The multiparty communication complexity of interleaved group products

October 2016

Emanuele Viola

NEU

Joint work with Timothy Gowers

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

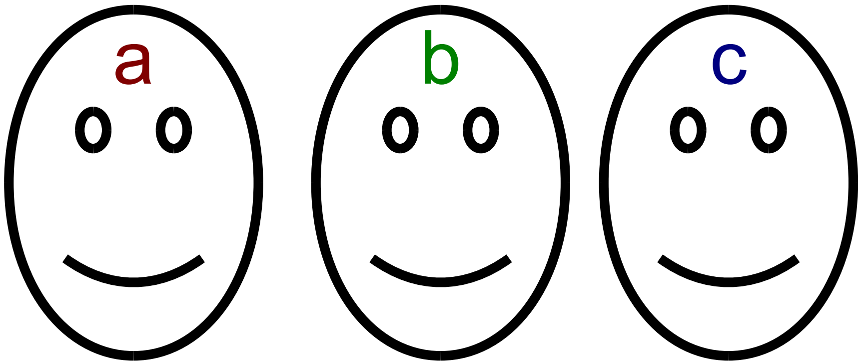
Interleaved products in group G

[Miles V]

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

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

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



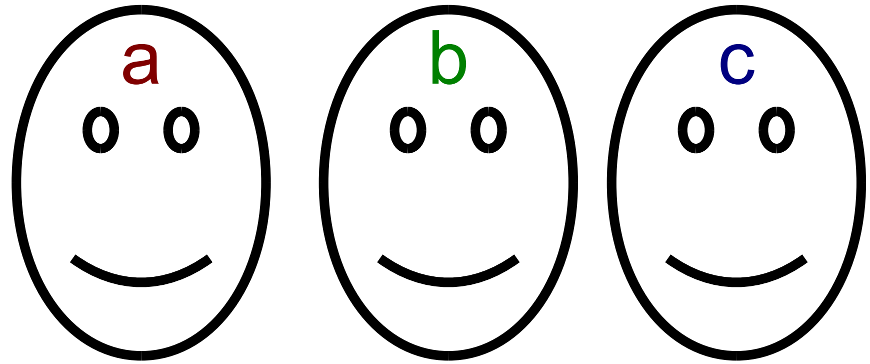
- Decide if $a_1\, b_1\, c_1\, a_2\, b_2\, c_2 \bullet\bullet\bullet\, a_t\, b_t\, c_t = 1_G$ or $= h$

- Communication:

G abelian: ???

Interleaved products in group G
[Miles V]

- 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) reduce to equality
G non-solvable: ???

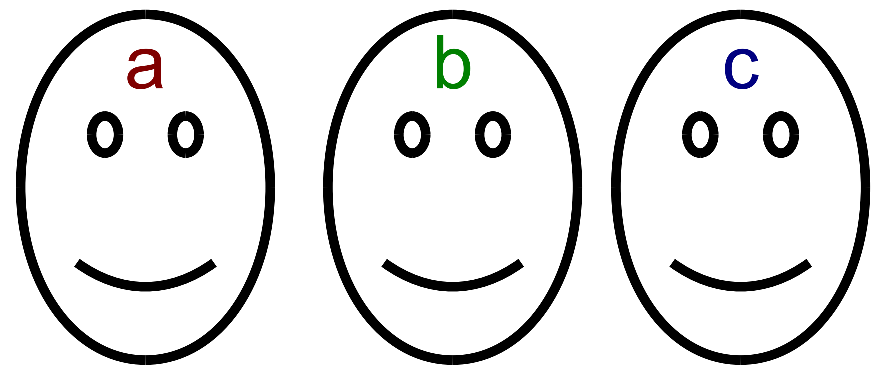
Interleaved products in group G

[Miles V]

- 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: $O(1)$ reduce to equality

  G non-solvable: $\Omega(t/2^k)$, k parties [Babai Nisan Szegedy Barrington]

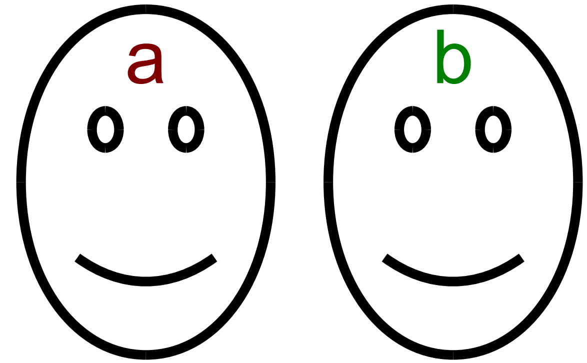
- Question: Improve for large $|G|$? $\Omega(t/2^k)\log|G|$?

Previous work for k = 2 parties

[Gowers V]

- Alice: a_1 , a_2 , …, $a_t \in G$

  Bob: b_1 , b_2 , …, $b_t \in G$



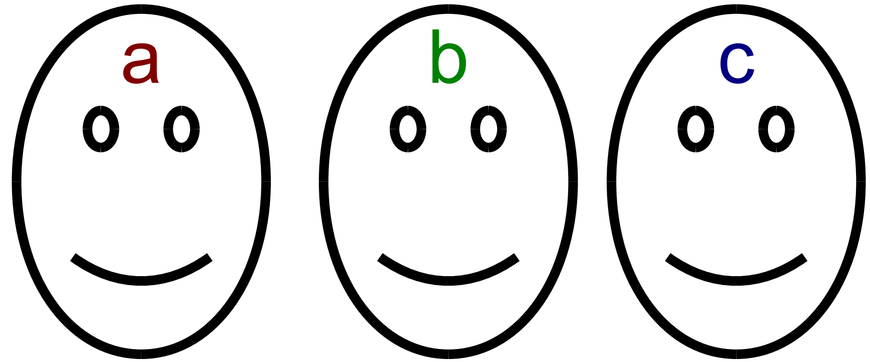
- Decide if $a_1\ b_1\ a_2\ b_2 \cdots a_t\ b_t = 1_G$ or $= h$

- Theorem: Communication complexity
  - $\Omega(t)$ log $|G|$ for G = SL(2,q) = 2x2 matrices in F_q
  - $\omega(1)$ for G simple, non-abelian

- [Shalev] quantifies ω

This work

- 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 $= h$

- Theorem Communication $\Omega(t / 2^{2^k}) \log |G|$

  With k parties, $G = SL(2,q)$, and $t \geq 2^{2^k}$

  Tight for $k = O(1)$

Outline

- Communication complexity
- Cryptography
- Boosting independence, proofs

Cryptographic application
[Miles V 2013]

- Leakage-resilient circuits based on group products

  - Secure in computationally-bounded model

  - Secure in “only computation leaks” [Micali Reyzin]
    assuming $\Omega(t) \log |G|$ bound for 8 parties

Cryptographic application

[Miles V 2013]

- Leakage-resilient circuits based on group products

  - Secure in computationally-bounded model

  - Secure in "only computation leaks" [Micali Reyzin]
    ~~assuming $\Omega(t) \log |G|$ bound for 8 parties~~
    using $\Omega(t) \log |G|$ bound for 8 parties in this work

Outline

- Communication complexity
- Cryptography
- Boosting independence, proofs

Boosting independence

- Lemma: $\forall m\ \exists s$: $G = SL(2,q)$,

$D_1, D_2, \ldots, D_s$ independent distributions on G^m

each D_i pairwise independent.

$$\Downarrow$$

$D = D_1 \bullet D_2 \bullet \bullet \bullet D_s$ close to uniform:

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

- Can be proved using result for k = 2 parties

Boosting independence → lower bound

- Recall $P(a,b,c) = a_1\ b_1\ c_1\ a_2\ b_2\ c_2 \cdots a_t\ b_t\ c_t$

  Goal: hard to tell $P(a,b,c) = 1_G$ from $P(a,b,c) = h$

- Define $f(a,b,c) = 1\ /\ {-1}\ /\ 0$ if $P(a,b,c) = 1_G\ /\ h\ /$ else

- [BNS, CT, R, VW] Enough to bound,

  for uniform $a^0, a^1, b^0, b^1, c^0, c^1 \in G^t$,

  $$E\,[f(a^0,b^0,c^0)\cdot f(a^0,b^0,c^1)\cdot f(a^0,b^1,c^0)\cdot f(a^0,b^1,c^1)\cdot f(a^1,b^0,c^0)\cdot f(a^1,b^0,c^1)\cdot f(a^1,b^1,c^0)\cdot f(a^1,b^1,c^1)\,]$$

- Prove stronger: the 8 factors nearly independent

Boosting independence → lower bound

- Recall $P(a,b,c) = a_1\ b_1\ c_1\ a_2\ b_2\ c_2 \cdots a_t\ b_t\ c_t$

- Prove stronger result:

  $D(t) :=$

  $(P(a^0,b^0,c^0),P(a^0,b^0,c^1),P(a^0,b^1,c^0),P(a^0,b^1,c^1)$

  $P(a^1,b^0,c^0),P(a^1,b^0,c^1),P(a^1,b^1,c^0),P(a^1,b^1,c^1)\ ) \in G^8$

  is nearly uniform over G^8

- Proof:

  $D(t)=$ product of s independent copies of $D(t/s) \in G^8$

  each copy pairwise independent

  Boosting independence lemma ■

Future work

- Improve $\Omega(t / 2^{2^k})$ log |G| to $\Omega(t/2^k)$ log |G|
- Conjecture [Gowers V] ~$\Omega(t)$ even for $k > \log t$
- Tight bounds for boosting independence
- Extend to other groups

Summary

- Interleaved group products over G = SL(2,q)
  $a_1\ b_1\ c_1\ a_2\ b_2\ c_2 \cdots a_t\ b_t\ c_t$

- Communication $\Omega(t) \log |G|$ for O(1) parties, tight

- [Miles V] secure even in "only-computation leaks"

- Boosting independence:

  Independent distributions $D_1, D_2, \ldots, D_s$ in G^m

  Each D_i pairwise indep. → $D_1\ D_2 \cdot\cdot\ D_s \approx$ uniform