An Improved Protocol for the Exactly-N Problem[*]

Nati Linial
Hebrew University of Jerusalem, Israel

Adi Shraibman
The Academic College of Tel-Aviv-Yaffo, Israel

Abstract

In the 3-players exactly-N problem the players need to decide whether $x + y + z = N$ for inputs x, y, z and fixed N. This is the first problem considered in the multiplayer Number On the Forehead (NOF) model. Even though this is such a basic problem, no progress has been made on it throughout the years. Only recently have explicit protocols been found for the first time, yet no improvement in complexity has been achieved to date. The present paper offers the first improved protocol for the exactly-N problem. This improved protocol has also interesting consequences in additive combinatorics. As we explain below, it yields a higher lower bound on the possible density of corner-free sets in $[N] \times [N]$.

2012 ACM Subject Classification Theory of computation → Computational complexity and cryptography

Keywords and phrases Communication complexity, Number-On-the-Forehead, Corner-free sets

Digital Object Identifier 10.4230/LIPIcs.CCC.2021.2

Funding *Nati Linial*: Supported in part by Grant 659/18 "High dimensional combinatorics" of the Israel Science Foundation.

Acknowledgements We thank Noga Alon, Aya Bernstine and Alex Samorodnitsky for insightful discussions.

1 Introduction

The multiplayer Number On the Forehead (NOF) model of communication complexity was introduced by Chandra, Furst and Lipton [9]. Given a function $f : [N]^k \to \{0, 1\}$, the k players in this scenario should jointly find out $f(x_1, \ldots, x_k)$. We think of x_i as being placed on player i's forehead, so that each player sees the whole input bar one argument. Players communicate by writing bits on a shared blackboard according to an agreed-upon protocol. This model is intimately connected to several key problems in complexity theory. E.g., lower bounds on the size of ACC^0 circuits for a natural function in P [23, 12], branching programs, time-space tradeoffs for Turing machines [13], and proof complexity [5]. In addition, progress in the NOF model, even for a specific problem and for $k = 3$, would have profound implications in graph theory and combinatorics [14, 3].

Much of Chandra, Furst and Lipton's seminal paper [9] is dedicated to the exactly-N function $f : [N]^k \to \{0, 1\}$, where $f(x_1, \ldots, x_k) = 1$ iff $\sum x_i = N$. They discovered a connection between the communication complexity of this function and well-known problems in additive combinatorics and Ramsey theory. They used Ramsey's theory to prove a (rather weak) lower bound on the NOF communication complexity of this function. Using the connection to additive number theory, they showed that a $O(\sqrt{\log N})$ protocol exists, although they have not made this protocol explicit.

[*] Our companion paper "Larger Corner-Free Sets from Better NOF Exactly-$\boldsymbol{N}$ Protocols" presents the same results, emphasizing the combinatorial perspective.

There are several reasons why it is highly significant to determine the communication complexity of the exactly-N function, aside of the very fundamental nature of the problem:

- Our poor understanding of this question is manifested by the huge gap between the upper and lower bounds that we currently have on the communication complexity of this problem. This gap is double exponential for three players, and is even worse for $k > 3$ players.
- Despite the significance of the NOF model, we still know very little about it. The rich web of mathematical and computational concepts surrounding the exactly-N function suggests that it may open the gate to progress in understanding numerous other NOF functions.
- The k-player exactly-N function is a *graph function* [4]. For most functions in this class the deterministic and randomized communication complexity differ substantially, but no explicit function with a significant gap is presently known.
- This problem is *equivalent* to corner theorems in additive combinatorics (e.g., [2]), and is closely related to other important problems such as constructing Ruzsa-Szemerédi graphs and the triangle removal lemma [14, 3].

Nevertheless, progress on the complexity of the NOF exactly-N problem has mostly been made on the additive combinatorics side and includes several breakthrough results such as Szemerédi's regularity lemma [21], and its extension to hypergraphs [11, 17, 16]. Translated back to the realm of NOF communication complexity, these advances bear on lower bounds in communication complexity, yet there is essentially nothing concerning upper bounds. We believe that the more promising line of attack is for advances in communication complexity to shed light on questions in additive combinatorics by exploiting the power of new algorithmic ideas.

As mentioned, the existence of a protocol for the exactly-N problem has already been known since [9]. However, this was just an existential statement and no actual protocol was provided. This lacuna was recently remedied with two protocols [14, 3] of the exact same complexity as the one whose existence was proven in [9], namely of complexity[1]

$$2\sqrt{2}\sqrt{\log N} + o(\sqrt{\log N}) = 2.828...\sqrt{\log N} + o(\sqrt{\log N}). \tag{1}$$

Here we give the first improved protocol for the exactly-N problem, and prove

▶ **Theorem 1.** *There is an explicit protocol for NOF exactly-N of complexity*

$$2\sqrt{\log e}\sqrt{\log N} + o(\sqrt{\log N}) = 2.4022...\sqrt{\log N} + o(\sqrt{\log N}). \tag{2}$$

Due to the connection between NOF complexity and additive combinatorics, our improved protocol has interesting implications in that area that we briefly mention now. More details are given in Section 3. Let $\rho_3(N)$ be the largest density of a subset of $[N]$ that contains no 3-term arithmetic progression. As Roth [18] showed, $\rho_3(N) = o(1)$. However, we still do not know the rate at which $\rho_3(N)$ tends to 0. The upper bounds have gradually improved over the years and the current "world record" found in 2020 by Bloom and Sisask [8] is

$$\rho_3(N) \leq (\log N)^{-1-c} \text{ for some absolute constant } c > 0.$$

[1] All logarithms in this paper are in base 2.
Also, unless otherwise specified, all asymptotic statements are taken with $N \to \infty$.

Much less has happened with the lower bound. Behrend's construction [6] yields

$$\rho_3(N) \geq 2^{-2\sqrt{2}\sqrt{\log N}+o(\sqrt{\log N})} = 2^{-2.828\ldots\sqrt{\log N}+o(\sqrt{\log N})}.$$

But in the ensuing 75 years, only the little-oh term saw an improvement (Elkin [10]).

A *corner* in $\mathbb{N}^2$ is a triple of points $(x, y), (x + \delta, y), (x, y + \delta)$ for some $\delta \neq 0$. Let $\rho_3^{\angle}(N)$ be the largest density of a subset of $[N] \times [N]$ that contains no corner. Ajtai and Szemerédi's *corner theorem* [2] shows that $\rho_3^{\angle}(N) = o(1)$. This readily implies Roth's theorem that $\rho_3(N) = o(1)$.

The best previously known lower bound on $\rho_3^{\angle}(N)$ again comes from Behrend's construction:

$$\rho_3^{\angle}(N) \geq 2^{-2\sqrt{2}\sqrt{\log N}+o(\sqrt{\log N})} = 2^{-2.828\ldots\sqrt{\log N}+o(\sqrt{\log N})}.$$

Our work gives the first improvement in decades, showing (Theorem 3)

$$\rho_3^{\angle}(N) \geq 2^{-2\sqrt{\log e}\sqrt{\log N}+o(\sqrt{\log N})} = 2^{-2.4022\ldots\sqrt{\log N}+o(\sqrt{\log N})}.$$

2 Proof of Theorem 1

The three players in our protocol are called P_x, P_y and P_z. The inputs that they get to see are $(y, z), (x, z)$ and (x, y) respectively.

Here is a similar problem in the realm of vector addition. Given integers $q, d > 1$, define $g = g_{q,d}(\alpha, \beta, \gamma)$ to be 1 if $\alpha + \beta = \gamma$ and 0 otherwise. Here $\alpha, \beta \in [q]^d$, $\gamma \in [2q]^d$ and addition is vector addition in $\mathbb{R}^d$. The following one-round protocol [3] for g is correct because the inequality $\|2\alpha - \gamma\|^2 + \|2\beta - \gamma\|^2 \geq 2\|\alpha - \beta\|^2$ holds always and is an equality iff $\gamma = \alpha + \beta$.

▶ **Protocol 1.** A protocol for $g_{q,d}$

1. *P_z computes $\|\alpha - \beta\|_2^2$, and writes the result on the board.*

2. *P_y writes 1 iff $\|\alpha - \beta\|_2^2 = \|2\alpha - \gamma\|_2^2$.*

3. *P_x writes 1 iff $\|\alpha - \beta\|_2^2 = \|2\beta - \gamma\|_2^2$.*

The cost of this protocol is $2 + \log dq^2$.

The above is an efficient method to decide high-dimensional vector addition, but our objective is to decide the integer addition relation $X + Y + Z = N$. We let $x = X, y = Y$ and $z = N - Z$, so the relation we need to consider is $x + y = z$.

Our protocol to decide whether $x + y = z$ builds on the protocol for $g_{q,d}$. It is the issue of carry bits in integer addition that makes this decision problem harder. The integers $q, d > 1$ are chosen so that

$$2qN > q^d \geq 2N. \tag{3}$$

the specific choice is made below so as to minimize the cost of the protocol.

We denote by w_q the vector that corresponds to the base q representation of the integer w.

As usual, e_i is the d-dimensional vector with 1 in the i-th coordinate and zeros elsewhere. Let $C(x, y) \in \{0, 1\}^d$ be the carry vector when x and y are added in base q. The relation $x + y = z$ among integers is equivalent to the vector relation

$$x_q + y_q = \zeta,$$

where the i-th coordinate of ζ is

$$\zeta_i = z_i + q \cdot C(x, y)_i - C(x, y)_{i-1}$$

(Here $C(x, y)_0 = 0$).

The protocol from [3] now suggests itself: P_z posts $C(x,y)$, and Protocol 1 is used to decide the relation $x_q + y_q = \zeta$. This yields again the estimate (1).

The alternative approach that we adopt here considers instead the equivalent vector relation

$$x_q + \eta = z_q$$

where

$$\eta = (x+y)_q - x_q.$$

Concretely, the i-th coordinate of η is:

$$\eta_i = y_i - q \cdot C(x,y)_i + C(x,y)_{i-1}.$$

In order to run Protocol 1, P_z needs to know η and x_q, which he does. The situation with P_y is even simpler, since he needs to know x_q and z_q which are his inputs. The only difficulty is with P_x who needs to know z_q (which he does) and η. The latter is not part of his input and P_z fills in the missing information for him.

The obvious solution is for P_z to reveal C to P_x using d bits of information. However, we can save communication by exploiting the fact that P_x and P_z share some information, i.e., they both know y for every $y \neq 0$.

By a standard argument in this area which we detail below (Proposition 2), a protocol that works for *typical* pairs x, y can be easily modified to work in *all* cases. So, let us pick x and y uniformly at random from among the d-digit numbers in base q and think of C, the vector of carry bits as a random variable on this probability space. The number of bits that P_z needs to post so that P_x gets to know C, and therefore know η, is $H(C|y)$, the entropy of C given y. The gain is clear, since $H(C) \geq H(C|y)$.

It remains to estimate $H(C|y)$. Fix some integers $s \geq t \geq 0$, and let X be the random variable that is a uniformly sampled subset of $[s]$ of cardinality $\geq t$. It is easily verified that $H(X) = (1 + o_s(1)) \cdot s \cdot h(t/s)$, where $h(\cdot)$ is the univariate entropy function. The entropy of X is the same also if we sample subsets of $[s]$ of cardinality $< t$. Let r be an integer in the range $d \gg r \gg 1$, e.g., $r \approx \sqrt{d}$. For $j = 1, \ldots, r$, let

$$S_j = \{i \mid \frac{qj}{r} > y_i \geq \frac{q(j-1)}{r}\},$$

where $q > y_i \geq 0$ is the i-th digit of y. A carry occurs in digit $i \in S_j$ only if $x_i > \frac{q(r-j)}{r}$, where x_i is the i-th digit of x. Then

$$H(C|y) \leq (1 + o_r(1)) \sum_{j=1}^{r} \frac{|S_j|}{d} h(\frac{j}{r}).$$

Since y is chosen at random, $|S_j| \leq (1 + o_r(1))\frac{d}{r}$, and so

$$H(C|y) \leq (1 + o_r(1)) \sum_{j=1}^{r} \frac{1}{r} h(\frac{j}{r}).$$

The limit of this expression as $r \to \infty$ is

$$\lambda = \int_0^1 h(u)du = \frac{\log e}{2} = 0.721...$$

It is left to optimize on q and d. The complexity of our protocol is

$$\lambda d + \log dq^2 + 2,$$

where recall that $2qN > q^d \geq 2N$. It is not hard to verify that choosing

$$d = \sqrt{\frac{2}{\lambda}\log 2N} \qquad q = 2^{\sqrt{\frac{\lambda}{2}\log 2N}}, \tag{4}$$

we get a protocol with complexity

$$2\sqrt{2\lambda \log N} + o(\sqrt{\log N}),$$

and this is asymptotically optimal in our setting.

To sum up, here is the protocol which proves Theorem 1:

▶ **Protocol 2.** A protocol for exactly-N, for typical pairs x, y

For d, q as in Equation (4)

1. *P_z publishes the vector $\eta = (x+y)_q - x_q$ in a way that P_x can read.*
2. *The players run protocol 1 for $g_{q,d}$ on inputs x_q, η, z_q. That is:*

   a. *P_z writes $\|\eta - x_q\|_2^2$ on the board*
   b. *P_y writes 1 iff $\|\eta - x_q\|_2^2 = \|2x_q - z_q\|_2^2$.*
   c. *P_x writes 1 iff $\|\eta - x_q\|_2^2 = \|2\eta - z_q\|_2^2$.*

▶ **Proposition 2.** *Let $\mathcal{P}$ be an NOF protocol for the exactly-N that works correctly for an $\Omega(1)$-fraction of the input pairs x, y (and every z) with communication complexity $\Phi(N)$. Then there is an NOF protocol that works for all inputs with communication complexity $\Phi(N) + O(\log\log N)$.*

Proof. Let $S \subseteq [N] \times [N]$ be the set of input pairs x, y on which $\mathcal{P}$ succeeds. We claim that there is a collection F of $O(\log N)$ vectors $\Delta \in [N] \times [N]$ such that

$$\cup_{\Delta \in F}(S + \Delta) \supseteq [N] \times [N].$$

In the modified protocol, P_z sees x, y and announces the index of some $\Delta = (\Delta_1, \Delta_2) \in F$ for which $(x - \Delta_1, y - \Delta_2) \in S$. Then the players run Protocol 2 with inputs $(x - \Delta_1, y - \Delta_2, z - \Delta_1 - \Delta_2)$.

The construction of F uses a standard fact about the set-cover problem. For a family of finite sets $\mathcal{X} \subseteq 2^\Omega$ we denote by $c(\mathcal{X})$ the least number of members in $\mathcal{X}$ whose union is Ω. Also $c^*(\mathcal{X})$ is the minimum cost of a fractional cover. Namely,

$$c^*(\mathcal{X}) = \min \sum_{\mathcal{X}} \omega_{\mathrm{X}}, \text{ where } \omega_{\mathrm{X}} \geq 0 \text{ for every } \mathrm{X} \in \mathcal{X} \text{ and } \sum_{\mathrm{x} \in \mathrm{X}} \omega_{\mathrm{X}} \geq 1 \text{ for every } \mathrm{x} \in \Omega.$$

Then

$$c(\mathcal{X}) \leq \log(|\Omega|) \cdot c^*(\mathcal{X})$$

(e.g., Lovász [15]) and actually the greedy algorithm yields a set cover that meets this bound.

In our case $\Omega = [N] \times [N]$, and

$$\mathcal{X} = \{(S + \Delta) \cap ([N] \times [N]) \mid \Delta \in [-N, N] \times [-N, N]\}.$$

It is easily verified that the weights $\omega_x = \frac{10}{N^2}$ constitute a fractional cover, so that $c^*(\mathcal{X}) \leq 40$ and hence $c(\mathcal{X}) \leq 80 \log N$, as claimed. ◀

3 Applications in additive combinatorics

In this section we briefly explain the connections and implications in additive combinatorics.

Van der Waerden's well known theorem [22] states that for every r, k and every large enough N, if the elements of $[N] := \{1, \ldots, N\}$ are colored by r colors, then there must exist a length-k monochromatic arithmetic progression. Erdős and Turán introduced the density version of this theorem. Let $\rho_k(N)$ be the largest density of a subset of $[N]$ without an arithmetic progression of length k. Szemerédi's famous theorem [21] shows that $\rho_k(N) = o(1)$ for every $k \geq 3$.

Extending van der Waerden's theorem, Gallai proved that in every finite coloring of $\mathbb{Z}^2$ some color contains arbitrarily large monochromatic square subarrays. In search of a density version of Gallai's theorem, Erdős and Graham asked about the largest density of a subset of the integer grid $[N] \times [N]$ without a *corner*, i.e., a triple $(x, y), (x + \delta, y), (x, y + \delta)$ for some $\delta \neq 0$. Denote this quantity by $\rho_3^{\angle}(N)$.

Ajtai and Szemerédi [2] proved the first *corners theorem*, showing that $\rho_3^{\angle}(N) = o(1)$. Namely, for every $\varepsilon > 0$ and large enough N, every subset of $[N] \times [N]$ of cardinality εN^2 must contain a corner. This theorem easily yields that $\rho_3(N) = o(1)$, namely, the $k = 3$ case of Szemerédi's theorem (a result of Roth [18], proved two decades before Szemerédi's theorem). Later on, Solymosi [20] showed how to derive Ajtai and Szemerédi's corners Theorem from the Triangle Removal Lemma [19].

The quantitative aspects of all these results: Szemerédi's theorem, the corner theorem, and the triangle removal lemma remain unfortunately poorly understood. In particular, we know very little concerning the lower bounds in these problems. Behrend [6] has famously constructed a large subset of $[N]$ without a 3-term arithmetic progression. This construction implies that

$$\rho_3(N) \geq 2^{-2\sqrt{2}\sqrt{\log N} + o(\sqrt{\log N})}.$$

Using similar tools Elkin [10] improved Behrend's construction. However, his construction only improves the little-o term. Behrend's construction also yields the previously best known lower bounds on $\rho_3^{\angle}(N)$, viz.

$$\rho_3^{\angle}(N) \geq 2^{-2\sqrt{2}\sqrt{\log N} + o(\sqrt{\log N})} = 2^{-2.828\ldots\sqrt{\log N} + o(\sqrt{\log N})}. \tag{5}$$

As mentioned in the introduction, the NOF communication complexity of f is closely related to corners theorems. Our Theorem 1 immediately implies,

▶ **Theorem 3.**

$$\rho_3^{\angle}(N) \geq 2^{-2\sqrt{\log e}\sqrt{\log N} + o(\sqrt{\log N})} = 2^{-2.4022\ldots\sqrt{\log N} + o(\sqrt{\log N})}.$$

There is an explicit corner-free subset of $[N] \times [N]$ *of size*

$$N^2 / 2^{2\sqrt{\log e}\sqrt{\log N} + o(\sqrt{\log N})}.$$

The derivation of Theorem 3 from Theorem 1 is an easy consequence of the following claim.

▷ Claim 4 ([9], implicit).

1. There is an optimal one-round protocol for the addition problem.
2. Let $T = \mathbb{T}(x, y)$ be the message that the P_z sends on inputs (x, y) in a one-round protocol for the addition problem. Then the set

$$S(T) = \{(x, y) : \mathbb{T}(x, y) = T\}$$

is corner-free.

See [9, 7, 1, 14, 3] for more details about the above claim and the relation between communication complexity and additive combinatorics. The same comments and corollaries above apply also verbatim to the $(6,3)$ Theorem (e.g., [19]) and to the quantitative version of the triangle removal lemma.

4 Discussion

The strong relation between the exactly-N problem in the NOF model and questions in additive combinatorics has been discovered decades ago, in the seminal paper of Chundra, Furst and Lipton [9]. However, this subject remains under-developed. We believe that there is a lot to be done here, and many interesting avenues of research that this study can take. One obvious candidate for improvement is the addition problem. We conjecture:

▶ **Conjecture 5.** *The NOF communication complexity of exactly-N is $o(\sqrt{\log N})$. Possibly it is much smaller, even as small as $(\log\log N)^{O(1)}$.*

In the realm of additive combinatorics these conjectures translate to:

▶ **Conjecture 6.**

$$\rho_3^{\angle}(N) \geq 2^{-o(\sqrt{\log N})}.$$

and possibly even

$$\rho_3^{\angle}(N) \geq 2^{-(\log\log N)^{O(1)}}.$$

References

1 A. Ada, A. Chattopadhyay, O. Fawzi, and P. Nguyen. The NOF multiparty communication complexity of composed functions. *computational complexity*, 24(3):645–694, 2015.

2 M. Ajtai and E. Szemerédi. Sets of lattice points that form no squares. *Stud. Sci. Math. Hungar*, 9(1975):9–11, 1974.

3 N. Alon and A. Shraibman. Number on the forehead protocols yielding dense ruzsa–szemerédi graphs and hypergraphs. *Acta Mathematica Hungarica*, 161(2):488–506, 2020.

4 P. Beame, M. David, T. Pitassi, and P. Woelfel. Separating deterministic from randomized nof multiparty communication complexity. In *Proceedings of the 34th International Colloquium On Automata, Languages and Programming*, Lecture Notes in Computer Science. Springer-Verlag, 2007.

5 P. Beame, T. Pitassi, and N. Segerlind. Lower bounds for Lovász-Schrijver systems and beyond follow from multiparty communication complexity. *SIAM Journal on Computing*, 37(3):845–869, 2006.

6 F. A. Behrend. On sets of integers which contain no three terms in arithmetical progression. *Proceedings of the National Academy of Sciences*, 32(12):331–332, 1946.

7 R. Beigel, W. Gasarch, and J. Glenn. The multiparty communication complexity of Exact-T: Improved bounds and new problems. In *International Symposium on Mathematical Foundations of Computer Science*, pages 146–156. Springer, 2006.

8 T. F. Bloom and O. Sisask. Breaking the logarithmic barrier in Roth's theorem on arithmetic progressions. *arXiv preprint*, 2020. `arXiv:2007.03528`.

9 A. Chandra, M. Furst, and R. Lipton. Multi-party protocols. In *Proceedings of the 15th ACM Symposium on the Theory of Computing*, pages 94–99. ACM, 1983.

10 M. Elkin. An improved construction of progression-free sets. In *Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms*, pages 886–905. Society for Industrial and Applied Mathematics, 2010.

11 W. T. Gowers. Hypergraph regularity and the multidimensional szemerédi theorem. *Annals of Mathematics*, pages 897–946, 2007.

12 J. Håstad and M. Goldmann. On the power of small-depth threshold circuits. *Computational Complexity*, 1:113–129, 1991.

13 E. Kushilevitz and N. Nisan. *Communication Complexity.* Cambridge University Press, 1997.

14 N. Linial, T. Pitassi, and A. Shraibman. On the communication complexity of high-dimensional permutations. In *10th Innovations in Theoretical Computer Science Conference, ITCS San Diego, California, USA*, volume 124, pages 54:1–54:20, 2019.

15 L. Lovász. On the ratio of optimal integral and fractional covers. *Discrete Mathematics*, 13:383–390, 1975.

16 B. Nagle, V. Rödl, and M. Schacht. The counting lemma for regular k-uniform hypergraphs. *Random Structures & Algorithms*, 28(2):113–179, 2006.

17 V. Rödl and J. Skokan. Regularity lemma for k-uniform hypergraphs. *Random Structures & Algorithms*, 25(1):1–42, 2004.

18 K. F. Roth. On certain sets of integers. *Journal of the London Mathematical Society*, 1(1):104–109, 1953.

19 I. Ruzsa and E. Szemerédi. Triple systems with no six points carrying three triangles. *Combinatorics (Keszthely, 1976), Coll. Math. Soc. J. Bolyai*, 18:939–945, 1978.

20 J. Solymosi. Note on a generalization of Roth's theorem. *Discrete and Computational Geometry: The Goodman-Pollack Festschrift*, pages 825–827, 2003.

21 E. Szemerédi. On sets of integers containing no k elements in arithmetic progression. *Acta Arith*, 27(199-245):2, 1975.

22 B. L. van der Waerden. Beweis einer Baudetschen Vermutung. *Nieuw Arch. Wiskunde*, 15:212–216, 1927.

23 A. Yao. On ACC and threshold circuits. In *Proceedings of the 31st IEEE Symposium on Foundations of Computer Science*, pages 619–627. IEEE, 1990.