Mixing in groups

2021 11

Emanuele Viola

NEU

Based on joint works with Timothy Gowers

Outline

- **Quasirandom groups, mixing**
- Applications of quasirandom groups
- Interleaved groups products
- Mixing in non-quasirandom groups

- Setup: Group G. All results asymptotic in |G|

  2 independent, high-entropy distributions X, Y over G
  think X, Y uniform on 0.1 |G| elements

- Goal: XY (= X*Y = convolution) nearly uniform over G:

  $|XY - U|_1 \leq \epsilon$ (Statistical distance, aka total variation)

- Setup: Group G. All results asymptotic in |G|

  2 independent, high-entropy distributions X, Y over G
  think X, Y uniform on 0.1 |G| elements

- Goal: XY (= X*Y = convolution) nearly uniform over G:

  $|XY - U|_1 \leq \epsilon$ (Statistical distance, aka total variation)

Obstacles	
$H \subseteq G$, $H \neq G$ dense subgroup	No. X=Y=XY=H

- Setup: Group G. All results asymptotic in |G|

  2 independent, high-entropy distributions X, Y over G
  think X, Y uniform on 0.1 |G| elements

- Goal: XY (= X*Y = convolution) nearly uniform over G:

  $|XY - U|_1 \leq \epsilon$ (Statistical distance, aka total variation)

Obstacles	
$H \subseteq G$, $H \neq G$ dense subgroup	No. X=Y=XY=H
$G = Z_p$ (integers mod p)	No. X=Y={1, 2, …, 0.1p}. X+Y $\subseteq$ {1, 2, …, 0.2 p}

- What about other groups?

Definition/Theorem [Gowers, Babai Nikolov Pyber]:
G is d-quasi-random if every non-trivial irrep has dim $\geq d$
$\Rightarrow$ for every independent X, Y: $|XY - U|_1 \leq |G|\,|X|_2\,|Y|_2/\sqrt{d}$

Notation: $|X|_2^2 = \sum_{g\in G} \Pr[X = g]^2$ = collision probability
X uniform on 0.1 |G| elements, $|X|_2^2 \leq O(1/|G|)$

$$\Rightarrow |XY - U|_1 \leq O\left(\frac{1}{\sqrt{d}}\right)$$

G	d
Abelian	1
Non-abelian, simple	0.5 $\sqrt{}$ log |G|
SL(2,q)	$\|G\|^{1/3}$

Non-abelian Fourier analysis

$$f: G \to \mathbb{C}$$

Fourier inversion: $f(x) = \sum_\rho d_\rho \, tr(\hat{f}_\rho \;\; \rho(x)^T)$,

ρ ranges over irreducible representations

d_ρ dimension of ρ

Fourier coefficient: $\hat{f}_\rho = \mathbb{E}_x \, f(x)\overline{\rho(x)}$

Convolution: $\widehat{f * g}_\rho = |G| \, \hat{f}_\rho \, \hat{g}_\rho$

Parseval: $\mathbb{E} f(x)\overline{g(x)} = \sum_\rho d_\rho \, tr(\hat{f}_\rho \, \hat{g}_\rho^*)$

$$\mathbb{E} f(x)\overline{f(x)} = |G|^{-1} \, |f|_2^2 = \sum_\rho d_\rho \, |\, \hat{f}_\rho \,|^2_{\mathrm{HS}}$$

$|\, M \,|^2_{HS} = \sum_{i,j} M_{i,j}^2$ $\qquad$ $|\, AB \,|_{HS} \leq |A|_{HS} \, |B|_{HS}$

Definition/Theorem [Gowers, Babai Nikolov Pyber]:
G is d-quasi-random if every non-trivial irrep has dim $\geq d$
$\Rightarrow$ for every independent X, Y: $| XY - U |_1 \leq |G| \, |X|_2 \, |Y|_2 / \sqrt{d}$

Proof

$$| X * Y - U |^2_1 \leq |\mathrm{G}| \, | X * Y - U \, |^2_2$$

$$= |\mathrm{G}| \left(|\mathrm{X} * \mathrm{Y}|_2^2 - \frac{1}{|G|^2} \right)$$

$$= |\mathrm{G}|^2 \sum_{\rho \neq 1} d_\rho \, |\widehat{(X * Y)}_\rho \, |^2_{HS} \qquad \text{(Parseval)}$$

$$= |\mathrm{G}|^4 \sum_{\rho \neq 1} d_\rho \, |\hat{X}_\rho \ \hat{Y}_\rho \, |^2_{HS}$$

$$\leq |\mathrm{G}|^4 \sum_{\rho \neq 1} d_\rho \, |\hat{X}_\rho \, |^2_{HS} \ |\hat{Y}_\rho \, |^2_{HS}$$

$$\leq |G|^3 \frac{|X|_2^2}{d} \sum_{\rho \neq 1} d_\rho \ |\hat{Y}_\rho \, |^2_{HS} \qquad \text{(Parseval)}$$

$$\leq |G|^2 \frac{|X|_2^2}{d} |Y|_2^2 \qquad \text{(Parseval)}$$

Outline

- Quasirandom groups, mixing
- **Applications of quasirandom groups**
- Interleaved groups products
- Mixing in non-quasirandom groups

Applications of quasirandom groups

Theorem: L_∞ mixing in 3 steps: $\left|\Pr[XYZ = 1] - \frac{1}{|G|}\right| \leq \frac{\epsilon}{|G|}$,
X,Y,Z independent, high-entropy

$\Rightarrow$ groups w/out large product-free sets; asked [Babai Sos 85]

Proof:

$$\sum_h \Pr[XY = h] \Pr\left[Z = h^{-1}\right] - 1/|G| =$$

$$\sum_h \Pr[XY = h] \left(\Pr\left[Z = h^{-1}\right] - 1/|G|\right) =$$

$$\leq |XY|_2 \quad |\, Z - U\,|_2$$

$$\leq \frac{1}{\sqrt{|G|d}} \frac{1}{\sqrt{|G|}}$$

Applications of quasirandom groups

- Theorem [Mixing of three-term progressions g, gh, gh^2]

For any $H \subseteq G$: $\Pr_{g,h \in G}[g \in H, gh \in H, gh^2 \in H] = \left(\frac{|H|}{|G|}\right)^3 \pm \epsilon$

- Tao: SL(2,q), complicated
- Peluse: Simple groups, complicated
- Just out: Bhangale, Harsha, Roy:
  Any quasi-random group
  What I call a “norm-al” proof:
  Just use norms, Cauchy-Schwarz, triangle inequality, etc.

Applications of quasirandom groups

- Theorem: [Corners]
  Any dense $H \subseteq G^2$ contains corner { (x,y), (xz,y), (x,zy) }

- Ajtai-Szemeredi G = $\mathbb{Z}$

- Austin: Any quasirandom group
  exponential loss in parameters

- Polynomial loss ⇒ breakthrough in communication complexity

Outline

- Quasirandom groups, mixing
- Applications of quasirandom groups
- **Interleaved groups products**
- Mixing in non-quasirandom groups

- What if there are dependencies?

  A, A' dependent, (A, A') uniform over ≥ 0.1 $|G|^2$ elements

  Y independent, uniform over ≥ 0.1 |G| elements of G

- Is A•Y•A' nearly uniform? ($\forall g \; |Pr[A \bullet Y \bullet A' = g] - 1/|G| \; | \leq \varepsilon/|G|$)

- What if there are dependencies?

A, A' dependent, (A, A') uniform over ≥ 0.1 $|G|^2$ elements

Y independent, uniform over ≥ 0.1 |G| elements of G

- Is A•Y•A' nearly uniform? ($\forall g \; |Pr[A \bullet Y \bullet A' = g] - 1/|G| \; | \leq \varepsilon/|G|$)

No: Y uniform over 0.5 |G| elements
A uniform over G
A' uniform over G - Support$(Y)^{-1}$ A^{-1}

(A, A') uniform over 0.5 $|G|^2$ element

$A \bullet Y \bullet A' \neq 1_G$

Interleaved mix:[Gowers V.] $G = SL(2, q)$

(A, A'), (B, B') uniform over $\geq 0.1\ |G|^2$ elements of G^2

(A, A') independent from (B, B')

$\forall\ g,\ |\ \Pr[A \bullet B \bullet A' \bullet B' = g] - 1/|G|\ |\ \leq 1/|G|^{1+\Omega(1)}$

- $\Rightarrow$ $A \bullet B \bullet A' \bullet B'$ is $1/\text{poly}(|G|)$-close to uniform in statistical dist.
-

Interleaved mix:[Gowers V.] $G = SL(2, q)$

(A, A'), (B, B') uniform over $\geq 0.1\ |G|^2$ elements of G^2

(A, A') independent from (B, B')

$\forall\ g,\ |\ \Pr[A \bullet B \bullet A' \bullet B' = g] - 1/|G|\ |\ \leq 1/|G|^{1+\Omega(1)}$

- $\Rightarrow$ $A \bullet B \bullet A' \bullet B'$ is $1/\text{poly}(|G|)$-close to uniform in statistical dist.
- $\Rightarrow$ X • Y • Z result [G,BNP] for G=SL(2,q)
- Also non-trivial bounds for any non-abelian simple group

Longer mix: [Gowers V.] $G = SL(2, q)$

$A=(A_1,\ldots,A_t)$, $B=(B_1,\ldots,B_t)$ uniform over $\geq 0.1\ |G|^t$ elements

A independent from B

$\forall\ g,\ |\ \Pr[\ \prod_{i \leq t} A_i \bullet B_i = g] - 1/|G|\ | \leq 1/|G|^{1 + \Omega(t)}$

- $\Rightarrow\ \prod_{i \leq t} A_i \bullet B_i$ is $1/|G|^{\Omega(t)}$ close to uniform in statistical dist.

- Generalizes previous result, t = 2

Application of interleaved mixing: Boosting pairwise uniformity

- Lemma Let $G = SL(2,q)$, $s > 100^m$.

Let $D_1, D_2, \ldots, D_s$ be independent distributions on G^m .
In every D_i , every two coordinates uniform over G^2

$\Rightarrow$

$D = D_1 D_2 \bullet \bullet D_s$ close to uniform over G^m :
For any $g \in G^m$, $| \Pr[D = g] - 1/|G|^m | \leq \varepsilon / |G|^m$

Open problem: s = poly(m) suffices?

- Proof of interleaved mixing

Interleaved mix: $G = SL(2, q)$

(A, A'), (B, B') uniform over $\geq 0.1\ |G|^2$ elements of G^2

(A, A') independent from (B, B')

$\forall\ g,\ |\ \Pr[A \bullet B \bullet A' \bullet B' = g] - 1/|G|\ | \leq 1/|G|^{1+\Omega(1)}$

- **$C(g) = U^{-1}gU$** = uniform over conjugacy class of $g \in G$

- Lemma, specific to $G = SL(2,q)$:

With prob. $1-1/|G|^{\Omega(1)}$ over $a, b \in G$, $|C(a)C(b)-U|_1 \leq 1/|G|^{\Omega(1)}$

- Claim, for any G: Main lemma $\Rightarrow$ interleaved mixing

Claim: W.h.p. over $a,b \in G$, $|C(a)C(b) - U| \leq 1/|G|^{\Omega(1)}$

$\Rightarrow$ $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G|| \leq 1/|G|^{1+\Omega(1)}$

if (A, A'), (B, B') i.i.d, uniform over $S \subseteq G^2$. $|S| = \alpha |G|^2$

Proof: $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G||$

Claim: W.h.p. over $a,b \in G$, $|C(a)C(b) - U| \le 1/|G|^{\Omega(1)}$

$\Rightarrow$ $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G|| \le 1/|G|^{1+\Omega(1)}$

if (A, A'), (B, B') i.i.d, uniform over $S \subseteq G^2$. $|S| = \alpha |G|^2$

Proof: $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G||$

$= |E_{u,v,u',v': uvu'v'=1} S(u,u') S(v,v') - \alpha^2 | 1/(\alpha^2 |G|)$ Bayes

Claim: W.h.p. over $a,b \in G$, $|C(a)C(b) - U| \le 1/|G|^{\Omega(1)}$

$\Rightarrow$ $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G|| \le 1/|G|^{1+\Omega(1)}$

if (A, A'), (B, B') i.i.d, uniform over $S \subseteq G^2$. $|S| = \alpha |G|^2$

Proof: $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G||$

$= \underbrace{|E_{u,v,u',v':\, uvu'v'=1}\, S(u,u')\, S(v,v') - \alpha^2|}\, 1/(\alpha^2 |G|)$ Bayes

$E_{v,v'}\ [\, E_{u,\, u' :\, uvu'v'=1}\, (S(u,u') - \alpha)] \bullet S(v,v')$

Claim: W.h.p. over $a,b \in G$, $|C(a)C(b) - U| \le 1/|G|^{\Omega(1)}$

$\Rightarrow$ $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G|| \le 1/|G|^{1+\Omega(1)}$

if (A, A'), (B, B') i.i.d, uniform over $S \subseteq G^2$. $|S| = \alpha |G|^2$

Proof: $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G||$

$= |E_{u,v,u',v': uvu'v'=1} S(u,u') S(v,v') - \alpha^2| \; 1/(\alpha^2 |G|)$ Bayes

$E_{v,v'} [E_{u, u' : uvu'v'=1} (S(u,u') - \alpha)] \bullet S(v,v')$

$\le \sqrt{[E_{v,v'} E^2_{u,u': uvu'v'=1} S(u,u') - \alpha^2]} \sqrt{\alpha}$ Cauchy-Schwarz

Claim: W.h.p. over $a,b \in G$, $|C(a)C(b) - U| \le 1/|G|^{\Omega(1)}$

$\Rightarrow$ $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G|| \le 1/|G|^{1+\Omega(1)}$

if (A, A'), (B, B') i.i.d, uniform over $S \subseteq G^2$. $|S| = \alpha |G|^2$

Proof: $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G||$

$= \underbrace{|E_{u,v,u',v':\, uvu'v'=1} S(u,u') S(v,v') - \alpha^2|}\, 1/(\alpha^2 |G|)$ Bayes

$E_{v,v'} [E_{u,\, u' :\, uvu'v'=1} (S(u,u') - \alpha)] \bullet S(v,v')$

$\le \sqrt{[\underbrace{E_{v,v'} E^2_{u,u':\, uvu'v'=1} S(u,u')}} - \alpha^2] \sqrt{\alpha}$ Cauchy-Schwarz

$E_{v,\, u,u',\, x,\, x' :\, uvu' = xvx'} S(u,u') S(x,x')$

Claim: W.h.p. over $a,b \in G$, $|C(a)C(b) - U| \le 1/|G|^{\Omega(1)}$

$\Rightarrow$ $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G|| \le 1/|G|^{1+\Omega(1)}$

if (A, A'), (B, B') i.i.d, uniform over $S \subseteq G^2$. $|S| = \alpha |G|^2$

Proof: $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G||$

$= |\underbrace{E_{u,v,u',v': uvu'v'=1} S(u,u') S(v,v') - \alpha^2}| \, 1/(\alpha^2 |G|)$ Bayes

$E_{v,v'} [E_{u, u' : uvu'v'=1} (S(u,u') - \alpha)] \bullet S(v,v')$

$\le \sqrt{[\underbrace{E_{v,v'} E^2_{u,u': uvu'v'=1} S(u,u')}} - \alpha^2] \sqrt{\alpha}$ Cauchy-Schwarz

$E_{v, u,u', x, x' : uvu' = xvx'} S(u,u') S(x,x')$

$= E S(u,u') S(ux, u' C(x))$. $\rightarrow$ $x' = v^{-1}x^{-1}uvu'$

Claim: W.h.p. over $a,b \in G$, $|C(a)C(b) - U| \le 1/|G|^{\Omega(1)}$

$\Rightarrow$ $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G|| \le 1/|G|^{1+\Omega(1)}$

if (A, A'), (B, B') i.i.d, uniform over $S \subseteq G^2$. $|S| = \alpha |G|^2$

Proof: $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G||$

$= |E_{u,v,u',v': uvu'v'=1} S(u,u') S(v,v') - \alpha^2| \, 1/(\alpha^2 |G|)$ Bayes

$E_{v,v'} [E_{u, u' : uvu'v'=1} (S(u,u') - \alpha)] \bullet S(v,v')$

$\le \sqrt{[E_{v,v'} E^2_{u,u': uvu'v'=1} S(u,u') - \alpha^2]} \sqrt{\alpha}$ Cauchy-Schwarz

$E_{v, u,u', x, x' : uvu' = xvx'} S(u,u') S(x,x')$

$= E\, S(u,u') S(ux, u' C(x))$.

$x' = v^{-1}x^{-1}uvu'$

$(u,u') \to (ux, u' C(x))$ hits like $(u,u') \to (u\,x\,y, u' C(x) C(y))$ □

- Lemma: $G = SL(2, q)$

With prob. $1-1/|G|^{\Omega(1)}$ over $a, b \in G$, $|C(a)C(b)-U|_1 \leq 1/|G|^{\Omega(1)}$

- Large literature on products of conjugacy classes.
- Actually for all other results need a stronger condition (For $a \in G$, the distribution $C(ab^{-1})C(b)$ for uniform b is close to uniform in 2-norm)
- The proof we show gives the stronger condition

- Lemma: G = SL(2, q)

With prob. $1-1/|G|^{\Omega(1)}$ over a, b ∈ G, $|C(a)C(b)-U|_1 \leq 1/|G|^{\Omega(1)}$

- Observation: for every a, b: C(a)C(b) = C(C(a) C(b)) .

Proof: $U^{-1}aU\ V^{-1}bV = W^{-1}\ U^{-1}\ a\ U\ W\ W^{-1}\ V^{-1}\ b\ V\ W$ □

- Suffices to show C(a) C(b) hits every class with right prob.

- SL(2,q)= group of 2 x 2 matrices over F_q with determinant 1

a_1	a_2
a_3	a_4

: $a_1a_4 - a_2a_3 = 1$

- $q^3 - q$ elements. $q+O(1)$ conjugacy classes

All but O(1) classes have size = $q^2 + \Theta(q)$

- Uniform element ⇒ uniform class

- Almost 1-1 correspondence between classes and

Trace

a_1	a_2
a_3	a_4

$= a_1 + a_4 \in F_q$, invariant under conjugation

- Show: a, b typical ⇒ $|\text{Trace } C(a)C(b) - U_q|_1 \leq 1/q^{\Omega(1)}$

- Show: a, b typical $\Rightarrow$ |Trace C(a)C(b) - U_q $|_1 \leq 1/q^{\Omega(1)}$

- Proof

Trace C(a)C(b) = Trace a C(b)

= Trace $\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix}^{-1} \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix}$

= polynomial in u_1 , u_2 , u_3 , u_4 subject to $u_1 u_4 - u_2 u_3 = 1$

Conclude with elementary algebraic geometry.

- Another open problem in interleaved mixing

Recap: For every group

(1) Interleaved mixing | Pr[A•B•A'•B' = 1] - 1/|G| | small

(2) “Hitting” of random walk (u,u') → (ux, u' C(x)) in G^2

(1) W.h.p. over a,b ∈ G, |C(a)C(b) - U| ≤ $1/|G|^{\Omega(1)}$

Can prove: (3) true for every non-abelian simple group

(3) false for quasi-random group $G = H^m$

Question: Do (1), (2) hold for every quasi-random group?

What about $G = H^m$?

Outline

- Quasirandom groups, mixing
- Applications of quasirandom groups
- Interleaved groups products
- Mixing in non-quasirandom groups

Types of groups

- Not mixing (e.g., abelian)
  ∃ X, Y independent, high-entropy, distributions over group:
  XY far from uniform

- Quasirandom groups (e.g. $SL(2,q)$)
  ∀ X, Y as above:
  XY close to uniform

- Next: Somewhat random groups
  ∀ X, Y as above:
  XY gets “closer” to uniform

- Definition: G mixes via distribution $F: G \to G$ if
  (1) $\forall\, x,\ F(x) \neq x$ often
  (2) $\forall$ independent, high-entropy distributions X, Y:
  $|XY - F(XY)|_1 \leq \epsilon$ "invariant under F"

- Sufficient for application to communication complexity
- Abelian/Almost abelian groups don't mix (not obvious)
- G quasirandom ⇒ can take F random function
- Next: mixing in various groups "in-between"

- Definition: G mixes via distribution $F: G \to G$ if
  (1) $\forall\ x,\ F(x) \neq x$ often
  (2) $\forall$ independent, high-entropy distributions X, Y:
  $|XY - F(XY)|_1 \leq \epsilon$ "invariant under F"

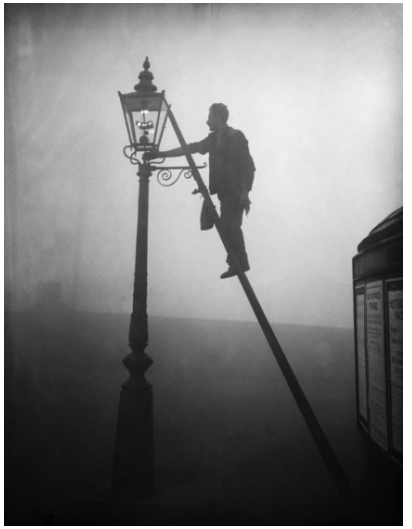
- Example 1:

Affine group: Matrices $\begin{pmatrix} a_1 & a_2 \\ 0 & 1 \end{pmatrix}$ over $\mathbb{F}_q$ with $a_1 \neq 0$

Can take F($\begin{pmatrix} x_1 & x_2 \\ 0 & 1 \end{pmatrix}$) := $\begin{pmatrix} x_1 & U \\ 0 & 1 \end{pmatrix}$, U uniform

Strongest possible: can't change x_1

- Definition: G mixes via distribution $F: G \to G$ if
  (1) $\forall\ x,\ F(x) \neq x$ often
  (2) $\forall$ independent, high-entropy distributions X, Y:
  $|\ XY\ - F(XY)|_1 \leq \epsilon$ "invariant under F"



- Example 2:

Finite lamplighter group $\mathbb{Z}_2 \wr \mathbb{Z}_n$

Elements: $(x1, x2, \ldots, xn; s), x_i \in \mathbb{Z}_2\ , s \in \mathbb{Z}_n$
Operation: shift $(x1, x2, \ldots, xn)$ by s then sum coordinates

For n prime, take $F(x1, x2, \ldots, xn; s) := (y1, y2, \ldots, yn; s)$
for uniform $(y1, y2, \ldots, yn) : \sum_i y_i = \sum_i x_i \ mod\ 2$

Strongest possible: Can't change $\sum_i x_i \ mod\ 2$ or s

- Definition: G mixes via distribution $F: G \to G$ if
  (1) $\forall\ x,\ F(x) \neq x$ often
  (2) $\forall$ independent, high-entropy distributions X, Y:
  $|\ XY\ - F(XY)|_1 \leq \epsilon$ "invariant under F"

- Example 3:

$G = H^n$, H not abelian (can think $|H| = O(1)$)

$F(h1, h2, \ldots, hn) := (h1, h2, \ldots, C(h_I), \ldots, hn)$
uniform coordinate I, uniform conjugate $C(h_I)$ of h_I

If H has no 1-dimensional representation, can set h_I to U

Open problem: error $\geq 1/n$ (choice of I)

- Definition: G mixes via distribution $F: G \to G$ if
  (1) $\forall\, x,\ F(x) \neq x$ often
  (2) $\forall$ independent, high-entropy distributions X, Y:
  $|\, XY\ - F(XY)|_1 \leq \epsilon$ "invariant under F"

- Open problem: Characterize groups that mix

- Definition: G mixes via distribution $F: G \to G$ if
  (1) $\forall\, x,\ F(x) \neq x$ often
  (2) $\forall$ independent, high-entropy distributions X, Y:
  $|\, XY\ - F(XY)|_1 \leq \epsilon$ "invariant under F"

- Open problem: Characterize groups that mix

- Question/conjecture
  G mixes $\Leftrightarrow$ has some irrep of large dimension ?

- Proof ($\Rightarrow$)
  All irreps have dim O(1) $\Leftrightarrow$ abelian subgroup of index O(1)
  $\Rightarrow$ does not mix
  Does converse hold?

- Proof of mixing via F

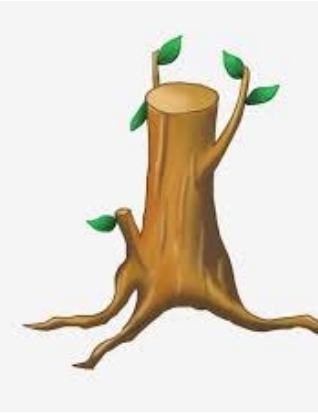
- Lemma: Can approximate XY by coefficients with small sum of dimensions

- Norm-al proof (Parseval, Cauchy-Schwarz, …):

$$f(g) := \mathbb{P}[XY = g] = \sum_\rho d_\rho \, tr(\hat{f}_\rho \ \rho(g)^T)$$

$R := \{\rho : \left|\hat{X}_\rho\right|_{HS} \geq \theta/|G|\}$, "heavy" coefficients

TrunKation $K(x) := \sum_{\rho \in R} d_\rho \, tr(\hat{f}_\rho \ \rho(x)^T)$



$|f - K|_1 \leq O(\theta)$ if Y high entropy

$\sum_{\rho \in R} d_\rho \leq O\left(\frac{1}{\theta^2}\right)$ if X high entropy

QED

Kernel method

- Theorem:
  If $h \in G$ is in kernel of every irrep of dim $\leq d$
  Then mix via $F(g) := hg$, error $d^{-\Omega(1)}$

- Proof:
  Approximate XY by K with coeffs of dim $\leq d$

$$|XY - F(XY)|_1 \leq$$
$$|XY - K_{XY}| \quad \text{Small by lemma}$$
$$+|F(XY) - K_{hXY}| \quad \text{Small by lemma}$$
$$+|K_{XY} - K_{hXY}| \quad \text{Zero because}$$
$$\rho(hg) = \rho(h)\rho(g) = \rho(g)$$

QED

Applying kernel method

- Affine group: Matrices $\begin{pmatrix} a_1 & a_2 \\ 0 & 1 \end{pmatrix}$ over $\mathbb{F}_q$ with $a_1 \neq 0$
  - $q-1$ irreps of dim 1: $\chi(a_1)$
  - 1 irrep of dim $q-1$
- $\Rightarrow$ for rep ρ of dim $< q-1$: $\rho\left(\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}\right) = 1$
- Lamplighter group:
  Representations related to orbits of vectors $\in \mathbb{Z}_2^n$
  Show vectors with period t are in space of dim t

Product groups $G = H^n$

- Cannot use kernel method. Instead:
- Irrep ρ of H^n = tensor of irreps of H, dimensions multiply

Product groups $G = H^n$

- Cannot use kernel method. Instead:
- Irrep ρ of H^n = tensor of irreps of H, dimensions multiply
- $\Rightarrow \rho = \rho' \cdot \prod \rho_i$ where ρ_i have dimension 1, ρ' depends on $\leq \log d_\rho$ coordinates
- Approximation $\Rightarrow d_\rho$ small $\Rightarrow \rho'$ depends on few coords
- Mix via $F(h1, h2, \ldots, hn) := (h1, h2, \ldots, C(h_I), \ldots, hn)$
  $\mathbb{P}[\rho'$ depends on $I]$ small; $\rho_i\big(C(g)\big) = \rho_i(g)$

Outline

- Quasirandom groups, mixing
- Applications of quasirandom groups
- Interleaved groups products
- Mixing in non-quasirandom groups