Quasirandom groups enjoy interleaved mixing

Harm Derksen* Emanuele Viola†

July 3, 2022

Abstract

Let G be a group such that any non-trivial representation has dimension at least d. Let $X = (X_1, X_2, \ldots, X_t)$ and $Y = (Y_1, Y_2, \ldots, Y_t)$ be distributions over G^t. Suppose that X is independent from Y. We show that for any $g \in G$ we have

$$|\mathbb{P}[X_1 Y_1 X_2 Y_2 \cdots X_t Y_t = g] - 1/|G|| \leq \frac{|G|^{2t-1}}{d^{t-1}} \sqrt{\mathbb{E}_{h \in G^t} X(h)^2} \sqrt{\mathbb{E}_{h \in G^t} Y(h)^2}.$$

Our results generalize, improve, and simplify previous works.

Quasirandom groups, introduced by Gowers [Gow08], are groups whose non-trivial representations have large dimension. Multiplication in such groups is known to behave like a random function in several respects. The prime example of this is that if X and Y are independent, high-entropy distributions over a quasirandom group then XY (i.e., sample from each and output the product) becomes closer to uniform in L_2 norm. For a discussion of this result and its many proofs we refer to Section 13 of [Gow17]. Other random-like behaviors are known with respect to, for example, *progressions* [BHR22] and *corners* [Aus16] (cf. [Vio19]).

In this work we are interested in a question posed by Miles and Viola [MV13]. Let $X = (X_1, X_2)$ and $Y = (Y_1, Y_2)$ be high-entropy distributions over G^2 such that X is independent from Y (but X_1 needs not be independent from X_2 and Y_1 needs not be independent from Y_2). They asked if the *interleaved product* $X_1 Y_1 X_2 Y_2$ "mixes," i.e., if it is close to uniform, for suitable groups G. Their question was motivated by an application to cryptography (which follows from a positive answer to a more general question they asked).

Gowers and Viola give a positive answer to this question for non-abelian simple groups, which are known to be quasirandom. For the special case of $G = SL(2, q)$ they prove a strong error bound. A simpler exposition of the latter proof appears in [Vio19]. A follow-up paper by Shalev [Sha16] gives stronger error bounds for non-abelian simple groups.

These proofs are somewhat complicated and use substantial machinery, and they only apply to simple groups. Here we give a very short and elementary proof that applies to any quasirandom group, as stated in the abstract. (But if one is interested only in $G = SL(2, q)$ and is not willing to use representation theory, the proof in [GV19] may be more accessible, especially with the simplification presented in [Vio19].)

*Partially supported by NSF grant DMS 2147769.

†Supported by NSF grant CCF-2114116.

To illustrate the bound in the abstract, suppose that X is uniform over a set of density α and Y is uniform over a set of density β. Then the right-hand side is $|G|^{2t-1} \cdot d^{-t+1} \cdot (\alpha\beta)^{-1/2}/|G|^{2t} = |G|^{-1} \cdot d^{-t+1} \cdot (\alpha\beta)^{-1/2}$. Our results also slightly improve the parameters in the cases where interleaved mixing could be established. For example for $t > 2$ the bounds in [GV19] and [Sha16] have $(\alpha\beta)^{-1}$ instead of $(\alpha\beta)^{-1/2}$.

The paper [GV19] also shows that from interleaved mixing there follow a number of other results (including the solution to the more general question in [MV13], thus enabling the motivating application). Hence our results yield these applications for any quasirandom group. Since this is an immediate composition of proofs in [GV19] and this paper, we refer the reader to [GV19] for precise statements.

Proof of statement in the abstract We follow standard notation for non-abelian Fourier analysis, see for example Section 13 of [Gow17] or [GV22]. It suffices to prove the theorem for $g = 1_G$. Let Z be a distribution over G. By Fourier inversion, and using that $\rho(1) = I$ and $\widehat{Z}(1) = 1/|G|$ we have

$$|\mathbb{P}[Z = 1] - 1/|G|| = |\sum_{\rho} d_\rho \mathrm{tr}(\widehat{Z}(\rho)\rho(1)^T) - 1/|G|| = |\sum_{\rho \neq 1} d_\rho \mathrm{tr}(\widehat{Z}(\rho))| \leq \sum_{\rho \neq 1} d_\rho |\mathrm{tr}(\widehat{Z}(\rho))|, \tag{1}$$

where ρ ranges over irreducible representations.

The main claim is that if Z is the interleaved product $X_1Y_1X_2Y_2 \cdots X_tY_t$ then for any ρ

$$|\mathrm{tr}(\hat{Z}(\rho))| \leq |G|^{2t-1} |\hat{X}(\rho^{\otimes t})|_2 |\hat{Y}(\rho^{\otimes t})|_2. \tag{2}$$

Assuming the claim the proof is completed as follows. Plugging Inequality (2) into (1) and multiplying by $(d_\rho/d)^{t-1}$ which is ≥ 1 for $\rho \neq 1$, the error is at most

$$\frac{|G|^{2t-1}}{d^{t-1}} \sum_{\rho \neq 1} \left(d_\rho^{t/2} \left| \hat{X}(\rho^{\otimes t}) \right|_2 \right) \left(d_\rho^{t/2} \left| \hat{Y}(\rho^{\otimes t}) \right|_2 \right).$$

By Cauchy-Schwarz this is at most

$$\frac{|G|^{2t-1}}{d^{t-1}} \sqrt{\sum_{\rho \neq 1} d_\rho^t \left| \hat{X}(\rho^{\otimes t}) \right|_2^2} \sqrt{\sum_{\rho \neq 1} d_\rho^t \left| \hat{Y}(\rho^{\otimes t}) \right|_2^2}.$$

Note that d_ρ^t is the dimension of $\rho^{\otimes t}$. Each sum can be bounded above by summing over all irreducible representations. Hence by Parseval the sum with X is at most $\mathbb{E}_{h \in G^t} X^2(h)$ and the same for Y, proving the theorem.

Next we verify Inequality (2). By definition we have

$$\hat{Z}(\rho) = \mathbb{E}_g Z(g) \overline{\rho(g)} = \mathbb{E}_g \sum_{g_1, g_2, \ldots, g_{2t} : \prod g_i = g} X(g_1, g_3, \ldots, g_{2t-1}) Y(g_2, g_4, \ldots, g_{2t}) \overline{\rho(g)}.$$

This summation is the same as summing over all g_i and setting g to be the product. Further, because ρ is a representation one has $\rho(\prod_i g_i) = \prod_i \rho(g_i)$. Hence we get

$$\hat{Z}(\rho) = \frac{1}{|G|} \sum_{g_1, g_2, \ldots, g_{2t}} X(g_1, g_3, \ldots, g_{2t-1}) Y(g_2, g_4, \ldots, g_{2t}) \overline{\prod_{i \leq 2t} \rho(g_i)}.$$

And now the critical equation:

$$\begin{aligned}
\mathrm{tr}\hat{Z}(\rho) &= \sum_i \frac{1}{|G|} \sum_{g_1,g_2,\ldots,g_{2t}} X(g_1,g_3,\ldots,g_{2t-1})Y(g_2,g_4,\ldots,g_{2t}) \sum_{i_2,i_3,\ldots,i_{2t}} \bar{\rho}(g_1)_{i,i_2}\bar{\rho}(g_2)_{i_2,i_3}\cdots\bar{\rho}(g_{2t})_{i_{2t},i} \\
&= \frac{1}{|G|} \sum_{i,i_2,i_3,\ldots,i_{2t}} \left(\sum_{g_1,g_3,\ldots,g_{2t-1}} X(g_1,g_3,\ldots,g_{2t-1})\bar{\rho}(g_1)_{i,i_2}\cdot\bar{\rho}(g_3)_{i_3,i_4}\cdots\bar{\rho}(g_{2t-1})_{i_{2t-1},i_{2t}} \right) \\
&\cdot \left(\sum_{g_2,g_4,\ldots,g_{2t}} Y(g_2,g_4,\ldots,g_{2t})\bar{\rho}(g_2)_{i_2,i_3}\cdot\bar{\rho}(g_4)_{i_4,i_5}\cdots\bar{\rho}(g_{2t})_{i_{2t},i} \right) \\
&= |G|^{2t-1} \sum_{i,i_2,i_3,\ldots,i_{2t}} \left(\hat{X}(\rho^{\otimes t})_{i,i_2,i_3,\ldots,i_{2t}}\right)\left(\hat{Y}(\rho^{\otimes t})_{i_2,i_3,\ldots,i_{2t},i}\right).
\end{aligned}$$

Inequality (2) now follows by applying the Cauchy-Schwarz inequality.

References

[Aus16] Tim Austin. Ajtai-Szemerédi theorems over quasirandom groups. In *Recent trends in combinatorics*, volume 159 of *IMA Vol. Math. Appl.*, pages 453–484. Springer, [Cham], 2016.

[BHR22] Amey Bhangale, Prahladh Harsha, and Sourya Roy. Mixing of 3-term progressions in quasirandom groups. In Mark Braverman, editor, *ACM Innovations in Theoretical Computer Science conf. (ITCS)*, volume 215 of *LIPIcs*, pages 20:1–20:9. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.

[Gow08] W. T. Gowers. Quasirandom groups. *Combinatorics, Probability & Computing*, 17(3):363–387, 2008.

[Gow17] W. T. Gowers. Generalizations of Fourier analysis, and how to apply them. *Bull. Amer. Math. Soc. (N.S.)*, 54(1):1–44, 2017.

[GV] W. T. Gowers and Emanuele Viola. The multiparty communication complexity of interleaved group products. *SIAM J. on Computing*.

[GV15] W. T. Gowers and Emanuele Viola. The communication complexity of interleaved group products. In *ACM Symp. on the Theory of Computing (STOC)*, 2015.

[GV19] W. T. Gowers and Emanuele Viola. Interleaved group products. *SIAM J. on Computing*, 48(3):554–580, 2019. Special issue of FOCS 2016.

[GV22] W. T. Gowers and Emanuele Viola. Mixing in non-quasirandom groups. In *ACM Innovations in Theoretical Computer Science conf. (ITCS)*, 2022.

[MV13] Eric Miles and Emanuele Viola. Shielding circuits with groups. In *ACM Symp. on the Theory of Computing (STOC)*, 2013.

[Sha16] Aner Shalev. Mixing, communication complexity and conjectures of Gowers and Viola. *Combinatorics, Probability and Computing*, pages 1–13, 6 2016. arXiv:1601.00795.

[Vio19] Emanuele Viola. Non-abelian combinatorics and communication complexity. *SIGACT News, Complexity Theory Column*, 50(3), 2019.