Interleaved group products

October 2017

Emanuele Viola

NEU

Joint work with Timothy Gowers

Interleaved group products

Octo 2017

Multiplicative combinatorics

- 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|?

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

- 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 $1_G \notin \mathrm{Support}(X \bullet Y)$

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

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

- Answer: ?

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

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

- Answer: Depends on the group.

Obstacles

- 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

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

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

- Answer: Depends on the group.

Obstacles	
$H \subseteq G$, $H \neq G$ dense subgroup	No. $X=Y=Z=X \bullet Y \bullet Z=H$
$G = Z_p$ (integers mod p)	No. $X=Y=Z=\{1, 2, \ldots, 0.1p\}$. $X+Y+Z \subseteq \{1, 2, \ldots, 0.3\,p\} \neq G$

- 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

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

d = minimum dimension of non-trivial representation of G

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

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

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

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

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

d = minimum dimension of non-trivial representation of G

G	d
Abelian	1
Non-abelian, simple	$0.5 \sqrt{\log |G|}$

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	$0.5 \sqrt{\log \lvert G \rvert}$
SL(2,q)	$\lvert G \rvert^{1/3}$

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?

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

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

- Is $A \bullet Y \bullet A'$ 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 $\geq 0.1\ |G|^2$ elements

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

- Is $A \bullet Y \bullet A'$ 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')

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

- ➔ $A \cdot B \cdot A' \cdot B'$ is $1/\mathrm{poly}(|G|)$-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')

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

- ➔ $A \bullet B \bullet A' \bullet B'$ is $1/\mathrm{poly}(|G|)$-close to uniform in statistical dist.
- ➔ $X \bullet Y \bullet Z$ result [G,BNP] for $G=SL(2,q)$
  (a proof without representation theory)
- 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, $t = 2$

Outline

- Introduction and our results
- Proof of interleaved mixing
- Communication complexity viewpoint, boosting independence
- Proof of boosting independence

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')

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

- **$C(g) = U^{-1}gU$** = 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 ➔ 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: $|\Pr[A \bullet B \bullet A' \bullet B' = 1] - 1/|G||$

$$= \Big|\underbrace{E_{u,v,u',v' : uvu'v'=1} S(u,u')\, S(v,v') - \alpha^2}_{E_{v,v'} \left[E_{u,\, u' : uvu'v'=1} (S(u,u') - \alpha) \right] \bullet S(v,v')}\Big| \, 1/(\alpha^2 |G|) \qquad \text{Bayes}$$

$\le$

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

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

Bayes

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

Cauchy-
Schwarz

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

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

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

Bayes

Cauchy-Schwarz

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

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

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

$(u,u') \to (ux, u'\, C(x))$ 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 $a, b \in G$, $|C(a)C(b)-U|_1 \le 1/|G|^{\Omega(1)}$

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

- 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. $q+O(1)$ conjugacy classes

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

- Uniform element ➔ uniform class

- Almost 1-1 correspondence between classes and

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

- Proof

Trace C(a)C(b) = 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 g(x,y,z)

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

Need: $| g(x, y, z) - U_q |_1 \leq 1/q^{\Omega(1)}$ 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-O(1) values $s \in F_q$, g(x, y, z) - s irreducible.

- Sum over s, apply Lemma:

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

Outline

- Introduction and our results
- Proof of interleaved mixing
- Communication complexity viewpoint, boosting independence
- Proof of boosting independence

Interleaved products in group G
[Miles V.]

- Alice: a_1 , a_2 , …, $a_t \in$ group G
  Bob: b_1 , b_2 , …, $b_t \in$ group G

- Decide if $a_1\, b_1\, a_2\, b_2 \bullet\bullet\bullet\, a_t\, b_t = 1_G$ or $= h$

Communication complexity:
- G abelian:

Interleaved products in group G
[Miles V.]

- Alice: a_1 , a_2 , …, $a_t \in$ group G

  Bob: b_1 , b_2 , …, $b_t \in$ group G

- Decide if $a_1\, b_1\, a_2\, b_2 \cdots a_t\, b_t = 1_G$ or $= h$

Communication complexity:

- G abelian: O(1) Equality

- G non-solvable:

Interleaved products in group G
[Miles V.]

- Alice: $a_1 , a_2 , \ldots, a_t \in$ group G
  Bob: $b_1 , b_2 , \ldots, b_t \in$ group G

- Decide if $a_1 \, b_1 \, a_2 \, b_2 \bullet\bullet\bullet \, a_t \, b_t = 1_G$ or $= h$

Communication complexity:
- G abelian: O(1) Equality

- G non-solvable: $\Omega(t)$ [Barrington + Chor Goldreich]

- G = SL(2,q):

Interleaved products in group G

[Miles V.]

- Alice: $a_1, a_2, \ldots, a_t \in$ group G

  Bob: $b_1, b_2, \ldots, b_t \in$ group G

- Decide if $a_1\, b_1\, a_2\, b_2 \bullet \bullet \bullet a_t\, b_t = 1_G$ or $= h$

Communication complexity:

- G abelian: $O(1)$ Equality

- G non-solvable: $\Omega(t)$ [Barrington + Chor Goldreich]

- G = SL(2,q): $\Theta(t \log |G|)$ [This work, equivalently]

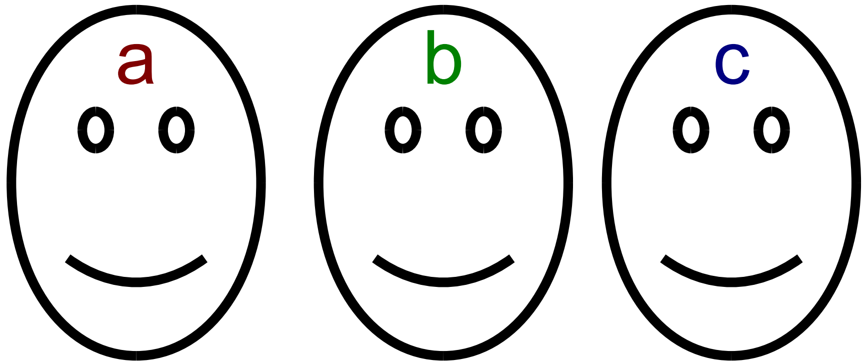
Number-on-forehead communication

[Yao, Chandra Furst Lipton '83]

- k parties wish to compute function of k inputs
- Party **i** knows all but **i**-th input (on forehead)
- Fascinating, useful, and challenging model

Interleaved products in group G

- Alice: a_1 , a_2 , …, a_t $\in$ G
  Bob: b_1 , b_2 , …, b_t $\in$ G
  Clio: c_1 , c_2 , …, c_t $\in$ G



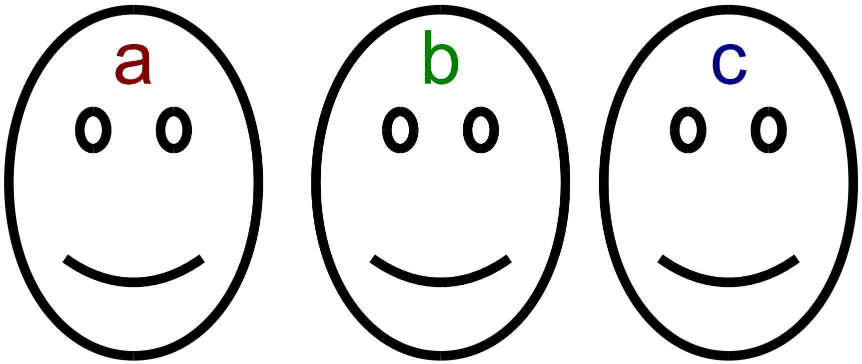
- Decide if $a_1\, b_1\, c_1\, a_2\, b_2\, c_2 \cdots a_t\, b_t\, c_t = 1_G$ or $= h$

- Communication:

G abelian: ???

Interleaved products in group G

- Alice: $a_1 , a_2 , \ldots, a_t \in G$
  Bob: $b_1 , b_2 , \ldots, b_t \in G$
  Clio: $c_1 , c_2 , \ldots, c_t \in G$



- Decide if $a_1 b_1 c_1 a_2 b_2 c_2 \cdots a_t b_t c_t = 1_G$ or $= h$

- Communication:

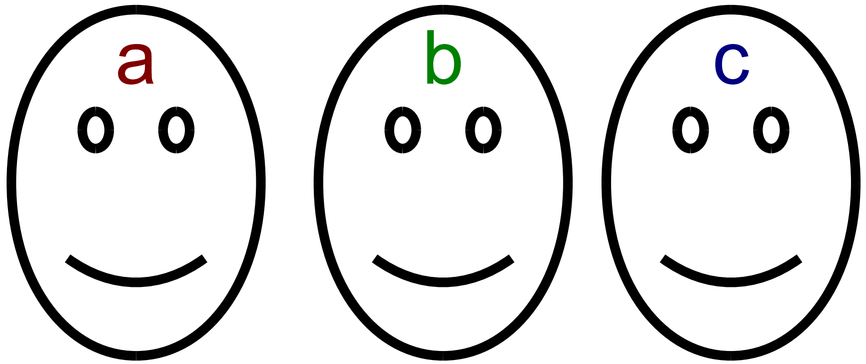
G abelian: O(1)
G non-solvable: ???

Interleaved products in group G

- Alice: $a_1 , a_2 , \ldots, a_t \in G$

  Bob: $b_1 , b_2 , \ldots, b_t \in G$

  Clio: $c_1 , c_2 , \ldots, c_t \in G$



- Decide if $a_1\, b_1\, c_1\, a_2\, b_2\, c_2 \cdots a_t\, b_t\, c_t = 1_G$ or $= h$

- Communication:

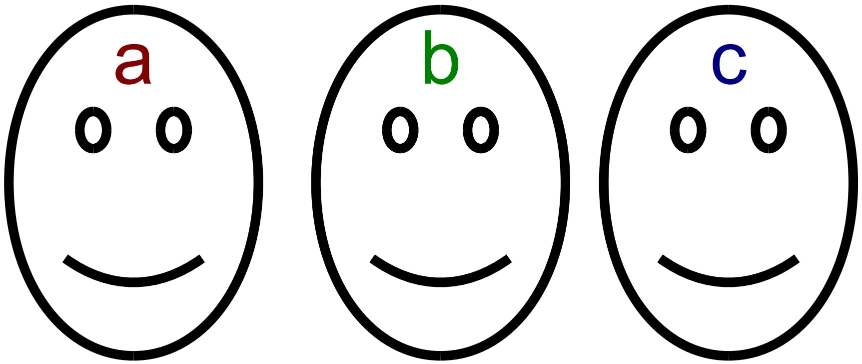
  G abelian: $O(1)$

  G non-solvable: $\Omega(t/2^k)$

  $G = SL(2,q)$:

Interleaved products in group G

- Alice: $a_1, a_2, \ldots, a_t \in G$
  Bob: $b_1, b_2, \ldots, b_t \in G$
  Clio: $c_1, c_2, \ldots, c_t \in G$



- Decide if $a_1 b_1 c_1 a_2 b_2 c_2 \cdots a_t b_t c_t = 1_G$ or $= h$

- Communication:

G abelian: $O(1)$

G non-solvable: $\Omega(t/2^k)$

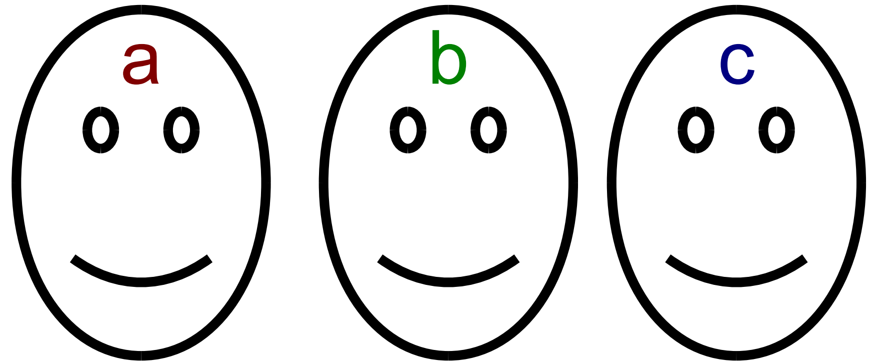
$G = SL(2,q)$: $\Omega(t / 2^{2^k}) \log |G|$ [This work]

Interleaved products in group G

- Alice: a_1 , a_2 , …, $a_t \in G$

  Bob: b_1 , b_2 , …, $b_t \in G$

  Clio: c_1 , c_2 , …, $c_t \in G$



- Decide if $a_1\, b_1\, c_1\, a_2\, b_2\, c_2 \cdots a_t\, b_t\, c_t = 1_G$ or $= h$

- Communication:

  G abelian: $O(1)$

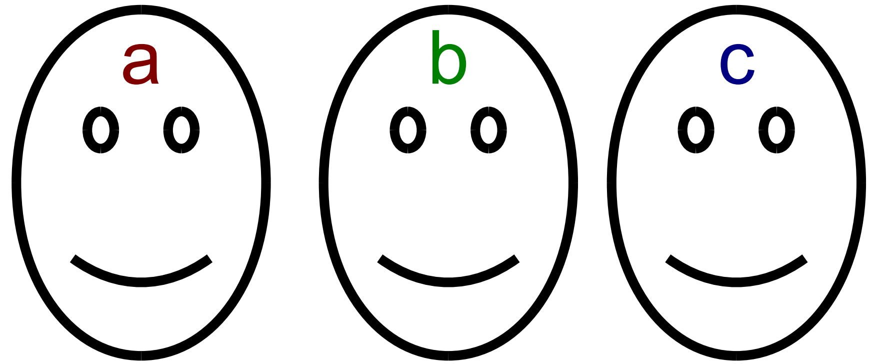
  G non-solvable: $\Omega(t/2^k)$

  $G = SL(2,q)$: $\Omega(t / 2^{2^k}) \log |G|$ [This work]

Conjecture: $t/2^k \log |G|$

Interleaved products in group G

- Alice: $a_1, a_2, \ldots, a_t \in G$
  Bob: $b_1, b_2, \ldots, b_t \in G$
  Clio: $c_1, c_2, \ldots, c_t \in G$



- Decide if $a_1 b_1 c_1 a_2 b_2 c_2 \cdots a_t b_t c_t = 1_G$ or $= h$

- Communication:

G abelian: $O(1)$

G non-solvable: $\Omega(t/2^k)$

$G = SL(2,q)$: $\Omega(t / 2^{2^k})$ $\log |G|$ [This work]

Conjecture: $t/2^k \log |G|$

Bolder: even k >> log t

Boosting independence

● Proof of last result (multiparty lower bound) relies on

● Lemma Let $G = SL(2,q)$, $s >> m$.
Let $D_1, D_2, \ldots, D_s$ be independent distributions on G^m.
Each D_i is pairwise independent.
➔
Component-wise product $D = D_1 D_2 \bullet \bullet D_s$ close to uniform:
For any $g \in G^m$, $| \Pr[D = g] - 1/|G|^m | \leq \varepsilon / |G|^m$

● False for abelian groups

Outline

- Introduction and our results
- Proof of interleaved mixing
- Communication complexity viewpoint, boosting independence
- Proof of boosting independence

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

Let D_1 , D_2 , …, D_s be independent distributions on G^m .

Each D_i is pairwise independent.

➔

Component-wise product $D = D_1 D_2 \bullet \bullet D_s$ close to uniform:

For any $g \in G^m$, $| \Pr[D = g] - 1/|G|^m | \leq \varepsilon / |G|^m$

- Proof outline.

Enough to show m = 3.

Multiplying pairwise independent distributions flattens them

Unexpectedly, all we use of G is interleaved mixing.

- Lemma p and q pairwise independent over G^3 , $\theta \in [0,1]$:

$|p|_\infty$, $|q|_\infty \le 1/|G|^{2+\theta}$ $\Rightarrow$ $|pq|_2^2 \le 1/|G|^3 + 1/|G|^{2+\theta+\Omega(1)}$

$\Rightarrow$ $|pqpq|_\infty \le 1/|G|^3 + 1/|G|^{2+\theta+\Omega(1)}$

- Proof idea: $|pq|_2^2$

$= \sum$ p(x1,x2,x3) q(y1,y2,y3) p(z1,z2,z3) q(w1,w2,w3)

over x1y1=z1w1, x2y2=z2w2, x3y3=z3w3

$= \ldots \le \sum_{xy=zw} A(x,w)\, B(y,z)$, for suitable A, B

Apply previous result. ■

Summary

- Interleaved group products over G = SL(2,q)
- A•B•A'•B' nearly uniform, if (A,A') independent from (B,B')

  Product of conjugacy classes ➔ uniform

- TIght multiparty communication bound, for O(1) parties

  Boosting independence:
  Product of pairwise independent distrib. in G^m ➔ uniform

End of talk

Next: deleted scenes

$$A(x, w) = \sum_a p(x1a, x2, x) \, q(ay1, y2, w)$$

$$|A|_1 = \sum_{x,w} \sum_a p(x1a, x2, x) \, q(ay1, y2, w)$$

$$= \sum_a \left(\sum_x p(x1a, x2, x)\right) \left(\sum_w q(ay1, y2, w)\right)$$

$$= \sum_a (1/|G|^2)(1/|G|^2)$$ Pairwise independence

$$= 1/|G|^3 .$$

Assumption on $|p|_\infty$ and $|q|_\infty$ used in $|A|_2$ bound

■

$= \sum\ p(x1\ a, x2, x3)\ q(y1, b\ y2, y3)\ p(x1, x2\ b, z3)\ q(a y1, y2, w3)$

over $a, b, x1, x2, y1, y2,\ x3y3 = z3w3$

Fix x1, x2, y1, y2 that maximize.

Let $A(x, w) = \sum_a\ p(x1a, x2, x) \ q(ay1, y2, w)$

$B(y, z) = \sum_b\ q(y1, b\ y2, y)\ p(x1, x2\ b, z)$

Then $|\ pq\ |_2^2 \leq |G|^4 \sum_{xy=zw} A(x,w)\ B(y,z)$.

Apply version of previous result.

$\sum_{xy=zw} A(x,w)\ B(y,z) \leq |A|_1\ |B|_1\ /|G| + |A|_2\ |B|_2/|G|^{1+\ \Omega(1)}$

Assumptions $\rightarrow$ bound on $|A|_1$, $|A|_2$, $|B|_1$, $|B|_2$.

Mixing in 4 steps implies mixing in 3:

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

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

Proof for X=Y=Z:

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

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

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

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

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

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

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

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