

Mixing in Non-Quasirandom Groups

W. T. Gowers

Collège de France, Paris, France

Emanuele Viola 

Khoury College of Computer Sciences, Northeastern University, Boston, MA, USA

Abstract

We initiate a systematic study of mixing in non-quasirandom groups. Let A and B be two independent, high-entropy distributions over a group G . We show that the product distribution AB is statistically close to the distribution $F(AB)$ for several choices of G and F , including:

- (1) G is the affine group of 2×2 matrices, and F sets the top-right matrix entry to a uniform value,
- (2) G is the lamplighter group, that is the wreath product of \mathbb{Z}_2 and \mathbb{Z}_n , and F is multiplication by a certain subgroup,
- (3) G is H^n where H is non-abelian, and F selects a uniform coordinate and takes a uniform conjugate of it.

The obtained bounds for (1) and (2) are tight.

This work is motivated by and applied to problems in communication complexity. We consider the 3-party communication problem of deciding if the product of three group elements multiplies to the identity. We prove lower bounds for the groups above, which are tight for the affine and the lamplighter groups.

2012 ACM Subject Classification Mathematics of computing \rightarrow Combinatorics; Theory of computation \rightarrow Communication complexity

Keywords and phrases Groups, representation theory, mixing, communication complexity, quasirandom

Digital Object Identifier 10.4230/LIPIcs.ITCS.2022.80

Related Version *Full Version:* <https://eccc.weizmann.ac.il/report/2021/017>

Funding *Emanuele Viola:* Supported by NSF CCF awards CCF-1813930 and CCF-2114116.

Acknowledgements Emanuele Viola is grateful to Peter Ivanov for stimulating discussions.

1 Introduction and our results

Computing the product of elements from a group is a fundamental problem in theoretical computer science that arises and has been studied in a variety of works including [16, 22, 9, 15, 5, 24, 1, 2, 26, 21, 20, 14, 27], some of which are discussed more below. In this work we study this problem in the model of *communication complexity* [32, 17, 25]. Previous work in this area [21, 14] has found applications in cryptography, specifically to the construction of leakage-resilient circuits [21], and mathematics [27].

We consider the following basic communication problem. Each of several parties receives an element from a finite group G . The parties need to decide if the product of their elements is equal to 1_G . They have access to public randomness, and can err with constant probability say $1/100$. For two parties, this is the *equality* problem (because $ab = 1_G$ iff $a = b^{-1}$) and can be solved with constant communication. Thus the first interesting case is for 3 parties.

► **Definition 1.** We denote by $R_3(G)$ the randomized 3-party communication complexity of deciding if $abc = 1_G$, where the first party receives a , the second b , and the third c .



© W. T. Gowers and Emanuele Viola;

licensed under Creative Commons License CC-BY 4.0

13th Innovations in Theoretical Computer Science Conference (ITCS 2022).

Editor: Mark Braverman; Article No. 80; pp. 80:1–80:9

Leibniz International Proceedings in Informatics



Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

The simplest efficient protocol is over $G = \mathbb{Z}_2^n$. The parties use the public randomness to select a *linear hash function* $f_S : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2$ defined as $f_S(x) = \sum_{i \in S} x_i \pmod 2$. The parties then send $f_S(a), f_S(b), f_S(c)$ and compute $f_S(a) + f_S(b) + f_S(c) = f_S(a + b + c)$. The latter is always 0 if $a + b + c = 0$, while it is 0 with probability $1/2$ over the choice of S if $a + b + c \neq 0$. By repeating the test a bounded number of times, one can make the failure probability less than 1%. This shows $R_3(\mathbb{Z}_2^n) = O(1)$. Throughout this paper $O(\cdot)$ and $\Omega(\cdot)$ denote absolute constants.

The communication is also constant over the cyclic group \mathbb{Z}_n of integers modulo n : $R_3(\mathbb{Z}_n) = O(1)$ [28]. But this is a bit more involved, because linear hash functions (with small range) do not exist. One can use instead a hash function which is *almost linear*. Such a hash function was analyzed in the work [11] and has found many other applications, for example to the study of the 3SUM problem [7, 23].

The above raises the following natural question: For which groups G is $R_3(G)$ small?

It is fairly straightforward to prove lower bounds on $R_3(G)$ when G is *quasirandom* [12], a type of group that is discussed more in detail below. Such lower bounds for $R_3(G)$ appear in the survey [30] and also follow from the results in this paper (using what we later call the kernel method).

In this paper we prove lower bounds for groups to which the results for quasirandom groups do not apply. The groups we consider are natural, and they were considered before in the computer science literature, for example in the context of expander graphs [31, 19, 33] and low-distortion embeddings [18, 4]. We also complement the lower bounds with some new upper bounds. These results are closely related to the study of *mixing* in groups. We discuss these two perspectives in turn.

1.1 Communication complexity

To set the stage, we begin by discussing upper bounds on $R_3(G)$. We show that for any abelian group G we have $R_3(G) = O(1)$. This result generalizes the results for \mathbb{Z}_2^n and \mathbb{Z}_n mentioned earlier. More generally we can prove upper bounds for groups which contain large abelian subgroups, or that have *irreps* of bounded dimension. Here and throughout, *irrep* is short for *irreducible representation*. Representation theory plays a key role in this paper and is reviewed later.

► **Theorem 2.** *We have the following upper bounds on $R_3(G)$:*

- (1) *Suppose G is abelian. Then $R_3(G) = O(1)$*
- (2) *Suppose H is a subgroup of G . Then $R_3(G) \leq O(|G|/|H| + R_3(H))$.*
- (3) *Suppose every irrep of G has dimension $\leq c$. Then $R_3(G) \leq c'$ where c' depends only on c .*

Our main results are lower bounds. We show that for several groups that are “slightly less abelian” than those covered in Theorem 2 the value R_3 is large. First, we prove tight bounds for the *affine* group.

► **Definition 3.** *The affine group over the field \mathbb{F}_q with q elements is denoted by $\text{Aff}(q)$. This is the group of invertible affine transformations $x \rightarrow ax + b$ where $a, b \in \mathbb{F}_q$ and $a \neq 0$. Equivalently, it is the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a \neq 0$. Note $|\text{Aff}(q)| = q(q - 1)$.*

► **Theorem 4.** $R_3(\text{Aff}(q)) = \Theta(\log |\text{Aff}(q)|)$.

The upper bound is trivial since for any group G the input length is $O(\log |G|)$.

Then we consider the so-called finite *lamplighter group*. This group is obtained from \mathbb{Z}_2^n by adding a “shift” of the coordinates, formally by taking the *wreath product* \wr of \mathbb{Z}_2 and \mathbb{Z}_n .

► **Definition 5.** *The finite lamplighter group is $L_n := \mathbb{Z}_2 \wr \mathbb{Z}_n$. Elements of L_n can be written as $(x_0, x_1, \dots, x_{n-1}; s)$ where $x_i \in \mathbb{Z}_2$ and $s \in \mathbb{Z}_n$ and we have $(x_0, x_1, \dots, x_{n-1}; s) \cdot (x'_0, x'_1, \dots, x'_{n-1}; s') = (x_0 + x'_{0+s}, x_1 + x'_{1+s}, \dots, x_{n-1} + x'_{n-1+s}; s + s')$ where addition is modulo n . For $(x; s) \in L_n$ we call x the \mathbb{Z}_2^n part and s the \mathbb{Z}_n part. Note $|L_n| = 2^n \cdot n$.*

In other words, when multiplying $(x; s)$ and $(x'; s')$ we first shift x' by s , and then we sum component-wise. We prove a tight communication bound for $R_3(L_n)$.

► **Theorem 6.** $R_3(L_n) = \Theta(\log \log |L_n|)$.

The upper bound is as follows. The parties can first communicate the \mathbb{Z}_n parts. This takes $O(\log n) = O(\log \log |L_n|)$ communication. Then the parties can shift their \mathbb{Z}_2^n parts privately, and finally use the constant-communication protocol for \mathbb{Z}_2^n .

We then move to groups of the form H^n . An interesting setting is when $|H|$ is small compared to n , say H has constant size.

► **Theorem 7.** *Let H be a non-abelian group. Then $R_3(H^n) = \Omega(\log n)$.*

It is an interesting open question whether a bound of $\Omega(n)$ holds. We note that for the corresponding 4-party problem of deciding if $abcd = 1_G$ such an $\Omega(n)$ bound can be established by a reduction from lower bounds for *disjointness*. The proof proceeds by encoding the And of two bits by a group product of length four, see [30]. However, those techniques do not seem to apply to the three-party problem, and appear unrelated to mixing.

1.2 Mixing in groups

At a high level, mixing refers to the general phenomenon that when we have several independent, high-entropy distributions over a group and we combine them in natural ways, for example by multiplying, the resulting random variable becomes closer to the uniform distribution, closer than the original distributions are. Our notion of (non) entropy of a distribution A is the *collision probability* $\Pr[A = A']$ where A and A' are independent and identically distributed. We define next a scaled version which is more convenient.

► **Definition 8.** *The scaled collision probability of a distribution A over G is $N(A) := |G| \Pr[A = A']$, where A and A' are independent and identically distributed. Equivalently, $N(A) = (|G| \|A\|_2)^2$ where $\|A\|_2$ is the L_2 norm $\sqrt{\mathbb{E}_x \mathbb{P}[A = x]}$.*

To illustrate the normalization, note that, for any distribution A , $N(A) \leq |G|$ and it can be shown $N(A) \geq 1$. If A is uniform over a set of size $\delta|G|$ we have $N(A) = \delta^{-1}$. The uniform distribution has $\delta = 1$ and $N = 1$, the distribution concentrated on a single point has $\delta = 1/|G|$ and $N = |G|$. Distributions that are uniform on a constant fraction of the elements have $N \leq O(1)$; in the latter setting the main ideas in this paper are already at work, so one can focus on it while reading the paper.

To measure the distance between distributions we use *total variation distance*.

► **Definition 9.** *The total variation distance between distributions A and B is $\Delta(A, B) = \sum_x |\mathbb{P}[A = x] - \mathbb{P}[B = x]|$. Equivalently, $\Delta(A, B)$ is the ℓ_1 norm $\sum_x |f(x)|$ of the function $f(x) = \mathbb{P}[A = x] - \mathbb{P}[B = x]$.*

We can now illustrate a basic result about mixing. Suppose that A and B are independent random variables over a group G such that $N(A)$ and $N(B)$ are $O(1)$. We would like to show that the random variable AB is close to the uniform distribution U over G . This is false for example over the group \mathbb{Z}_2^n . Indeed, A and B could each be the uniform distribution where the first coordinate is 0, and then AB would be the same as A , which has $\Delta(A, U) \geq \Omega(1)$.

Remarkably, however, for other groups one can show that $\Delta(AB, U)$ is small. We state this fundamental result next.

► **Theorem 10.** *Let A and B be two independent random variables over G . We have*

$$\Delta(AB, U) \leq \sqrt{\frac{N(A)N(B)}{d}},$$

where d is the minimum dimension of a non-trivial irrep of G .

This theorem appears in equivalent form as Lemma 3.2 in [12]. The formulation above appears in [6]. Other proofs were discovered later, and the result is now considered folklore. The importance of this result is that for several groups the value d is large, and so the theorem shows that AB is close to U . In particular, for non-abelian *simple* groups we have that d grows with the size of the group, and for the *special-linear* group $SL_2(q)$ d is polynomial in the size of the group. For more discussion and pointers, we refer the reader to Section 13 in [13] and to the original paper [12]. The latter calls *quasirandom* the groups that have a large d .

In this work we consider several groups for which one cannot prove a good bound on $\Delta(AB, U)$ for every two independent distributions with small N . In particular, the group has an irrep of small dimension. The question arises of what type of mixing result, if any, makes sense.

Our approach to mixing

Our approach is to show that even though $\Delta(AB, U)$ might be large, nevertheless AB acquires some “invariance property” of U which the distributions A and B in isolation may not have. One natural property of U is that it is invariant under multiplication by a fixed element: for any $y \in G$ we have that yU and U are the same distribution. So a first attempt is to say that G mixes if there exists a non-identity element y such that $\Delta(AB, yAB)$ is small, for any independent A and B with small N .

We show that this is indeed the case for the affine and the lamplighter group.

However, for groups like H^n this notion cannot be met: for any fixed $y \neq 1_G$, one can define A and B which fix one coordinate i where $y_i \neq 1_H$ and are uniform on the others; these distributions have small N but $\Delta(AB, yAB)$ is large. To overcome this obstacle we will use randomness in our definition of the invariance property.

In the special case that H does not have irreps of dimension one, we show that AB is almost invariant under selecting a uniform coordinate and replacing that coordinate with a uniform element. In other words, if Y is the uniform distribution over H^n obtained by setting a uniformly selected coordinate to a uniform element in H and the others to 1 then $\Delta(AB, YAB)$ is small. For general non-abelian H , which might have a unidimensional irrep, this does not work. For example, if $H = H' \times \mathbb{Z}_2$ we cannot change the \mathbb{Z}_2 part. Rather than replacing a coordinate with a uniform element, we take a uniform conjugate. That is, we show that $\Delta(AB, YABY^{-1})$ is small where Y is as before.

To capture these various possibilities, we say that the group mixes if there exists a distribution F on functions from G to G such that $\Delta(AB, F(AB))$ is small. For example, F could be the (fixed, deterministic) function $F(x) = yx$ corresponding to multiplication

by a fixed element y . Over a group of the form H^n , F could be the random function $F(x) = YxY^{-1}$ which selects a uniform coordinate and takes a uniform conjugate of that coordinate.

Intuitively, in all these cases AB becomes somewhat uniform in the sense that it doesn't change much if we apply F to it. Of course for this to be of any use we need that $F(AB) \neq AB$ often. We have arrived to the following definition.

► **Definition 11.** A group G is (ϵ, β) -mixing for (scaled collision probability) $N \leq \eta$ if there exists a distribution F on functions from G to G such that for every distributions A and B with $N(A), N(B) \leq \eta$ we have:

(1) $\Delta(AB, F(AB)) \leq \epsilon$, and

(2) $\Pr[F(AB) = AB] \leq \beta$.

We also say that G mixes via F .

Another important motivation for this definition is given by the following result which links our notion of mixing to communication lower bounds.

► **Lemma 12.** Suppose a group G is $(\epsilon, 0.99)$ -mixing for $N \leq 1/\epsilon$. Then $R_3(G) \geq \Omega(\log(1/\epsilon))$.

The communication lower bounds in the previous section are obtained by establishing mixing results and then using this Lemma 12. We also use this lemma in the contrapositive: by the communication upper bounds from Theorem 2 we obtain non-mixing results. As evident from the statement of the lemma, for the application to communication complexity the setting $\epsilon = \eta$ in Definition 11 suffices, but below we state the more general tradeoff.

The above definition of mixing can be considered “least-useful.” It is a bare-minimum notion that in particular suffices for the communication lower bounds. It is also natural to try to prove a “most-general” mixing result by identifying F such that $F(x)$ has the largest possible entropy. In several cases, our results also identify such F . This also gives additional information in the communication lower bounds. As the proofs will show, the communication lower bounds will establish that the parties, on input $a, b, c \in G$, cannot distinguish $c = (ab)^{-1}$ from $c = F((ab)^{-1})$. Thus understanding via what functions F the group mixes is useful in understanding what information about the product abc the parties can compute.

We now state our mixing results. First we obtain a mixing result for the affine group.

► **Theorem 13.** The affine group $\text{Aff}(q)$ is $(O(s/\sqrt{q}), 0)$ mixing for $N \leq s$ via

$$F(x) := \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \cdot x$$

for any $u \neq 0$.

The error parameter $O(s/\sqrt{q})$ is tight up to polynomials, as the size of the group is $q(q-1)$. Specifically, $\text{Aff}(q)$ is not $(s/q^c, 0.99)$ -mixing for $N \leq s$ for some constant c . This result also achieves a “most general” mixing in terms of F . Note that the matrices $\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$ with $u \in \mathbb{F}_q$ form a subgroup H of $\text{Aff}(q)$, in fact the additive group of \mathbb{F}_q . In particular the theorem gives $(O(s/\sqrt{q}), 1/q)$ -mixing via $F(x) := Hx$, where Hx stands for multiplying x by a uniform element from H , and the $1/q$ is to account for the probability that $u = 0$. In turn, note that for any $a, b \in \mathbb{F}_q$ we have

$$H \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & U \\ 0 & 1 \end{pmatrix}$$

where U is the uniform distribution over \mathbb{F}_q . Thus, the theorem is saying that for any high-entropy distributions A and B , the distribution AB is close to the distribution obtained from AB by replacing the top-right entry with a uniform element in \mathbb{F}_q . This result is the strongest possible in the sense that the top-left entry of AB cannot be changed by F with noticeable probability. This is because that entry is the multiplicative group of \mathbb{F}_q , an abelian group which does not have mixing, as follows from Theorem 2 and Lemma 12.

Then we obtain a mixing result for the lamplighter group.

► **Theorem 14.** *The lamplighter group L_n is $(O(s/n^{1/4}), 0)$ mixing for $N \leq s$ via*

$$F(x) := y \cdot x$$

where $y \in L_n$ depends only on n .

The error parameter $O(s/n^{1/4})$ is tight up to polynomials. As mentioned earlier, $R_3(L_n) = O(\log n)$ and hence for some constant c the group L_n is not $(1/n^c, 0.99)$ -mixing for $N \leq n^c$ by Lemma 12.

As in Theorem 13, the group L_n also mixes via $F(x) = Hx$ where H is the uniform distribution over a subgroup. The definition of H depends on the prime factorization of n . The simplest case is when n is prime. In that case H is the subgroup $\{(z; 0) : \sum_i z_i = 0 \pmod 2\}$ and note that for any $(x; s) \in L_n$ we have

$$H(x; s) = (Z; s)$$

where Z is uniform over \mathbb{Z}_2^n conditioned on $\sum_i Z_i = \sum_i x_i \pmod 2$. Thus, the theorem for n prime is saying that for any high-entropy A and B , the distribution AB is close to the distribution obtained from AB by replacing the \mathbb{Z}_2^n part x (i.e., $AB = (x; s)$) with a uniform element with the same parity as x . This result is strongest possible in the sense that $F(x; s)$ must preserve both the parity of x and the value s with high probability. One way to see this is to note that if F changes either the parity of x or s with high probability then the parties can in fact distinguish inputs of the form $a, b, (ab)^{-1}$ from those of the form $a, b, F((ab)^{-1})$. To do so, the parties can send the parities of the \mathbb{Z}_2^n parts, and can use the efficient protocol for the \mathbb{Z}_n part.

Then we consider direct-product groups H^n . We show that we have mixing for any non-abelian H . Mixing occurs via taking a random coordinate and computing a uniform conjugate of that coordinate.

► **Theorem 15.** *Let H be a non-abelian group. The group H^n is $(O(s^{2/3}/n^{1/3}), 0.99)$ mixing for $N \leq s$ via*

$$F(x_1, x_2, \dots, x_n) := (x_1, x_2, \dots, x_{i-1}, u^{-1}x_i u, x_{i+1}, \dots, x_n),$$

where $i \in \{1, 2, \dots, n\}$ and $u \in H$ are uniform.

The error cannot be improved to $o(1/n)$ even for $N = |H|$, as A and B can just fix a coordinate. But an interesting question is whether the bound on N can be increased to exponential.

Under the stronger assumption that H does not have an irrep of dimension one we improve the bound in several respects, none of which affects the communication results. First, instead of taking a random conjugate of a coordinate we can simply set that coordinate to uniform. Second, we improve the error to about $1/\sqrt{n}$. And third, we show that the bound still holds if one distribution has exponential N (see the proof for this statement).

► **Theorem 16.** *Let H be a group with no non-trivial irrep of dimension one. The group H^n is $(O(s\sqrt{\log(sn)}/\sqrt{n}), 1/|H|)$ mixing for $N \leq s$ via*

$$F(x_1, x_2, \dots, x_n) := (x_1, x_2, \dots, x_{i-1}, x_i u, x_{i+1}, \dots, x_n),$$

where $i \in \{1, 2, \dots, n\}$ and $u \in H$ are uniform.

The smallest group H with no non-trivial irrep of dimension one is the alternating group on five elements, of size 60.

1.3 Techniques for mixing results, and organization

Our main tool for the mixing results is *non-abelian Fourier analysis*. We prove that (the probability mass function of) AB can be approximated by a function whose Fourier coefficients are *few* and have *small dimension*. Then we give different ways in which this fact can be exploited. First, we show that if the *intersection of the kernels of irreps of small dimension* is non-trivial, then we can take F to be multiplication by any non-identity element in that intersection. We call this method the *kernel method*. Using known facts about the representation theory of the affine group, Theorem 13 is proved. For the lamplighter group we also use known facts about its representation theory, and we show that the small-dimensional representations lie, in a suitable sense, within a small-dimensional vector space.

Note that the kernel $K = \{k \in G : \rho(k) = I\}$ of an irrep ρ , where I is the identity matrix, is a *normal subgroup* of G . (The latter means that $g^{-1}kg \in K$ for every $k \in K$ and $g \in G$, which is true because $\rho(g^{-1}kg) = \rho(g^{-1})\rho(k)\rho(g) = \rho(g^{-1}g) = I$.) In particular, the intersection of kernels is also a normal subgroup, and it is in fact known that all normal subgroups arise in this way. Hence, the kernel method shows that $\Delta(AB, HAB)$ is small, where H is the uniform distribution over a normal subgroup. The applicability of the method hinges on our understanding of what normal subgroups arise when considering intersection of kernels of irreps of *bounded dimension*.

The kernel method cannot be applied to groups of the form H^n . For such groups, we use the fact that the irreps ρ of H^n are *tensor products* $\rho_1 \otimes \rho_2 \otimes \dots \otimes \rho_n$ of irreps ρ_i of H , and in particular the dimension of ρ is the product of the dimensions of the ρ_i . Then the key observation is that *low-dimensional irreps of H^n must be tensor products of mostly one-dimensional ρ_i* . And then we use the fact that unidimensional irreps are constant on conjugacy classes. In the special case that H does not have irreps of dimension one we can conclude the stronger fact that most ρ_i are trivial. And then we can get the refined result by extending a well-known Fourier expression for average sensitivity to the non-abelian setting.

We briefly comment on how we prove the communication upper bounds (or equivalently the non-mixing results) in Theorem 2. Item (1) builds on the result for \mathbb{Z}_n that we mentioned earlier and is obtained using the characterization of abelian groups, the Chinese remainder theorem, and hashing. Item (2) uses the random self-reducibility of the $abc = 1_G$ problem together with efficient protocols for disjointness. While (3) follows from (2) and (1) and a known characterization of groups whose irreps all have bounded dimension.

The full version appears at <https://eccc.weizmann.ac.il/report/2021/017/>.

1.4 Open problems

This work raises several interesting questions. First, can we characterize groups which admit non-trivial mixing? (We can define non-trivial as (ϵ, β) -mixing for $N = \omega(1)$ where ϵ and β are bounded constants.) We ask whether a group G has non-trivial mixing if and only if G

has irreps of unbounded dimension. Note that we prove the “only if” direction in this work. Can we prove this at least for some important classes of groups? Can we characterize the groups for which the kernel method suffices?

Another question is whether the bound on N in the H^n results can be improved to exponential, for both distributions. This points to the interesting question of discovering suitable generalizations of classical results in additive combinatorics, such as the Freiman-Ruzsa theorem, for groups of the form H^n .

It would also be interesting to study if the results in this paper can be extended to the *number-on-forehead* [10] model. The study of group products in this model could lead to the solution of several outstanding problems. For example, it is conjectured in [14] that computing the product of many elements is hard even for more than logarithmically many parties (a well-known barrier, see e.g. [29]). Moreover, the problem of computing the product of just three elements could also lead to stronger separations between deterministic and randomized communication. Specifically, it is pointed out in [30] that the “corners” result in [3] can be used to obtain a separation whose parameters match the state-of-the-art [8] but hold for a different function. And as remarked in [3] stronger results could be within reach. For an exposition of the relevant result in [3] see [30]. Can the results for interleaved products in [14] or for “corners” in [3] be suitably extended to other groups such as those in this paper? Those groups might be easier to understand than quasirandom groups, possibly leading to improved results.

References

- 1 Andris Ambainis. Upper bounds on multiparty communication complexity of shifts. In *Symp. on Theoretical Aspects of Computer Science (STACS)*, pages 631–642, 1996.
- 2 Andris Ambainis and Satyanarayana V. Lokam. Improved upper bounds on the simultaneous messages complexity of the generalized addressing function. In *Latin American Symposium on Theoretical Informatics (LATIN)*, pages 207–216, 2000.
- 3 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. doi:10.1007/978-3-319-24298-9_19.
- 4 Tim Austin, Assaf Naor, and Alain Valette. The euclidean distortion of the lamplighter group. *Discret. Comput. Geom.*, 44(1):55–74, 2010. doi:10.1007/s00454-009-9162-6.
- 5 László Babai, Anna Gál, Peter G. Kimmel, and Satyanarayana V. Lokam. Communication complexity of simultaneous messages. *SIAM J. on Computing*, 33(1):137–166, 2003.
- 6 László Babai, Nikolay Nikolov, and László Pyber. Product growth and mixing in finite groups. In *ACM-SIAM Symp. on Discrete Algorithms (SODA)*, pages 248–257, 2008.
- 7 Ilya Baran, Erik D. Demaine, and Mihai Pătraşcu. Subquadratic algorithms for 3sum. *Algorithmica*, 50(4):584–596, 2008.
- 8 Paul Beame, Matei David, Toniann Pitassi, and Philipp Woelfel. Separating deterministic from randomized multiparty communication complexity. *Theory of Computing*, 6(1):201–225, 2010. doi:10.4086/toc.2010.v006a009.
- 9 Michael Ben-Or and Richard Cleve. Computing algebraic formulas using a constant number of registers. *SIAM J. on Computing*, 21(1):54–58, 1992.
- 10 Ashok K. Chandra, Merrick L. Furst, and Richard J. Lipton. Multi-party protocols. In *15th ACM Symp. on the Theory of Computing (STOC)*, pages 94–99, 1983.
- 11 Martin Dietzfelbinger, Torben Hagerup, Jyrki Katajainen, and Martti Penttonen. A reliable randomized algorithm for the closest-pair problem. *J. Algorithms*, 25(1):19–51, 1997.
- 12 W. T. Gowers. Quasirandom groups. *Combinatorics, Probability & Computing*, 17(3):363–387, 2008.

- 13 W. T. Gowers. Generalizations of Fourier analysis, and how to apply them. *Bull. Amer. Math. Soc. (N.S.)*, 54(1):1–44, 2017. doi:10.1090/bull/1550.
- 14 W. T. Gowers and Emanuele Viola. Interleaved group products. *SIAM J. on Computing*, 48(3):554–580, 2019. Special issue of FOCS 2016.
- 15 Neil Immerman and Susan Landau. The complexity of iterated multiplication. *Inf. Comput.*, 116(1):103–116, 1995.
- 16 Kenneth Krohn, W. D. Maurer, and John Rhodes. Realizing complex Boolean functions with simple groups. *Information and Control*, 9:190–195, 1966.
- 17 Eyal Kushilevitz and Noam Nisan. *Communication complexity*. Cambridge University Press, 1997.
- 18 James R. Lee, Assaf Naor, and Yuval Peres. Trees and Markov convexity. *Geom. Funct. Anal.*, 18(5):1609–1659, 2009. doi:10.1007/s00039-008-0689-0.
- 19 Shachar Lovett, Cristopher Moore, and Alexander Russell. Group representations that resist random sampling. *Random Struct. Algorithms*, 47(3):605–614, 2015. doi:10.1002/rsa.20555.
- 20 Eric Miles. Iterated group products and leakage resilience against NC^1 . In *ACM Innovations in Theoretical Computer Science conf. (ITCS)*, 2014.
- 21 Eric Miles and Emanuele Viola. Shielding circuits with groups. In *ACM Symp. on the Theory of Computing (STOC)*, 2013.
- 22 David A. Mix Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC^1 . *J. of Computer and System Sciences*, 38(1):150–164, 1989.
- 23 Mihai Pătraşcu. Towards polynomial lower bounds for dynamic problems. In *ACM Symp. on the Theory of Computing (STOC)*, pages 603–610, 2010.
- 24 Pavel Pudlák, Vojtěch Rödl, and Jiří Sgall. Boolean circuits, tensor ranks, and communication complexity. *SIAM J. on Computing*, 26(3):605–633, 1997.
- 25 Anup Rao and Amir Yehudayoff. *Communication complexity*. Cambridge University Press, 2019. <https://homes.cs.washington.edu/~anuprao/pubs/book.pdf>.
- 26 Ran Raz. The BNS-Chung criterion for multi-party communication complexity. *Computational Complexity*, 9(2):113–122, 2000.
- 27 Aner Shalev. Mixing, communication complexity and conjectures of Gowers and Viola. *Combinatorics, Probability and Computing*, pages 1–13, June 2016. arXiv:1601.00795. doi:10.1017/S096354831600016X.
- 28 Emanuele Viola. The communication complexity of addition. *Combinatorica*, pages 1–45, 2014.
- 29 Emanuele Viola. Challenges in computational lower bounds. *SIGACT News, Open Problems Column*, 48(1), 2017.
- 30 Emanuele Viola. Non-abelian combinatorics and communication complexity. *SIGACT News, Complexity Theory Column*, 50(3), 2019.
- 31 Avi Wigderson. Representation theory of finite groups, and applications. Available at <http://www.math.ias.edu/~avi/TALKS/>, 2010.
- 32 Andrew Chi-Chih Yao. Some complexity questions related to distributive computing. In *11th ACM Symp. on the Theory of Computing (STOC)*, pages 209–213, 1979.
- 33 Yufei Zhao. Group representations that resist worst-case sampling, 2017. arXiv:1705.04675.