# THE WORK OF MARK BRAVERMAN

RAN RAZ

**ABSTRACT**

Mark Braverman was awarded the 2022 IMU Abacus medal for his work on Information Complexity and additional work. Mark is a world leader of the research area of information complexity and his works are among the most influential in this research area. Mark has a broad research interest and key works in several other research areas, that in some cases solved central long-standing open problems. We describe some of his work, focusing mainly on contribution to information complexity and related topics at the interface of computational complexity and information theory.

**MATHEMATICS SUBJECT CLASSIFICATION 2020**

Primary 68Q11; Secondary 68P30, 94A15, 68Q01, 68Q17

**KEYWORDS**

Computational complexity, communication complexity, information theory, information complexity

INTERNATIONAL CONGRESS OF MATHEMATICIANS
2022 JULY 6–14


Proc. Int. Cong. Math. 2022, Vol. 1, pp. 106–117
DOI 10.4171/ICM2022/214

Published by EMS Press

## 1. COMMUNICATION COMPLEXITY

Communication complexity, first introduced by Yao [54], is a central model in complexity theory that studies the amount of communication needed to solve a problem, when the input to the problem is distributed among two or more parties.

In the two-player distributional model, each of two players gets an input, where the two inputs $X, Y$ are random variables sampled from some joint distribution (known to both players). The players' goal is to solve a communication task that depends on both inputs, such as computing a function $f(X, Y)$, where $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is known to both players and $X, Y$ are inputs of length $n$ bits. The players communicate in rounds, where in each round one of the players sends a message to the other player. At the end of the protocol, in the example given above, both players need to know the value of $f(X, Y)$. The players are allowed to use both public and private random strings and are allowed to err with some fixed small probability.

The communication complexity of a protocol is the maximal number of bits communicated by the players in the protocol, where the maximum is taken over all possible inputs (in the support of the input distribution). The communication complexity of a communication task is the minimal communication complexity of a protocol that solves the task with high probability (say, probability larger than $\frac{2}{3}$).

## 2. INFORMATION COMPLEXITY

Information complexity, introduced by [1, 2, 25], studies the amount of information that two players need to reveal about their inputs in order to solve a communication task. The model was motivated by fundamental information-theoretical questions of compressing communication, as well as by fascinating relations to communication complexity, and in particular to proving lower bounds for communication complexity and to the direct-sum problem in communication complexity, a problem that has a rich history and has been studied in many works and various settings.

The paper by Barak, Braverman, Chen, and Rao distinguishes between internal and external information complexity of a communication protocol [2]. Roughly speaking, the external information complexity of a protocol, first defined in [25], is the amount of information that an external observer, who watches the execution of the protocol, learns about the players' inputs, while the internal information complexity of a protocol, implicit in [1] and explicitly defined in [2], is the amount of information that the players learn about each other's input, when running the protocol.

Formally, if $M$ is the transcript of the protocol and $R$ is the public random string, external and internal information complexity are defined by

$$\begin{aligned} \mathrm{Ext} &= I\big((X, Y); M \mid R\big), \\ \mathrm{Int} &= I(X; M \mid Y, R) + I(Y; M \mid X, R), \end{aligned}$$

where $I$ is the conditional mutual information function. (It is known that the private random strings of the protocol can be ignored here.)

The (internal or external) information complexity of a communication task is the infimum of the (internal or external) information complexity of a protocol that solves the task with high probability (say, probability larger than $\frac{2}{3}$).

It is not hard to prove that for any protocol (and thus also for any communication task), the internal information complexity of the protocol is at most its external information complexity, which, in turn, is at most its communication complexity. This motivated the study of information complexity as a tool for proving lower bounds for communication complexity.

A beautiful and useful property of internal information complexity, that motivated its definition, is the additivity property, or direct-sum property. Roughly speaking, the internal information complexity of performing two communication tasks, on two independent pairs of inputs, is equal to the sum of the internal information complexities of the two tasks. Consequently, the internal information complexity of performing $k$ copies of a communication task, on $k$ independent pairs of inputs, is equal to $k$ times the internal information complexity of the communication task ([1, 2, 20], using techniques from [43, 45]). The direct-sum property also relates information complexity to the direct-sum problem in communication complexity.

Finally, we note that in the case where the inputs $X, Y$ for the two players are sampled independently, the internal and external information complexity of any protocol are equal.

Much of the work on information complexity was consolidated into a theory in Braverman's works [2, 6, 7, 20]. Braverman also defined a variant of information complexity that does not depend on the prior distribution of the input, proving that several possible definitions are essentially equivalent [7].

A priori, it was not clear whether information complexity is computable, in the sense that there is an algorithm that approximates it, but this was proved by Braverman and Schneider (for the zero-error case) [23].

## 3. INTERACTIVE COMPRESSION

The classical works of Shannon, Fano, and Huffman show that if a player wants to send a message $X$ to another player, it is sufficient for her to send $\lceil H(X) \rceil$ bits, in expectation, where $H$ denotes Shannon's entropy function [29, 35, 50]. That is, the length of the message can be compressed to roughly $H(X)$, the information content of the message. Are there analogous results in the interactive setting, where two players engage in an interactive communication protocol?

Barak, Braverman, Chen, and Rao initiated a study of the interactive compression problem [2]. Given a communication protocol with small information complexity, can the protocol be compressed so that the total number of bits communicated by the protocol is also small? More formally, given a communication protocol $\Pi$ with communication complexity $C$ and (internal or external) information complexity $I \ll C$, is there always an equivalent protocol $\Pi'$ (possibly with slightly higher error probability), with communication complexity significantly smaller than $C$ (and arbitrary information complexity)?

Barak, Braverman, Chen, and Rao gave two different compression protocols, one for internal and one for external information complexity. For internal information complexity, they proved that any communication protocol $\Pi$ with communication complexity $C$ and internal information complexity $I$ can be compressed to an equivalent protocol $\Pi'$, with communication complexity $O(\sqrt{C \cdot I} \cdot \log C)$. For external information complexity, they proved that any communication protocol $\Pi$ with communication complexity $C$ and external information complexity $I$ can be compressed to an equivalent protocol $\Pi'$, with communication complexity $O(I \cdot \log C)$ [2]. Recall that internal information complexity is always smaller or equal to external information complexity, and hence compressing the communication complexity to an expression close to the external information complexity of the original protocol is easier.

These results were followed by many additional works that further studied the interactive compression problem. Braverman and Rao proved that any one-round (or small number of rounds) communication protocol with internal information complexity $I$ can be compressed to an equivalent protocol, with communication complexity $O(I)$ [20]. Braverman proved that any communication protocol with internal information complexity $I$ can be compressed to an equivalent protocol, with communication complexity $2^{O(I)}$ [7].

Kol's breakthrough work proved that in the important special case where the two inputs $X, Y$ are independent, any communication protocol with internal/external information complexity $I$ can be compressed to an equivalent protocol, with communication complexity $O(I^2 \cdot \text{polylog}(I))$ [37]. This was culminated by Sherstov who improved the last communication complexity to $O(I \cdot \text{polylog}(I))$ [51]. Note that this last expression does not depend on the communication complexity of the original protocol at all and almost matches the lower bound of $\Omega(n)$. Recall that in the case where $X, Y$ are independent, the internal and external communication complexity are equal. Building on these works, Braverman and Kol proved that any communication protocol with communication complexity $C$ and external information complexity $I$ can be compressed to an equivalent protocol, with communication complexity $\text{poly}(I) \cdot \text{loglog}(C)$ [15].

As for lower bounds, Braverman suggested a candidate for a communication task with communication complexity exponentially larger than (internal or external) information complexity [5]. This task and other communication tasks were analyzed in subsequent works, establishing exponential gaps between communication complexity and information complexity [30–32, 42], namely, examples for communication tasks with (internal or external) information complexity $I$ and communication complexity $2^{\Omega(I)}$. In particular, these works show that Braverman's compression of the communication complexity of a protocol to $2^{O(I)}$ [7] is the best possible, and one cannot hope for compression to $\text{poly}(I)$ in the general case (as obtained by Kol and Shesrtov for the special case of independent inputs $X, Y$ [37, 51]). Building on this line of works, Braverman and Minzer established exponential gaps between internal and external information complexity [17]. An important open problem asks whether compression to $\text{poly}(I) \cdot \text{polylog}(C)$, where $I$ is the internal information complexity, is possible in the general case [11]. (As described above, the best known today are compressions to $O(\sqrt{C \cdot I} \cdot \log C)$ [2] and $2^{O(I)}$ [7].)

In each of the above mentioned compression protocols, the two players manage to sample together, with low communication, a transcript of the original protocol, such that the transcript is sampled (approximately) from the correct distribution on transcripts and both players agree on the same transcript with high probability. One of the challenges is that none of the players knows the correct distribution of transcripts.

As an illustration of the flavor of techniques used in these results, we state a brilliant theorem from the work of Braverman and Rao [20]:

**Theorem.** *Assume that player 1 knows a distribution $P$ and player 2 knows a distribution $Q$ over the same finite set $U$. For every $\varepsilon > 0$, there is a public coin communication protocol that uses an expected number of $D(P \| Q) + 2\log(1/\varepsilon) + O(\sqrt{D(P \| Q)} + 1)$ bits of communication (where $D(P \| Q) = \sum_x P(x)\log(P(x)/Q(x))$ is the Kullback–Leibler informational divergence), such that at the end of the protocol Player 1 outputs an element $a$ distributed according to $P$ and Player 2 outputs an element $b$ such that for every $x \in U$,* $\Pr[b = x | a = x] > 1 - \varepsilon$.

## 4. DIRECT SUM

One of the first motivations for studying information complexity came from relations to the direct-sum problem in communication complexity. The direct-sum problem asks what are the relations between the communication complexity of a communication task and the communication complexity of performing $k$ copies of the same task on $k$ independently chosen inputs.

Let $T$ be a communication task. For every $k$, let $T^k$ be the task of performing $k$ copies of the task $T$, on $k$ inputs that are independently chosen according to the input distribution of $T$, and allowing to err on each copy with the same probability of error that is allowed for the task $T$. The amortized communication complexity of a task $T$ is defined by

$$\lim_{k \to \infty} \frac{\mathrm{CC}(T^k)}{k}$$

where CC denotes communication complexity.

Braverman and Rao proved that the amortized communication complexity of any task $T$ exactly equals to its internal information complexity [20] (see also [41]). This surprising result relates the direct-sum problem in communication complexity to the interactive compression problem.

A priori, one could think that the amortized communication complexity of a task should always be close to its communication complexity. However, using Braverman and Rao's equivalence between amortized communication complexity and internal information complexity, the above mentioned exponential gaps between communication complexity and internal information complexity also imply exponential gaps between communication complexity and amortized communication complexity, showing that there are communication tasks with communication complexity $C$ and amortized communication complexity $O(\log C)$ [30,31,42]. This shows that a strong direct-sum property does not hold for communication complexity.

Conversely, each of the above mentioned compression protocols, in terms of internal information complexity, implies a lower bound on amortized communication complexity. For example, the compression protocols of Kol and Sherstov [37,51] imply that for the special case of independent $X, Y$, communication complexity and amortized communication complexity are essentially equal (up to polylogarithmic factors), and the compression protocol of Braverman [7] implies that amortized communication complexity is at least logarithmic in the communication complexity.

Additional works by Braverman, Rao, Weinstein and Yehudayof [22] and Braverman and Weinstein [24] show that if a protocol tries to solve $T^k$ with communication complexity significantly smaller than $k$ times the amortized communication complexity of $T$, then the success probability of the protocol is exponentially small.

## 5. COMMUNICATION COMPLEXITY OF SET-INTERSECTION

Set-Intersection, or Set-Disjointness, is a central problem in communication complexity. In this problem, each of two (or more) players gets a vector in $\{0,1\}^n$ and their goal is to determine whether there exists a coordinate $i \in [n]$ where they both (or all) have 1. This simple problem inspired a lot of progress in both communication complexity and information complexity.

It has been known since 1987 that the probabilistic communication complexity of Set-Intersection is at least $\Omega(n)$ [36,45]. The main result of the paper by Bar-Yossef, Jayram, Kumar, and Sivakumar, one of the papers that started the research area of information complexity, was a new proof for the lower bound of $\Omega(n)$ for Set-Intersection, using information complexity [1]. This proof was one of their main motivations for studying information complexity.

Braverman used information complexity to study many additional aspects of the communication complexity of Set-Intersection.

While it was known that the probabilistic communication complexity of Set-Intersection is $\Theta(n)$ [1,36,45], Braverman, Garg, Pankratov, and Weinstein studied the information complexity of the Boolean AND function and from that analysis they figured out the exact constant in the $\Theta(n)$ expression, that is, they computed the probabilistic communication complexity of Set-Intersection exactly, up to second-order terms [14].

Braverman and Moitra studied communication protocols for Set-Intersection that get advantage of at least $\varepsilon$ over a random guess. They proved a tight lower bound of $\Omega(\varepsilon n)$ for the communication complexity of any such protocol [18], while previous proofs only implied a lower bound of $\Omega(\varepsilon^2 n)$. From their improved lower bound, they obtained as an application lower bounds for the size of linear programs.

Braverman, Ellen, Oshman, Pitassi, and Vaikuntanathan [10] and Braverman and Oshman [19] used information complexity to prove tight lower bounds for the communication complexity of Set-Intersection with more than two players. Braverman, Garg, Kun-Ko, Mao, and Touchette used a quantum variant of information complexity to prove lower bounds for the quantum communication complexity of Set-Intersection with bounded number of rounds [13].

## 6. PARALLEL REPETITION OF TWO-PROVER GAMES

Information complexity is closely related to the study of parallel repetition of two-prover games. Both areas make substantial use of information theory, but the connection is deeper; the two areas use many similar ideas, intuitions, definitions, tools, and techniques (such as, subadditivity of entropy, correlation-breaking events, and correlated sampling).

In a two-prover (two-player) game, a referee samples questions $(x, y)$ from some (publicly known) distribution, and sends $x$ to the first player and $y$ to the second player. The first player responds by $a = a(x)$ and the second by $b = b(y)$ (without communicating with each other). The players jointly win if a (publicly known) predicate $V(x, y, a, b)$ is satisfied. The value of the game is the maximal probability of success that the players can achieve, where the maximum is taken over all protocols $a = a(x)$, $b = b(y)$.

Roughly speaking, a parallel repetition of a two-prover game is a game where the players try to win $n$ copies of the original game simultaneously. More precisely, the referee generates questions $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$, where each pair $(x_i, y_i)$ is chosen independently according to the original distribution. The players respond by $a = (a_1, \dots, a_n) = a(x)$ and $b = (b_1, \dots, b_n) = b(y)$. The players win if they win simultaneously on all the coordinates, that is, if for every $i$, $V(x_i, y_i, a_i, b_i)$ holds.

The parallel repetition theorem states that for any two-prover game, with value smaller than 1, the value of the game repeated in parallel $n$ times decreases exponentially fast in $n$ [43]. The parallel repetition theorem, and other results about parallel repetition of two-prover games, have many applications in computational complexity and other research areas.

While it was known for a long time that parallel repetition reduces the value of two-prover games exponentially fast, the exact rate of exponential decrease was not known when the value of the game was already small, to begin with. (A tight analysis for games with small value was only known for the special case of projection games [27]).

Braverman and Garg solved this problem. They proved that if the value of the game is $v < 1/2$ and the length of answers is $s$ then the value of the game repeated in parallel $n$ times is at most $v^{\Omega(n \log(1/v)/s)}$ [12]. Only a bound of $2^{-\Omega(n/s)}$ was previously known [43].

## 7. INTERACTIVE CODING THEORY

Shannon's celebrated 1948 paper, "A Mathematical Theory of Communication," initiated (among many other famous contributions) the field of error correcting codes. Suppose that a player wants to send a message of length $n$ bits to another player, but the only available channel is noisy and changes every bit that is sent with some constant probability (smaller than $1/2$). Shannon proved that the player can send a message of length $O(n)$ bits, over the noisy channel, such that from that message the original message can be retrieved with high probability and with no errors [50]. Are there analogous results in the interactive setting, where two players engage in an interactive communication protocol?

This question was first asked and answered by Schulman in 1992. Schulman showed how to translate any interactive communication protocol to an equivalent noise-resilient protocol that runs over a noisy channel, with only a constant overhead in the communication complexity (even when the noise is adversarially chosen) [47–49]. These results initiated interactive coding theory, the study of how to perform an interactive communication protocol reliably in the presence of noise.

In 2011, Braverman and Rao initiated a study of the question of what is the maximal fraction of errors that can be recovered in an interactive protocol. While Schulman's work only recovered a fraction of errors that is bounded by $1/240$, Braverman and Rao showed how to recover $1/4 - \varepsilon$ fraction of errors, when the encoding alphabet size is some constant, and $1/8 - \varepsilon$ fraction of errors, when the encoding alphabet size is just 2. The result holds even in the adversarial case, and at a cost of increasing the communication complexity of the protocol by only a constant factor [21]. (The fraction of errors of $1/8 - \varepsilon$ for an encoding alphabet of size 2 was recently improved to an optimal fraction of $1/6 - \varepsilon$ [28, 34].)

This work by Braverman and Rao initiated a renewed interest in interactive coding theory and inspired many follow-up works. Braverman studied additional aspects of interactive coding theory in many subsequent works. For example, Braverman and Efremenko studied list decoding for interactive communication [8], and Braverman, Efremenko, Gelles, and Haeupler proved that constant-rate coding for multiparty interactive communication is impossible [9].

## 8. LOWER BOUNDS FOR BOUNDED-DEPTH CIRCUITS

Bounded-depth Boolean circuits are among the most important subclasses of Boolean circuits and have been extensively studied in numerous works. They are central in many subareas of complexity theory, as well as in analysis of Boolean functions. Roughly speaking, a Boolean circuit computes a Boolean function of $n$ binary input variables using AND, OR, and NOT gates, where the fan-in of the AND and OR gates is unbounded. The size of the circuit is the number of wires in it and the depth of the circuit is the length of the longest directed path from an input variable to the output (not counting NOT gates).

In 1990, Linial and Nisan conjectured that circuits of size $m$ and depth $d$ cannot distinguish between the uniform distribution over the inputs and any $k$-wise independent distribution over the inputs, with $k \geq (\log m)^{d-1}$ [40]. The conjecture means that a bounded-depth circuit cannot recognize global structure, as long as it does not come with some local structure. This was an important conjecture but there was very little progress for many years and the conjecture was only proved for DNFs (that is, for circuits of depth 2) [3, 46].

In 2009, Braverman proved that circuits of size $m$ and depth $d$ cannot distinguish between the uniform distribution over the inputs and any $k$-wise independent distribution over the inputs, with $k \geq (\log m)^{O(d^2)}$ [4]. This result qualitatively proves the conjecture, with somewhat weaker parameters.

To prove this result, Braverman brilliantly combines two different types of approximation of bounded-depth circuits by low-degree polynomials. The first, by Razborov and Smolensky [44, 52], gives a polynomial that is equal to the function computed by the circuit almost everywhere but may be very different from it on a small fraction of inputs. Braverman observes that the difference between the function computed by the circuit and the approximating polynomial can itself be computed by a bounded-depth circuit. He then approximates that difference by a low-degree polynomial using a different type of approximation, the approximation given by Linial, Mansour, and Nisan [39], that approximates a bounded-depth circuit by a low-degree polynomial that is close to the function computed by the circuit on average. The final result is a low-degree polynomial that approximates the original circuit so well that the trivial proof that low-degree polynomials cannot distinguish between the uniform distribution and $k$-wise independent distributions (with $k$ larger or equal to the degree of the polynomial) works [4].

Since Braverman published his work, it was improved and became more important in two ways. First, Tal's breakthrough work [53] improved the approximation given by Linial, Mansour, and Nisan [39] and by plugging in the new parameters into Braverman's proof he obtained an improved result: Circuits of size $m$ and depth $d$ cannot distinguish between the uniform distribution over the inputs and any $k$-wise independent distribution over the inputs, with $k \geq (\log m)^{O(d)}$ [53]. This comes even closer to proving the original conjecture. Additionally, Chattopadhyay and Zuckerman used these results in their breakthrough construction of explicit two-source extractors [26].

## 9. GROTHENDIECK'S CONSTANT VS. KRIVINE'S BOUND

In 1953, Grothendieck proved that there is a positive constant $K \in \mathbb{R}$, such that, for any $m \times n$ real matrix $(a_{ij})_{i \in [m], j \in [n]}$,

$$\max_{\{X_i\},\{Y_j\}} \sum_{i,j} a_{ij} \langle X_i, Y_j \rangle \leq K \cdot \max_{\{x_i\},\{y_j\}} \sum_{i,j} a_{ij} x_i y_j,$$

where $X_i$, $Y_j$ (on the left-hand side) are unit vectors in $\mathbb{R}^{m+n}$ and $x_i$, $y_j$ (on the right-hand side) are in $\{-1, 1\}$ [33]. The smallest value of $K$ that satisfies this inequality is called Grothendieck's constant.

This is an important theorem, with applications in several areas. In computer science, Grothendieck's constant can be viewed as the integrality gap between a maximum obtained over values in $\{-1, 1\}$, on the right-hand side, that is many times desirable but is often hard to compute, and the maximum obtained over unit vectors, on the left-hand side, that can be computed in polynomial time.

The exact value of Grothendieck's constant is still not known. In 1979, Krivine proved that Grothendieck's constant is at most $\frac{\pi}{2 \ln(1+\sqrt{2})}$ and conjectured that this is an equality [38]. The conjecture was disproved by Braverman, Makarychev, Makarychev, and Naor [16].

### FUNDING

Supported by the Simons Collaboration on Algorithms and Geometry, by a Simons Investigator Award and by the National Science Foundation grants No. CCF-1714779, CCF-2007462.

### REFERENCES

[1] Z. Bar-Yossef, T. S. Jayram, R. Kumar, and D. Sivakumar, An information statistics approach to data stream and communication complexity. *J. Comput. System Sci.* **68** (2004), no. 4, 702–732.

[2] B. Barak, M. Braverman, X. Chen, and A. Rao, How to compress interactive communication. *SIAM J. Comput.* **42** (2013), no. 3, 1327–1363.

[3] L. M. J. Bazzi, Polylogarithmic independence can fool DNF formulas. *SIAM J. Comput.* **38** (2009), no. 6, 2220–2272.

[4] M. Braverman, Polylogarithmic independence fools AC0 circuits. *J. ACM* **57** (2010), no. 5, 28:1–28:10.

[5] M. Braverman, A hard-to-compress interactive task? In *51th Annual Allerton Conference on Communication, Control, and Computing*, pp. 8–12, IEEE, 2013.

[6] M. Braverman, Interactive information and coding theory. In *Proceeding of the international congress of mathematicians, ICM 2014*, pp. 535–559, KYUNG MOON SA Co. Ltd, 2014.

[7] M. Braverman, Interactive information complexity. *SIAM J. Comput.* **44** (2015), no. 6, 1698–1739.

[8] M. Braverman and K. Efremenko, List and unique coding for interactive communication in the presence of adversarial noise. *SIAM J. Comput.* **46** (2017), no. 1, 388–428.

[9] M. Braverman, K. Efremenko, R. Gelles, and B. Haeupler, Constant-rate coding for multiparty interactive communication is impossible. *J. ACM* **65** (2018), no. 1, 4:1–4:41.

[10] M. Braverman, F. Ellen, R. Oshman, T. Pitassi, and V. Vaikuntanathan, A tight bound for set disjointness in the message-passing model. In *FOCS*, pp. 668–677, IEEE, 2013.

[11] M. Braverman, A. Ganor, G. Kol, and R. Raz, A candidate for a strong separation of information and communication. In *ITCS*, pp. 11:1–11:13, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018.

[12] M. Braverman and A. Garg, Small value parallel repetition for general games. In *STOC*, pp. 335–340, ACM, 2015.

[13] M. Braverman, A. Garg, Y. Kun-Ko, J. Mao, and D. Touchette, Near-optimal bounds on the bounded-round quantum communication complexity of disjointness. *SIAM J. Comput.* **47** (2018), no. 6, 2277–2314.

[14] M. Braverman, A. Garg, D. Pankratov, and O. Weinstein, From information to exact communication. In *STOC*, pp. 151–160, ACM, 2013.

[15] M. Braverman and G. Kol, Interactive compression to external information. In *STOC*, pp. 964–977, ACM, 2018.

[16] M. Braverman, K. Makarychev, Y. Makarychev, and A. Naor, The Grothendieck constant is strictly smaller than Krivine's bound. In *FOCS*, pp. 453–462, IEEE, 2011.

[17] M. Braverman and D. Minzer, New separations results for external information. In *STOC*, pp. 248–258, ACM, 2021.

[18] M. Braverman and A. Moitra, An information complexity approach to extended formulations. In *STOC*, pp. 161–170, ACM, 2013.

[19] M. Braverman and R. Oshman, A rounds vs. communication tradeoff for multi-party set disjointness. In *FOCS*, pp. 144–155, IEEE, 2017.

[20] M. Braverman and A. Rao, Information equals amortized communication. *IEEE Trans. Inf. Theory* **60** (2014), no. 10, 6058–6069.

[21] M. Braverman and A. Rao, Toward coding for maximum errors in interactive communication. *IEEE Trans. Inf. Theory* **60** (2014), no. 11, 7248–7255.

[22] M. Braverman, A. Rao, O. Weinstein, and A. Yehudayoff, Direct products in communication complexity. In *FOCS*, pp. 746–755, IEEE, 2013.

[23] M. Braverman and J. Schneider, Information complexity is computable. In *ICALP*, pp. 87:1–87:10, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016.

[24] M. Braverman and O. Weinstein, An interactive information odometer and applications. In *STOC*, pp. 341–350, ACM, 2015.

[25] A. Chakrabarti, Y. Shi, A. Wirth, and A. C. C. Yao, Informational complexity and the direct sum problem for simultaneous message complexity. In *FOCS*, pp. 270–278, IEEE, 2001.

[26] E. Chattopadhyay and D. Zuckerman, Explicit two-source extractors and resilient functions. In *STOC*, pp. 670–683, ACM, 2016.

[27] I. Dinur and D. Steurer, Analytical approach to parallel repetition. In *STOC*, pp. 624–633, ACM, 2014.

[28] K. Efremenko, G. Kol, and R. Saxena, Binary interactive error resilience beyond $1/8$ (or why $(1/2)^3 > 1/8$). In *FOCS*, pp. 470–481, IEEE, 2020.

[29] R. M. Fano, *The transmission of information*. Massachusetts Institute of Technology, Research Laboratory of Electronics, 1949.

[30] A. Ganor, G. Kol, and R. Raz, Exponential separation of information and communication. In *FOCS*, pp. 176–185, IEEE, 2014.

[31] A. Ganor, G. Kol, and R. Raz, Exponential separation of information and communication for boolean functions. *J. ACM* **63** (2016), no. 5, 46:1–46:31.

[32] A. Ganor, G. Kol, and R. Raz, Exponential separation of communication and external information. *SIAM J. Comput.* **50** (2021), no. 3.

[33] A. Grothendieck, Résumé de la Théorie Métrique des Produits Tensoriels Topologiques. *Bol. Soc. Mat. São Paulo* **8** (1953), 1–79.

[34] M. Gupta and R. Y. Zhang, The optimal error resilience of interactive communication over binary channels. In *STOC*, pp. 948–961, ACM, 2022.

[35] D. A. Hufman, A method for the construction of minimum redundancy codes. *Proc. IRE* **40** (1952), no. 9, 1098–1101.

[36] B. Kalyanasundaram and G. Schnitger, The probabilistic communication complexity of set intersection. *SIAM J. Discrete Math.* **5** (1992), no. 4, 545–557.

[37] G. Kol, Interactive compression for product distributions. In *STOC*, pp. 987–998, ACM, 2016.

[38] J. L. Krivine, Constantes de Grothendieck et Fonctions de Type Positif sur les Spheres. *Adv. Math.* **31** (1979), no. 1, 16–30.

[39] N. Linial, Y. Mansour, and N. Nisan, Constant depth circuits, Fourier transform, and learnability. *J. ACM* **40** (1993), no. 3, 607–620.

[40] N. Linial and N. Nisan. Approximate inclusion-exclusion. *Combinatorica* **10** (1990), no. 4, 349–365.

[41] N. Ma and P. Ishwar, The infinite-message limit of two-terminal interactive source coding. *IEEE Trans. Inf. Theory* **59** (2013), no. 7, 4071–4094.

[42] A. Rao and M. Sinha, Simplified separation of information and communication. *Theory Comput.* **14** (2018), no. 1, 1–29.

[43] R. Raz, A parallel repetition theorem. *SIAM J. Comput.* **27** (1998), no. 3, 763–803.

[44] A. A. Razborov, Lower bounds on the size of bounded-depth networks over a complete basis with logical addition. *Math. Notes Acad. Sci. USSR* **41** (1987), no. 4, 333–338.

[45] A. A. Razborov, On the distributional complexity of disjointness. *Theoret. Comput. Sci.* **106** (1992), no. 2, 385–390.

[46] A. A. Razborov, A simple proof of Bazzi's theorem. *ACM Trans. Comput. Theory* **1** (2009), no. 1, 3:1–3:5.

[47] L. J. Schulman, Communication on noisy channels: a coding theorem for computation. In *FOCS*, pp. 724–733, IEEE, 1992.

[48] L. J. Schulman, Deterministic coding for interactive communication. In *STOC*, pp. 747–756, ACM, 1993.

[49] L. J. Schulman, Coding for interactive communication. *IEEE Trans. Inf. Theory* **42** (1996), no. 6, 1745–1756.

[50] C. E. Shannon, A mathematical theory of communication. *Bell Syst. Tech. J.* 1948.

[51] A. A. Sherstov, Compressing interactive communication under product distributions. *SIAM J. Comput.* **47** (2018), no. 2, 367–419.

[52] R. Smolensky, Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *STOC*, pp. 77–82, ACM, 1987.

[53] A. Tal, Tight bounds on the Fourier spectrum of AC0. In *Computational Complexity Conference*, pp. 15:1–15:31, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017.

[54] A. C. C. Yao, Some complexity questions related to distributive computing (preliminary report). In *STOC*, pp. 209–213, ACM, 1979.

**RAN RAZ**

Department of Computer Science, Princeton University, Princeton, NJ 08540, USA, ranr@princeton.edu