# Communication Complexity of Simultaneous Messages*

László Babai † Anna Gál ‡ Peter G. Kimmel § Satyanarayana V. Lokam ¶

May 19, 2003

**Abstract**

In the multiparty communication game (CFL-game) of Chandra, Furst, and Lipton (*Proc. 15th ACM STOC*, 1983, 94–99) $k$ players collaboratively evaluate a function $f(x_0, \ldots, x_{k-1})$ in which player $i$ knows all inputs except $x_i$. The players have unlimited computational power. The objective is to minimize communication.

In this paper, we study the *Simultaneous Messages* (SM) model of multiparty communication complexity. The SM model is a restricted version of the CFL-game in which the players are not allowed to communicate with each other. Instead, each of the $k$ players simultaneously sends a message to a *referee*, who sees none of the inputs. The referee then announces the function value.

We prove lower and upper bounds on the SM-complexity of several classes of explicit functions. Our lower bounds extend to randomized SM complexity via an entropy argument. A lemma establishing a tradeoff between average Hamming distance and range size for transformations of the Boolean cube might be of independent interest.

Our lower bounds on SM-complexity imply an exponential gap between the SM-model and the CFL-model for up to $(\log n)^{1-\epsilon}$ players, for any $\epsilon > 0$. This separation is obtained by comparing the respective complexities of the *generalized addressing function*, $\mathrm{GAF}_{G,k}$, where $G$ is a group of order $n$. We also combine our lower bounds on SM complexity with ideas of Håstad and Goldmann (*Computational Complexity* **1** (1991), 113–129) to derive superpolynomial lower bounds for certain depth-2 circuits computing a function related to the GAF function.

We prove some counter-intuitive upper bounds on SM-complexity. We show that $\mathrm{GAF}_{\mathbb{Z}_2^t,3}$ has SM-complexity $O(n^{0.92})$. When the number of players is at least $c \log n$, for some constant $c > 0$, our SM protocol for $\mathrm{GAF}_{\mathbb{Z}_2^t,k}$ has polylog$(n)$ complexity. We also examine a class of functions defined by certain depth-2 circuits. This class includes the "Generalized Inner Product" function and "Majority of Majorities." When the number of players is at least $2+\log n$, we obtain polylog$(n)$ upper bounds for this class of functions.

**Key Words:** Communication Complexity, Circuit Complexity, Lower Bounds, Group Theory.
**AMS Subject Classification:** 68Q05, 68Q17, 68R05.

*This is a significantly expanded version of the conference paper [BaKL].

†Email: laci@cs.uchicago.edu. Department of Computer Science, University of Chicago. Partially supported by NSF Grants CCR-9014562 and CCR-9732205.

‡Email: panni@cs.utexas.edu. Department of Computer Science, University of Texas at Austin. Partially supported by NSF CAREER Award CCR-9874862 and an Alfred P. Sloan Research Fellowship.

§Email: P-Kimmel@neiu.edu. Northeastern Illinois University.

¶Email: satyalv@eecs.umich.edu. EECS Department, University of Michigan, Ann Arbor. Partially supported by NSF Grant CCR-9988359. Part of the work done while at School of Mathematics, Institute for Advanced Study, Princeton, supported by NSF Grant DMS 97-29992.

‡§¶ A substantial part of the present work was done while the last three authors were students at The University of Chicago.

# 1 Introduction

## 1.1 The Model

Chandra, Furst, and Lipton [CFL] introduced the following multiparty communication game: Let $f(x_0, \ldots, x_{k-1})$ be a Boolean function, where each $x_i$ is a bit-string of fixed length $\leq n$ bits. $k$ players collaborate to evaluate $f(x_0, \ldots, x_{k-1})$. Each player has full knowledge of the function $f$. The $i$-th player knows each input argument except $x_i$; we will refer to $x_i$ as the input *missed* by player $i$. We can imagine input $x_i$ written on the forehead of player $i$. Each player has unlimited computational power. They share a blackboard, viewed by all players, where in each round of the game, some player writes a bit. The last bit written on the board must be the function value.

**Definition 1.1** A *multiparty protocol* is a specification of which player writes in each round and what that player writes. The protocol must specify the following information for each possible sequence of bits that is written on the board so far:

1. Whether or not the game is over, and in case it is not over, which player writes the next bit: This information should be completely determined by the information written on the board so far.

2. What that player writes: this should be a function of the information written on the board so far and of the input seen by that player.

The *cost* of a multiparty protocol is the number of bits written on the board for the worst case input. The *multiparty communication complexity* of $f$, denoted $C(f)$, is the minimum cost of a protocol computing $f$.

Fairly strong multiparty communication complexity lower bounds of the form $n/c^k$ were obtained by Babai, Nisan, and Szegedy [BNS] for some families of explicit functions. However, it seems that those methods do not extend to logarithmic number of players and beyond.

Håstad and Goldmann [HG] found a curious application of the [BNS] bounds to lower bounds for small depth threshold circuits. Subsequent work by Yao [Y] and Beigel and Tarui [BT] reduces ACC circuits (bounded depth, polynomial size circuits with Boolean and MOD $m$ gates) to small depth circuits similar to those considered by [HG]. These results imply that a super-polylogarithmic lower bound for the communication complexity of a function $f$ with super-polylogarithmic number of players would show that $f \notin$ ACC.

In fact, this separation would already follow from similar lower bounds in a weaker model which we call the *simultaneous messages* (SM) model (see Definition 2.1). This connection was pointed out to us by Avi Wigderson.

The SM model is a restricted version of the general multiparty communication model in which the players are not allowed to communicate with each other. Instead, each player can send a single message to a *referee* who sees none of the inputs. The referee announces the value of the function based on the messages sent by the players.

The subject of this paper is the complexity of explicit functions in the SM model.

## 1.2 Lower Bounds

We prove lower bounds on the SM complexity of the *Generalized Addressing Function* ($\mathrm{GAF}_{G,k}$), where $G$ is a group of order $n$ (see Definition 2.3). The input to $\mathrm{GAF}_{G,k}$ consists of $n + (k-1)\log n$

bits partitioned among the players as follows: player 0 gets a function $x_0 : G \longrightarrow \{0,1\}$ (represented as an $n$-bit string) on her forehead whereas players 1 through $k-1$ get group elements $x_1, \ldots, x_{k-1}$, respectively, on their foreheads. The output of $\mathrm{GAF}_{G,k}$ for this input is the value of the function $x_0$ on the product $x_1 \cdot \ldots \cdot x_{k-1}$.

Our first result is an $\Omega\left(\frac{|G|^{1/(k-1)}}{k-1}\right)$ lower bound on the SM complexity of $\mathrm{GAF}_{G,k}$ for any finite group $G$ (Theorem 2.8).

The result uses a decomposition theorem for finite groups (Theorem 2.17). A related body of work, going back to a 1937 conjecture of Rohrbach [Ro1, Ro2], is discussed in a separate section, partly for the sake of its own interest (Section 7).

In Section 3, we prove a lower bound similar to Theorem 2.8 on the *randomized* SM complexity of $\mathrm{GAF}_{G,k}$. Specifically, we show that any randomized SM protocol for $\mathrm{GAF}_{G,k}$ with a success probability $\geq (1+\epsilon)/2$ must have a cost of $\Omega\left(\frac{|G|^{1/(k-1)}\epsilon^2}{k-1}\right)$. The proof of this result is based on an "Entropy Loss Lemma" which may be of independent interest (Lemma 3.7 and Lemma 3.9). The lemma provides a tradeoff between the *average* Hamming distance travelled and the number of destinations reached by a transformation of the Boolean cube.

It is easy to see that the general multiparty communication complexity of $\mathrm{GAF}_{G,k}$ is at most $\log n + 1$. Hence the lower bounds stated above show that the SM model is exponentially weaker than the general model for up to $(\log n)^{1-\epsilon}$ players. In fact, we prove this *exponential gap* between the SM model and an intermediate model called the "One-Way Communication Model" [NW] (see Definition 2.6). This result supports the hope that it might be easier to obtain stronger lower bounds in the SM model than in the general communication model. On the other hand, as mentioned in Section 1.1, sufficiently strong lower bounds in the SM model still have some of the same interesting consequences to circuit complexity as those in the general model.

As mentioned before, Håstad and Goldmann [HG] relate lower bounds on multiparty communication complexity to lower bounds on certain depth-2 circuits. In this paper, we use ideas from [HG] to relate SM complexity to depth-2 circuit complexity. In particular, we show that a circuit with an arbitrary symmetric gate at the top and AND gates at the bottom computing an explicit function on $n$ variables derived from $\mathrm{GAF}_{\mathbb{Z}_2^t,k}$ must have size $\exp((\log n/\log\log n)^2)$. We note that similar techniques applying the general multiparty communication complexity lower bounds were used by Razborov and Wigderson [RaW].

## 1.3 Upper Bounds

A curious development concerning SM complexity is the discovery of unexpected upper bounds. It appeared natural to expect that, when the number of players is constant, the SM complexity of GAF should be $\Omega(n)$. This, however, is false. In fact, we give a counter-intuitive upper bound of $O(n^{0.92})$ on the SM complexity[1] of $\mathrm{GAF}_{\mathbb{Z}_2^t,3}$. More generally, we show an upper bound of roughly $n^{O(\log k/k)} + \log n$ on the SM complexity of $\mathrm{GAF}_{\mathbb{Z}_2^t,k}$. This gives a polylog$(n)$ upper bound when the number of players is $\log n$; in fact, if the number of players is greater than $\log n$, an upper bound of $2 + \log n$ holds (Sections 5.1 and 5.2).

The $O(n^{0.92})$ upper bound, first published in [BaKL] (a preliminary version of this paper), together with related results about cyclic groups $\mathbb{Z}_n$ by Pudlák, Rödl, and Sgall [PR, PRS], has prompted a refinement of an approach proposed by Nisan and Wigderson [NW] toward superlinear

[1]This bound has subsequently been improved to $O(n^{0.73})$ in [AmL].

size lower bounds on log-depth circuits. This approach uses 3-party communication complexity lower bounds and exploits a graph-theoretic reduction due to Valiant [Va], building on earlier results by Erdős, Graham, and Szemerédi [EGS]. To explain this approach, let us consider a Boolean function $f_1 : \{0,1\}^{O(n)} \times \{0,1\}^{O(n)} \times \{0,1\}^{\log n} \longrightarrow \{0,1\}$. From this, let us construct an $n$-output function $f(x,y) = (z_1, \ldots, z_n)$ by setting $z_j := f_1(x,y,j)$. Then, an $\Omega(n)$ lower bound on the *total* number of bits communicated in a 3-party SM protocol for $f_1$ (with $x$, $y$, and $j$ on the foreheads of players 0, 1, and 2 respectively) would imply a superlinear lower bound on log-depth circuits computing the function $f$. In particular, if there were an $\Omega(n)$ lower bound on the 3-party SM communication complexity of $\mathrm{GAF}_{\mathbb{Z}_2^t,3}$, where $n = 2^t$, then the above connection would have yielded an explicit function requiring superlinear size circuits of log-depth.

However, we have a 3-party SM protocol for $\mathrm{GAF}_{\mathbb{Z}_2^t,3}$ that uses only $n^{0.92}$ bits of communication. Analogously, [PR, PRS] prove a $o(n)$ upper bound on the 3-party SM complexity of $\mathrm{GAF}_{\mathbb{Z}_n,k}$. On the other hand, these and several similar functions are conjectured to require superlinear size circuits of log-depth. This situation motivated a refined version of the approach from [NW]. This refined version seeks 3-party SM lower bounds when there are certain constraints on the lengths of messages from individual players. Indeed, in response to the surprising upper bounds from [BaKL] and [PR], Kushilevitz and Nisan present such an approach in their book [KuN, Section 11.3]. We describe this new formulation below.

Let $f$ be an $n$-bit output function and $f_1$ its single-bit output counterpart as defined above. Then Valiant's lemma implies the following: if $f$ has log-depth linear size circuits, then $f_1$ has an SM protocol in which, for any fixed $\epsilon > 0$, (*i*) player 2 sends at most $O(n/\log\log n)$ bits, and (*ii*) players 0 and 1 send $O(n^\epsilon)$ bits each. Thus a lower bound showing that any 3-party SM protocol for an explicit $f_1$ must violate (*i*) or (*ii*) would yield an explicit $f$ that cannot be computed simultaneously in linear size and logarithmic depth.

It is interesting to note that, in contrast to the lower bound, our upper bound depends heavily on the structure of the elementary abelian 2-group $G = \mathbb{Z}_2^t$. In particular, the upper bound does not apply to the cyclic group $G = \mathbb{Z}_n$. For $\mathrm{GAF}_{\mathbb{Z}_n,k}$, Pudlák, Rödl, and Sgall [PRS] prove an upper bound of $O(n \log\log n/\log n)$ for $k = 3$ (three players) and of $O(n^{6/7})$ for $k \geq c \log n$. Their upper bounds have been significantly improved by Ambainis [Am] to $O\left(\frac{n \log^{1/4} n}{2^{\sqrt{\log n}}}\right)$ for $k = 3$ and to $O(n^\epsilon)$ for an arbitrary $\epsilon > 0$ for $k = O((\log n)^{c(\epsilon)})$. However, these bounds for $\mathbb{Z}_n$ are still much weaker than the corresponding bounds for $\mathbb{Z}_2^t$ presented in this paper.

We also give surprising upper bounds on the SM-complexity of a different class of functions defined by certain depth-2 circuits (Section 6). For this class of functions, we prove polylog($n$) upper bounds on the SM complexity when the number of players is at least $\log n+2$. This class of functions includes "Generalized Inner Product (GIP)" and "Majority of Majorities." The special case of GIP improves a result due to Grolmusz [G] where the same upper bound is given for 2-round protocols. We note that GIP is a prime example in the study and applications of multiparty communication complexity [BaNS, G, HG, RaW]. "Majority of Majorities" is an interesting candidate function to be outside ACC.

The circuits defining the class of functions mentioned above have an arbitrary symmetric gate of fan-in $n$ at the top and gates of fan-in $k$ (= number of players) at the bottom. Furthermore, each bottom gate is assumed to compute a symmetric function with very small two-party, one-way communication complexity (we call such functions *compressible*, see Definition 6.1). We partition the input so that each player misses one bit from each bottom gate.

We also give an example of an explicit symmetric function that is not compressible (in the sense of Definition 6.1). The proof of this result uses Weil's character sum estimates.

### 1.4 Comparison with [BaKL]

Finally a comment on how the present paper relates to its preliminary version [BaKL]. Most results of [BaKL] have been superseded both in generality and in the elegance of the proof. This is especially true for the (deterministic and randomized) lower bounds which have been extended to all groups. A discussion of circuit complexity applications has been added. The main new additions are the counter-intuitive upper bounds for the case of more than $\log n$ players for a significant class of functions, including the "Majority of Majorities" function.

### 1.5 Organization of the Paper

In Section 2, we introduce the model of Simultaneous Messages and prove a lower bound on the SM complexity of the *Generalized Addressing Function* (GAF) with respect to an arbitrary finite group $G$ (see Definition 2.3). Section 3 extends this lower bound to the randomized SM complexity of $\mathrm{GAF}_{G,k}$. In Section 4 we present some consequences of our lower bounds on SM complexity to certain depth-2 circuits. Sections 5 and 6 deal with upper bounds on SM complexity. In Section 5 we give nontrivial upper bounds for GAF with respect to elementary abelian 2-groups, whereas in Section 6, we define a natural class of functions and show very efficient SM protocols for them. In Section 7 we discuss a group-decomposition problem arising from the GAF lower bounds; this section may be of interest in its own right. Section 8 concludes the paper with several open problems.

## 2 A Simultaneous Messages Lower Bound

Let $f(x_0, \ldots, x_{k-1})$ be a Boolean function, where each $x_i$ is a bit-string of fixed length $\leq n$. A referee and $k$ players collaborate to evaluate $f(x_0, \ldots, x_{k-1})$. Each participant (referee and players) has full knowledge of the function $f$. For $0 \leq i \leq k-1$, the $i$-th player, $p_i$, knows each input argument except $x_i$. The referee does not know any of the input. Each player $p_i$ simultaneously passes a message of fixed length to the referee, after which the referee announces the function value. Each participant is a function of the arguments it "knows."

**Definition 2.1** A *Simultaneous Messages (SM) protocol $P$ for $f$* is a set of players along with a referee that correctly computes $f$ on all inputs. The *cost* of an SM protocol for $f$ is the length of the longest message sent to the referee by any individual player[2]. The *SM complexity* of $f$, denoted $C_0(f)$, is the minimum cost of a protocol computing $f$.

**Remark 2.2** This model is implicit in the work of Nisan and Wigderson [NW, Theorem 7], where they consider the case $k = 3$. The first papers investigating the SM model in detail are the conference version of the current paper [BaKL] and a paper by Pudlák, Rödl, and Sgall [PRS]; the latter uses the name "Oblivious Communication Complexity."

[2]This definition of the cost, as the $\ell_\infty$-norm of the vector of message lengths of the players, differs from that of the STACS' 95 version [BaKL], where we consider the $\ell_1$-norm. We continue to use the total communication for $C$ and $C_1$ (Definitions 1.1 and 2.6).

## 2.1 The Generalized Addressing Function $\mathrm{GAF}_{G,k}$

The function that we use to show an exponential gap between the SM and general multiparty communication models is the *generalized addressing function*, defined as follows.

**Definition 2.3** Let $G$ be a group of order $n$. Elements of $G$ are represented by binary strings of length $\log n$. Let $x_0 : G \longrightarrow \{0,1\}$ be a function represented as an $n$-bit string and let $x_1, \ldots, x_{k-1} \in G$. Then the *Generalized Addressing Function for the group $G$ and $k$ players*, denoted by $\mathrm{GAF}_{G,k}$, is defined as follows:

$$\mathrm{GAF}_{G,k}(x_0, \ldots, x_{k-1}) := x_0[x_1 \cdot \ldots \cdot x_{k-1}].$$

Here $\cdot$ denotes the group operation in $G$.

The notation $C_0(\mathrm{GAF}_{G,k})$ refers to the SM complexity of the $\mathrm{GAF}_{G,k}$ function under the natural partition of the input among the players, i.e. player $i$ misses input $x_i$. Note that the partition of the input among the players is not balanced since player 0 has $|x_0| = n$ bits "on her forehead," whereas player $i$ for $1 \leq i \leq k-1$ has $|x_i| = \log n$ bits on her forehead.

Recall that $C(f)$ denotes the $k$-party communication complexity of the function $f$ (where $f$ is a function in $k$ variables) (see Section 1.1).

**Observation 2.4** $C(GAF_{G,k}) \leq \log n + 1$.

**Proof:** Player $p_0$ writes $g = x_1 \cdot \ldots \cdot x_{k-1}$; then $p_1$ writes $x_0[g]$. ∎

**Remark 2.5** This is a special case of the observation that $C(f) \leq 1+$ the length of the shortest input.

**Definition 2.6** A special case of the communication model is *one-way communication*, in which each player may write on the blackboard only once, and they proceed in the prescribed order $p_0, p_1, \ldots, p_{k-1}$. Let $C_1(f)$ denote the *one-way communication complexity of $f$.*

Clearly $n \geq C_0(f) \geq C_1(f)/k \geq C(f)/k$, for any function $f$ of $k$ variables. For $\mathrm{GAF}_{G,k}$, the proof of Observation 2.4 gives a one-way protocol, so we obtain the following consequence.

**Corollary 2.7** $C_1(GAF_{G,k}) \leq \log n + 1$. ∎

The main result of this section is an SM lower bound on the Generalized Addressing Function of the form $\Omega(n^{1/(k-1)}/(k-1))$. This bound implies an exponential separation between $C_0(f)$ and $C_1(f)$ (and hence also between $C_0(f)$ and $C(f)$) for up to $k = (\log n)^{1-\epsilon}$ players. We state the result.

**Theorem 2.8** *For any group $G$ of order $n$ and any $k \geq 2$, $C_0(GAF_{G,k}) \geq \dfrac{cn^{1/(k-1)}}{k-1}$, where $c = (1 - 1/\sqrt{\mathrm{e}})/2 > 0.19$.*

The proof of this lower bound is given in the next two subsections.

**Remark 2.9** For $k = 3$, Theorem 2.8 gives an $\Omega(\sqrt{n})$ lower bound. Nisan and Wigderson [NW] give an $\Omega(\sqrt{n})$ lower bound for a different function, based on hash functions [MNT]. They actually show this lower bound for one-way complexity, establishing an exponential gap between $C_1(f)$ and $C(f)$ for $k = 3$.

**Remark 2.10** Theorem 2.8 states an SM lower bound for all finite groups $G$. Special cases of this result were found independently by Pudlák, Rödl, and Sgall (the cyclic group $G = \mathbb{Z}_n$) [PRS, Proposition 2.3] and by the authors of the conference version of the present paper (the elementary abelian group $G = \mathbb{Z}_2^t$) [BaKL]. Those bounds were extended in a preliminary version of this paper to a large class of groups, including all solvable groups. For arbitrary groups, however, our original lower bound was worse by a logarithmic factor than the bound stated in Theorem 2.8. We express our gratitude to an anonymous referee for pointing out that a simple modification of our argument yields the improved result stated as Theorem 2.8.

All proofs use essentially the same strategy, an information-theoretic argument combined with a group-decomposition result. Simple cases of the group-decomposition result are discussed as Examples 1 and 2. The general group-decomposition theorem appears as Theorem 2.17.

## 2.2 SM Lower Bound for $\mathbf{GAF}_{G,k}$ and Group Decompositions

In this subsection, we give an SM lower bound for $\mathrm{GAF}_{G,k}$ in terms of a parameter $\rho$ of $G$ and $k$ related to optimal decompositions of a large fragment of a group. In the next subsection we shall estimate $\rho$ within a constant factor. From this bound, our SM lower bound for $\mathrm{GAF}_{G,k}$ (Theorem 2.8) will be immediate.

**Definition 2.11** For a finite group $G$ and $A, B \subseteq G$, the product $AB$ is defined as $AB = \{a \cdot b : a \in A, b \in B\}$.

Note that $|AB| \leq |A| \cdot |B|$.

**Definition 2.12** Let $\alpha$ be a real number, $0 < \alpha \leq 1$. For a finite group $G$ and a positive integer $u$ we define

$$\rho_\alpha(G, u) = \min_{H_1,\dots,H_u \subseteq G} \{\rho : |H_1 \cdot \ldots \cdot H_u| \geq \alpha|G| \text{ and } \forall i, |\widehat{H}_i| \leq \rho\},$$

where $\widehat{H}_i$ is defined to be the Cartesian product of all $H_j$ except $H_i$.

**Remark 2.13** Note that $|\widehat{H}_i| = \prod_{j \neq i} |H_j|$. Also note that $\widehat{H}_i$ is not the product $\prod_{j \neq i} H_j$ in the sense of Definition 2.11; in fact, $\widehat{H}_i$ is not even a subset of $G$. (It is a subset of $G \times \cdots \times G$ ($u - 1$ times).)

The following two examples give upper bounds on $\rho$ for two special groups. In Section 7, we will see that these upper bounds are optimal to within a constant factor.

**Example 1:** $\rho_1(\mathbb{Z}_2^t, u) \leq 2n^{1-1/u}$, where $n = 2^t$.
**Proof:** Let $V = \mathbb{Z}_2^t$. Decompose $V$ into a direct sum of $u$ subspaces: $V = H_1 \oplus \cdots \oplus H_u$, where for each $i$, $1 \leq i \leq u$, $\lfloor t/u \rfloor \leq \dim H_i \leq \lceil t/u \rceil$. This implies

$$\rho_1(V, u) \leq \max_i |\widehat{H}_i| = \max_i \frac{n}{|H_i|} = \frac{n}{\min_i |H_i|} \leq \frac{n}{2^{\lfloor t/u \rfloor}} \leq \frac{2n}{2^{t/u}} = \frac{2n}{n^{1/u}} = 2n^{1-1/u}. \tag{1}$$

■

**Example 2:** $\rho_{1/2}(\mathbb{Z}_n, u) \leq 2n^{1-1/u}$ and $\rho_1(\mathbb{Z}_n, u) \leq 4n^{1-1/u}$.
**Proof:** Let $2^t < n \leq 2^{t+1}$. We consider the elements of $\mathbb{Z}_n$ to be binary strings of length $t+1$. Let $K$ be the subset of $\mathbb{Z}_n$ given by binary strings with their most significant ($(t+1)$st) bit equal to zero.

Identify $K$ with $H_1 \oplus \cdots \oplus H_u$, where $H_i$ is the set of binary numbers with $t$ digits in which all digits are 0 except for the $i$-th segment of $\lfloor t/u \rfloor$ or $\lceil t/u \rceil$ digits, which can be either 0 or 1. Thus each $H_i$ has size $\geq 2^{\lfloor t/u \rfloor}$. Clearly $|K| = 2^t \geq n/2$. By (1), we have that $\max_i |\widehat{H}_i| \leq 2|K|^{1-1/u} \leq 2n^{1-1/u}$. Hence $\rho_{1/2}(\mathbb{Z}_n, u) \leq 2n^{1-1/u}$.

To cover the entire group $\mathbb{Z}_n$, apply the above argument to bit strings of length $(t+1)$ (but perform group operations in $\mathbb{Z}_n$). Then, we get that $\max_i |\widehat{H}_i| \leq 2 \cdot 2^{(t+1)(1-1/u)} \leq 4n^{1-1/u}$ and this gives us the bound on $\rho_1(\mathbb{Z}_n, u)$.

As a concrete example, consider $\mathbb{Z}_{25}$, $u = 3$, and $\alpha = 1$. It is easy to see that a (complete) cover is given by $\mathbb{Z}_{25} = \{0, 16\} + \{0, 4, 8, 12\} + \{0, 1, 2, 3\}$. Note that in this cover, some elements (eg. 5) have more than one factorization (under the group operation addition modulo 25). ■

**Lemma 2.14** *For any finite group $G$ and any $\alpha$ $(0 < \alpha \leq 1)$,* $C_0(GAF_{G,k}) \geq \dfrac{\alpha|G|}{(k-1)\,\rho_\alpha(G, k-1)}$.

**Proof of Lemma 2.14:** We prove a lower bound on the length of the longest message sent by $p_1, \ldots, p_{k-1}$. We ignore $p_0$ by assuming that the referee knows whatever $p_0$ knows. This assumption can only make our lower bound stronger.

The proof is by an information-theoretic argument. Pick a factorization $K = \prod_{i=1}^{k-1} H_i$ of some subset $K \subseteq G$ which is optimal in the sense that $|K| \geq \alpha|G|$, $H_1, \ldots, H_{k-1} \subseteq G$, and $\max_i |\widehat{H}_i| = \rho_\alpha(G, k-1)$.

We shall restrict player $p_0$'s inputs to functions $x_0 : G \longrightarrow \{0,1\}$ such that $x_0(g) = 0$ for all $g \in G \setminus K$. For $i = 1, \ldots, k-1$, we shall restrict player $p_i$'s inputs to $H_i$. For a fixed $x_0$ (on $p_0$'s forehead and hence visible to all $p_i, 1 \leq i \leq k-1$), player $p_i$ can send at most $|\widehat{H}_i|$ different messages. Hence the total number of bits received by the referee (for all combinations of these restricted inputs) is at most $\rho_\alpha(G, k-1)(k-1)\ell$, where $\ell$ is the length of the longest message sent by the players $p_i, 1 \leq i \leq (k-1)$. But this collection of messages must determine every bit of $x_0$ corresponding to the set $K \subseteq G$. Hence we must have $\rho_\alpha(G, k-1)(k-1)\ell \geq \alpha n$, giving the claimed bound. The foregoing ideas are formalized below.

Let $P$ be any SM protocol for $\mathrm{GAF}_{G,k}$. Let $r$ denote the referee function. Let $\ell$ be the cost of $P$. For notational convenience, we assume, without loss of generality, that each player sends a message of length $\ell$ (padding their messages if necessary).

We define a function $F$ in terms of the player and referee functions. The input to $F$ will be a binary string of length $(k-1)\rho_\alpha(G, k-1)\ell$, and the output will be a $|K|$-bit string. We will then show that $F$ is surjective, which will yield the theorem.

**Definition 2.15** For each $g \in K$, we fix elements $h_1 \in H_1, \ldots h_{k-1} \in H_{k-1}$ such that $g = h_1 \cdot \ldots \cdot h_{k-1}$ and refer to this as "the" *decomposition* of $g$.

Now we define a function $F : \{0,1\}^{\ell|\widehat{H}_1|} \times \cdots \times \{0,1\}^{\ell|\widehat{H}_{k-1}|} \longrightarrow \{0,1\}^K$ as follows. Let $(w_1, w_2, \ldots, w_{k-1})$ be an input to $F$, where $w_i \in \{0,1\}^{\ell|\widehat{H}_i|}$. The $\ell$-bit substrings of $w_i$ are indexed by elements of $\widehat{H}_i$. The output bit $y(g)$ corresponding to $g \in K$ is determined as follows. Let $g = h_1 \cdot \ldots \cdot h_{k-1}$ be the decomposition of $g$. For $1 \leq i \leq k-1$, let $m_i(g)$ be the $\ell$-bit substring of $w_i$ at index $\widehat{h}_i := (h_1, \ldots, h_{i-1}, h_{i+1}, \ldots, h_{k-1}) \in \widehat{H}_i$. Let $m_0(g) = p_0(h_1, \ldots, h_{k-1})$. Now define $y(g) = r(m_0(g), m_1(g), \ldots, m_{k-1}(g))$.

**Claim 2.16** *$F$ is surjective.*

**Proof:** Let $x_0 \in \{0,1\}^G$ such that $x_0(g) = 0$ for all $g \in G \setminus K$. Define the input $w_{x_0} = (w_1, \ldots, w_{k-1})$ to $F$ as follows: For each $i$, $1 \le i \le k-1$ and each $\widehat{h}_i \in \widehat{H}_i$, define the $\ell$-bit substring of $w_i$ at index $\widehat{h}_i$ to be $p_i(x_0, \widehat{h}_i)$, i.e., the message sent by $p_i$ when she sees $x_0$ and $\widehat{h}_i$. We now show that $F(w_{x_0}) = x_0^K$ (the restriction of $x_0$ to $K$), which will prove the claim. Recalling our notation that $y = F(w_{x_0})$, we want to show that for each $g \in K$, $y(g) = x_0(g)$.

Let $g \in K$ and let $g = h_1 \cdot \ldots \cdot h_{k-1}, h_i \in H_i$, be the decomposition of $g$.

From the definition of $w_{x_0}$, for $1 \le i \le k-1$, we have $m_i(g) =$ ($\ell$-bit substring of $w_i$ at index $\widehat{h}_i$) $= p_i(x_0, \widehat{h}_i)$, and also $m_0(g) = p_0(h_1, \ldots, h_{k-1})$. Now using the definition of $F$ we have,

$$\begin{aligned} y(g) &= r(m_0(g), m_1(g), \ldots, m_{k-1}(g)) \\ &= r(p_0(h_1, \ldots, h_{k-1}), p_1(x_0, h_2, \ldots, h_{k-1}), \ldots, p_{k-1}(x_0, h_1, \ldots, h_{k-2})) \\ &= \mathrm{GAF}_{G,k}(x_0, h_1, \ldots, h_{k-1}) \qquad \text{by the correctness of the protocol} \\ &= x_0(g) \qquad \text{by definition of } \mathrm{GAF}_{G,k}. \end{aligned}$$

Thus $F(w_{x_0}) = x_0^K$ and $F$ is surjective. ■ Claim 2.16.

Claim 2.16 implies that the domain of $F$ is at least as large as the range of $F$. Thus $\ell(k-1)\rho_\alpha(G, k-1) \ge \ell(|\widehat{H}_1| + \ldots + |\widehat{H}_{k-1}|) \ge |K| \ge \alpha|G|$, and hence $\ell \ge n/(k-1)\rho_\alpha(G, k-1)$. ■ Lemma 2.14.

### 2.3 Decomposition of groups

In this subsection we estimate the quantity $\rho_\alpha(G, u)$ for a specific positive constant $\alpha$.

**Theorem 2.17** *Given a finite group $G$ and a positive integer $u$, there exist subsets $H_1, \ldots, H_u \subseteq G$ such that $|\widehat{H}_i| < 2|G|^{1-1/u}$ for $i = 1, \ldots, u$, and $|H_1 \cdot \ldots \cdot H_u| > (1 - 1/\sqrt{\mathrm{e}})|G| > 0.39|G|$.*

**Corollary 2.18** *Let $\alpha = 1 - 1/\sqrt{\mathrm{e}} \approx 0.39$. Then for any finite group $G$ and any positive integer $u$,*

$$\rho_\alpha(G, u) < 2|G|^{1-1/u}.$$

Combining Corollary 2.18 and Lemma 2.14, our lower bound for the SM complexity of $\mathrm{GAF}_{G,k}$ (Theorem 2.8) is immediate. ■

For the proof of Theorem 2.17, we use the following result. Let $G$ be a group and $a_1, \ldots, a_k \in G$. The *cube* based on the sequence $a_1, \ldots, a_k$ is the set $C(a_1, \ldots, a_k) := \{1, a_1\} \cdot \ldots \cdot \{1, a_k\}$. In other words, $C(a_1, \ldots, a_k)$ consists of the $2^k$ *subproducts* $a_1^{\epsilon_1} \ldots a_k^{\epsilon_k}$ where $\epsilon_i \in \{0, 1\}$.

**Theorem 2.19 ([BaE])** *Let $G$ be a finite group of order $n$ and let $\ell$ be a positive integer. Then there exists a sequence of elements $a_1, \ldots, a_\ell \in G$ such that $|C(a_1, \ldots, a_\ell)| > n(1 - \exp(-2^\ell/n))$.*

For completeness we include the proof.

**Lemma 2.20** *Let $A$ be a subset of a finite group $G$. Then for some $x \in G$ we have*

$$\frac{|G \setminus (A \cup Ax)|}{|G|} \le \left(\frac{|G \setminus A|}{|G|}\right)^2. \tag{2}$$

**Proof.** Let $|G| = n$ and $|A| = k$. Let us select $x \in G$ at random from the uniform distribution. Then for every $g \in G$, the probability that $g \notin Ax$ is $(n-k)/n$. Therefore the expected number of those $g \in G \setminus A$ which do not belong to $Ax$ is $(n-k)^2/n$. So this is the expected size of the set $G \setminus (A \cup Ax)$. Pick an $x$ for which $|G \setminus (A \cup Ax)|$ is not less than its expected value. ∎

**Proof** of Theorem 2.19. We choose $a_1, \ldots, a_\ell \in G$ successively as follows. Set $A_1 = \{a_1\}$ and $A_{i+1} = A_i \cup A_i a_{i+1}$. Let $a_1 \in G$ be arbitrary; given $a_1, \ldots, a_i$, we choose $a_{i+1} \in G$ so as to maximize $|A_{i+1}|$.

Let $p_i = |G \setminus A_i|/n$.

We have $p_1 = 1 - 1/n$ and by Lemma 2.20 we have $p_{i+1} \le p_i^2$. Therefore

$$p_\ell \le \left(1 - \frac{1}{n}\right)^{2^\ell} < \exp\left(-2^\ell/n\right). \tag{3}$$

Noting that $|C(a_1, \ldots, a_\ell)| = n(1 - p_\ell)$ completes the proof. ∎

**Proof** of Theorem 2.17: Let $n = |G|$ and let $\ell$ denote the integer satisfying $n/2 \le 2^\ell \le n$. Let $a_1, \ldots, a_\ell \in G$ be the sequence of $\ell$ elements in $G$ guaranteed by Theorem 2.19.

Let us split $\ell$ into $u$ parts as evenly as possible: $\ell = k_1 + \ldots + k_u$, where $k_i \in \{\lfloor \ell/u \rfloor, \lceil \ell/u \rceil\}$. Let $H_j = C(a_{k_1+\ldots+k_{j-1}+1}, \ldots, a_{k_1+\ldots+k_j})$. (So $H_1$ is the cube based on the first $k_1$ members of the sequence $\{a_i\}$; $H_2$ is the cube based on the next $k_2$ members of the sequence, etc.) Then, $H_1 \ldots H_u = C(a_1, \ldots, a_\ell)$ and therefore $|H_1 \ldots H_u| > n(1 - \exp(-2^\ell/n)) \ge n(1 - 1/\sqrt{\mathrm{e}})$.

Moreover, $|\widehat{H_i}| = 2^{\ell - k_i} < 2^{\ell(1-1/u)+1} \le 2n^{1-1/u}$. ∎

# 3 Randomized Complexity of Simultaneous Messages

In this section, we give lower bounds on the randomized SM complexity of the function $\mathrm{GAF}_{G,k}$ (Theorem 3.3, Lemma 3.4). Up to a constant factor, the bounds match our lower bounds on deterministic SM complexity (Theorem 2.8, Lemma 2.14).

In a *randomized SM protocol* all the players and the referee are allowed to use coin flips.

We consider public coin protocols, i. e., protocols where the random strings used are visible to all parties, including the referee. This is clearly the strongest possible model in the sense that it can simulate at no extra cost the models which allow private or partially private (e. g., hidden from the referee) coins. Therefore, any lower bound in the public coin model will automatically remain valid in models with private or partially private coins.

**Definition 3.1** A randomized SM protocol $P$ for a function $f$ is said to have $\epsilon$ *advantage* $(0 \le \epsilon \le 1)$ if

$$\text{for } \textit{every} \text{ input } x, \quad \Pr[P(x) = f(x)] - \Pr[P(x) \ne f(x)] \ge \epsilon, \tag{4}$$

where the probability is taken over the random choices of the players and the referee.

**Definition 3.2** The *cost* of a randomized SM protocol is the maximum number of bits communicated by any player on any input and for any choice of the random bits. We define the *$\epsilon$-randomized SM complexity of $f$*, denoted $R_0^\epsilon(f)$, as the minimum cost of a randomized SM protocol for $f$ achieving an advantage $\ge \epsilon$.

Note that a deterministic protocol has advantage $\epsilon = 1$, so $C_0(f) = R_0^1(f)$.

We also note, for future reference, that inequality (4) is equivalent to the following:

$$\Pr[P(x) = f(x)] \geq \frac{1+\epsilon}{2}. \tag{5}$$

The main result of this section is a lower bound on the randomized SM-complexity of the $\mathrm{GAF}_{G,k}$ function, extending the deterministic lower bound of Theorem 2.8.

**Theorem 3.3** *For any finite group $G$, and $k \geq 2$, $R_0^\epsilon(GAF_{G,k}) = \Omega\left(\frac{|G|^{1/(k-1)}\,\epsilon^2}{k-1}\right)$.*

This bound will follow from Lemma 3.4 below.

In this and later sections we will express our bounds in terms of the *Binary Entropy Function* H defined as follows:

$$\mathrm{H}(x) := -x\log_2 x - (1-x)\log_2(1-x) \qquad (0 \leq x \leq 1). \tag{6}$$

Note that $\mathrm{H}(0) = \mathrm{H}(1) = 0$. The maximum of H is taken at $x = 1/2$ where $\mathrm{H}(1/2) = 1$.

**Lemma 3.4** *For any finite group $G$, $0 \leq \epsilon \leq 1$, and $0 \leq \alpha \leq 1$,*

$$R_0^\epsilon(GAF_{G,k}) \geq \frac{\alpha|G|}{(k-1)\rho_\alpha(G,k-1)}(1 - \mathrm{H}(1/2 - \epsilon/2)).$$

This Lemma extends the deterministic lower bound of Lemma 2.14. Its proof generalizes the strategy from the deterministic case. While we completely recover $x_0$ (restricted to the part of the group covered by the decomposition) from all the messages of the players in the proof of Lemma 2.14, here we will only be able to recover "most" bits of an "average" $x_0$. Lemma 3.7 provides a means to lower bound the amount of information from which such a reconstruction is possible and can be thought of a generalization of Claim 2.16.

Our main result for this section (Theorem 3.3) is now immediate by combining Corollary 2.18 and Lemma 3.4 and using the following well known estimate for the binary entropy function:

$$\text{For } |\delta| \leq 1/2, \quad 1 - \frac{\pi^2}{3\ln 2}\,\delta^2 \;\leq\; \mathrm{H}\left(\frac{1}{2} - \delta\right) \;\leq\; 1 - \frac{2}{\ln 2}\,\delta^2. \tag{7}$$

■(Theorem 3.3)

Following Yao [Ya1], we prove our lower bound on randomized complexity (Lemma 3.4) via a lower bound on *distributional complexity.*

**Definition 3.5** Given a Boolean function $f$, a probability distribution $\mu$ on its input space, and an $\epsilon$, $0 \leq \epsilon \leq 1$, a $(\mu,\epsilon)$*-SM protocol* for $f$ is a *deterministic* SM protocol $P$ such that

$$\Pr_\mu[P(x) = f(x)] - \Pr_\mu[P(x) \neq f(x)] \geq \epsilon,$$

where the probability is with respect to the distribution $\mu$ on the input space. We define the $(\mu,\epsilon)$-*distributional complexity of $f$*, denoted $C_0^{\mu,\epsilon}(f)$, as the minimum cost of a $(\mu,\epsilon)$-SM protocol for $f$.

Next we state Yao's key observation which reduces the question of lower bounds on randomized complexity to lower bounds on distributional complexity with respect to any distribution on inputs.

**Theorem 3.6 ([Ya1])** *For any function $f$ and any $0 \leq \epsilon \leq 1$, $R_0^\epsilon(f) = \max_\mu C_0^{\mu,\epsilon}(f)$.* ■

The following lemma provides a tradeoff between the *average* Hamming distance travelled and the number of destinations reached by a transformation of the Boolean cube. The lemma may be of independent interest, in addition to being central to our proof of Lemma 3.4.

**Lemma 3.7 (Distance–range tradeoff)** *Let $\phi : \{0,1\}^m \longrightarrow \{0,1\}^m$ be a function with range $R$. Let $0 \leq \delta \leq 1/2$. Suppose the average Hamming distance between $X \in \{0,1\}^m$ and $\phi(X)$ is $\leq \delta m$. Then*

$$|R| \geq 2^{(1-\mathrm{H}(\delta))m}. \tag{8}$$

**Remark 3.8** Using a random cover of the Boolean cube by Hamming balls one can show that for $\delta < 1/2$, the lower bound (8) is optimal within a factor of $c_1(\delta)\sqrt{m}$.

Lemma 3.7 is an immediate consequence of Lemma 3.9 below. $\mathbb{H}(X)$ denotes the entropy of the random variable $X$. For the concept of entropy of random variables and related facts, we refer to the second edition of Alon–Spencer [AlS, Section 14.6].

**Lemma 3.9 (Entropy Loss Lemma)** *Let $\phi : \{0,1\}^m \longrightarrow \{0,1\}^m$. Let $X \in \{0,1\}^m$ be a random element of the domain chosen according to a probability distribution $\mu$. Let $0 \leq \delta \leq 1/2$. Suppose that*

$$\mathbb{E}[\mathrm{dist}(X, \phi(X))] \leq \delta m,$$

*where* dist$(\cdot,\cdot)$ *refers to Hamming distance and* $\mathbb{E}(\cdot)$ *denotes the expected value. Then*

$$\mathbb{H}(X) - \mathbb{H}[\phi(X)] \leq \mathrm{H}(\delta)m.$$

Note that if $\mu$ is the uniform distribution then the conditions in Lemmas 3.7 and 3.9 become identical and $\mathbb{H}(X) = m$. So the conclusion of Lemma 3.7 follows from the known fact that for any random variable $Y$ with range $R$, the entropy of $Y$ is bounded by

$$\mathbb{H}[Y] \leq \log_2(|R|). \tag{9}$$

This completes the proof of Lemma 3.7. ■

For the proof of the Entropy Loss Lemma we will use the following elementary facts from Information Theory [AlS, Section 14.6]:

- For any two random variables $U$ and $V$,

$$\mathbb{H}[U, V] = \mathbb{H}[V] + \mathbb{H}[U|V]. \tag{10}$$

- $$\mathbb{H}[U|V] \leq \mathbb{H}[U]. \tag{11}$$

- If $V$ is completely determined by $U$, then

$$\mathbb{H}[U,V] = \mathbb{H}[U]. \tag{12}$$

- Let $X = (X_1, \ldots, X_m)$. Then,

$$\mathbb{H}[X] = \mathbb{H}[X_1, \ldots, X_m] \leq \sum_{i=1}^{m} \mathbb{H}[X_i]. \tag{13}$$

- The binary entropy function H defined in (6) is *concave* :

$$\sum_i \alpha_i = 1, \quad 0 \leq \alpha_i \leq 1 \quad \Longrightarrow \quad \sum_i \alpha_i \mathrm{H}(p_i) \leq \mathrm{H}\left(\sum_i \alpha_i p_i\right). \tag{14}$$

**Proof of the Entropy Loss Lemma.**
Let $Y = \phi(X)$. Note that

$$\mathbb{H}[X] - \mathbb{H}[Y] = \mathbb{H}[X,Y] - \mathbb{H}[Y] = \mathbb{H}[X|Y], \tag{15}$$

where the first equality follows from (12) since $Y$ is completely determined by $X$, the second follows from (10). So the conclusion of Lemma 3.9 is equivalent to the inequality

$$\mathbb{H}[X|Y] \leq m\mathrm{H}(\delta). \tag{16}$$

Let $X = (X_1, \ldots, X_m)$ and $Y = (Y_1, \ldots, Y_m)$. For $1 \leq i \leq m$, let $Z_i$ denote the indicator random variable of the event $X_i \neq Y_i$, i.e.,

$$Z_i := \begin{cases} 1 & \text{if } X_i \neq Y_i, \\ 0 & \text{otherwise.} \end{cases}$$

Let $\delta_i := \Pr[Z_i = 1] = \mathbb{E}[Z_i]$. Then, $\sum_i Z_i = \mathrm{dist}(X,Y)$. It follows that

$$\sum_{i=1}^{m} \delta_i = \sum_{i=1}^{m} \mathbb{E}[Z_i] = \mathbb{E}[\sum_{i=1}^{m} Z_i] = \mathbb{E}[\mathrm{dist}(X,Y)] \leq \delta m. \tag{17}$$

**Claim 3.10** *For $1 \leq i \leq m$, we have*

$$\mathbb{H}[X_i|Y] \leq \mathrm{H}(\delta_i). \tag{18}$$

Assuming the validity of the Claim, the following string of inequalities yields the bound (16).

$$\begin{aligned} \mathbb{H}[X|Y] &\leq \sum_{i=1}^{m} \mathbb{H}[X_i|Y] \qquad \text{using (13)} \\ &\leq \sum_{i=1}^{m} \mathrm{H}(\delta_i) \qquad \text{by the Claim} \\ &\leq m\mathrm{H}\left(\frac{1}{m}\sum_{i=1}^{m} \delta_i\right) \qquad \text{by (14)} \\ &\leq m\mathrm{H}(\delta) \qquad \text{since for } 0 \leq x \leq 1/2,\ \mathrm{H}(x) \text{ is increasing.} \end{aligned}$$

Finally, we need to prove Claim 3.10. We use $a \oplus b$ to denote the mod 2 sum of $a$ and $b$.

$$
\begin{aligned}
\mathbb{H}[X_i|Y] &= \mathbb{H}[X_i \oplus Y_i|Y] \quad \text{since for any fixed } y,\ X_i \text{ and } X_i \oplus y_i \text{ have identical entropies} \\
&\leq \mathbb{H}[X_i \oplus Y_i] = \mathbb{H}[Z_i] \quad \text{using (11) and the definition of } Z_i \\
&= \mathrm{H}(\delta_i) \quad \text{since } Z_i \text{ is a binary random variable with } \Pr[Z_i = 1] = \delta_i.
\end{aligned}
$$

■(Entropy Loss Lemma)

Next we prove our main result.

**Proof of Lemma 3.4:** We will prove a lower bound on $C_0^{\mu,\epsilon}(\mathrm{GAF}_{G,k})$ for some distribution $\mu$ and apply Theorem 3.6.

Let $G$ be a group of order $n$. Let $H_1, \ldots, H_{k-1}$ be an optimal collection of subsets of $G$ from Definition 2.12 and let $K = H_1 \cdot \ldots \cdot H_{k-1}$. Let $C = H_1 \times \cdots \times H_{k-1}$. Note that $K \subseteq G$ and $C \subseteq G \times \ldots \times G$ ($(k-1)$ times). Note further that $|K| \leq |C|$ and multiplication provides a natural onto map $C \to K$. Let $B \subseteq C$ be a set of representatives of the preimages under this map; so $|K| = |B|$ and each element of $g \in K$ can be uniquely factored as $g = h_1 \cdot \ldots \cdot h_{k-1}$, where $(h_1, \ldots, h_{k-1}) \in B$.

The distribution $\mu$ we will use is the uniform distribution on $\{0,1\}^K \times B$, i.e., player 0 will be given a uniformly chosen $x_0 : K \longrightarrow \{0,1\}$ and players 1 through $k-1$ will be given a uniformly chosen $(k-1)$-tuple from $B$. (Strictly speaking $x_0$ will be taken from functions $G \longrightarrow \{0,1\}$ that are fixed to zero on $G \setminus K$.)

Given $x_0 \in \{0,1\}^K$, we define $w_{x_0} \in \{0,1\}^{\ell|\widehat{H}_1|} \times \cdots \times \{0,1\}^{\ell|\widehat{H}_{k-1}|}$ as before in the proof of Lemma 2.14 from the players' functions $p_i$ for $1 \leq i \leq k-1$. The $\ell$-bit segment $(w_{x_0})_{\widehat{h}_i}$ of $w_{x_0}$ corresponding to $\widehat{h}_i \in \widehat{H}_i$ is defined as $(w_{x_0})_{\widehat{h}_i} = p_i(x_0, \widehat{h}_i)$. We again define a function $F$:

$$F : \{0,1\}^{\ell|\widehat{H}_1|} \times \cdots \times \{0,1\}^{\ell|\widehat{H}_{k-1}|} \longrightarrow \{0,1\}^K.$$

The function $F$ is defined as in the proof of Lemma 2.14 from the referee's function $r$ and Player 0's function $p_0$. Specifically, for $g \in K$, let $(h_1, \ldots, h_{k-1}) \in B$ be the unique factorization of $g$ in $B$. For $w \in \mathrm{domain}(F)$, we set

$$(F(w))(g) = r(p_0(h_1, \ldots, h_{k-1}), w_{\widehat{h}_1}, \ldots, w_{\widehat{h}_{k-1}}).$$

For $x_0 \in \{0,1\}^K$, define $y_0 := F(w_{x_0}) \in \{0,1\}^K$. We claim that the average Hamming distance between $x_0$ and $y_0$ (averaging over $x_0 \in \{0,1\}^K$) is at most $|K|(1-\epsilon)/2$. Indeed, let us form a $\{0,1\}^K \times B$ (0,1)-matrix $M$ as follows: $M(x_0, (h_1, \ldots, h_{k-1})) = 1$ if and only if the protocol $P$ makes an error when player 0 has $x_0$ on her forehead and player $i$ for $1 \leq i \leq k-1$ has $h_i$ on her forehead, i.e., $x_0(h_1 \cdot \ldots \cdot h_{k-1}) \neq r(p_0(h_1, \ldots, h_{k-1}), p_1(x_0, \widehat{h}_1), \ldots, p_{k-1}(x_0, \widehat{h}_{k-1})))$. By the definition of $y_0$, we have $M(x_0, (h_1, \ldots, h_{k-1})) = 1$ if and only if $x_0(h_1 \cdot \ldots \cdot h_{k-1}) \neq y_0(h_1 \cdot \ldots \cdot h_{k-1})$. Moreover, since the protocol $P$ has $\epsilon$ advantage, by inequality (5) it follows that the fraction of 1's in $M$ is at most $(1-\epsilon)/2$. Hence the average distance between $x_0$ and $y_0$ is at most $|K|(1-\epsilon)/2$.

Now an application of the distance-range tradeoff lemma (Lemma 3.7) concludes the proof as follows. Let $m = |K| = \alpha|G|$. Define $\phi : \{0,1\}^m \to \{0,1\}^m$ by setting $\phi(x_0) = y_0 = F(w_{x_0})$. Let $\delta = (1-\epsilon)/2$. We have just verified the average-distance condition, so Lemma 3.7 implies that the range $R$ of $y_0$ satisfies $\log|R| \geq |K|\mathrm{H}(1/2 - \epsilon/2)$. On the other hand, the range of $y_0$ is not larger than the domain of $F$:

$$(k-1)\ell\rho_\alpha(G, k-1) \geq \log|R| \geq \alpha|G|(1 - \mathrm{H}(1/2 - \epsilon/2)),$$

and hence

$$C_0^{\mu,\epsilon}(\mathrm{GAF}_{G,k}) = \ell \geq \frac{\alpha|G|}{(k-1)\rho_\alpha(G, k-1)}\,(1 - \mathrm{H}(1/2 - \epsilon/2))\,.$$

■(Lemma 3.4)

This completes the proof of the main results of this section. The rest of the section is devoted to a discussion of the need to use information theory (entropy) arguments and to clarifying the connections with the papers [BJKS] and [BaKL].

**Remark 3.11** Our central "entropy" tool was Lemma 3.7; its proof was the only place where the concept of entropy was used. The question arises whether the use of entropy was necessary at all.

The key word in Lemma 3.7 is "average." If we impose the bound $\mathrm{dist}(X, \phi(X)) \leq \delta m$ on *all* $X \in \{0,1\}^m$ then the conclusion will follow from a straightforward Hamming bound on coverings of the Boolean cube. Indeed, in this case the Hamming balls of radius $\delta m$ about $R$ would cover the entire Boolean cube; therefore

$$2^m \leq |R| \sum_{k \leq \delta m} \binom{m}{k} \leq |R| 2^{m\mathrm{H}(\delta)}, \tag{19}$$

proving the desired inequality. In the last step we used the bound $\sum_{k\leq\delta m}\binom{m}{k} \leq 2^{m\mathrm{H}(\delta)}$, which is valid for all $m$ and $\delta$ ($0 \leq \delta \leq 1/2$) (see, e. g., [MacS, p. 310]). (For $\delta < 1/2$ and large $m$, the bound can be improved by a factor of $\sim c(\delta)/\sqrt{m}$, cf. equation (23).)

More significantly, even if the condition is on *average* distance, the use of entropy can be avoided to obtain a slightly weaker result by a Markov inequality argument combined with the Hamming bound indicated above.

Indeed, under the conditions of Lemma 3.7 one can prove, without the use of entropies, the following lower bound on $|R|$ for any constant $c > 0$:

$$|R| \geq \frac{c}{\delta + c} 2^{(1-\mathrm{H}(\delta+c))m}. \tag{20}$$

To see (20), note that by Markov's inequality on nonnegative random variables, there exists a subset $S \subseteq \{0,1\}^m$ such that $|S| \geq 2^m c/(\delta + c)$ and for *all* $X \in S$, $\mathrm{dist}(X, \phi(X)) \leq (\delta + c)m$. Now, apply the Hamming bound argument as in (19) above to get a lower bound on $|\phi(S)|$ and hence on $|R|$.

Furthermore, an application of this weaker inequality would essentially suffice for a proof of the main result of this section, the lower bound for $R_0^\epsilon$ (Lemma 3.4).

To deduce a lower bound on $R_0^\epsilon$ from inequality (20), we can choose $c = \epsilon/4$ and note that (cf. proof of Lemma 3.4) $\delta = (1-\epsilon)/2$. This implies $c/(\delta + c) \geq \epsilon/2$ and leads to a bound only slightly weaker than Lemma 3.4:

$$R_0^\epsilon(\mathrm{GAF}_{G,k}) \geq \frac{\alpha|G|(1 - \mathrm{H}(1/2 - \epsilon/4)) + \log(\epsilon/2)}{(k-1)\rho_\alpha(G, k-1)}.$$

Using this inequality we obtain the lower bound

$$R_0^\epsilon(\mathrm{GAF}_{G,k}) = \Omega\left(\frac{|G|^{1/(k-1)}\ \epsilon^2 + \log \epsilon}{k-1}\right),$$

only slightly weaker than the lower bound on $R_0^\epsilon$ given in Theorem 3.3.

The conclusion is that in essence, entropy arguments are not needed for the main results of this section. On the other hand, our simple and elegant entropy argument makes the conclusions also more elegant.

**Remark 3.12** A key step in our entropy argument is Claim 3.10. We note that the Claim is in fact "Fano's Inequality" [CT] for the special case of Boolean variables.

First we state Fano's Inequality on the prediction errors for Boolean variables.

**Proposition 3.13 (Fano's Inequality for Boolean Variables)** *Let $X$ be a Boolean random variable and $Y$ a random variable over the domain $S_Y$. Let $g : S_Y \to \{0,1\}$ be a "prediction function" (given the value of $Y \in S_Y$, $g$ guesses the value of $X$). Let $\delta$ be the "prediction error:" $\delta = \Pr[g(Y) \neq X]$. Then $\mathbb{H}[X \mid Y] \leq \mathrm{H}(\delta)$.*

Claim 3.10 follows from Proposition 3.13 as follows.

For $1 \leq i \leq m$, let us define $g_i : \{0,1\}^m \to \{0,1\}$ by setting $g_i(Y) = Y_i$. Let us use $g_i$ to predict $X_i$ given $Y$. The prediction error is $\delta_i = \Pr[X_i \neq Y_i]$. Fano's Inequality gives $\mathbb{H}[X_i|Y] \leq \mathrm{H}(\delta_i)$, which is exactly inequality (18), completing the proof. ■(Claim 3.10)

Conversely, our proof of Claim 3.10 in effect proves Proposition 3.13. Indeed, our proof of Claim 3.10 can be found in the last three lines of the proof of the Entropy Loss Lemma above. To see how to adapt those three lines to prove Proposition 3.13, replace $X_i$ by $X$, $Y_i$ by $g(Y)$, $Z_i$ by $Z := X \oplus g(Y)$, and $\delta_i$ by $\delta$. ■(Fano's Inequality)

**Remark 3.14 (Comparison with [BJKS] and [BaKL])** Independent of our work, Bar-Yossef et al. [BJKS] describe an information-theoretic approach to proving lower bounds on the distributional SM complexity of $\mathrm{GAF}_{G,k}$ analogous to our Lemma 3.4.

The [BJKS] result differs from ours in their definition of the $\rho$ parameter (based, apparently, on an optimistic interpretation of the $\rho$ parameter defined in the original [BaKL] paper).

The [BJKS] definition of $\rho$ assumes a decomposition of the *entire* group $G$ as a product of *subgroups*. These assumptions apparently lead to large values of $\rho$ and thus to poor estimates of the complexity. [BJKS] make no attempt to estimate the value of their $\rho$ parameter.

The [BaKL] definition of $\rho$ used *subsets* rather than subgroups of $G$ as factors in the decomposition of the entire group $G$. It is shown in [BaKL] that this approach gives a bound for every group of order $n$ which is only slightly worse than the bound obtained for the "nicest" groups (cyclic and elementary abelian groups), namely, by a factor of $O(\sqrt{\log n})$. A positive outcome of the "Modified Rohrbach Problem (Section 7)" would eliminate this factor.

In the present paper we eliminate this factor in a different way, by bypassing the obstacle posed by the Rohrbach problem. In Section 2.3 we have constructed optimal (up to a constant factor) decompositions of a *positive fraction* of $G$ into a product of *subsets* (Theorem 2.17). This approach yields SM lower bounds for *all groups* that are within a constant factor of the results for the "nicest" groups.

The foregoing comments apply to the deterministic lower bound. The actual contribution of [BJKS] is an information theoretic argument to extend the proof of the deterministic lower bound to distributional complexity. Specifically, [BJKS] uses "Fano's Inequality for Boolean Variables" on prediction errors in terms of conditional entropy (see above, Proposition 3.13).

The information theoretic arguments presented in [BJKS] remain valid in the context of the more general decompositions considered in our paper which correspond to the $\rho_\alpha$ parameter defined in Definition 2.12.

[BJKS] use their entropy argument to prove their analogue of Lemma 3.4. Although our proof of Lemma 3.4 is also entropy-based, the two proofs look rather different. Our attempt to find the "common core" of the two proofs yielded only a modest result (see Remark 3.12).

# 4 Applications to Lower Bounds in Circuit Complexity

In this section, we derive some consequences of the SM lower bounds from Section 2.2 to super-polynomial lower bounds on certain depth-2 circuits. These circuits are described by the following definition.

**Definition 4.1** A $(\mathsf{SYMM},\mathsf{AND})$-*circuit* is defined to be a depth-2 circuit with a symmetric gate at the top and AND gates at the bottom. (We draw circuits with the output at the top. Hence inputs to the bottom gates are input variables and their negations).

We note that Beigel and Tarui [BeT] reduce ACC circuits to $(\mathsf{SYMM},\mathsf{AND})$-circuits of quasipolynomial size with bottom fan-in $\mathrm{polylog}(n)$. We present below a lower bound of $\exp((\log n/\log\log n)^2)$ on the size of $(\mathsf{SYMM},\mathsf{AND})$-circuits (of arbitrary bottom fan-in) computing some very weak functions. In fact, our lower bound applies to a function in ACC that contains $\mathrm{GAF}_{\mathbb{Z}_2^t,k}$ as a subfunction.

The following remarkable observation by Håstad and Goldmann [HG] relates multiparty communication complexity to certain depth-2 circuits.

**Lemma 4.2 (Håstad-Goldmann)** *Suppose a function $f$ is computed by a depth-2 circuit consisting of an arbitrary symmetric gate of fan-in $s$ at the top and bottom gates computing* arbitrary functions of at most $k-1$ variables. *Then, for any partition of the input among the players, the $k$-party communication complexity of $f$ is $O(k\log s)$.*

For completeness, we give a proof of Lemma 4.2.

**Proof:** Since each bottom gate of the circuit has fan-in at most $k-1$, there is at least one player who can evaluate that gate. Partition the bottom gates among the players such that all the gates assigned to a player can be evaluated by that player. Now, each player broadcasts the number of her gates that evaluate to 1. This takes $O(\log s)$ bits per player since the top gate has fan-in at most $s$. Now one of the players can add up all the numbers broadcast to compute the symmetric function given by the top gate and announce the value of the function. ∎

It is obvious that this proof works in the SM model as well: each player sends to the referee the number of gates evaluating to 1 among his gates, and the referee adds these numbers to compute $f$. The SM-complexity of the protocol is clearly $O(\log s)$. Hence, we get

**Corollary 4.3** *Suppose a function $f$ is computed by a depth-2 circuit consisting of an arbitrary symmetric gate of fan-in $s$ at the top and bottom gates computing* arbitrary functions of at most $k-1$ variables. *Then, for any partition of the input among the players, the $k$-party SM-complexity of $f$ is $O(\log s)$.*

This observation, pointed out to us by Avi Wigderson, serves as the main motivation for considering SM-complexity.

The next lemma uses the method of random restrictions [Aj, FSS] to reduce the fan-in of the bottom gates and at the same time to ensure that the "target function" (with high SM complexity) is computed by the restricted circuit. We note that a similar technique is used by Razborov and Wigderson [RaW].

First, we introduce a definition.

**Definition 4.4** Let $f(x_1, \ldots, x_v)$ be a Boolean function of $v$ variables. Let $S_1, \ldots, S_v$ be disjoint sets of variables, where $|S_i| = b$ for all $i$. Then the $\mathsf{Parity}_b$ $\mathsf{Blow\text{-}up}$ of $f$ is the function $g$ on $vb$ variables defined by

$$g(y_1, \ldots, y_{vb}) = f(\oplus_{i \in S_1} y_i, \cdots, \oplus_{i \in S_v} y_i).$$

**Definition 4.5** For a set $X$ of Boolean variables a *restriction* $\rho$ is defined to be a mapping $\rho : X \longrightarrow \{0, 1, *\}$. We interpret a variable assigned a $*$ to be "free", i.e., not fixed to a constant. Given a function $f$ on $X$, its restriction $f_{|\rho}$ is the induced function on variables assigned a $*$ by $\rho$ obtained by evaluating $f$ when the non-free variables are fixed according to $\rho$. For a circuit $C$, its restriction $C_{|\rho}$ is the circuit (with variables from $\rho^{-1}(*)$) obtained by fixing the variables of $C$ assigned 0 or 1 by $\rho$ and simplifying wherever possible.

**Lemma 4.6** *Let $g$ be the* $\mathsf{Parity}_b$ $\mathsf{Blow\text{-}up}$ *of $f$. Let $\ell$ be a parameter satisfying $\ell \leq \log b - \log \ln v + 1$, and let $0 < c < 1$ be a constant. Suppose that $g$ is computed by a circuit $C$ consisting of at most $2^{c \cdot \ell^2}$ AND gates at the bottom. Then there is a restriction $\rho$ such that*

- *All AND gates at the bottom level of $C_{|\rho}$ have fan-in at most $\ell$.*
- *$C_{|\rho}$ has $v$ input variables, exactly one from each block $S_i$, and*
- *$C_{|\rho}$ computes $f$.*

**Proof:** We define $\rho$ in two stages. First, we obtain a random restriction $\rho_1$ that reduces the fan-in of each bottom AND gate to at most $\ell$ and keeps alive at least two variables from each block $S_i$. We prove the existence of $\rho_1$ below. Second, we define $\rho_2$ by assigning values to all but one of the variables from each $S_i$ left alive by $\rho_1$ so that we are left with exactly one *unnegated* variable from each $S_i$, i.e., $\rho_2(\rho_1(\oplus_{j \in S_i} y_j)) = y_{i'}$ for some $y_{i'} \in S_i$. The desired restriction $\rho$ is the composition of $\rho_1$ and $\rho_2$. Moreover, by the definition of $g$, the restricted circuit computes $f(y_{1'}, \ldots, y_{v'})$.

Let $p := (2 \ln v)/b$. Note that $p \leq 2^{-\ell}$. We choose $\rho_1$ by independently assigning to each variable a $*$ (keep it alive) with probability $p$ and a 0 or 1 each with probability $(1-p)/2$. Let $\gamma$ be a bottom level AND gate of $C$ and let $m$ be the fan-in of $\gamma$.

First consider the case when $m \leq \ell^2$. W.l.o.g, $m \geq \ell$. Then,

$$\begin{aligned}
\Pr[\gamma_{|\rho_1} \text{ has fan-in } > \ell] &\leq \sum_{i > \ell} \binom{m}{i} p^i \left(\frac{1-p}{2}\right)^{m-i} \\
&\leq (1 + o(1)) \binom{m}{\ell} p^\ell \left(\frac{1-p}{2}\right)^{m-\ell} \qquad \text{since } \ell \gg mp \\
&\leq (1 + o(1))(pe\ell)^\ell \quad \text{since } m \leq l^2 \\
&\leq 2^{-\ell^2 \cdot (1 - o(1))} \quad \text{since } p \leq 2^{-\ell}.
\end{aligned}$$

Next consider the case when $m > \ell^2$. Then,

$$\begin{aligned}\Pr[\gamma_{|\rho_1} \text{ has fan-in } > \ell] &\leq \Pr[\gamma_{|\rho_1} \not\equiv 0] \leq \left(\frac{1+p}{2}\right)^m \\ &\leq 2^{-\ell^2\cdot(1-o(1))} \quad \text{since } m > \ell^2 \text{ and } p \leq 2^{-\ell}.\end{aligned}$$

Since $C$ has at most $2^{c\cdot\ell^2}$ AND gates at the bottom (where $c < 1$ is a constant), from the preceding two cases it follows that

$$\Pr[\text{ some bottom AND gate of } C_{|\rho_1} \text{ has fan-in} > l] = o(1) \tag{21}$$

Moreover, for a fixed $i$, $1 \leq i \leq v$, we have

$$\begin{aligned}\Pr[\rho_1(S_i) \text{ has } < 2 *\text{'s}] &= (1-p)^b + bp(1-p)^{b-1} \\ &\leq e^{-pb}(1 + bp/(1-p)) \\ &\leq O(\log v/v^2) \quad \text{since } p \geq 2\ln v/b.\end{aligned}$$

Hence, we also have

$$\Pr[\ \rho_1 \text{ assigns fewer than 2 } *\text{'s to some block } S_i\ ] = o(1). \tag{22}$$

From Eqs. (21) and (22), we see that with high probability all bottom AND gates of $C_{|\rho_1}$ have fan-in at most $\ell$ and furthermore the inputs of $C_{|\rho_1}$ will have at least two variables from each block $S_i$. Hence such a restriction $\rho_1$ exists.

By composing $\rho_1$ with an additional restriction $\rho_2$ as described in the beginning of the proof, we complete the proof of the lemma. ■

**Theorem 4.7** *Suppose an $n$ variable function $f$ has $k$-party SM-complexity at least $c_0(n,k)$ for some partition of the input among the players. Then any* (SYMM,AND)*-circuit computing the* Parity$_n$ Blowup *of $f$ must have size at least* $\min\{\exp(k^2), \exp(c_0(n,k))\}$.

**Proof:** Let $g$ denote the Parity$_n$ Blowup of $f$ and let $C$ be a minimal size (SYMM,AND) circuit computing $g$. If $C$ has size $> 2^{(k-1)^2}$, we are done.

So, suppose size of $C$ is $\leq 2^{(k-1)^2}$. We apply Lemma 4.6 to obtain a restriction $\rho$ such that bottom gates of $C_{|\rho}$ have fan-in at most $k-1$ and $C_{|\rho}$ computes $f$.

Now applying Corollary 4.3, we see that the size of $C_{|\rho}$ must be exponential in the SM complexity $c_0(n,k)$ of $f$. Hence $C$ itself must have size at least $\exp(c_0(n,k))$. ■

Using our lower bound on SM complexity from Section 2 we immediately get

**Corollary 4.8** *Let $G$ be any group of order $n$ and let $k = \epsilon \log n/\log\log n$ for a sufficiently small constant $\epsilon > 0$ . Then any* (SYMM,AND)*-circuit computing the* Parity$_n$ Blowup *of $GAF_{G,k}$ must have size* $\exp((\log n/\log\log n)^2)$.

**Proof:** From Theorem 2.8, we have that for $c_0(n,k) := C_0(\mathrm{GAF}_{G,k}) = \Omega(n^{1/(k-1)}/(k-1))$. Hence, if $k \leq \epsilon \log n/\log\log n$ for sufficiently small $\epsilon > 0$, $c_0(n,k) \geq k^2$. Now, we get the claimed bound from Theorem 4.7. ■

# 5 A Simultaneous Messages Protocol for $\mathbf{GAF}_{\mathbb{Z}_2^t,k}$

In this section we give a nontrivial protocol for $\mathrm{GAF}_{G,k}$ for $G = \mathbb{Z}_2^t$. Our protocol yields an upper bound of about $n^{(\log k)/k}$, where $n = 2^t$ (see Theorem 5.5). In particular, for 3 players we obtain a nontrivial $O(n^{0.92})$ upper bound (see Theorem 5.3). These upper bounds have been subsequently improved in [AmL], giving in particular, an upper bound of $O(n^{0.73})$ for 3 players. These upper bounds should be compared with our lower bound of $\Omega(n^{1/(k-1)}/(k-1))$ (Theorem 2.8).

It is curious to remark that, in contrast to the lower bound, our protocol heavily depends on the specific structure of this group. In particular, it does not apply to the cyclic group $G = \mathbb{Z}_n$. For cyclic groups, Pudlák, Rödl, and Sgall [PRS] give upper bounds of $O(n(\log\log n/\log n)^k)$, for constant $k$, and $O(n^{6/7})$ for $k \geq c \log n$, for some constant $c$. These upper bounds have been significantly improved by Ambainis [Am] to $O\left(\frac{n \log^{1/4} n}{2^{\sqrt{\log n}}}\right)$ for $k = 3$ and to $O(n^{\epsilon})$ for an arbitrary $\epsilon > 0$ for $k = O((\log n)^{c(\epsilon)})$. However, the bounds for $\mathbb{Z}_n$ are still much weaker than the corresponding bounds for $\mathbb{Z}_2^t$ presented in this paper.

We will think of the $n$-bit string $A$ held by $p_0$ (previously denoted $x_0$) as a Boolean function on $t := \log n$ variables $z_1, \ldots, z_t$, i.e., $A : \{0,1\}^t \longrightarrow \{0,1\}$. For $1 \leq i \leq k-1$, let $x_i$ be the $t$-bit string held by player $p_i$. Then we have

$$\mathrm{GAF}_{\mathbb{Z}_2^t,k}(A, x_1, \ldots, x_{k-1}) = A(x_1 + \cdots + x_{k-1}),$$

where '+' denotes addition in $\mathbb{Z}_2^t$.

## 5.1 Three Players

We will first describe the protocol for three players. The idea extends naturally to the general case. For simplicity of notation, let $p_1$ hold $x$ and $p_2$ hold $y$. At the cost of $2t$ bits, $p_0$ sends the strings $x$ and $y$ to the referee. Since this communication will be insignificant, we can henceforth ignore $p_0$ and assume that the referee knows $x$ and $y$ (but not $A$). Then we want to minimize the number of bits sent by $p_1$ and $p_2$ that will enable the referee to compute $A(x+y)$.

The protocol will be based on the fact that the Boolean function $A$ can be represented as a multilinear polynomial of (total) degree at most $t$. In fact, the following lemma is the crucial observation in the protocol. We use the notation

$$\Lambda(m, b) = \sum_{j=0}^{b} \binom{m}{j},$$

and the fact that for fixed $\delta$, $0 < \delta < 1/2$,

$$\Lambda(m, \delta m) \sim c(\delta) 2^{m\mathrm{H}(\delta)}/\sqrt{m}. \tag{23}$$

**Lemma 5.1** *Given the promise that $A$ is a multilinear polynomial of degree $d$ over $\mathbb{Z}_2$, $x, y \in \mathbb{Z}_2^t$, $GAF_{\mathbb{Z}_2^t,3}(A, x, y)$ has an SM- protocol with cost $\Lambda(t, \lfloor d/2 \rfloor)$.*

**Proof:** Let $A$ be given by $A(z) = \sum_{S \subseteq [t],\, |S| \leq d} a_S\, Z_S$, where $Z_S$ denotes the monomial $\prod_{i \in S} z_i$. Thus,

$$A(x+y) = \sum_{|S| \leq d} a_S \prod_{i \in S} (x_i + y_i) = \sum_{|S| \leq d} a_S \sum_{T_1 \dot\cup T_2 = S} X_{T_1} Y_{T_2},$$

where $X_{T_1} := \prod_{i\in T_1} x_i$ and $Y_{T_2} := \prod_{i\in T_2} y_i$.

We can rewrite this as follows:

$$A(x+y) = \sum_{|T_1|\le\lfloor d/2\rfloor} \left( \sum_{|T_1\dot\cup T_2|\le d} a_{T_1\dot\cup T_2}\, Y_{T_2} \right) \cdot X_{T_1} + \sum_{|T_2|\le\lfloor d/2\rfloor} \left( \sum_{|T_1\dot\cup T_2|\le d} a_{T_1\dot\cup T_2}\, X_{T_1} \right) \cdot Y_{T_2},$$

where $T_1$ and $T_2$ are disjoint subsets of $[t]$, and, we assume w.l.o.g. that terms $a_{T_1\dot\cup T_2}\, X_{T_1}\, Y_{T_2}$ with both $|T_1|$ and $|T_2|$ less than or equal to $\lfloor d/2\rfloor$ are placed in the first sum.

We now observe that the first sum in the last equation is a polynomial in $x$ whose coefficients (which depend only on $a_{T_1\dot\cup T_2}\, Y_{T_2}$) are known to $p_1$. Similarly, the second sum is a polynomial in $y$ whose coefficients are known to $p_2$. The degree of both polynomials is bounded by $\lfloor d/2\rfloor$. Hence, using at most $\Lambda(t, \lfloor d/2\rfloor)$ bits, each player can communicate the coefficients of their corresponding polynomial to the referee. Since the referee already knows $x$ and $y$, he can evaluate the two polynomials and add them up to announce the value of $A(x+y)$. Since $p_0$ used only $2t$ bits to send $x$ and $y$ to the referee, the cost of the protocol is simply $\Lambda(t, \lfloor d/2\rfloor)$. ■

**Remark 5.2** For small enough $d$, the protocol is a quadratic improvement over the trivial one where the entire function $A$ is communicated to the referee.

Suppose now that $A$ is an arbitrary Boolean function. We will use Lemma 5.1 on the low-degree part of $A$ and the trivial protocol on the high-degree part. Since there are not too many high-degree terms, we will be able to keep the communication within $n^c$ for some $c < 1$.

**Theorem 5.3** $C_0(GAF_{\mathbb{Z}_2^t,3}) = o(n^{0.92})$.

**Proof:** Let $A : \mathbb{Z}_2^t \longrightarrow \{0,1\}$ and $x, y \in \mathbb{Z}_2^t$ be the inputs on the foreheads of players 0, 1, and 2 respectively. Write $A$ as a multilinear polynomial over $\mathbb{Z}_2$ of degree at most $t$: $A(z) = \sum_{S\subseteq[t]} a_S\, Z_S$. Define $A'$ to be the part of $A$ corresponding to degree less than or equal to $2t/3$, and let $A''$ be the remaining part of $A$. That is,

$$A(z) = \sum_{|S|\le 2t/3} a_S\, Z_S \; + \sum_{|S|>2t/3} a_S\, Z_S = A'(z) + A''(z).$$

Players $p_1$ and $p_2$ use the protocol of Lemma 5.1 on $A'$. They just send the high degree terms $a_S$ for $|S| > 2t/3$ directly to the referee (each sends half of them). The number of bits used by each of $p_1$ and $p_2$ is at most

$$\Lambda(t, t/3) + \frac{1}{2} \sum_{j>2t/3} \binom{t}{j} \le \frac{3}{2}\Lambda(t, t/3) \le O(2^{t\,\mathrm{H}(1/3)}/\sqrt{t}),$$

using the estimate (23). Since $p_0$ sends fewer bits than $p_1$ or $p_2$ ($p_0$ sends only $2t$ bits), the protocol has cost $O(n^{\mathrm{H}(1/3)}/\sqrt{\log n})$. As $\mathrm{H}(1/3) = 0.91829...$, the theorem follows. ■

### 5.2 $k$ Players

We generalize the idea from the preceding section to $k$ players. An extension of Lemma 5.1 follows:

**Lemma 5.4** *Given the promise that $A$ is a $t$-variable multilinear polynomial of degree $d$ over $\mathbb{Z}_2$, and for $1 \le i \le k-1$, $x_i \in \mathbb{Z}_2^t$, $GAF_{\mathbb{Z}_2^t,k}(A, x_1, \ldots, x_{k-1})$ has an SM-protocol with cost at most* $\Lambda(t, \lfloor d/(k-1) \rfloor) + t$ .

**Proof:** In the 3-player protocol, player $p_0$ passes the two short inputs. In the $k$-player protocol, the task of passing the short inputs $x_1, \ldots, x_{k-1}$ will be divided among players $p_1$ through $p_{k-1}$, and $p_0$ will remain silent. This avoids having one player ($p_0$) communicate too many bits in case $k$ is large.

Letting $A(z) = \sum_{S \subseteq [t],\, |S| \le d} a_S\, Z_S$, we have,

$$\begin{aligned} A(x_1 + \cdots + x_{k-1}) &= \sum_{|S| \le d} a_S \prod_{j \in S} (x_{1,j} + \cdots + x_{k-1,j}) \\ &= \sum_{|S| \le d} a_S \sum_{T_1 \dot\cup \cdots \dot\cup T_{k-1} = S} X_{1,T_1} \cdots X_{k-1,T_{k-1}}, \qquad \text{where } X_{i,T_i} = \textstyle\prod_{j \in T_i} x_{ij}. \end{aligned}$$

Let us consider a monomial $a_S\, Z_S$. Since the $T_i$ are disjoint, $\sum_{i=1}^{k-1} |T_i| = |S| \le d$, and hence the smallest $T_i$ is of size at most $\lfloor d/(k-1) \rfloor$. Thus in the expansion,

$$\sum_{T_1 \dot\cup \cdots \dot\cup T_{k-1} = S} a_S\, X_{1,T_1} \cdots X_{k-1,T_{k-1}},$$

each term can be "owned" by a player $p_i$ such that $T_i$ is the smallest set in that term. (In case of ties, take the smallest such $i$.) As a result, the value of this monomial on $x_1 + \cdots + x_{k-1}$ can be distributed among the $k$ players by giving them each a polynomial of degree at most $\lfloor |S|/(k-1) \rfloor$.

The proof follows by linearity and proceeds similarly to that of Lemma 5.1. We conclude that for $1 \le i \le k-1$, player $p_i$ needs to send $\Lambda(t, \lfloor d/(k-1) \rfloor)$ bits for the terms they own and $t$ bits to send $x_{i+1}$ (player $p_{k-1}$ sends $x_1$). ∎

**Theorem 5.5** $C_0(GAF_{\mathbb{Z}_2^t,k}) \le \dfrac{k}{k-1} \Lambda(t, \lfloor t/k \rfloor) + t.$

**Proof:** Let $A : \mathbb{Z}_2^t \longrightarrow \{0,1\}$ be player 0's input and let $x_i \in \mathbb{Z}_2^t$ be player $i$'s input for $1 \le i \le k-1$. The proof is similar to the proof of Theorem 5.3: separate the low-degree and high-degree parts of $A$ as follows. Monomials of $A$ of degree higher than $t(1-1/k)$ are sent directly to the referee. (For simplicity, we ignore floors and ceilings in this proof.) By dividing these high degree monomials equally among the $k-1$ players, we see that each player sends at most $\frac{1}{k-1} \sum_{t(1-1/k) \le i \le t} \binom{t}{i} = \Lambda(t, t/k)/(k-1)$ bits. The remaining low-degree part of $A$ has degree at most $t(1-1/k)$. Applying Lemma 5.4 with $d = t(1-1/k)$, each player sends at most $\Lambda(t, t/k) + t$ bits to handle the low-degree part and to transmit $x_{i+1}$ (player $p_{k-1}$ transmits $x_1$). Adding up, we get that each player sends at most $\frac{k}{k-1} \Lambda(t, t/k) + t$ bits to the referee. ∎

**Corollary 5.6** *For $3 \le k \le \log n$, $C_0(GAF_{\mathbb{Z}_2^t,k}) \le n^{O((\log k)/k)} + \log n$.*

**Proof:** Use estimate (23) and note further that, for $k \ge 3$, $\mathrm{H}(1/k) \le \log(ek)/k$. ∎

**Remark 5.7** It follows that if $k \ge c \log n$ for any constant $c > 0$, then each player sends at most polylog$(n)$ bits to the referee. Moreover, it is easy to see from the proof of Lemma 5.4 that if $k = \log n + 1$, each player sends at most $2 + \log n$ bits and if $k > \log n + 1$, each player need only send at most $1 + \log n$ bits.

# 6 SM Upper Bounds for Other Functions

In this section, we give nontrivial upper bounds on the SM-complexity of a class of functions defined by certain depth-2 circuits and for a partition of the input variables in which each of the $k$ players misses one input bit from each bottom gate. The $n$ bottom gates are identical with fan-in $k$ and compute certain symmetric functions called symmetric *compressible* functions (see Definition 6.1). The top gate is an arbitrary symmetric gate. We call this class of communication problems the *SymCom*$(n, k)$ problems (see Definition 6.7). It includes for example, Majority of Majorities, Generalized Inner Product, and Parity of Thresholds.

We start by defining the functions that are allowed on the bottom level, i.e. the *compressible* functions. Let $X = \{x_1, \ldots, x_k\}$ be a set of Boolean variables and $f(x_1, \ldots, x_k)$ a Boolean function. Alice sees a subset $A \subseteq X$ of the variables, and Bob sees the remaining set $B = X \setminus A$. Consider the one-way communication model where Alice sends a message to Bob, and Bob must deduce the value of $f$ from Alice's message and the part of the input he sees. For a given partition of the set of variables $A \dot{\cup} B = X$, we denote by $C_{A \to B}(f)$ the minimum number of bits that Alice must send.

**Definition 6.1** A class of Boolean functions $\mathcal{F}$ is called *compressible* if for any partition $A, B \neq \emptyset$, $A \dot{\cup} B = X$, and any $f \in \mathcal{F}$ we have $C_{A \to B}(f) = O(\log |B|)$.

**Remark 6.2** We refer to a function $f$ as a compressible function if it belongs to a compressible class of functions. The constant implied by the $O$ notation may depend on the class, but not on the particular function.

We shall be interested only in compressible *symmetric* functions. Note that in this case, it is clear that $C_{A \to B} \leq \log(|A| + 1)$. The point of our definition is that we require $C_{A \to B} \leq \log |B|$ even when $|B|$ is very small compared to $|A|$. Indeed, we shall use this property for $|B| = \Theta(\log k)$.

**Example 6.3** The following Boolean functions are compressible:

1. *Parity*$(x_1, \ldots, x_k) = x_1 \oplus \ldots \oplus x_k$.
2. *Mod*$_{m,T}(x_1, \ldots, x_k) = 1$ *if and only if* $\sum_{i=1}^{k} x_i \in T \pmod{m}$.
3. $Th_t^k(x_1, \ldots, x_k) = 1$ *if and only if* $\sum_{i=1}^{k} x_i \geq t$.

**Remark 6.4** *We will give an example of a function which is not compressible in Section 6.1 below (see Definition 6.12 and Proposition 6.15).*

**Proposition 6.5** *For every partition* $A \dot{\cup} B = X = \{x_1, \ldots x_k\}$ $(A, B \neq \emptyset)$ *we have the following:*

1. $C_{A \to B}(Parity) \leq 1$ .
2. $C_{A \to B}(Mod_{m,T}) \leq \lceil \log m \rceil$ .
3. $C_{A \to B}(Th_t^k) \leq \lceil \log(|B| + 2) \rceil$ .

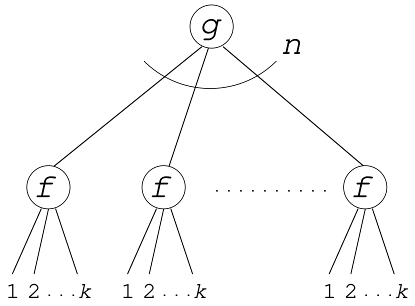


Figure 1: The depth-2 circuit defining $g \circ f$.

**Proof of Proposition 6.5:** The statements about the Parity and $Mod_m$ functions are trivial. We prove the statement of the Proposition for threshold functions. Let $A, B \neq \emptyset$, $A \dot\cup B = X = \{x_1, \ldots, x_k\}$ be some partition of the input variables. Let $\ell$ be the number of 1's in part $A$. If $\ell < t - |B|$, the value of $Th_t^k$ must be 0, and if $\ell \geq t$ the result must be 1, regardless of part $B$ of the input. For $\ell = t - i, i = 1, \ldots, |B|$ the value of the function depends on part $|B|$. Therefore, for Bob to compute the value of $f$, it is enough for Alice to send one of $|B| + 2$ messages to Bob: one for the case where $\ell < t - |B|$, one for the case where $\ell \geq t$, and one for each value of $\ell$ from $t - |B|$ to $t - 1$. This requires only $\lceil \log(|B| + 2) \rceil$ bits. ■

Let $f : \{0,1\}^k \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$ be Boolean functions. Consider the following depth 2 circuit. The first level has $n$ $f$-gates whose inputs are disjoint, so there are $nk$ input bits to the circuit. The second level consists of a $g$-gate which takes the outputs of the $f$-gates as its $n$ inputs. We denote the function computed by this circuit by $g \circ f$ (see Figure 6).

**Definition 6.6** We define the $(g, f)$-*communication problem* as the problem of $k$ players computing $g \circ f$, where $k$ is the same number as the fan-in of the $f$-gates, and the input variables are partitioned among the $k$ players so that the $j$-th player misses the $j$-th input bit of each $f$-gate.

**Definition 6.7** We call the $(g, f)$-communication problem a *SymCom*$(n, k)$ *problem*, if the function $g$ is symmetric and the function $f$ is compressible and symmetric.

**Remark 6.8** Observe that the AND function is compressible (cf. Proposition 6.5(3)). Hence the circuits used to define a *SymCom*$(n, k)$ communication problem above are somewhat similar to the (SYMM,AND)-circuits defined in Section 4. However, there are some crucial differences. First, inputs to distinct bottom gates of circuits in this section (Figure 6) are required to be *disjoint* whereas no such restriction is imposed in (SYMM,AND)-circuits. Second, the number of players in this section is *equal* to the bottom fan-in of the circuits and this is not necessarily true of (SYMM,AND)-circuits.

In Theorem 6.11, we will show that there are efficient SM protocols for SymCom$(n, k)$ problems for $k > 1 + \log n$ players. First, we need two lemmas.

**Lemma 6.9** *Let $t$ and $n$ be positive integers such that $t > 1 + \log n$. Let $b_0, \ldots, b_{t-1}$ be integers. Consider the following system of $t$ equations in $t+1$ unknowns:*

$$(t-i)y_i + (i+1)y_{i+1} = b_i, \quad i = 0, 1, \ldots, t-1. \tag{24}$$

*Assume further that*

$$y_i \geq 0, \quad i = 0, 1, \ldots, t; \quad \sum_{i=0}^{t} y_i \leq n. \tag{25}$$

*Then, under constraints (25), the system of equations (24) has at most one integral solution.*

**Proof:** Let $y = (y_0, \ldots, y_t)$ and $y' = (y'_0, \ldots, y'_t)$ be two solutions of (24), each consisting of nonnegative integers whose sum is at most $n$. For $i = 0, 1, \ldots, t$, let $d_i = y_i - y'_i$. Since $y \neq y'$, we know there exists at least one $d_i \neq 0$.

From (24), we obtain the following equations:

$$(t-i)d_i + (i+1)d_{i+1} = 0, \quad i = 0, 1, \ldots, t-1. \tag{26}$$

From the $i = 0$ equation, we can express $d_1$ in terms of $d_0$: $d_1 = -td_0 = -\binom{t}{1}d_0$. From this and the $i = 1$ equation, we get

$$d_2 = \frac{-(t-1)}{2}d_1 = \frac{(t-1)t}{2}d_0 = \binom{t}{2}d_0.$$

Continuing in this way, we see that for $i = 0$ to $t, d_i = (-1)^i\binom{t}{i}d_0$. Since some $d_i$ is not 0, we know that $d_0 \neq 0$. Furthermore, since the $d_i$ are integers, we know that $|d_0| \geq 1$, and thus $|d_i| \geq \binom{t}{i}$. We also note that since $y_i, y'_i \geq 0$, we have

$$y_i + y'_i \geq |y_i - y'_i| = |d_i|.$$

Now we use the fact that the sum of the $y_i$ and the sum of the $y'_i$ are both at most $n$ to derive a contradiction and complete the proof:

$$2n \geq \sum_{i=0}^{t}(y_i + y'_i) \geq \sum_{i=0}^{t}|d_i| \geq \sum_{i=0}^{t}\binom{t}{i} = 2^t > 2^{1+\log n} = 2n.$$

■

**Lemma 6.10** *Let $n$ be a positive integer, and let $M$ be a $t \times m$ (0,1)-matrix, with $m \leq n$ and $t = \lceil \log n \rceil + 2$. For $i = 0, 1, \ldots, t$, let $y_i$ be the number of columns of $M$ with $i$ ones. For $j = 1, \ldots, t$, let player $j$ see all of $M$ except row $j$. Then there exists an SM protocol in which each player sends $O(\log^2 n)$ bits to the referee, after which the referee can calculate $y_0, \ldots, y_t$.*

**Proof:** For $j = 1, \ldots, t$, player $j$ sends $(a_j(0), a_j(1), \ldots, a_j(t-1))$ to the referee, where $a_j(i)$ is the number of columns player $j$ sees with $i$ ones. Note that each player sees only $t-1$ of the rows, and thus cannot see $t$ ones in any column. For $i = 0, 1, \ldots, t-1$, the referee computes $b_i := \sum_{j=1}^{t} a_j(i)$.

We observe that $y_0, \ldots, y_t$ are nonnegative integers whose sum is $m \leq n$, and that for the $b_i$ defined above, they satisfy the system of equations (24). Thus, by Lemma 6.9, there is no other such solution. The referee, being arbitrarily powerful, can thus compute $y_0, \ldots, y_t$.

How many bits does each player send? Clearly each $a_j(i) \leq n$, so each $a_j(i)$ can be communicated with $\lceil \log n \rceil$ bits. Since each player communicates $t = 1 + \lceil \log(n+1) \rceil$ such numbers to the referee, we have the complexity of this SM protocol is $O(\log^2 n)$ as desired. ■

We now state the theorem regarding SM protocols for SymCom functions.

**Theorem 6.11** *If $(g, f)$ is a SymCom$(n,k)$ problem and $k > 1 + \log n$ then $C_0(g \circ f) \leq$ polylog$(n)$.*

**Proof:** Arrange the $nk$ input bits of $g \circ f$ in a $k \times n$ matrix $M$ such that player $i$ knows all of $M$ except the $i$-th row. Each column of $M$ contains the $k$ input bits of a given $f$-gate. Let $t = \lceil \log n \rceil + 2$. The first $t$ players will be the only ones who speak, so we call them the *active players.* We also call their rows and the entries in those rows *active.* The remaining players, rows, and entries are called *passive.*

Consider a single column $v \in \{0,1\}^k$ of $M$. Since $f$ is compressible, there is a one-way 2-party protocol $P$ for Alice and Bob, where Alice sees the passive entries of $v$ and Bob sees the active entries of $v$, such that Alice sends Bob $O(\log t) = O(\log \log n)$ bits. Note that since $f$ is symmetric, the only thing that Bob needs to know about the input he sees is how many ones there are. Thus, the value of $f(v)$ is determined by the message Alice sends on $v$, and the number of ones among $v$'s active entries.

For every column $v$ of $M$, the $t$ active players see all of the passive entries of $v$ and thus know what message Alice would send under $P$ upon seeing $v$. Let $c > 0$ be such that Alice sends at most $c \log \log n$ bits, and hence at most $r = \log^c n$ possible messages. Let $m_1, \ldots, m_r$ be the possible messages Alice can send under $P$.

From $M$, the active players form $r$ new matrices $M_1, \ldots, M_r$, where $M_i$ consists of the columns of $M$ for which Alice sends Bob message $m_i$ under protocol $P$. For each $j, 1 \leq j \leq r$, the $t$ players and the referee execute the protocol of Lemma 6.10 on the submatrix of $M_j$ consisting of the active rows. Thus the referee can deduce, for each $i, 0 \leq i \leq t$, the number of columns of $M_j$ which have $i$ ones among their active entries. From this and the fact that under $P$, Alice would send message $m_j$ for every column of $M_j$, the referee can deduce the number of columns $v$ of $M_j$ for which $f(v) = 1$. By summing over all $j$, the referee calculates the total number of $f$-gates that evaluate to 1, which suffices to evaluate $g \circ f$, as $g$ is symmetric.

The cost of this protocol is $r \cdot O(\log^2 n) = O(\log^{c+2} n)$. ■

## 6.1 A function which is not compressible

It is easy to check that a random symmetric function is incompressible. In this subsection we give an example of an explicit symmetric function which is not compressible (see Definition 6.1).

**Definition 6.12** For an odd prime $p$, we define the function "quadratic character of the sum of the bits," $\mathrm{QCSB}_p : \{0,1\}^p \to \{0,1\}$ by $\mathrm{QCSB}_p(x_1, \ldots, x_p) = 1$ iff $x_1 + \ldots + x_p$ is a quadratic residue mod $p$, where the $x_i$ are single bits. Recall that $y \neq 0$ is a quadratic residue mod $p$ if $y$ is a square mod $p$.

Let $p$ be an odd prime, and let $r = \lfloor (\frac{1}{2} - c_1) \log p \rfloor$, for any constant $c_1, 0 < c_1 < \frac{1}{2}$. Let $M$ be the $(r+1) \times (p+1)$ $\pm 1$-matrix defined by $M(i,j) = 1$ iff $i + j$ is a quadratic residue mod $p$ and $-1$ otherwise, for $0 \leq i \leq r, 0 \leq j \leq p$.

**Lemma 6.13** *For any $y \in \{-1,1\}^{r+1}$, the number of columns of $M$ identical to $y$ is $O(p/2^r)$.*

**Proof:** This is an immediate consequence of André Weil's character sum estimates (cf. [Sch], see also [Bo], pp. 311, 319): Let $q$ be an odd prime power, and let $U_0, U_1$ be disjoint subsets of $\mathbb{F}_q$. For $x, y$ in $\mathbb{F}_q$, let $\chi(x) = 1$ if $x \neq 0$ is a square in $\mathbb{F}_q$, 0 if $x = 0$, and $-1$ otherwise. Let

$$S = \{x \in \mathbb{F}_q \mid \text{for } i = 0, 1, (\forall u \in U_i)(\chi(x - u_i) = (-1)^i)\}.$$

Let $m = |U_0 \cup U_1|$, and let $s = |S|$. Then

$$|s - 2^{-m}q| \leq m\sqrt{q}. \tag{27}$$

Let $q := p$. Let $y = (y_0, y_1, \ldots, y_r) \in \{-1, 1\}^{r+1}$. Let $U_0 = \{p - i : 0 \leq i \leq r, y_i = 1\}$. Let $U_1 = \{p - i : 0 \leq i \leq r, y_i = -1\}$. Clearly column $j$ of $M$ is identical to $y$ exactly if $j \in S$. Setting $m := |U_0 \cup U_1| = r + 1$ gives us

$$s \leq p/2^{r+1} + (r + 1)\sqrt{p} = O(p/2^r).$$

■

**Theorem 6.14** *Let $p$ and $r$ be as above, and let $b$ be an integer $r < b < (1 - c_2)p$, for any constant $c_2$. For any 2-party one-way (Alice to Bob) protocol for $QCSB_p$, if Bob sees $b$ of the $p$ input bits, Alice sees the other $a = p - b$ bits, then Alice must send Bob $r - O(1)$ bits.*

**Proof:** Assume that there is such a one-way protocol $P$. We set $b - r$ of Bob's bits to 0, and tell both players this. This is extra information, so $P$ will still work for this restricted problem.

This new communication problem can be represented by the $(r + 1) \times (a + 1)$ $\pm 1$-matrix $M'$, obtained by deleting the last $b$ columns of $M$. The rows represent the number of ones that Bob sees, and the columns represent the number of ones Alice sees. From Lemma 6.13, we know that every $y \in \{-1, 1\}^{r+1}$ occurs in $M$ and thus in $M'$ at most $O(p/2^r)$ times. Since there are $p - b = \Omega(p)$ columns in $M'$, the number of distinct columns in $M'$ is $\Omega(2^r)$, and so Alice must send Bob $r - O(1)$ bits. ■

**Corollary 6.15** *If $p$ is an odd prime, then $QCSB_p$ is not compressible.*

**Proof:** If Bob sees $b = (\log p)^{O(1)}$ bits, then Alice must send at least $r - O(1) = \Omega(\log p) = b^{\Omega(1)}$ bits, which greatly exceeds the requirement for compressible functions. ■

## 7 Decompositions of Groups: the Rohrbach conjecture

In this section, we prove results about $\rho(G, u) := \rho_1(G, u)$ (i.e., when $\prod_{i=1}^{u} H_i = G$ in Definition 2.12) and indicate related conjectures. We shall see that $\rho(G, u)$ behaves roughly as $|G|^{1-1/u}$.

First, we observe the following easy lower bound:

**Proposition 7.1** *For any finite group $G$, $\rho(G, u) \geq |G|^{1-1/u}$.*

**Proof:** Let $G = H_1 \cdot \ldots \cdot H_u$ be an optimal decomposition. If $|H_i| \geq |G|^{1/u}$ for each $i$, then $|\widehat{H}_i| \geq |G|^{1-1/u}$. Otherwise, assume $|H_i| < |G|^{1/u}$ for some fixed $i$. Observe that $|H_i| \cdot |\widehat{H}_i| \geq |G|$. Therefore, in this case also $|\widehat{H}_i| > |G|^{1-1/u}$. ■

For arbitrary finite groups, an upper bound on $\rho(G, u)$ that is not too far from optimal follows from Theorem 2.19.

**Corollary 7.2 (of Theorem 2.19)** *For any finite group $G$ of order $n$, $\rho(G,u) \le 2(4n\ln n)^{1-1/u}$.*

**Proof:** Partition the two-element sets of Theorem 2.19 into $u$ classes, each containing at least $\lfloor m/u \rfloor$ of the $m$ two-element sets. This means that there are at most $m - \lfloor m/u \rfloor$ two-element sets in any $u-1$ of the classes. Therefore,

$$\rho(G,u) \le \max_i |\widehat{H}_i| \le 2^{m-\lfloor m/u \rfloor} \le 2^{1+m-m/u} = 2 \cdot 2^{m(u-1)/u} \le 2(4n\ln n)^{1-1/u}.$$

■

The parameter $\rho(G,u)$ is closely related to a question posed by Rohrbach [Ro1, Ro2] in 1937.

**Definition 7.3** A sequence $H_1, \ldots, H_u$ of subsets of a finite group $G$ is called a *$u$-decomposition* of $G$ if $G = H_1 \cdot \ldots \cdot H_u$. If $H_1 = \cdots = H_u = H$, we denote $H^u = H_1 \cdot \ldots \cdot H_u$. A subset $H$ of $G$ is called a *$u$-basis* of $G$ if $H^u = G$.

**Rohrbach's Problem:** Is there a constant $c = c(u)$ such that every finite group $G$ has a $u$-basis $H$ where $|H| \le c|G|^{1/u}$?

Note that if Rohrbach's Problem has an affirmative answer, then we will have, for every finite group $G$, $\rho(G,u) \le (c(u))^{u-1}|G|^{1-1/u}$. On the other hand, if we have a $u$-decomposition $G = H_1 \cdot \ldots \cdot H_u$ with $|H_i| \le \alpha|G|^{1/u}$, then we will have a $u$-basis $H$ of $G$ with $|H| \le (\alpha u)|G|^{1/u}$ by simply taking $H = H_1 \cup \cdots \cup H_u$. Moreover, such a decomposition will also give that $\rho(G,u) \le \alpha^{u-1}|G|^{1-1/u}$. Hence the following question appears to be of more general interest.

**Modified Rohrbach Problem:** Is there an absolute constant $c$ such that every finite group $G$ has a $u$-decomposition $G = H_1 \cdot \ldots \cdot H_u$ where $|H_i| \le c|G|^{1/u}$?

Both Rohrbach's Problem and its modified version have been answered affirmatively for several special classes of finite groups. Of particular interest in our context is the following result of Kozma and Lev [KoL] (for our purposes, $\lambda_i = 1/u$ in the following theorem).

**Theorem 7.4 (KL)** *Let $G$ be a finite group such that every composition factor of $G$ is either a cyclic group or an alternating group. Then for every positive integer $u$ and nonnegative real numbers $\lambda_i$ such that $\lambda_1 + \cdots + \lambda_u = 1$, there is a $u$-decomposition $G = H_1 \cdot \ldots \cdot H_u$ where $|H_1| \le |G|^{\lambda_1}$ and $H_i \le 2|G|^{\lambda_i}$ for $2 \le i \le u$. In particular, this conclusion holds if $G$ is an alternating group or if $G$ is solvable.*

This result answers the modified Rohrbach Problem affirmatively for some important special classes of finite groups. As a consequence, we have the following corollary about $\rho(G,u)$:

**Corollary 7.5** *Let $G$ be a finite group such that every composition factor of $G$ is either a cyclic group or an alternating group. Then for every positive integer $u$, $\rho(G,u) \le 2^{u-1}|G|^{1-1/u}$. In particular, this bound holds if $G$ is an alternating group or if $G$ is solvable.*

These results have been extended to groups with linear ($PSL(n,q)$) and symplectic ($Psp(2n,q)$) composition factors (in addition to cyclic and alternating composition factors) with a suitable small constant in place of the coefficient 2 (Pyber [Py]). There is hope that the Modified Rohrbach Problem will be settled in the affirmative in the foreseeable future. (As mentioned above, this will also settle Rohrbach's original problem.)

In Examples 1 and 2, we gave upper bounds of $O(|G|^{1-1/u})$ on $\rho(G,u)$ of two special cases of greatest interest to us, namely $G = \mathbb{Z}_2^t$ and $G = \mathbb{Z}_n$. Thus in these cases we reduce the gap between the trivial lower bound $|G|^{1-1/u}$ (Proposition 7.1) and the upper bound to an absolute constant. These bounds are therefore stronger than those implied by an affirmative answer to the Modified Rohrbach Problem.

We propose the following stronger version of the Modified Rohrbach Problem.

**Problem:** Is there an absolute constant $c$ such that for any finite group $G$ and any positive integer $u$, $\rho(G,u) \leq c|G|^{1-1/u}$?

We have given the positive answer for cyclic groups and for elementary abelian 2-groups.

# 8 Open Problems

1. The main open problem in multiparty communication complexity theory remains to find a nontrivial lower bound for some explicit function for more than $\log n$ players. Some candidate functions are:

   (a) Let $T_t^{k,r}$ be defined as follows: $T_t^{k,r}(x_1,\ldots,x_k) = 1$ iff $x_1 + \ldots + x_k \geq t$, where the $x_i$ are $r$-bit integers. The candidate function is Majority of Thresholds $MT_{n,k,r}$, defined by the following depth two circuit: the bottom level has $n$ $T_t^{k,r}$ gates, whose inputs are disjoint (so $MT$ is a function of $knr$ bits), and the top gate is a Majority gate. There are $k$ players, and the $i$-th player misses the $i$-th integer of each threshold gate. We recommend $n = k = r$.

   The (Majority, $T_t^{k,1}$)-communication problem is a SymCom$(n,k)$ problem (see Section 6), and hence for $k \geq 2 + \log n$, it has an efficient SM protocol. However, for $r \geq 2$, $\mathrm{MT}_{n,k,r}$ does not fit our description of SymCom functions (because players miss more than one input bit at each "$f$-gate"). So our protocol does not work, even though for bounded $r$, $\mathrm{T}_t^{k,r}$ is a compressible function.

   (b) Quadratic Character of the Sum of the coordinates, defined as follows. Let $p$ be an $n$-bit prime, and for $1 \leq i \leq k$, let $x_i$ be an $n$-bit integer missed by player $i$. $\mathrm{QCS}_{p,k}(x_1,\ldots,x_k) :=$ 1 iff $x_1 + \ldots + x_k$ is a quadratic residue mod $p$. It is shown in [BaNS] that $C(\mathrm{QCS}_{p,k}) \geq \Omega(n/2^k)$.

   (c) Let $F$ be a finite field of order $q$. Give each player a $t \times t$ matrix over $F$. Let $M$ be the product (in a given order) of these matrices. Estimate the SM complexity of decision problems associated with $M$, such as, "Is trace$(M)$ a quadratic residue in $F$?" (for odd $q$). Here $n \approx q^{t^2}$. The case $t = 2$ is of particular interest.

2. Consider the SM problem $\mathrm{GAF}_{G,3}$. Show that there exists an $\epsilon > 0$ such that in any SM protocol for $\mathrm{GAF}_{G,3}$, if player 2 sends at most $n^\epsilon$ bits, then player 1 must send $\omega(n/\log\log n)$ bits. As explained in Section 1.3, such a lower bound would imply that the $n$-bit output function $f(x_0,x_1) = (\mathrm{GAF}_{G,3}(x_0,x_1,x_2))_{x_2\in G}$, cannot be computed by circuits of size $O(n)$ and depth $O(\log n)$. Note that our lower bound proof in Section 2 implies[3] that for *any* $\epsilon > 0$, if player 2 sends at most $n^\epsilon$ bits, then player 1 must send $\Omega(n^{1-\epsilon})$ bits. On the other hand,

[3] In general, methods of Section 2 can be used to prove that, in any SM protocol for $\mathrm{GAF}_{G,k}$, if player $i$ sends $\ell_i$ bits, then $\Pi_{i=1}^{k-1}\ell_i \geq n/2^{O(k\log k)}$ must hold.

by the upper bound of [AmL] (improving the protocol in Section 5), it suffices if both player s send $O(n^{0.73})$ bits.

3. Find nontrivial SM lower or upper bounds for Majority of QCSBs for any partition of the input bits (see Section 6).

4. Obtain an $n^{1-\epsilon}$ SM upper bound for $\mathrm{GAF}_{G,k}$ for the case where $G$ is a cyclic group. The best upper bound known is due to Ambainis [Am]. He shows that $C_0(\mathrm{GAF}_{\mathbb{Z}_n,3}) = O\left(\frac{n \log^{1/4} n}{2^{\sqrt{\log n}}}\right)$, and that $C_0(\mathrm{GAF}_{\mathbb{Z}_n,k}) = O(n^\epsilon)$ for an arbitrary $\epsilon > 0$ for $k = O((\log n)^{c(\epsilon)})$.

5. The lower bound on the randomized SM complexity of $\mathrm{GAF}_{\mathbb{Z}_2^t,k}$ from Section 3 is useful only when the advantage $\epsilon$ is $n^{-O(1/k)}$. Improve this to yield meaningful (polylog($n$)) lower bounds on the randomized SM complexity even for advantages as small as $2^{-\mathrm{polylog}(n)}$. Such an improvement would enable the extension of circuit lower bounds from Section 4 to depth-3 in the spirit of [HG, RaW] exploiting an "approximation lemma" from [HMPST]. Note that the [BaNS] lower bound in the CFL-model works even for advantages as small as $2^{-n/c^k}$.

6. *This problem, stated as an open question in an earlier version of this paper [BaKL], was resolved in [BaHK]. We repeat the problem and state its current status.*

   Find a function $f$ for which the one-way complexity $C_1(f)$ is exponentially larger than $C(f)$, for $k \geq 4$ players.

   Such a gap was found for $k = 3$ [NW], cf. Remark 2.9. For all $k \leq c \log n$, the gap was established in [BaHK]. We note that lower bounds for $C_1$ complexity have been applied in [BaNS] to lower bounds on branching programs and formula size.

## Acknowledgments

We are grateful to Avi Wigderson for suggesting to us the SM model and pointing out the connection of ACC with the model considered in this paper. In October of 1994, P. Pudlák kindly sent us the manuscript [PRS] by P. Pudlák, V. Rödl, and J. Sgall. Among many other things, that paper considers SM complexity under the name "Oblivious Communication Complexity" and deduces the $\mathrm{GAF}_{G,k}$ lower bound for cyclic groups by essentially the same methods as ours [PRS, Proposition 2.3].

Finally, we are grateful to an anonymous referee for suggestions which have lead to considerable improvement of our paper in two ways: the improvement discussed in Remark 2.10 and the use of entropy arguments for distributional complexity.

## References

[Aj] M. Ajtai: $\Sigma_1^1$-formulae on finite structures. *Annals of Pure and Applied Logic* **24** (1983), 1–48.

[AlS] N. Alon, J. H. Spencer: *The Probabilistic Method.* Second Edition. Wiley, 2000.

[Am] A. Ambainis: Upper Bounds on Multiparty Communication Complexity of Shifts. *Proc. 13th Ann. Symp. on Theoretical Aspects of Computer Science (STACS),* Springer LNCS, Vol. 1046, 1996, 631–642.

[AmL] A. Ambainis, S. V. Lokam: Improved Upper Bounds on Simultaneous Messages Complexity. *Proc. LATIN 2000*, Springer LNCS Vol. 1776, 2000, 207–216.

[BaE] L. Babai, P. Erdős: Representation of Group Elements as Short Products. *Theory and Practice of Combinatorics* (J. Turgeon, A. Rosa, G. Sabidussi, editors) Ann. Discr. Math., Vol. 12, North-Holland, 1982, 21–26.

[BaHK] L. Babai, T. Hayes, P. Kimmel: The cost of the missing bit: Communication complexity with help. *Combinatorica* **21** (2001), 455–488.

[BaKL] L. Babai, P. Kimmel, S. V. Lokam: Simultaneous Messages vs. Communication. *Proc. 12th Symp. on Theor. Aspects of Computer Science* (STACS), Springer LNCS Vol 900, 1995, 361–372. (Preliminary version of this paper.)

[BaNS] L. Babai, N. Nisan, M. Szegedy: Multiparty Protocols, Pseudorandom Generators for Logspace and Time-Space Trade-offs. *J. Computer and System Sciences* **45** (1992), 204–232.

[BeT] R. Beigel, J. Tarui: On ACC. *Proc. 32nd IEEE FOCS*, 1991, 783–792.

[BJKS] Z. Bar-Yossef, T. S. Jayram, Ravi Kumar, D. Sivakumar: Information Theory Methods in Communication Complexity. *Proc. 17th IEEE Conf. Computational Complexity (CCC '02)*, 2002, 72–81.

[Bo] B. Bollobás: *Random Graphs.* Academic Press, 1985.

[CFL] A. K. Chandra, M. L. Furst, R. J. Lipton: Multiparty protocols. *Proc. 15th ACM STOC*, 1983, 94–99.

[CT] T. M. Cover, J. A.,Thomas: *Elements of Information Theory.* Wiley, 1991.

[EGS] P. Erdős, R. Graham, E. Szemerédi: On Sparse Graphs with Dense Long Paths. *Comp. and Maths. with Appls.,* **1** (1975), 365 – 369.

[FSS] M. Furst, J. Saxe, M. Sipser: Parity, Circuits, and the Polynomial Time Hierarchy. *Mathematical Systems Theory* **17** (1984), 13–27.

[G] V. Grolmusz: The BNS Lower Bound for Multi-Party Protocols is Nearly Optimal. *Information and Computation* **112** (1994), 51–54.

[HG] J. Håstad, M. Goldmann: On the Power of Small-Depth Threshold Circuits. *Computational Complexity* **1** (1991), 113–129.

[HMPST] A. Hajnal, W. Maass, P. Pudlák, M. Szegedy, G. Turán: Threshold Circuits of Bounded Depth. *Proc. 28th IEEE FOCS*, 1987, 99–110.

[KaT] J. Katz, L. Trevisan: On the Efficiency of Local Decoding Procedures for Error-Correcting Codes. *Proc. 32nd ACM Symposium on Theory of Computing (STOC)*, 2000, pp.80 – 86.

[KoL] G. Kozma, A. Lev: On $H$-bases and $H$-Decompositions of Finite Solvable and Alternating Groups. *J. Number Theory* **49** (1994), 385–391.

[KuN] E. Kushilevitz, N. Nisan: *Communication Complexity.* Cambridge University Press, 1997.

[MacS] F. J. MacWilliams, N. J. A. Sloane: *The Theory of Error-Correcting Codes.* North-Holland – Elsevier, Amsterdam, 1977.

[Man] Mann, E. : Private Access to Distributed Information. *Master's Thesis, Technion, 1998.*

[MNT] Y. Mansour, N. Nisan, P. Tiwari: The Computational Complexity of Universal Hashing. *Theoretical Computer Science* **107** (1993), 121-133.

[NW] N. Nisan, A. Wigderson: Rounds in Communication Complexity Revisited. *SIAM J. Computing* **22** (1993), 211–219.

[PR] P. Pudlák, V. Rödl: Modified Ranks of Tensors and the Size of Circuits. *Proc. 25th ACM STOC*, 1993, 523–531.

[PRS] P. Pudlák, V. Rödl, J. Sgall: Boolean circuits, tensor ranks and communication complexity. *SIAM J. Computing* **26** (1997), 605–633.

[Py] L. Pyber: *private communication.*

[RaW] A. Razborov, A. Wigderson: $n^{\Omega(\log n)}$ Lower Bounds on the Size of Depth 3 Circuits with AND Gates at the Bottom. *Information Processing Letters* **45** (1993), 303–307.

[Ro1] H. Rohrbach: Ein Beitrag zur additiven Zahlentheorie. *Math. Z.* **42** (1937), 1–30.

[Ro2] H. Rohrbach: Anwendung eines Satzes der additiven Zahlentheorie auf eine gruppentheoretische Frage. *Math. Z.* **42** (1937), 538–542.

[Sch] W. M. Schmidt: *Equations over Finite Fields: An Elementary Approach.* Springer Lect. Notes in Math. vol. 536, 1976.

[Va] L. Valiant: Graph-Theoretic Arguments in Low-level Complexity. *Proc. 6th Symp. on Math. Foundations of Comp.* (MFCS), Spriner LNCS, Vol. 53, 1977, 162–176.

[Ya1] A. C-C. Yao: Lower Bounds by Probabilistic Arguments. *Proc. 24th IEEE FOCS*, 1983, 420–428.

[Ya2] A. C-C. Yao: On ACC and Threshold Circuits. *Proc. 31st IEEE FOCS*, 1990, 619–627.