Special Topics in Complexity Theory, Fall 2017. Instructor: Emanuele Viola

1 Lecture 15, Scribe: Chin Ho Lee

In this lecture fragment we discuss multiparty communication complexity, especially the problem of separating deterministic and randomized communication, which we connect to a problem in combinatorics.

2 Number-on-forehead communication complexity

In number-on-forehead (NOH) communication complexity each party i sees all of the input $(x_1, \ldots, x_k)$ except its own input x_i. For background, it is not known how to prove negative results for $k \geq \log n$ parties. We shall focus on the problem of separating deterministic and randomizes communication. For $k = 2$, we know the optimal separation: The equality function requires $\Omega(n)$ communication for deterministic protocols, but can be solved using $O(1)$ communication if we allow the protocols to use public coins. For $k = 3$, the best known separation between deterministic and randomized protocol is $\Omega(\log n)$ vs $O(1)$ [BDPW10]. In the following we give a new proof of this result, for a simpler function: $f(x, y, z) = 1$ if and only if $x \cdot y \cdot z = 1$ for $x, y, z \in SL_2(q)$.

For context, let us state and prove the upper bound for randomized communication.

Claim 1. f has randomized communication complexity $O(1)$.

Proof. In the NOH model, computing f reduces to 2-party equality with no additional communication: Alice computes $y \cdot z =: w$ privately, then Alice and Bob check if $x = w^{-1}$. □

To prove a $\Omega(\log n)$ lower bound for deterministic protocols, where $n = \log |G|$, we reduce the communication problem to a combinatorial problem.

Definition 2. A *corner* in a group G is $\{(x, y), (xz, y), (x, zy)\} \subseteq G^2$, where x, y are arbitrary group elements and $z \neq 1_G$.

For intuition, consider the case when G is Abelian, where one can replace multiplication by addition and a corner becomes $\{(x, y), (x+z, y), (x, y+z)\}$ for $z \neq 0$.

We now state the theorem that gives the lower bound.

Theorem 3. Suppose that every subset $A \subseteq G^2$ with $\mu(A) := |A|/|G^2| \geq \delta$ contains a corner. Then the deterministic communication complexity of $f(x, y, z) = 1 \iff x \cdot y \cdot z = 1_G$ is $\Omega(\log(1/\delta))$.

It is known that when G is Abelian, then $\delta \geq 1/\text{polyloglog}|G|$ implies a corner. We shall prove that when $G = SL_2(q)$, then $\delta \geq 1/\text{polylog}|G|$ implies a corner. This in turn implies communication $\Omega(\log\log|G|) = \Omega(\log n)$.

Proof. We saw that a number-in-hand (NIH) c-bit protocol can be written as a disjoint union of 2^c rectangles. Likewise, a number-on-forehead c-bit protocol P can be written as a disjoint union of 2^c *cylinder intersections* $C_i := \{(x, y, z) : f_i(y, z)g_i(x, z)h_i(x, y) = 1\}$ for some $f_i, g_i, h_i \colon G^2 \to \{0, 1\}$:

$$P(x, y, z) = \sum_{i=1}^{2^c} f_i(y, z)g_i(x, z)h_i(x, y).$$

The proof idea of the above fact is to consider the 2^c transcripts of P, then one can see that the inputs giving a fixed transcript are a cylinder intersection.

Let P be a c-bit protocol. Consider the inputs $\{(x, y, (xy)^{-1})\}$ on which P accepts. Note that at least 2^{-c} fraction of them are accepted by some cylinder intersection C. Let $A := \{(x, y) : (x, y, (xy)^{-1}) \in C\} \subseteq G^2$. Since the first two elements in the tuple determine the last, we have $\mu(A) \geq 2^{-c}$.

Now suppose A contains a corner $\{(x, y), (xz, y), (x, zy)\}$. Then

$$\begin{aligned}
(x, y) \in A &\implies (x, y, (xy)^{-1}) \in C &&\implies h(x, y) = 1, \\
(xz, y) \in A &\implies (xz, y, (xzy)^{-1}) \in C &&\implies f(y, (xyz)^{-1}) = 1, \\
(x, zy) \in A &\implies (x, zy, (xzy)^{-1}) \in C &&\implies g(x, (xyz)^{-1}) = 1.
\end{aligned}$$

This implies $(x, y, (xzy)^{-1}) \in C$, which is a contradiction because $z \neq 1$ and so $x \cdot y \cdot (xzy)^{-1} \neq 1_G$. □

References

[BDPW10] Paul Beame, Matei David, Toniann Pitassi, and Philipp Woelfel. Separating deterministic from randomized multiparty communication complexity. *Theory of Computing*, 6(1):201–225, 2010.