Boosting uniformity in quasirandom groups: fast and simple

October 2024

Emanuele Viola

NEU

Joint work with Harm Derksen and Chin Ho Lee

Book ad

Mathematics of the impossible

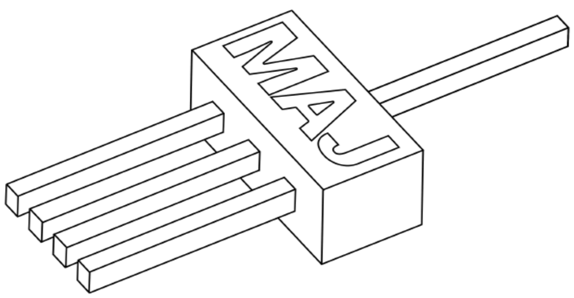
Draft on my homepage

MATHEMATICS OF THE IMPOSSIBLE

THE UNCHARTED COMPLEXITY OF COMPUTATION

Compiled on October 9, 2024

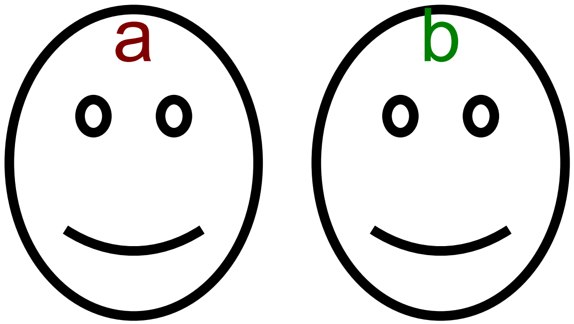
Emanuele "Manu" Viola



1

Now the talk

Interleaved group products

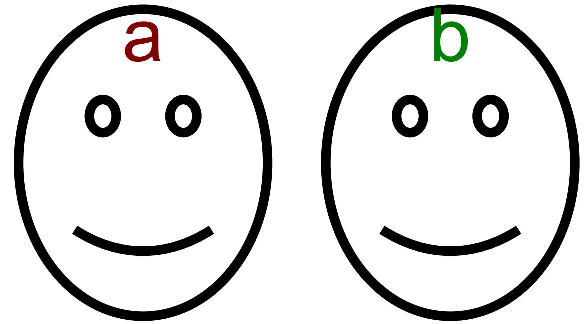


- Alice: a_1 , a_2 , …, a_t ∈ group G
  Bob: b_1 , b_2 , …, b_t ∈ G

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

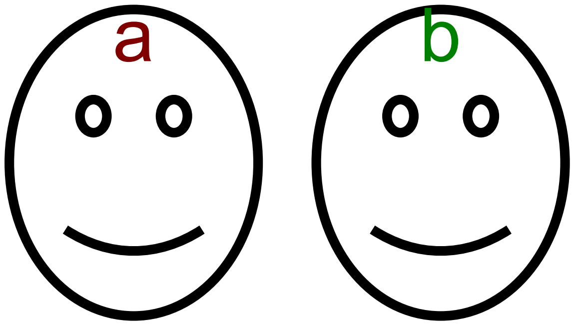
- G abelian ⇒ how much communication ??

Interleaved group products



- Alice: a_1 , a_2 , …, a_t ∈ group G
  Bob: b_1 , b_2 , …, b_t ∈ G
- Decide if $a_1\ b_1\ a_2\ b_2 \bullet\bullet\bullet\ a_t\ b_t = 1_G$ or $= h$
- G abelian ⇒ constant (reduce to equality)
- G simple ⇒ ?? (Hint: encode inner product)

Interleaved group products

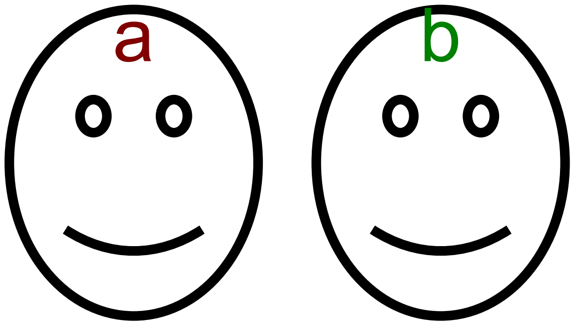


- Alice: a_1 , a_2 , …, a_t ∈ group G
  Bob: b_1 , b_2 , …, b_t ∈ G

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

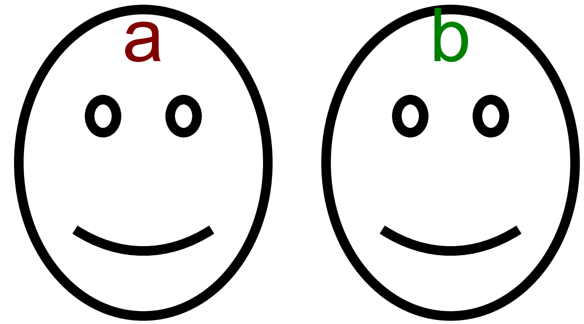
- G abelian ⇒ constant (reduce to equality)
- G simple ⇒ ct (encode inner product)
- Question [Miles V]: c t log |G| for some G? (crypto app.)

Interleaved group products



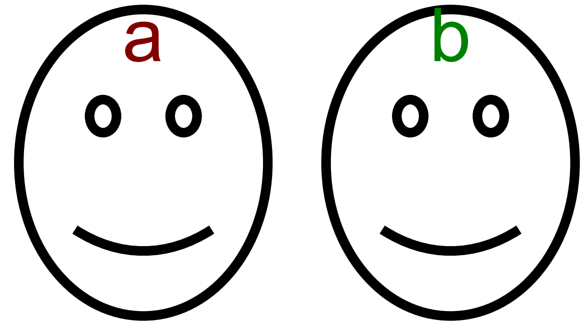
- Alice: a_1 , a_2 , …, a_t ∈ group G
  Bob: b_1 , b_2 , …, b_t ∈ G
- Decide if $a_1\ b_1\ a_2\ b_2 \bullet \bullet \bullet\ a_t\ b_t = 1_G$ or $= h$
- G abelian ⇒ constant (reduce to equality)
- G simple ⇒ ct (encode inner product)
- Question [Miles V]: c t log |G| for some G? (crypto app.)
- [Gowers V] Yes for G = SL(2,q) = 2x2 matrices over F_q

Interleaved group products



- Alice: a_1 , a_2 , …, a_t ∈ group G
  Bob: b_1 , b_2 , …, b_t ∈ G
- Decide if $a_1\, b_1\, a_2\, b_2 \bullet\bullet\bullet\, a_t\, b_t = 1_G$ or $= h$
- G abelian ⇒ constant (reduce to equality)
- G simple ⇒ ct (encode inner product)
- Question [Miles V]: c t log |G| for some G? (crypto app.)
- [Gowers V] Yes for G = SL(2,q) = 2x2 matrices over F_q
- [Shalev] refines bounds for other groups

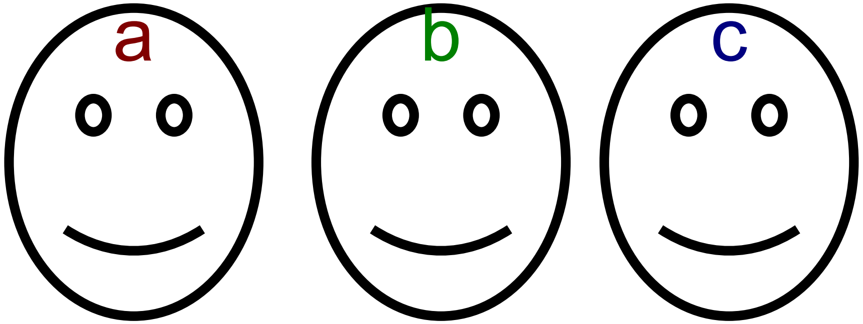
Interleaved group products



- Alice: a_1 , a_2 , …, a_t ∈ group G
  Bob: b_1 , b_2 , …, b_t ∈ G
- Decide if $a_1\, b_1\, a_2\, b_2 \bullet\bullet\bullet\, a_t\, b_t = 1_G$ or $= h$
- G abelian ⇒ constant (reduce to equality)
- G simple ⇒ ct (encode inner product)
- Question [Miles V]: c t log |G| for some G? (crypto app.)
- [Gowers V] Yes for G = SL(2,q) = 2x2 matrices over F_q
- [Shalev] refines bounds for other groups
- [Derksen V] Quasirandom G, 3-line “book proof”
  Generalizes, simplifies, improves all above

k-party number-on-forehead

- 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 $= h$

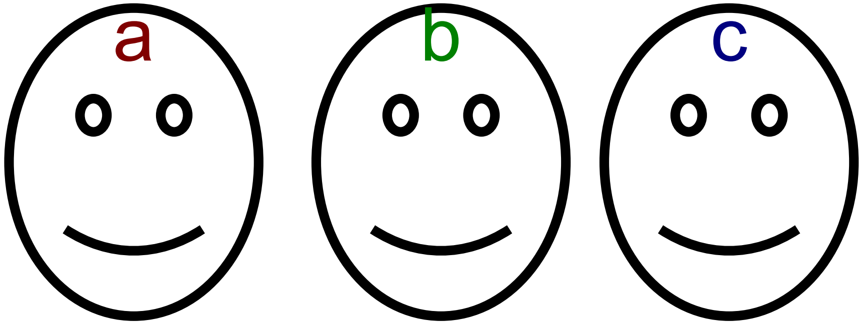
- Note: Candidate or solving major open questions:

  - Separating deterministic, randomized communication
    Simplify/improve [Kelley Lovett Meka '23] ?

  - Hard even for k >> log n parties ?

k-party number-on-forehead

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

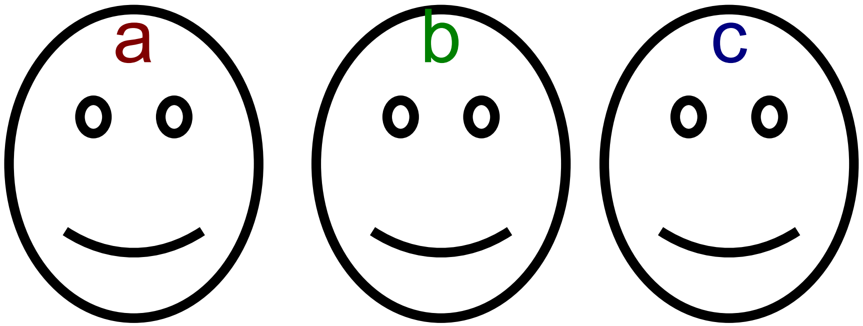


- Decide if $a_1\, b_1\, c_1\, a_2\, b_2\, c_2 \cdots a_t\, b_t\, c_t = 1_G$ or $= h$

- G abelian ⇒ ??

k-party number-on-forehead

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

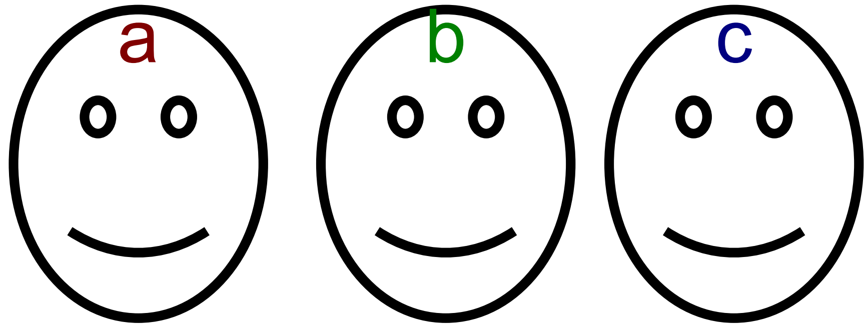


- Decide if $a_1\, b_1\, c_1\, a_2\, b_2\, c_2 \cdots a_t\, b_t\, c_t = 1_G$ or $= h$

- G abelian ⇒ constant (reduce to equality)
- G simple ⇒ ??

k-party number-on-forehead

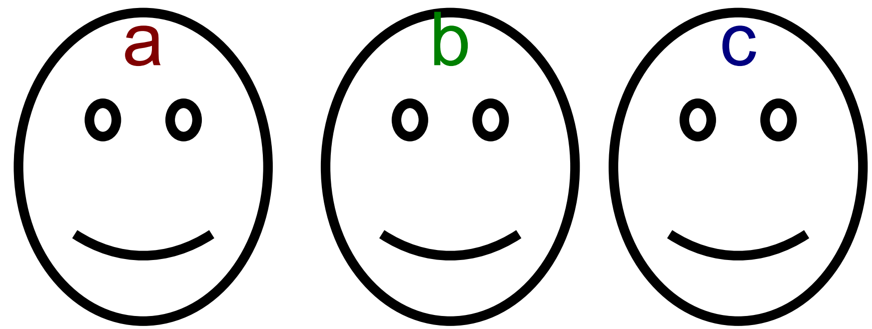
- Alice: $a_1, a_2, \ldots, a_t \in G$
  Bob: $b_1, b_2, \ldots, b_t \in G$
  Clio: $c_1, c_2, \ldots, c_t \in G$



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

- G abelian ⇒ constant (reduce to equality)
- G simple ⇒ $t\, c^{-k}$ (encode generalized inner product)
- Question [Miles V]: $t\, c^{-k} \log |G|$ for some G? (crypto app.)

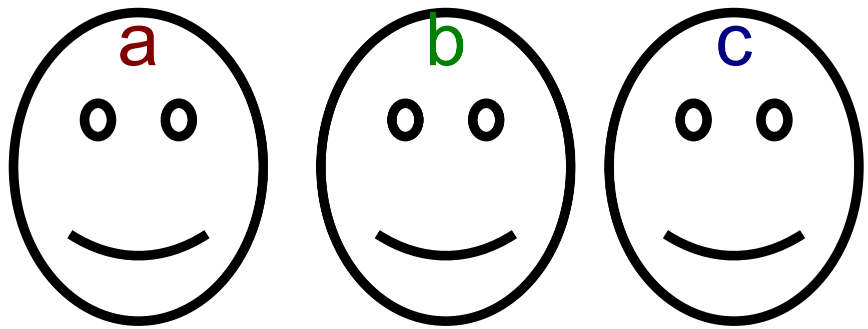
k-party number-on-forehead



- Alice: a_1 , a_2 , …, a_t ∈ G
  Bob: b_1 , b_2 , …, b_t ∈ G
  Clio: c_1 , c_2 , …, c_t ∈ 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 $= h$
- G abelian ⇒ constant (reduce to equality)
- G simple ⇒ t c^{-k} (encode generalized inner product)
- Question [Miles V]: t c^{-k} log |G| for some G? (crypto app.)
- [Gowers V] t 2^{-c^k} log |G|, G = SL(2,q)

k-party number-on-forehead

- 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 $= h$

- G abelian ⇒ constant (reduce to equality)
- G simple ⇒ $t\, c^{-k}$ (encode generalized inner product)
- Question [Miles V]: $t\, c^{-k} \log |G|$ for some G? (crypto app.)
- [Gowers V] $t\ 2^{-c^k} \log |G|$, $G = SL(2,q)$
- [this work] $t\, c^{-k} \log |G|$, quasirandom G

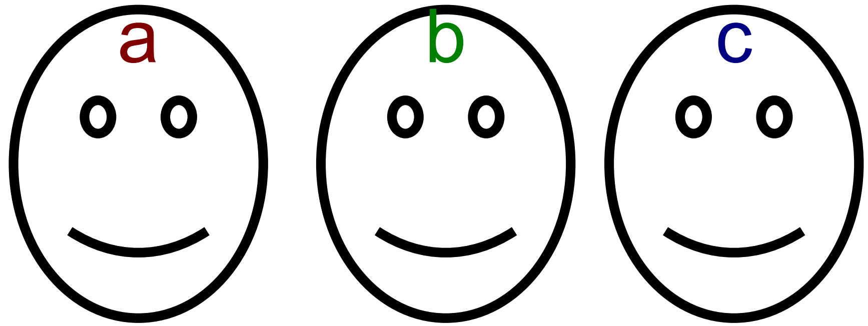
  Generalizes, simplifies*, improves all above

k-party number-on-forehead

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

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

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



- Decide if $a_1 \, b_1 \, c_1 \, a_2 \, b_2 \, c$

- G abelian ⇒ constar
- G simple ⇒ t c^{-k} ct)
- Question [Miles V]: t c^{-k} log |G| (crypto app.)
- [Gowers V] t 2^{-c^k} log |G|, G = SL(
- [this work] t c^{-k} log |G|, quasirand m G

Generalizes, simplifies*, improves all above

Simpler for groups like SL(2,q), others need [Gowers V] as first step

Proof technique: Boosting independence

- $G = SL(2,q)$. D distribution on G^m

- Lemma [Gowers V]:

  D h-uniform $\Rightarrow D_1 \bullet D_2 \bullet \bullet \bullet D_{100}$ close to (h+1)-uniform

- Proof: Technical reduction to 2-party case

- Lemma [this work]:

  D h-uniform $\Rightarrow D_1 \bullet D_2 \bullet \bullet \bullet D_{100}$ close to (2h)-uniform

- Proof: Representation analysis

- Lemma [this work]: D distribution on G^m

D h-uniform ⇒ $D_1 \cdot D_2 \cdot \cdot \cdot D_{100}$ close to (2h)-uniform

- High-level proof steps:

  Write distributions in representation basis

  Representation dimensions
  G abelian ⇔ dimensions = 1
  G quasirandom ⇔ dimensions are large ($|G|^c$ for SL(2,q))

  (1) D h-uniform ⇒ degree-h representations vanish
  (2) Representation dimensions multiply with degree

  $(1) + (2)$ ⇒ D • D "mixes" or "flattens" at rate about
  (representation dimension of G)^h QED

Message

- Representation theory convenient framework

- Another example: any almost h-uniform distribution is
  close to (exactly) h-uniform distribution

- [Alon Goldreich Mansour 2003] G = Z_2^m
- [Rubinfeld Xie 2013] G = H^m H abelian
  Work in ad hoc basis

- [This work] Any G = H^m
  Representation basis, simpler even for abelian H

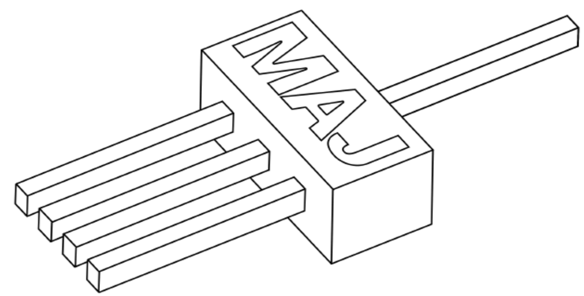
The end

MATHEMATICS OF THE IMPOSSIBLE

THE UNCHARTED COMPLEXITY OF COMPUTATION

Compiled on October 9, 2024

Emanuele “Manu” Viola



1