Interleaved products in special linear groups

October 2014

Emanuele Viola

Northeastern & Harvard University

Joint work with Timothy Gowers

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

  k high-entropy distributions X_i over G

  independent, later dependent

- Goal: $D := \prod_{i \le k} X_i$ nearly uniform over G:

  $\forall g \in G : | \Pr[D = g] - 1/|G| | \le \varepsilon / |G|$ (L_∞ bound)

  ➔ D is ε-close to uniform in statistical distance

- Applications: Group theory, communication complexity

- Warm-up: X, Y distributions over G.

  Independent

  X, Y uniform over 0.1|G| elements of G

- Question: Is X•Y nearly uniform over |G|?

  $\forall$ g $\in$ G, | Pr[X•Y = g] - 1/|G| | ≤ ε / |G| ?

- Answer: ?

- Warm-up: X, Y distributions over G.

  Independent

  X, Y uniform over 0.1|G| elements of G

- Question: Is X•Y nearly uniform over |G|?

$$\forall g \in G, | \Pr[X \bullet Y = g] - 1/|G| | \leq \varepsilon / |G| \quad ?$$

- Answer: No. $Y := G - X^{-1}$. Then $1_G \notin \text{Support}(X \bullet Y)$

- Warm-up 2: X, Y, Z independent,
  uniform over ≥ 0.1 |G| elements of G

- Question: ∀ g, | Pr[X•Y•Z=g] - 1/|G| | ≤ ε/|G| ?

- Answer: ?

- Warm-up 2: X, Y, Z independent,
  uniform over $\geq 0.1\,|G|$ elements of G

- Question: $\forall g,\ |\ \Pr[X \bullet Y \bullet Z = g] - 1/|G|\ | \leq \epsilon/|G|$?

- Answer: Depends on the group.

Obstacles

- Warm-up 2: X, Y, Z independent,
  uniform over ≥ 0.1 |G| elements of G

- Question: ∀ g, | Pr[X•Y•Z=g] - 1/|G| | ≤ ε/|G| ?

- Answer: Depends on the group.

Obstacles	
H ⊆ G, H ≠ G dense subgroup	No. X=Y=Z=X•Y•Z=H

- Warm-up 2: X, Y, Z independent,
  uniform over ≥ 0.1 |G| elements of G

- Question: $\forall$ g, | Pr[X•Y•Z=g] - 1/|G| | ≤ ε/|G| ?

- Answer: Depends on the group.

Obstacles	
H ⊆ G, H ≠ G dense subgroup	No. X=Y=Z=X•Y•Z=H
G = Z_p (integers mod p)	No. X=Y=Z={1, 2, …, 0.1p}. X+Y+Z ⊆ {1, 2, …, 0.3 p} ≠ G

- What about other groups?

Mixing in 3 steps: [Gowers '06, Babai Nikolov Pyber]
X, Y, Z independent, uniform over ≥ 0.1 |G| elements of G

$\forall g$, $| \Pr[X \cdot Y \cdot Z = g] - 1/|G| \,| \le |X|_2 |Y|_2 |Z|_2 \sqrt{|G|}/\sqrt{d} \le O(d^{-1/2})/|G|$

d = minimum dimension of non-trivial representation of G

Representation theory, generalization of Fourier analysis.

Sounds hard?

Mixing in 3 steps: [Gowers '06, Babai Nikolov Pyber]
X, Y, Z independent, uniform over ≥ 0.1 |G| elements of G

$\forall g$, $| \Pr[X \bullet Y \bullet Z = g] - 1/|G| \, | \le |X|_2 |Y|_2 |Z|_2 \sqrt{|G|}/\sqrt{d} \le O(d^{-1/2})/|G|$

d = minimum dimension of non-trivial representation of G

Representation theory, generalization of Fourier analysis.

Sounds hard? Don't worry, we'll get rid of it.*

*For some groups, with possibly worse constants

Mixing in 3 steps: [Gowers '06, Babai Nikolov Pyber]

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

$\forall g$, $| \Pr[X \cdot Y \cdot Z = g] - 1/|G| | \le |X|_2 |Y|_2 |Z|_2 \sqrt{|G|} / \sqrt{d} \le O(d^{-1/2})/|G|$

d = minimum dimension of non-trivial representation of G

G	d
Abelian	1

Mixing in 3 steps: [Gowers '06, Babai Nikolov Pyber]

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

$\forall g, \ | \Pr[X \cdot Y \cdot Z = g] - 1/|G| \ | \leq |X|_2 |Y|_2 |Z|_2 \sqrt{|G|}/\sqrt{d} \leq O(d^{-1/2})/|G|$

d = minimum dimension of non-trivial representation of G

G	d
Abelian	1
Non-abelian, simple	0.5 log |G|

Mixing in 3 steps: [Gowers '06, Babai Nikolov Pyber]

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

$\forall g$, $| \Pr[X \bullet Y \bullet Z = g] - 1/|G| | \le |X|_2 |Y|_2 |Z|_2 \sqrt{|G|}/\sqrt{d} \le O(d^{-1/2})/|G|$

d = minimum dimension of non-trivial representation of G

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

SL(2,q) = 2x2 matrices over F_q with determinant 1

G=SL(2,q) ➔ X•Y•Z is 1/poly(|G|) close to uniform

- What if there are dependencies?

Is A•Y•A' nearly uniform: $\forall$ g, | Pr[A•Y•A'=g] - 1/|G| | $\leq$ ε/|G|

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

Y independent, uniform over $\geq$ 0.1 |G| elements of G

- Answer: ?

- What if there are dependencies?

Is $A \cdot Y \cdot A'$ nearly uniform: $\forall\, g,\ |\ \Pr[A \cdot Y \cdot A' = g] - 1/|G|\ | \le \varepsilon/|G|$

if A, A' dependent, (A, A') uniform over $\ge 0.1\ |G|^2$ elements

Y independent, uniform over $\ge 0.1\ |G|$ elements of G

- Answer: No.

Any Y over 0.5 |G| elements
A uniform over G. Given A, define A' as $G - Y^{-1} A^{-1}$

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

$A \cdot Y \cdot A' \ne 1$

Interleaved mix: [Gowers V.] G = SL(2, p), p prime =3 mod 4

(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•B•A'•B' = g] - 1/|G| | $\leq 1/|G|^{1+\Omega(1)}$

- ➔ A•B•A'•B' is 1/poly(|G|)-close to uniform in statistical dist.
-

Interleaved mix: [Gowers V.] $G = SL(2, p)$, p prime $=3 \bmod 4$

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

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

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

- ➔ $A \cdot B \cdot A' \cdot B'$ is $1/\text{poly}(|G|)$-close to uniform in statistical dist.
- ➔ $X \cdot Y \cdot Z$ result [G,BNP] – $G=SL(2,p)$, up to $\Omega(1)$
- Two proofs, one w/out representation theory, w/ Weil bound
- Conjecture: similar bounds for all (almost) simple groups

Longer mix: [Gowers V.] $G = SL(2, p)$, p prime $=3 \bmod 4$

$A=(A_1,\ldots,A_n)$, $B=(B_1,\ldots,B_n)$ uniform over $\geq 0.1\ |G|^n$ elements

A independent from B

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

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

- Generalizes previous result, $n = 2$

- Only one proof, w/out representation theory, w/ Weil bound

- Communication complexity.

Alice: $(A_1, A_2, \ldots, A_n) \in G^n$

Bob: $(B_1, B_2, \ldots, B_n) \in G^n$

Want to tell $\prod_{i \leq n} A_i \cdot B_i = g$ from $\prod_{i \leq n} A_i \cdot B_i = h$

- G abelian ➔ communication = 2

- Same as previous: $G=SL(2,p)$ ➔ communication $\Omega(n \log|G|)$ even public-coin protocols with advantage $1/|G|^{cn}$

- Reduction from IP ➔ $\Omega(n)$ lower bound. Nothing for n = 2.

- Such bounds that “grow with |G|” asked in [Miles V. '13].

Proof of interleaved mixing

A • B • A' • B'

Interleaved mix: $G = SL(2, p)$, p prime $= 3 \mod 4$

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

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

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

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

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

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 ➔ interleaved mixing

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

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

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

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

$=$

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

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

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

$\leq$

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

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

Bayes

$$\underbrace{}$$

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

Cauchy-Schwarz

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

$$\underbrace{}$$

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

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

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

Cauchy-Schwarz

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

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

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

$(u,u') \rightarrow (ux,\, u'C(x))$ hits like $(u,u') \rightarrow (u\, x\, y,\, u'\, C(x)\, C(y))$ ■

- Main Lemma: G = SL(2, p), p prime =3 mod 4

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.
  For SL(2,q) see [Adan-Bante Harris]

  Shortcomings:

  1) Focus on worst-case a, b. Insufficient for main lemma.

  2) Focus on Support(C(a)C(b)). We need statistical.

- Main Lemma: $G = SL(2, p)$, p prime =3 mod 4

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

- 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

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} : ad - bc = 1$$

- $q^3 - q$ elements. q+4 conjugacy classes, sizes $\leq q^2 + q$
  Uniform element ➔ uniform class

- q - 2 “typical” classes (q prime =3 mod 4)

$$\begin{vmatrix} r & 0 \\ 0 & r^{-1} \end{vmatrix} \qquad \begin{vmatrix} r & s \\ -s & r \end{vmatrix} : r^2 + s^2 = 1$$

- Almost 1-1 correspondence between classes and

$$\text{Trace} \begin{vmatrix} a & b \\ c & d \end{vmatrix} = a + d \in F_q$$, 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 $\Rightarrow$ $|\text{Trace } C(a)C(b) - U_q|_1 \leq 1/q^{\Omega(1)}$

- Proof of stronger:

Trace a C(b)

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

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

$u_4 = (1+u_2 u_3)/u_1$, multiply by u_1^4 $\Rightarrow$ polynomial $t(x,y,z)$

Need: $| t(x, y, z) - U_q |_1 \leq 1/q^{\Omega(1)}$ for uniform x, y, z

Need: $| t(x, y, z) - U_q |_1 \leq 1/q^{\Omega(1)}$ for uniform x, y, z

- **Lemma:** [Weil, Lang Weil '54]
  f(x, y, z) irreducible over any field extension, low-degree

  $\Rightarrow | \Pr_{x, y, z} [f(x, y, z) = 0] - 1/q | \leq O(1/q^{1.5})$

- Prove for q-2 values $D \in F_q$, t(x, y, z) - D irreducible.
  Just use information on zero/non-zero coefficients

- Sum over D, apply Lemma:

  $| t(x, y, z) - U_q |_1 \leq q\, O(1/q^{1.5}) \leq 1/q^{\Omega(1)}$ ∎

Interleaved mix: G = SL(2, p), p prime =3 mod 4

$(A_1,\ldots,A_n) \in G^n$ independent from $(B_1,\ldots,B_n)$. High entropy

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

- ➔ $\prod_{i \le n} A_i \cdot B_i$ is $1/|G|^{\Omega(n)}$ close to uniform in statistical dist.
- ➔ $\Omega(n \log |G|)$ communication to tell $\prod_{i \le n} A_i \cdot B_i$ = g or = h
- ➔ X • Y • Z result [G,BNP] – G=SL(2,p), up to $\Omega(1)$
- Saw proof n = 2, w/out represent. theory. C(a)C(b) uniform.
- **Conjecture:** Similar bounds for any (almost) simple group.

End of talk

Next: deleted scenes

Mixing in 4 steps implies mixing in 3:

$\forall$ X, Y, Z, W, g : $| \Pr[X \bullet Y \bullet Z \bullet W = g] - 1/|G| | \leq \varepsilon/|G|$

$\Rightarrow \forall$ X, Y, Z, g : $| \Pr[X \bullet Y \bullet Z = g] - 1/|G| | \leq (\sqrt{\varepsilon})/|G|$

Proof for X=Y=Z:

S := Indicator support(X). u,v,w $\in$ G uniform. $\alpha := E_u S(u)$

$$| \Pr[X \bullet X \bullet X = g] - 1/|G| |^2 =$$

$$= 1/(\alpha^3 |G|) | E_{u,v,w:\ uvw=g} S(u)S(v)S(w) - \alpha^3 |^2 \qquad \text{(Bayes)}$$

$$= 1/(\alpha^3 |G|) | E_u S(u) \bullet (E_{v,w:\ uvw=g} S(v)S(w) - \alpha^2)|^2$$

$$\leq 1/(\alpha^3 |G|) (E_u S(u)) E_u(E_{v,w:\ uvw=g} S(v)S(w) - \alpha^2)^2 \qquad \text{(C.-S.)}$$

$$= 1/(\alpha^2 |G|) E_u E^2_{v,w:\ uvw=g} S(v)S(w) - \alpha^4$$

$$= 1/(\alpha^2 |G|) E_u E_{v,w,v',w':\ uvw=g,\ uv'w'=g} S(v)S(w)S(v')S(w') - \alpha^4$$

$$= 1/(\alpha^2 |G|) E_{v,w,v',w':\ vw=v'w'} S(v)S(w)S(v')S(w') - \alpha^4 \qquad \blacksquare$$