Project: Communication complexity problem

Kovács Fruzsina 2023/2024/I.

1 Background of the problem: Communication complexity

Communication complexity examines the quantity of a form of communication to solve a certain problem, with an input between more than one parties. Its studies were introduced first by Andrew Yao (1979), based on computation distributed among several machines. The communication problem usually runs around more participants, to whom each belongs an n-bit long information, which is usually unknown to the others. One of the main conjecture in connection with complexity is the Log-rank conjecture, which states a polinomial connection between the function of a two-party communication complexity problem and the rank of its input matrix. Let's define the complexity S as

$$S(f) := \min_{\text{all protocols}} \max_{x,y} \{\text{numbers of bits exchanged by the protocol on } x; y\}.$$

The definition of complexity is similar even if the number of participants is more than two.
We use the following notations: $\mathbb{N}^+$ for positive integers, and $[n] = 1, 2, \ldots, n$.

2 Definition of the problem

In the following, we consider a three-player complexity problem. Let A, B and C be the participants of a communication, and x, y and z inputs in a three-participant function. Let's define the communication of a three party function $F : [n]^3 \to \{0; 1\}$ where $F(x, y, z) = 1$ if $x + y + z = n$ and 0 otherwise for a given n. A knows x, y, B knows y, z and C knows x, z (essentially it is called *'number-on-forehead model'*). Our task is to decide whether for any $n \in \mathbb{N}^+$ $n = x + y + z$ holds and we are looking for an algorithm to find the equation with the least possible complexity.

A trivial solution for the problem would be, when one of the participants sends its known inputs to the others (for example A sends x to B, and B can calculate the equation and send back the number 1 to the others, if the equation fulfills, and the number 0 otherwise). The cost of the transfer of the known input is the length of x (in bits), which is $\log_2 n$. Therefore we get, that $S(F) \leq \log_2 n + 2$. In the following section we give a protocol for a substantial improvement.

Let us remark, that if we use a random communication process, if an error has a value of 1/4 at most, we can state, that the complexity of the protocol is logarithmic in the input size, therefore equals a loglog(n) communication.

3 The Deterministic Protocol

Let us recall, that A knows x, y, B knows y, z and C knows x, z. For the protocol we use the method of coloring integers from 1 to n, without it including a three-term arithmetic progression (3-AP-free) in each color class. Let us denote k as the number of the used color classes. In the protocol A, B and C will send the color of their calculated numbers, which we will specialize below.

Let d be the difference $d = n-(x+y+z)$. A calculates $2x+y$, C calculates $2x+y+d = 2x+y+n-x-y-z = n+x-z$ and B calculates $2x + y + 2d = (n + x - z) + d = x - z + n + n - x - y = 2n - 2z - y$. It can be observed, that with the calculation of these values, the numbers form a three-term arithmetic progression respectively. Note that d=0 is true, if and only if all of the three sent colors are the same, since the color classes are 3-AP-free. Two of the participants (A and B) send their colors for the third party, which takes $2\log_2 k$ bits, and C will send back the number 1, if the equation fulfills, and a number 0 otherwise. So the complexity of this protocol is $2\log_2 k + 2$. In section 4 we state the main theorem, where k may be $2^{O(\sqrt{\log n})}$. Therefore we can state

Theorem 1

$$S(F) \leq O(\sqrt{\log n}).$$

4 Tools used for the solution

To calculate, weather the $n = x + y + z$ equation is fulfilled, we apply a celebrated theorem, namely how dense a sequence of integers can be: the possible number of colorings of integer numbers 1 to n, without it including a three-term arithmetic progression (3-AP-free) in each color class.

Theorem 2 *One can color the set $[n]$ with $2^{O(\sqrt{\log n})}$ colors with no monochromatic three-term arithmetic progression.*

4.1 Sketch of the coloring

With taking two parameters d, r and writing each number in base $(2d+1)$ we can color the numbers from 1 to n, i.e. for every $x \in [n]$

$$x = x_0 + x_1(2d+1) + \dots x_j(2d+1)^j + \dots x_r(2d+1)^r,$$

where $x_j \in [d]$, $j = 1, 2, \dots r$ (so there is no crossing if we add such type of two integers). For each x there is a one-to-one map to v, where $v = (x_0, x_1, \dots, x_r) \in \mathbb{N}^n$. A colour class becomes a sphere, i.e. where the norm

$$\|v\| = \sqrt{\sum_{i=1}^{n} x_i^2}$$

is constant. The matched colour classes fulfil the 3-AP-free condition, because no arithmetic progression is possible on the surface of the sphere, since given two points, they can form an arithmetic series only with the third point in their bisector (see Figure 1). Optimizing the parameters as $r = \sqrt{\log n}$ and $d = 2^{O(\sqrt{\log n})}$ we can obtain that the total number of the colorings equals to $2^{O(\sqrt{\log n})}$.

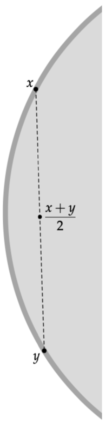

Figure 1: 3-AP[1]

4.2 Other tools

For the optimalization we use the upper bound estimation tools of analysis.

Claim 1 (Cauchy-Schwarz): Let $a_1; a_2; \dots; a_n$, $b_1; b_2; \dots; b_n$ be two sequences of real numbers. Then we have

$$|a_1b_1 + a_2b_2 + \dots + a_nb_n| \le \sqrt{\sum_{i=1}^{n} a_i^2} \cdot \sqrt{\sum_{i=1}^{n} b_i^2}$$

Claim 2 (Growing of functions): For every $m \in \mathbb{N}$, $0 < c < 1$ and $\varepsilon > 0$ we have

$$(\log x)^m \ll 2^{(\log x)^c} \ll x^{\varepsilon}$$

where we write $f(x) \ll g(x)$ if $\lim_{x\to\infty} f(x)/g(x) = 0$.

5 Concluding remarks

The above mentioned estimations are closely related to the core question of additive combinatorics. A celebrated consequence of Theorem 2 is the following.

Corollary 1 *(Behrend) There is a subset B of $[N]$ with cardinality at least $\dfrac{N}{2^{O(\sqrt{\log N})}}$.*

This estimation is the best known (see the book of Tao Vu in the Bibliography).

[1]Source: Rao A., Yehudayoff A. Discrepancy. In: Communication Complexity: and Applications. Cambridge: Cambridge University Press; 2020:67-92. doi:10.1017/9781108671644.008

BIBLIOGRAPHY

Behrend F. A. On sets of integers which contain no three terms in arithmetical progression. Proceedings of the National Academy of Sciences, 32:331-332, 1946.

Yao A.C. Some Complexity Questions Related to Distributed Computing. Proc. of 11th STOC, 1979.

Mitropolsky D. Number-on-forehead Communication Complexity. COMS 6998. 2022.

Rao A., **Yehudayoff** A. Discrepancy. In: Communication Complexity: and Applications. Cambridge: Cambridge University Press; 2020:67-92. doi:10.1017/9781108671644.008

Tao T., **Vu** V. H. Additive Combinatorics. Cambridge University Press.(ISBN-13: 9780521853866; ISBN-10: 0521853869)