\{z_i\})$ for

Numerical integration

Problem 2: Find good moduli d & multipliers b for PNGs.

"Solved" by Zaremba 1971: $1 \le b < d$

Thm (Zaremba) Let $(b, d) = 1$, then

$$\mathrm{Discr}\left(\left\{\frac{y}{d}, \frac{by}{d} \bmod 1\right\}\right) \le A \cdot \boxed{\frac{\log d}{d}},$$

where if

$$\frac{b}{d} = 0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \cfrac{1}{a_\ell}}} = [a_1, a_2, \ldots, a_\ell]$$

"partial quotients"

then $\underline{A = \max a_i\left(\frac{b}{d}\right)}$.

1's, 2's

Ex 7: $\frac{4217}{10{,}037} = [\_\_\ \_\_\ \_\_\ \_\_]$

4215

Bad sequence $\longrightarrow \frac{4015}{\underbrace{10{,}037}} = [2, 2, \underbrace{2007}]$.

"large partial quotient"

Conj (Zaremba '71): $\exists\, A\ (=5?)$ s.t.

$\forall d \geq 1$, $\exists\, (b, d) = 1$ s.t. $\frac{b}{d} = [a_1, \ldots, a_\ell]$

has $a_j \leq A\ (\forall j)$.

Ex 8: If $A = 4$, look at too big

$d = 6$, $b = \begin{cases} 1 & \frac{b}{d} = \frac{1}{6} = [6] \\ 5, & \frac{b}{d} = \frac{5}{6} = \underline{\qquad} ? \end{cases}$

Other d with $A = 4 \Rightarrow \{b\} = \emptyset$?

I.e., make all ctd fractions

$[a_1, a_2, \ldots, a_\ell] = \frac{b}{d}$ from $a_j \in \{1, \ldots, 5\}$

Does every d occur? — Huang, Kontorovich

Thm (Bourgain–K '14): With $A = 5$,

100% of d do occur.

i.e. $\frac{\#\{d < x \mid \text{occur}\}}{x} \to 1$.

McMullen's Classical Arithmetic Chaos Conj:

$\exists\, c > 1$ s.t.

$$\#\Big\{\underbrace{\overline{[a_0; a_1, a_2, \ldots, a_\ell]}}_{} = a_0 + \frac{1}{a_1 + \cdots \frac{1}{a_\ell + \frac{1}{a_0 + \cdots}}} \in \mathbb{Q}(\sqrt{5}) \;\Big|\; a_j \le 5\Big\} \ge c^\ell.$$

Total # possible values 5^ℓ

Ex: $\{\overline{1, 1, 1, 1 \ldots}\} = \frac{1+\sqrt{5}}{2}$.

Sieves "Beyond Expansion"

$\boxed{\text{Einsiedler – Lindenstrauss – Michel – Venkatesh}}$

§ Thin Orbits.

<u>Ex 10:</u> If $\frac{b}{d} = [0, a_1, a_2, \dots, a_\ell]$ $\begin{pmatrix} y & x \\ b & d \end{pmatrix}$?

then $\Updownarrow$ $\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_\ell & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$

<u>Ex 11:</u> If $\alpha = [a_0; \overline{a_1, a_2, \dots, a_\ell}] \in \mathbb{Q}(\sqrt{D})$.

then $\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_\ell & 1 \\ 1 & 0 \end{pmatrix} = \gamma$, $\boxed{\det \gamma = (-1)^{\ell+1}}$

$$\underline{\operatorname{tr}^2 \gamma} \pm 4 = D \cdot s^2.$$

Let $\Gamma_A = \left\langle \begin{pmatrix} a & 1 \\ 1 & 0 \end{pmatrix} : a \le A \right\rangle^+$

$\Rightarrow$ <u>Zaremba's</u> is map $\Gamma_A \to \mathbb{N} : \gamma \mapsto \gamma_{1,1}$ onto?.

<u>McMullen's</u> is map $\Gamma_A \to \mathbb{N} : \gamma \mapsto \underline{\operatorname{tr} \gamma}$ <u>onto?</u>.

Will need Expanders.

Ex 12*: $(SL_2 \cap \Gamma_A) \bmod q = SL_2(\mathbb{Z}/q)\ \forall q$?!

"strong approx"

Full ~~local-global~~ local-global K'19 "Soddy sphere packing",