Electronic Colloquium on Computational Complexity, Revision 2 of Report No. 182 (2026)

Tight Lower Bounds for Algebraic Communication and Applications

Manon Blanc[1] Prateek Dwivedi[1] Magnus Rahbek Dalgaard Hansen[1]
Nutan Limaye[1] Meena Mahajan[2]

Abstract

Communication complexity studies how much information must be exchanged to solve a problem whose input is split among two or more parties. The classical setting deals with Boolean inputs split between two parties. In this work, we study an algebraic variant, where the inputs are vectors over a field $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$.

There are two players, Alice and Bob, with inputs $X \in \mathbb{F}^n$ and $Y \in \mathbb{F}^n$, respectively. We consider two kinds of tasks. In the *polynomial evaluation problem*, the goal is to compute the value of a polynomial $g \in \mathbb{F}[X, Y]$ on the given input. In the *set-recognition problem*, the goal is to decide whether $(X, Y) \in S$, for a given set $S \subseteq \mathbb{F}^n \times \mathbb{F}^n$. In both settings, Alice and Bob send evaluations of polynomials depending only on their own inputs. In the polynomial evaluation problem, these messages are combined to compute the evaluation $g(X, Y)$. In the set-recognition problem, a referee receives the messages and may apply polynomial tests to the messages received so far; the outcomes of these tests determine acceptance or rejection. The protocols may be deterministic or probabilistic.

This algebraic communication viewpoint, initiated by Abelson (JACM, 1980) and later developed by Grigoriev (Computational Complexity, 2008), has remained comparatively unexplored. In this work, we revisit this model and demonstrate that it continues to offer a rich framework for new lower bound questions. We present three sets of results.

- **Upper bounds and reductions.** We give non-trivial upper bounds for a range of natural polynomial evaluation and set-recognition problems, showing that algebraic communication can be significantly more powerful than simply sending all input coordinates.

  We also prove reductions between different problems, which help organize the landscape of the model and identify which problems capture its main difficulties. These results serve two purposes: they illustrate the expressive power of the model, and they show that proving meaningful lower bounds in this setting is interesting.
- **A lower bound framework and tight lower bounds.** Our main technical contribution is a general framework for proving lower bounds for algebraic set-recognition problems.

  Using this framework, we prove several

  probabilistic lower bounds for natural problems introduced earlier in the paper. In a number of cases, these lower bounds match the corresponding upper bounds, giving tight or near-tight characterizations of their algebraic communication. Along the way, we also recover and generalize some of Grigoriev's original lower bound results.
- **Applications of the framework.** Finally, we give two applications of our framework. First, we use the communication lower bounds to prove lower bounds for a class of left-to-right algebraic algorithms, which we call algebraic scanners. Second, we show that our lower bound arguments extend beyond polynomials to a more general algebraic computational setting inspired by the Blum–Shub–Smale model.

[1]IT University of Copenhagen, Copenhagen, Denmark.
[2]The Institute of Mathematical Sciences, Chennai, India; Homi Bhabha National Institute, Mumbai, India.

ISSN 1433-8092

Funding. MB, PD, MH, and NL acknowledge support from the Independent Research Fund Denmark (grant agreement No. 10.46540/3103-00116B) and from Basic Algorithms Research Copenhagen (BARC), funded by VILLUM Foundation Grant 54451. NL is supported by the Carlsberg Foundation grant CF25-1645. MM acknowledges support from the J C Bose fellowship grant JCB/2023/000006 of the Anusandhan National Research Foundation (ANRF), India.

Contents

1 Introduction **3**
- 1.1 Our results and techniques . . . 5
- 1.2 Related work . . . 9
- 1.3 Discussion and open problems . . . 10

2 Preliminaries **10**
- 2.1 Communication complexity of a polynomial evaluation problem . . . 11
- 2.2 Protocol for set-recognition . . . 12

3 Communication bounds and reductions **13**
- 3.1 Upper bounds for equality and its variant . . . 14
- 3.2 Deterministic lower bound for equality . . . 15
- 3.3 Complexity of sparse difference . . . 17
- 3.4 Complexity of bilinear forms . . . 19

4 Communication complexity via mixed Hessian rank **21**

5 Framework for probabilistic lower bounds **23**
- 5.1 Over the real numbers . . . 23
- 5.2 Over the complex numbers . . . 27

6 New probabilistic lower bounds **29**
- 6.1 The ε-equality set . . . 29
- 6.2 The ε-hypercube set . . . 30
- 6.3 Inner product . . . 32
- 6.4 The ε-SI set . . . 34

7 Applications of communication lower bounds **36**

8 Extension to bounded-time BSS machines **38**
- 8.1 Bounded-time BSS machines . . . 39
- 8.2 Extension of the full-rank mixed Hessian criterion to rational functions . . . 39
- 8.3 Framework for BSS probabilistic lower bounds . . . 40

Acknowledgements **44**

References **44**

A Proof of the mixed Hessian rank bound **46**

1 Introduction

Communication complexity studies the amount of communication required to compute a function jointly by two or more parties on an input distributed among them. The standard setup has two players. The inputs are usually Boolean strings, and the two players aim to compute a Boolean function. This model was introduced by Yao [Yao79]. It is mathematically simple, and yet it captures many important aspects related to communication. It is extremely well-studied and has a large range of applications to other areas of algorithms and complexity theory such as circuit complexity, proof complexity, query complexity, and streaming algorithms [Mut05; RY20].

A related model for a more general class of functions was introduced by Abelson [Abe80] soon after Yao's two-party model for Boolean functions. Here, the two players, henceforth called Alice and Bob, receive inputs from $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. So, Alice receives $X = (X_1, \ldots, X_n) \in \mathbb{F}^n$ and Bob receives $Y = (Y_1, \ldots, Y_n) \in \mathbb{F}^n$. The goal is to evaluate a polynomial $g \in \mathbb{F}[X, Y]$ on the given input (X, Y). We will call this the *polynomial evaluation problem*. The way they are allowed to do this is as follows: There is a referee receiving messages from Alice and Bob, say $a_1(X), \ldots, a_{r_1}(X) \in \mathbb{F}[X]$ and $b_1(Y), \ldots, b_{r_2}(Y) \in \mathbb{F}[Y]$, respectively. Now, the referee computes $g(X, Y) = P(a_1(X), \ldots, a_{r_1}(X), b_1(Y), \ldots, b_{r_2}(Y))$, where $P \in \mathbb{F}[z_1, \ldots, z_{r_1+r_2}]$. Among all such representations of g, we wish to find the one that minimizes $r_1 + r_2$. The problem has both computational and algebraic motivations. From the computational point of view, it is closely related in spirit to Yao's communication model, since it studies computation under a partition of the input. From the algebraic point of view, it asks how succinctly can a polynomial in variables X and Y be represented using polynomials depending only on X and polynomials depending only on Y.

More than two decades after this, Grigoriev [Gri08] introduced a variant of the above model for decision problems in this setting. These problems are called set-recognition problems[1]. In this case, the goal is to recognize a set $S \subseteq \mathbb{F}^n \times \mathbb{F}^n$: given $X \in \mathbb{F}^n$ to Alice and $Y \in \mathbb{F}^n$ to Bob, check whether $(X, Y) \in S$ or not. Here, the protocol is visualized as a tree. Every node of the tree belongs to either Alice or Bob. At an Alice node, say v, she sends a message, a polynomial $a_v \in \mathbb{F}[X]$, to the referee. Similarly, at a Bob node, say u, Bob sends a polynomial $b_u(Y) \in \mathbb{F}[Y]$ to the referee. At each node, the referee applies *a test*[2] to the messages it has received so far. The tests are also polynomials (and not arbitrary functions). The tree branches based on the result of the test. For $\mathbb{F} = \mathbb{C}$, the protocol tests $\{= 0, \neq 0\}$, whereas, for $\mathbb{F} = \mathbb{R}$, the tests are $\{< 0, = 0, > 0\}$. The leaves of the protocol are labelled by outputs, either accept or reject; an input is accepted or rejected according to the label of the leaf reached by the protocol on that input. The depth of the tree is the complexity measure, which we want to minimize. A noteworthy aspect of Grigoriev's paper is that it also analyzes a probabilistic communication model. (Formal definitions appear in Section 2.) We write $\mathrm{DCC}_{\mathbb{F}}(S)$ and $\mathrm{PCC}_{\mathbb{F}}(S)$ for the deterministic and probabilistic communication complexities of recognizing S, respectively, over the field $\mathbb{F}$.

Our work focuses on Abelson and Grigoriev's models of communication. We study the polynomial evaluation problem as in Abelson's work, as well as the set-recognition problem, as in Grigoriev's work. We consider both deterministic and probabilistic communication. The set-recognition problem is a decision problem and, thus, bears some resemblance to decision problems arising in the communication complexity of Boolean functions, such as those studied in [KN97; RY20]. While Boolean communication complexity is often amenable to combinatorial techniques, our setting is inherently different: the domain is $\mathbb{F}^n \times \mathbb{F}^n$, rather than a discrete Boolean domain, and the com-

[1] Simultaneously, Bläser and Vicari [BV08] also introduced a closely related model. We will talk about it in detail in the section about related work.

[2] In the original model [Gri08], each node can perform multiple tests. Here, we assume that each node has only 1 test. However, all our results hold for the original model as well.

municated messages are evaluations of polynomials. This calls for a different set of tools, combining algebraic techniques with analytic reasoning.

In [Gri08], the first strong lower bounds for probabilistic communication were proved. In our work, we present a general framework for proving lower bounds for probabilistic communication complexity of set-recognition problems. This involves a substantial generalization of previous techniques [Gri08]. The generalization also achieves a quantitative improvement to the lower bounds obtained in [Gri08]. Furthermore, we give an extensive analysis of the deterministic model by providing new upper and lower bounds. We also give two applications of our results. The first application uses our lower bounds as a black-box to obtain lower bounds for algorithmic problems. This is similar to the standard communication-to-streaming connection. The second application involves modifying our lower bound proofs further in order to obtain lower bounds for a BSS-inspired communication model, which is more general than the communication model by [Gri08].

Polynomial evaluation problem. As mentioned above, the problem was first studied in [Abe80]. It is straightforward that the complexity of the problem is always upper bounded by $2n$. Alice and Bob can simply send their entire input to the referee and then the referee can compute $g(X, Y)$. Notice that Alice, Bob, and the referee are allowed to compute arbitrary polynomials of their inputs. That is, the complexity of computing a_i's, b_i's and P does not contribute towards the cost of solving the problem.

The main contribution of Abelson's work was an elegant mathematical statement showing that the complexity of the problem is lower bounded by twice the rank of a matrix, which we call the mixed Hessian matrix and denote it by $\mathsf{H}_{X|Y}(g)$. It is an $n \times n$ matrix, where the (i, j)th entry is $\partial^2 g / \partial X_i \partial Y_j$.

For example, consider the inner product polynomial $\mathsf{IP}_n(X, Y) = \sum_{i=1}^n X_i Y_i$. It is not hard to see that $\mathsf{H}_{X|Y}(\mathsf{IP}_n) = I_n$, where I_n is the $n \times n$ identity matrix. Thus, Abelson's bound [Abe80] gives a tight lower bound of $2n$ for the polynomial evaluation problem for $\mathsf{IP}_n(X, Y)$.

Set-recognition problem. Here is another instructive example of the equality polynomial. For this discussion, let us fix $\mathbb{F} = \mathbb{R}$. Let $\mathsf{EQ}_n(X, Y) = \sum_{i=1}^n (X_i - Y_i)^2$. Since a sum of squares over $\mathbb{R}$ vanishes exactly when every summand vanishes,

$$V(\mathsf{EQ}_n) = \{(X, X) \mid X \in \mathbb{R}^n\}.$$

The $2n$ deterministic upper bound is not hard to see: Alice sends X_i to the referee, then Bob sends Y_i to the referee, and the referee tests whether $(X_i - Y_i)^2 = 0$ or not. If it is equal to 0, then the protocol proceeds to check the next coordinate else it rejects and terminates. In our work, we show that $2n$ is tight for deterministic protocols. (We will elaborate on this in Section 1.1.[3])

In contrast, one can recognize $V(\mathsf{EQ}_n)$ using a probabilistic protocol with $O(1)$ communication. Using public randomness, Alice and Bob choose r uniformly from a fixed set $A \subseteq \mathbb{R}$ of size at least $3n$. Alice computes $a(X) = \sum_{i=1}^n X_i r^i$. Similarly, Bob computes $b(Y) = \sum_{i=1}^n Y_i r^i$. The referee accepts if and only if $a(X) = b(Y)$. As a univariate polynomial of degree at most n can have at most n roots, the probability that the protocol accepts when X and Y are not equal is at most $1/3$. This shows that the probabilistic protocols are provably stronger than deterministic protocols. A similar exponential gap was proved in [Gri08] for a set-recognition problem called the *Orthant problem*. These gaps underline the fact that the model is non-trivial and proving lower bounds for probabilistic communication in this model is significant. The bounds for $V(\mathsf{EQ}_n)$ mentioned above

[3] In [BV08] a $2n$ lower bound was proved, but this was for a restricted setting where a_i's and b_i's are homogeneous. We do not need such a restriction.

may remind the reader of analogous bounds for the communication complexity of the Boolean equality function. We emphasize, however, that this similarity is only superficial: as we will see below, the techniques involved here are quite different.

In [Gri08], such lower bounds were achieved. In particular, it proved the following statement.

Theorem 1.1 ([Gri08])**.** *Let* $\mathsf{IP}_n(X,Y) = \sum_{i=1}^{n} X_i Y_i$*, let* $S(\mathsf{IP}_n) = \{(X,Y) \in \mathbb{R}^n \times \mathbb{R}^n \mid \mathsf{IP}_n(X,Y) \leq 0\}$*, and let* $V(\mathsf{IP}_n) = \{(X,Y) \in \mathbb{C}^n \times \mathbb{C}^n \mid \mathsf{IP}_n(X,Y) = 0\}$*. Then,* $\mathrm{PCC}_{\mathbb{R}}(S(\mathsf{IP}_n))$ *is at least* $2n-6$ *and* $\mathrm{PCC}_{\mathbb{C}}(V(\mathsf{IP}_n))$ *is at least* $2n-6$*.*

Remark 1.2. The theorem above summarizes Proposition 3.1 and Corollary 3.2 of Grigoriev [Gri08]. In fact, these results establish a slightly more general lower bound than the version stated here, and our work generalizes those original statements as well. For ease of exposition, we state only this restricted form in this part of the introduction. We return to the more general formulation later, when discussing the proof techniques underlying our results.

1.1 Our results and techniques

We start with a summary of our results and organization. After this brief summary, we discuss the main theorems and the proof techniques used to prove them.

1.1.1 Summary and organization

- We provide non-trivial deterministic and probabilistic upper bounds for a broad array of set-recognition problems. These bounds show that both deterministic and probabilistic models are non-trivial. Additionally, we prove a tight deterministic lower bound for equality. These initial bounds also provide a gentle introduction to this model of computation. We present these results in Section 3.

- We extend and improve Theorem 1.1 above in two ways. In the statement above, we have $F_n(X,Y) = \mathsf{IP}_n(X,Y)$ and the lower bounds are for the sets $S(F_n) = \{(X,Y) \mid F_n(X,Y) \leq 0\}$ over $\mathbb{R}$ and $V(F_n) = \{(X,Y) \mid F_n(X,Y) = 0\}$ over $\mathbb{C}$.

  As our first extension, we prove that F_n can be more general and not necessarily restricted to IP_n. In fact, we show that if F_n satisfies a set of conditions (we formally provide these below), then we can prove strong lower bounds. Thus, this provides a new framework for lower bounds; to prove a lower bound, one can simply check these conditions. These results are presented in Section 5.

  We also provide tight lower bounds for several set-recognition problems in deterministic and probabilistic models. Along the way, we show that the lower bound in Theorem 1.1 can be improved to $2n-4$ (see Theorem 6.10). See Section 6.

- Finally, we give two applications of our results. First, we show that the lower bounds above can be used to prove lower bounds for a certain class of algebraic algorithms. These algorithms scan the input from left to right. We call them algebraic scanners. They are reminiscent of streaming algorithms, but with crucial differences. These results appear in Section 7.

  Second, we show that our lower bound proofs work for a more general setting. Specifically, we show that our lower bound arguments extend beyond polynomials to a more general algebraic computational model, inspired by the Blum–Shub–Smale model [Blu+98], for Alice, Bob, and the referee. These results appear in Section 8.

1.1.2 Communication bounds and reductions

We study the deterministic and probabilistic communication complexity of several natural sets. We prove reductions among these problems, allowing lower bounds for one set to be transferred to others.

For exact equality some field $\mathbb{F}$, we write

$$V(X-Y) \coloneqq \{(X,X) \mid X \in \mathbb{F}^n\} = V(X_1 - Y_1, \ldots, X_n - Y_n).$$

Thus, $V(X-Y) = V(\mathsf{EQ}_n)$ over $\mathbb{R}$, whereas $V(X-Y) \subsetneq V(\mathsf{EQ}_n)$ over $\mathbb{C}$ when $n \geq 2$.

Problem	Description
EQ_n	The inputs are equal: $X = Y$.
UEQ_n	The inputs agree up to a permutation of their coordinates: there exists $\sigma \in S_n$ such that $X_i = Y_{\sigma(i)}$ for every $i \in [n]$.
$\mathsf{SD}_{n,k}$	The inputs differ in at most k coordinates: $\#\{i \in [n] \mid X_i \neq Y_i\} \leq k$.
IP_n	Over $\mathbb{R}$, recognize the threshold condition $\sum_{i=1}^n X_i Y_i \leq 0$; over $\mathbb{C}$, recognize the zero condition $\sum_{i=1}^n X_i Y_i = 0$.
$\mathsf{BF}_{n,A}$	For a fixed public matrix A, recognize $X^T A Y \leq 0$ over $\mathbb{R}$ where $A \in \mathbb{R}^{n \times n}$ and $X^T A Y = 0$ over $\mathbb{C}$, where $A \in \mathbb{C}^{n \times n}$.
SI_n	The coordinate sets intersect: $X_i = Y_j$ for some $i, j \in [n]$, equivalently, $\prod_{i,j \in [n]} (X_i - Y_j) = 0$.

Table 1: Set-recognition problems considered in this paper. All problems are considered over $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$.

Let $V(\mathsf{UEQ}_n)$ denote the set of (X,Y) such that they agree up to a permutation of their coordinates. Similarly, let $V(\mathsf{SD}_{n,k})$ denote the set of inputs (X,Y) such that they differ in at most k coordinates.

Theorem 1.3. *The probabilistic communication complexity of $V(\mathsf{UEQ}_n)$ is $O(1)$ and that of $V(\mathsf{SD}_{n,k})$ is also $O(1)$ when $k = O(1)$.*

Note that $V(\mathsf{UEQ}_n)$ is simply asking whether X and Y are equal as multisets. We show that checking this can be reduced to checking whether n symmetric functions (polynomials) of X and Y are equal or not. Symmetric polynomials appear naturally in the argument because we are checking for a symmetric property. Thus, this observation allows us to obtain the same upper bound for $V(\mathsf{UEQ}_n)$ and $V(X-Y)$.

To prove the upper bound for $V(\mathsf{SD}_{n,k})$, there are several technical insights. The main argument hinges on creating $k+1$ vectors in $\mathbb{F}^{k+1}$ such that they are linearly dependent if $X = Y$, but they are linearly independent with high probability if X and Y differ at $\geq k+1$ coordinates.

Next, we consider bilinear forms, $\mathsf{BF}_{n,A} = X^T A Y$, where A is an $n \times n$ matrix over $\mathbb{F}$ and $X, Y \in \mathbb{F}^n$. It is clear that when $A = I_n$, this is exactly the same as IP_n. In fact, if A is a rank r matrix then, for any (X,Y), there exists $(\widetilde{X}, \widetilde{Y})$ such that $\mathsf{BF}_n(X,Y) = \mathsf{IP}_r(\widetilde{X}, \widetilde{Y})$. We observe that this conversion is local to Alice and Bob, i.e., given X to Alice (and Y to Bob), Alice

can compute $\widetilde{X}$ herself (and Bob can compute $\widetilde{Y}$ himself). Thus, the bounds for set-recognition problems related to IP_r transfer to that of $\mathsf{BF}_{n,A}$, where rank of A is r. This yields a family of problems whose complexity is neither necessarily as large as the full $2n$ bound nor as small as $O(1)$.

Finally, we consider exact equality, $V(X-Y)$. A natural approach to a constant-cost equality protocol is a polynomial encoding $\phi : \mathbb{F}^n \to \mathbb{F}$: Alice and Bob send $\phi(X)$ and $\phi(Y)$, and the referee compares them. For its correctness, such an encoding must be injective, which is impossible when $n > 1$; see Proposition 2.4. On restricted domains, however, injective polynomial encodings may exist. In particular, we construct one for $\mathbb{Z}^n$ in Observation 3.1, yielding a constant-cost equality protocol for integral inputs. Such restrictions are generally unnatural for equality over $\mathbb{R}$ or $\mathbb{C}$.

Thus, equality on unrestricted inputs should, in general, be expected to be hard. We prove a tight lower bound of $2n$ on the deterministic communication complexity of $V(X-Y)$.

Theorem 1.4 (Deterministic communication complexity of equality)**.** *For every $n \geq 1$ and $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$, the deterministic communication complexity of $V(X-Y)$ is $2n$.*

The theorem generalizes a lower bound from [BV08]. Their proof uses ideas from projective geometry and requires that all the polynomials in the communication protocol are homogeneous.

We do not assume homogeneity. Our proof is an adaptation of the classical *fooling-set argument* from communication complexity to the algebraic setting.

The idea can be described as follows. For a deterministic protocol C, and a root-to-leaf path π in C, let T_π denote the set of inputs that end up at the leaf of π. First, we observe that there must be an open set U such that the diagonal inputs (X, X) follows π for every $X \in U$. At a high level, this is a pigeonhole argument. Once we have such a leaf, then we can form a fooling set $\{(X, X) \mid X \in U\}$.

1.1.3 Framework for probabilistic communication

To describe the results in this section, we need some notation.

Notations. Recall that for a polynomial $p(X, Y) \in \mathbb{F}[X, Y]$, $\mathsf{H}_{X|Y}(p)$ is the mixed Hessian matrix. We will drop the suffix $X|Y$, if the partition of variables is clear from the context. Let $\nabla_X p$ denote an $n \times 1$ vector in $\mathbb{F}[X, Y]^n$ such that the ith entry of the vector is $\partial p / \partial X_i$. Similarly define $\nabla_Y p$. We use R_p to denote the determinant of the following $(n+1) \times (n+1)$ matrix.

$$R_p = \mathsf{Det} \begin{pmatrix} \mathsf{H}_{X|Y}(p) & \nabla_X p \\ (\nabla_Y p)^T & 0 \end{pmatrix}$$

We are now ready to state the new lower bound framework for probabilistic communication. To ease the exposition, we will focus on $\mathbb{F} = \mathbb{R}$ for the rest of the section.

Theorem 1.5 (Tight lower bound for real communication)**.** *Let $F \in \mathbb{R}[X, Y]$ be irreducible, and let $S(F) = \{(X, Y) \in \mathbb{R}^n \times \mathbb{R}^n \mid F(X, Y) \leq 0\}$. If there exists $u \in \mathbb{R}^n \times \mathbb{R}^n$ such that*

$$F(u) = 0 \qquad \text{and} \qquad R_F(u) \neq 0,$$

then, the probabilistic communication complexity of $S(F)$ over $\mathbb{R}$ is $\geq 2n$, i.e., $\mathrm{PCC}_{\mathbb{R}}(S(F)) \geq 2n$.

Proof technique. The proof generalizes several technical ideas from [Gri08].

In fact, Grigoriev's theorem can be stated more generally than the statement of Theorem 1.1, where the set one wants to recognize does not need to be $S(F)$ for a polynomial F, but instead can be any semialgebraic set S. Specifically, the general statement says that, for a semialgebraic set S, if $\dim(\partial S \cap V(\mathsf{IP}_n)) = 2n - 1$, then its probabilistic communication complexity is at least $2n - 6$.

Our first step is to observe that there is nothing special about IP_n in this setting. As long as the polynomial $F(X,Y)$ is irreducible and $F \nmid R_F$, where R_F is the determinant polynomial defined above, then, for any semialgebraic set S such that $\dim(\partial S \cap V(F)) = 2n-1$, we can obtain a lower bound for the set-recognition problem for S. This makes our framework widely applicable.

The second improvement comes from the fact we present a better analysis of the connection between the rank of $\mathsf{H}_{X|Y}(F)$ and the communication complexity of communication protocols. As mentioned above, Abelson proves that if $\mathsf{H}_{X|Y}(F)$ is high then the communication complexity of evaluating F is also high. Grigoriev presents a technique to *lift* lower bounds for polynomial evaluation problems to set-recognition problems for a related set. We fine-tune this lift to obtain better parameters and thus tight lower bounds.

The framework also has a complex analogue, with the boundary condition replaced with Zariski closure. This yields the following theorem.

Theorem 1.6 (Tight lower bound for communication over $\mathbb{C}$)**.** *Let $F \in \mathbb{C}[X,Y]$ be irreducible and let $V(F) = \{(X,Y) \in \mathbb{C}^n \times \mathbb{C}^n \mid F(X,Y) = 0\}$. If there exists $u \in \mathbb{C}^n \times \mathbb{C}^n$ such that*

$$F(u) = 0 \qquad \text{and} \qquad R_F(u) \neq 0,$$

then $\mathrm{PCC}_{\mathbb{C}}(V(F)) \geq 2n$.

1.1.4 New lower bounds

Our framework can be applied to obtain several new lower bounds.

Let $\mathsf{EQ}_n(X,Y) = \sum_{i=1}^{n}(X_i - Y_i)^2$ and $\mathsf{EQ}_{n,\varepsilon} = \mathsf{EQ}_n - \varepsilon$. For $\mathbb{F} = \mathbb{R}$, the polynomial EQ_n evaluates to 0 if and only if $X = Y$. The set $S(\mathsf{EQ}_{n,\varepsilon})$ consists of pairs (X,Y) whose squared Euclidean distance is at most ε. We show that its probabilistic communication complexity is $2n$. This contrasts the $O(1)$ upper bound for $V(\mathsf{EQ}_n)$. For $\mathbb{F} = \mathbb{C}$, we show that the probabilistic communication complexity of $V(\mathsf{EQ}_{n,\varepsilon})$ is also $2n$.

We also analyze $S(\mathsf{IP}_n)$ over $\mathbb{R}$ and $V(\mathsf{IP}_n)$ over $\mathbb{C}$, proving that their probabilistic communication complexities are at least $2n-4$. This slightly improves the lower bound of $2n-6$ obtained in [Gri08].

Next, we consider $V(\mathsf{SI}_n)$, where $\mathsf{SI}_n(X,Y) = \prod_{i\in[n]}\prod_{j\in[n]}(X_i - Y_j)$. Note that $\mathsf{SI}_n(X,Y) = 0$ if and only if X, Y have a non-empty intersection when thought of as sets. Grigoriev analyzed $V(\mathsf{SI}_n)$ and proved a probabilistic communication lower bound of $n/2$ over $\mathbb{C}$ and a lower bound of n over $\mathbb{R}$. We prove a lower bound of $2n-6$ for recognizing two closely related sets. Specifically, we show that the probabilistic communication complexity of $S(\mathsf{SI}_{n,\varepsilon})$ over $\mathbb{R}$ and $V(\mathsf{SI}_{n,\varepsilon})$ over $\mathbb{C}$ is at least $2(n-3)$, where $\mathsf{SI}_{n,\varepsilon} = \mathsf{SI}_n - \varepsilon$.

1.1.5 Applications of the lower bounds and the framework

We present two applications of the above communication lower bounds.

Algebraic Scanners. We define a class of algebraic algorithms, which we call *algebraic scanners*. An algebraic scanner processes its input from left to right. At each step, it can compute an univariate polynomial evaluation of the current input and store the resulting value in a memory register. In addition, it can perform polynomial tests on the contents of its memory registers, with the outcomes of these tests determining its subsequent actions. After completing a full scan of the input, the scanner either accepts or rejects. An (ℓ, t) algebraic scanner stores at most ℓ elements in its memory and makes at most t tests. The complexity of the scanner is $(\ell + t)$. We also consider probabilistic variants of algebraic scanners.

We show that communication lower bounds for set-recognition problems lead to lower bounds on the complexity of the algebraic scanners. This connection is closely inspired by the well-known relationship between communication complexity of Boolean functions and lower bounds for streaming algorithms [AMS99; Mut05].

We prove lower bounds for the following two natural geometric problems: (a) Given $X, Y \in \mathbb{F}^n$, check whether the ℓ_2 distance between X and Y is at most ε, for some fixed ε. (b) Given n green points followed by n red points, check if there exists a bichromatic pair that collides, i.e. there are two points of different color with the same value.

Alice, Bob, the referee, and BSS machines. So far, we have assumed that Alice and Bob communicate evaluations of polynomials and the referee performs polynomial tests. Thus, implicitly, the internal computations of all three parties can be carried out by algebraic circuits, possibly of exponential size. We ask whether our framework continues to apply when Alice, Bob, and the referee are allowed to use a more general computational model internally. In particular, we allow the parties to compute rational functions, and, additionally, allow Alice and Bob to perform local tests involving rational functions of their respective inputs. These extensions bring the internal computational model closer to the Blum–Shub–Smale (BSS) model. We prove that our lower bound framework continues to apply even in this more general setting. The proofs require a careful adaptation of the techniques we developed in Section 4 and Section 5. One interesting observation is that *lifting* lower bounds from polynomial evaluation problems to set-recognition problems continues to hold even when rational functions are allowed in place of polynomials.

1.2 Related work

As mentioned above, Abelson [Abe80] first studied the communication complexity of the polynomial evaluation problem. This was further developed by Luo and Tsitsiklis [LT93] in the setting of distributed algebraic computation. These papers study the amount of information that must be exchanged by parties who jointly compute algebraic functions whose inputs are distributed between them.

Grigoriev [Gri08], as well as Bläser and Vicari [BV08], studied the set-recognition problem. While our work mainly builds on Grigoriev's model, Bläser and Vicari also give a compelling formulation of algebraic communication. In their model, the parties may exchange arbitrary real or complex numbers. In particular, messages are not necessarily restricted to evaluations of polynomials. Moreover, Alice and Bob communicate with each other directly, rather than with a referee. Consequently, their later messages may depend not only on their own inputs, but also on the previous transcripts, including messages received from the other party. Some variants of their model allow comparisons and zero-tests. The final decision may be made by Alice or Bob and may depend on parts of the input that are never communicated with the other party throughout the protocol. A main distinction from our setting (which is also Grigoriev's setting) is that Bläser and Vicari [BV08] focus on deterministic communication complexity, whereas we also study probabilistic protocols.

Prior to [BV08], Krajícek had also introduced communication games where two parties exchange arbitrary messages rather than polynomial evaluations. This work aimed at generalizing the well-studied Karchmer-Wigderson games [KW90] and at connecting proof complexity to real communication complexity and monotone real formulas and circuits [Kra98].

Monotone real circuits form another related line of work connecting real algebraic computation, communication, and proof complexity. Pudlák introduced monotone real circuits in the context of proof complexity, and later work of Hrubeš and Pudlák studied their relationship to monotone Boolean complexity and real communication protocols [HP17; Pud97]. More recently, Applebaum,

Beimel, Nir, Peter, and Pitassi [App+22] connected monotone real circuits and separable variants of them to secret-sharing schemes.

Finally, we mention Ben-Or's algebraic computation tree lower bound [Ben83], another foundational result concerning exact decision problems over the reals. Our work differs from Ben-Or's in both the underlying model of computation and in the techniques used to prove lower bounds. Ben-Or's proofs rely on combinatorial properties of the set being recognized. Such arguments do not directly capture the difficulty in our model, where the main challenge is to bound the amount of algebraic interaction between the two sides of the input.

1.3 Discussion and open problems

We end the introduction with a discussion and several open problems.

- In our work, we have been able to show many tight lower bounds in deterministic as well as probabilistic communication models. Two problems which both Grigoriev's work and our work study are $S(\mathsf{IP}_n)$ over $\mathbb{R}$ and $V(\mathsf{IP}_n)$ over $\mathbb{C}$. Can we prove a lower bound of $2n$ for these problems? We are not able to apply our general framework for the polynomial IP_n because when $F = \mathsf{IP}_n$, there is no u such that $F(u) = 0$ and $R_F(u) \neq 0$. We prove the lower bound $2n - 4$ by refining individual steps of the proof and analyzing them for these two sets. Could we instead use some other properties of IP_n to obtain a tight lower bound?
- Our lower bound framework is quite easy to state and appears to be broadly applicable. It would be interesting to identify further natural set-recognition problems to which the framework applies, and to prove lower bounds for them.
- As mentioned above, the communication model studied in [BV08] is different from the model we study here. An interesting direction is to develop lower bound techniques for probabilistic communication in their model.

2 Preliminaries

For $n \in \mathbb{N}$ and $n \geq 1$, let $X = \{X_1, \ldots, X_n\}$ and $Y = \{Y_1, \ldots, Y_n\}$ be two sets of variables throughout this paper. We denote by S_n the symmetric group on $[n]$, and by $\mathbb{F}[X, Y]$ the ring of polynomials in the variables X and Y with coefficients over $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$.

For polynomials $p_1, \ldots, p_m \in \mathbb{F}[X, Y]$, their *common zero set* (or variety) is defined by

$$V(p_1, \ldots, p_m) \coloneqq \{(X, Y) \in \mathbb{F}^n \times \mathbb{F}^n \mid p_j(X, Y) = 0 \text{ for every } j \in [m]\}.$$

When $m = 1$, we simply write $V(p)$. Likewise, the *nonzero set* (or distinguished set) of p is defined as the complement of $V(p)$:

$$D(p) \coloneqq \{(X, Y) \in \mathbb{F}^n \times \mathbb{F}^n \mid p(X, Y) \neq 0\}.$$

Finally, for $p \in \mathbb{R}[X, Y]$ the threshold set (also known as the sublevel set) of p is defined as

$$S(p) \coloneqq \{(X, Y) \in \mathbb{R}^n \times \mathbb{R}^n \mid p(X, Y) \leq 0\}.$$

Definition 2.1 (Constructible set)**.** *A set $W \subseteq \mathbb{C}^N$ is* constructible *if it is a finite union of sets of the form*

$$\left\{z \in \mathbb{C}^N : f_1(z) = \cdots = f_k(z) = 0, \quad g(z) \neq 0\right\},$$

where $f_1, \ldots, f_k, g \in \mathbb{C}[z_1, \ldots, z_N]$.

Definition 2.2 (Boundary of a set)**.** *Let $S \subseteq \mathbb{R}^N$. The* Euclidean boundary *of S, denoted ∂S, is defined as the set of all points $x \in \mathbb{R}^N$ such that every open ball centered at x intersects both S and its complement $\mathbb{R}^N \setminus S$. Formally,*

$$\partial S = \{x \in \mathbb{R}^N \mid \forall r > 0,\, B_r(x) \cap S \neq \emptyset \text{ and } B_r(x) \cap (\mathbb{R}^N \setminus S) \neq \emptyset\},$$

where $B_r(x)$ denotes the open Euclidean ball of radius r centered at x.

The following proposition records the dimension of a hypersurface over $\mathbb{R}$ and $\mathbb{C}$. The real case follows from the Implicit Function Theorem and the dimension theory of real algebraic sets; see [BCR98, Proposition 3.3.10, 3.3.11] and [Spi65, Theorem 5-1]. The complex case follows from the Krull Principal Ideal Theorem.

Proposition 2.3. *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$, and let $p \in \mathbb{F}[x_1, \ldots, x_N]$ be a non-constant irreducible polynomial. If $\mathbb{F} = \mathbb{C}$, then*

$$\dim V(p) = N - 1.$$

If $\mathbb{F} = \mathbb{R}$ and if there exists $x_0 \in V(p)$ such that $\nabla p(x_0) \neq \mathbf{0}$, then

$$\dim V(p) = N - 1.$$

If, moreover, $\nabla p(x) \neq \mathbf{0}$ for every $x \in V(p)$, then $V(p)$ is a smooth real algebraic hypersurface.

One might hope to make communication highly efficient by uniquely encoding an input using fewer polynomial coordinates. The following proposition rules out such a compression on any nonempty open set.

Proposition 2.4 ([Tao14, Corollary 1.6.3])**.** *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$, let $U \subseteq \mathbb{F}^n$ be a nonempty Euclidean open set, and let $0 \leq r < n$. No polynomial map $\Phi : U \to \mathbb{F}^r$ is injective.*

In this work, we will also use the following classical bound on the number of zeros of a nonzero multivariate polynomial over a grid [DL78; LN96; Ore22; Sch80; Zip79].

Lemma 2.5 (Polynomial identity testing lemma)**.** *Let $0 \neq f \in \mathbb{F}[z_1, \ldots, z_m]$ have total degree at most d, and let $A \subseteq \mathbb{F}$ be finite. If $\alpha_1, \ldots, \alpha_m$ are chosen independently and uniformly from A, then*

$$\Pr\left[f(\alpha_1, \ldots, \alpha_m) = 0\right] \leq \frac{d}{|A|}.$$

2.1 Communication complexity of a polynomial evaluation problem

Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Alice holds $X = (X_1, \ldots, X_n)$ and Bob holds $Y = (Y_1, \ldots, Y_n)$. To evaluate g at (X, Y), Alice communicates the values of finitely many polynomials in X, and Bob communicates the values of finitely many polynomials in Y. The value of $g(X, Y)$ is then computed by applying a polynomial P to all the communicated values. The cost is the total number of values communicated.

Definition 2.6 (Communication Complexity of a Polynomial)**.** *For $r_1, r_2 \in \mathbb{N}$, a* polynomial-evaluation representation *of $g \in \mathbb{F}[X, Y]$ consists of polynomials $a_1, \ldots, a_{r_1} \in \mathbb{F}[X]$, $b_1, \ldots, b_{r_2} \in \mathbb{F}[Y]$, and a polynomial P over $\mathbb{F}$ in $r_1 + r_2$ variables such that*

$$g(X, Y) \quad = \quad P\big(a_1(X), \ldots, a_{r_1}(X), b_1(Y), \ldots, b_{r_2}(Y)\big).$$

The cost of this representation is $r_1 + r_2$. The communication complexity *of g, denoted $c(g)$, is the minimum cost of any such representation. In particular, constant polynomials have communication complexity 0.*

Example 2.7 (Inner product)**.** *Consider the inner product polynomial* $\mathsf{IP}_n(X,Y) = \sum_{i=1}^{n} X_i Y_i$*. Alice communicates the* n *values* $a_i(X) = X_i$*, and Bob communicates the* n *values* $b_i(Y) = Y_i$*. Taking*

$$P(z_1, \ldots, z_{2n}) \quad = \quad \sum_{i=1}^{n} z_i z_{n+i},$$

we obtain $\mathsf{IP}_n(X,Y) = P\left(a_1(X), \ldots, a_n(X), b_1(Y), \ldots, b_n(Y)\right)$*. Thus* $c(\mathsf{IP}_n) \leq 2n$*.*

In fact, for any polynomial $g \in \mathbb{F}[X,Y]$, $c(g)$ is bounded by $2n$. In the upcoming sections, we will see how Grigoriev uses linear algebra to prove a matching lower bound.

2.2 Protocol for set-recognition

While the previous section dealt with evaluating a polynomial, we now turn to the communication complexity of *recognizing a set*. Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. Alice receives $X \in \mathbb{F}^n$, and Bob receives $Y \in \mathbb{F}^n$. Let $S \subseteq \mathbb{F}^n \times \mathbb{F}^n$ be the set that they want to recognize, i.e., they want to check whether their input belongs to this set or not.

Definition 2.8 (Deterministic set-recognition protocol)**.** *A deterministic communication protocol over* $\mathbb{F}$ *is a finite rooted tree, with the root at level* 1*, whose leaves are labeled Accept or Reject. Each internal node* v *at level* r *is assigned*

- *a message polynomial* q_v*, associated with one of the parties: either* $q_v \in \mathbb{F}[X]$ *or* $q_v \in \mathbb{F}[Y]$*; and*
- *a testing polynomial* $P_v \in \mathbb{F}[z_1, \ldots, z_r]$*.*

On input (X,Y)*, for a* v *at level* r*, the associated party broadcasts* $h_r = q_v(X)$ *if the node* v *belongs to Alice or* $h_r = q_v(Y)$ *if* v *belongs to Bob. The outgoing edge is determined by evaluating* P_v *on the transcript* $h = (h_1, \ldots, h_r)$*, where* h_i *are the message polynomials along a path from the root to* v*. Over* $\mathbb{R}$*, the three possible outcomes are* $P_v(h) < 0$*,* $P_v(h) = 0$*, and* $P_v(h) > 0$*. Over* $\mathbb{C}$*, the two possible outcomes are* $P_v(h) = 0$ *and* $P_v(h) \neq 0$*. The outgoing edges are labeled by these outcomes, so every input determines a unique root-to-leaf path.*[4]

The protocol recognizes *a set* $S \subseteq \mathbb{F}^n \times \mathbb{F}^n$ *if this path ends at an Accept leaf exactly when* $(X,Y) \in S$*. The cost of the protocol is the maximum number of internal nodes on a root-to-leaf path. The* deterministic communication complexity $\mathrm{DCC}_{\mathbb{F}}(S)$ *is the minimum cost of a protocol recognizing* S*. We drop the suffix when the field is clear from the context.*

To familiarize ourselves with the model, consider the equality polynomial

$$\mathsf{EQ}_n(X,Y) = \sum_{i=1}^{n} (X_i - Y_i)^2$$

and its zero set

$$V(\mathsf{EQ}_n) = \{(X,Y) \in \mathbb{F}^n \times \mathbb{F}^n \;\mid\; \mathsf{EQ}_n(X,Y) = 0\}.$$

Over $\mathbb{R}$, $V(\mathsf{EQ}_n) = V(X-Y)$; over $\mathbb{C}$, $V(X-Y) \subsetneq V(\mathsf{EQ}_n)$ when $n \geq 2$. Nevertheless, the following protocol recognizes $V(\mathsf{EQ}_n)$ over either field.

[4] Grigoriev [Gri08] considers the more general model in which each node may have a finite family of testing polynomials. All results in this paper continue to hold in that model as well.

First, Alice broadcasts $h_i = X_i$ for $1 \le i \le n$, and Bob then broadcasts $h_{n+i} = Y_i$ for $1 \le i \le n$. The testing polynomials at the first $2n-1$ nodes are fixed nonzero constants, so the protocol simply continues. After the final message, the referee evaluates

$$P_{2n}(h) = \sum_{i=1}^{n} (h_i - h_{n+i})^2.$$

The protocol accepts if this value is zero and rejects otherwise. Thus, it recognizes $V(\mathsf{EQ}_n)$ with cost $2n$ over both $\mathbb{R}$ and $\mathbb{C}$.

Definition 2.9 (Probabilistic set-recognition protocol)**.** *A probabilistic communication protocol $\mathcal{C}$ consists of deterministic protocols $C_1, \dots, C_N$, for some finite N, as in Definition 2.8, together with probabilities $\mu_1, \dots, \mu_N > 0$ satisfying $\sum_{i=1}^{N} \mu_i = 1$. Here, μ is a probability distribution over the deterministic protocols $C_1, \dots, C_N$. The protocol recognizes $S \subseteq \mathbb{F}^n \times \mathbb{F}^n$ with bounded error if every input is classified correctly with probability at least $2/3$; that is,*

$$\Pr_{\mu}[\mathcal{C} \text{ accepts } (X,Y) \iff (X,Y) \in S] \ge \frac{2}{3}.$$

Its cost is $\max_i \operatorname{cost}(C_i)$*, and the* probabilistic communication complexity $\mathrm{PCC}_{\mathbb{F}}(S)$ *is the minimum cost of a probabilistic protocol recognizing S with bounded error. We use* $\mathrm{PCC}(S)$ *when the field is clear from the context.*

The following example demonstrates that probabilistic protocols can be significantly more efficient than deterministic protocols. (We will later show a tight lower bound for the same problem in the deterministic setting.)

Example 2.10 (Equality)**.** *The exact-equality set $V(X-Y)$ admits a probabilistic protocol of cost 2.*

Proof. Fix a set $A \subseteq \mathbb{F}$ of size $3n$, and choose $r \in A$ uniformly at random. For each choice of r, Alice and Bob respectively broadcast

$$h_1 = \sum_{i=1}^{n} X_i r^i \qquad \text{and} \qquad h_2 = \sum_{i=1}^{n} Y_i r^i.$$

The first testing polynomial is constant, while the second is $P(z_1, z_2) = z_1 - z_2$. The protocol accepts exactly when $P(h_1, h_2) = 0$. Thus every deterministic protocol in the distribution has cost 2.

If $X = Y$, the protocol always accepts. If $X \neq Y$, then

$$Q(z) = \sum_{i=1}^{n} (X_i - Y_i) z^i$$

is a nonzero polynomial of degree at most n. It has at most n roots, so the probability that $Q(r) = 0$ is at most $n/(3n) = 1/3$. Hence the protocol rejects unequal inputs with probability at least $2/3$. □

3 Communication bounds and reductions

In this section, we prove communication bounds for natural sets such as equality and sparse difference. The discussion in this section will also serve as a warm-up to the communication models.

3.1 Upper bounds for equality and its variant

In Section 2.2, we discussed a deterministic protocol for the set $V(\mathsf{EQ}_n)$. We now turn to exact equality, $V(X - Y)$, and show that integral inputs admit a constant-cost deterministic protocol. The following was also observed as a remark in [Vic08].

Observation 3.1 (Equality over integers)**.** *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ and $n \geq 1$. Under the promise that $X, Y \in \mathbb{Z}^n$, exact equality admits a deterministic protocol over $\mathbb{F}$ of complexity exactly 2.*

Proof. We will first construct an injective polynomial map for Alice and Bob, and then use it to construct a depth-2 protocol for recognizing equality over the integers.

Injective polynomial map. We first construct an injective polynomial $\Phi_n : \mathbb{Z}^n \to \mathbb{Z}_{\geq 0}$. Define

$$\varphi(z) = 2z^2 - z \qquad \text{and} \qquad \psi(u, v) = (u + v)^2 + v.$$

The map $\varphi : \mathbb{Z} \to \mathbb{Z}_{\geq 0}$ is injective: if $\varphi(z) = \varphi(w)$, then

$$(z - w)\,(2(z + w) - 1) = 0,$$

and the second factor cannot vanish for integers z, w. The map $\psi : \mathbb{Z}^2_{\geq 0} \to \mathbb{Z}_{\geq 0}$ is also injective. Suppose $\psi(u, v) = \psi(u', v')$, and set $s = u + v$ and $s' = u' + v'$. If $s > s'$, then $s \geq s' + 1$, and therefore

$$\psi(u, v) \geq s^2 \geq (s' + 1)^2 > s'^2 + s' \geq \psi(u', v').$$

Since $\psi(u, v) > \psi(u', v')$, we have a contradiction. By symmetry, $s < s'$ is also impossible, so $s = s'$. It follows that $s^2 + v = s^2 + v'$, hence $v = v'$ and then $u = u'$.

Now define recursively

$$\Phi_1(z_1) = \varphi(z_1), \qquad \Phi_k(z_1, \ldots, z_k) = \psi\left(\Phi_{k-1}(z_1, \ldots, z_{k-1}), \varphi(z_k)\right).$$

Since φ and ψ are injective polynomial maps, so is Φ_n. These maps have integer coefficients and therefore define valid message polynomials over both $\mathbb{R}$ and $\mathbb{C}$.

Set-recognition protocol. Consider the following depth-2 protocol. At the root, Alice uses the message polynomial $q_1(X) = \Phi_n(X)$ and broadcasts $h_1 = q_1(X)$. The testing polynomial at this node is the constant polynomial 1, so the protocol continues to the second node. There, Bob uses the message polynomial $q_2(Y) = \Phi_n(Y)$ and broadcasts $h_2 = q_2(Y)$. The testing polynomial is

$$P(z_1, z_2) = z_1 - z_2.$$

The protocol accepts on the zero branch and rejects otherwise. Hence, on the promised inputs, it accepts precisely when $\Phi_n(X) = \Phi_n(Y)$, which, by injectivity, is equivalent to $X = Y$.

Finally, a depth-1 protocol has only one message, belonging to one party, and its output therefore depends only on that party's input. It cannot recognize equality even on the promised inputs, since the answer depends on both inputs. Thus the complexity is exactly 2. □

Next, we consider unordered equality, in which Alice's and Bob's inputs are viewed as multisets rather than ordered vectors. Equivalently, their inputs are equal up to a permutation of the coordinates.

Observation 3.2 (Unordered equality reduces to equality)**.** *Let $\mathbb{F}$ be any field, and define*

$$V(\mathsf{UEQ}_n) = \left\{(X, Y) \in \mathbb{F}^n \times \mathbb{F}^n \;\middle|\; \text{there exists } \sigma \in S_n \text{ such that } X_i = Y_{\sigma(i)} \text{ for all } i \in [n]\right\}. \quad (3.3)$$

Every deterministic or probabilistic protocol recognizing $V(X-Y)$ gives a protocol of the same cost recognizing $V(\mathsf{UEQ}_n)$. Consequently,

$$\mathrm{DCC}_{\mathbb{F}}\left(V(\mathsf{UEQ}_n)\right) \le \mathrm{DCC}_{\mathbb{F}}\left(V(X-Y)\right) \qquad \textit{and} \qquad \mathrm{PCC}_{\mathbb{F}}\left(V(\mathsf{UEQ}_n)\right) \le \mathrm{PCC}_{\mathbb{F}}\left(V(X-Y)\right).$$

Proof. For $Z \in \mathbb{F}^n$, let $\mathsf{ESym}_k(Z)$ denote the kth elementary symmetric polynomial evaluated at Z, and define

$$\mathsf{ESym}(Z) = \left(\mathsf{ESym}_1(Z), \ldots, \mathsf{ESym}_n(Z)\right).$$

The vector $\mathsf{ESym}(Z)$ determines the monic polynomial with roots $Z_1, \ldots, Z_n$:

$$\prod_{i=1}^{n}(t - Z_i) \quad = \quad t^n - \mathsf{ESym}_1(Z)t^{n-1} + \cdots + (-1)^n\,\mathsf{ESym}_n(Z). \tag{3.4}$$

Consequently, the coordinates of X and Y agree as multisets if and only if $\mathsf{ESym}(X) = \mathsf{ESym}(Y)$. Thus

$$(X, Y) \longmapsto (\mathsf{ESym}(X), \mathsf{ESym}(Y))$$

transforms an instance of unordered equality into an instance of equality, with

$$(X, Y) \in V(\mathsf{UEQ}_n) \quad \Longleftrightarrow \quad (\mathsf{ESym}(X), \mathsf{ESym}(Y)) \in V(X - Y).$$

Indeed, the forward implication follows because every elementary symmetric polynomial is invariant under permutations. Conversely, if $\mathsf{ESym}(X) = \mathsf{ESym}(Y)$, then comparing coefficients in Eq. (3.4) gives

$$\prod_{i=1}^{n}(t - X_i) = \prod_{i=1}^{n}(t - Y_i).$$

By unique factorization in $\mathbb{F}[t]$, these polynomials have the same roots with the same multiplicities. Thus the coordinates of X and Y agree as multisets, so $(X, Y) \in V(\mathsf{UEQ}_n)$.

The reduction is local: Alice computes $\mathsf{ESym}(X)$ and Bob computes $\mathsf{ESym}(Y)$. Given a protocol for $V(X-Y)$, replace each Alice-message polynomial $q(X)$ by $q(\mathsf{ESym}(X))$ and each Bob-message polynomial $q(Y)$ by $q(\mathsf{ESym}(Y))$. These remain one-party polynomials, so the resulting protocol recognizes $V(\mathsf{UEQ}_n)$. □

3.2 Deterministic lower bound for equality

We now prove that deterministic recognition of $V(X-Y)$ requires each party to communicate n polynomial values. This set captures exact equality over both $\mathbb{R}$ and $\mathbb{C}$. The argument begins by finding one accepting path followed by an open set of diagonal inputs which traverse that path.

Lemma 3.5 (A common accepting path)**.** *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$, let $U \subseteq \mathbb{F}^n$ be a nonempty Euclidean open set, and let C be a deterministic protocol recognizing $V(X-Y)$ under the promise $X, Y \in U$. There exist a nonempty Euclidean open set $W \subseteq U$ and an accepting root-to-leaf path π in C such that (X, X) follows π for every $X \in W$.*

Proof. For every internal node v, let

$$A_v(X) = (a_{v,1}(X), \ldots, a_{v,s_v}(X)) \quad \text{and} \quad B_v(Y) = (b_{v,1}(Y), \ldots, b_{v,t_v}(Y))$$

collect Alice's and Bob's message polynomials along the path from the root to v, including the message at v. Let

$$(h_{v,1}(X,Y), \ldots, h_{v,r_v}(X,Y)), \qquad r_v = s_v + t_v,$$

be their chronological interleaving. Thus, each $h_{v,j}$ is either some $a_{v,k}(X)$ or some $b_{v,\ell}(Y)$. Define the restriction of the testing polynomial at v to the diagonal by

$$\widetilde{P}_v(X) \coloneqq P_v\left(h_{v,1}(X,X),\ldots,h_{v,r_v}(X,X)\right) \in \mathbb{F}[X].$$

Let

$$P(X) = \prod_{\substack{v \text{ internal} \\ \widetilde{P}_v \not\equiv 0}} \widetilde{P}_v(X),$$

where the empty product is 1. The tree is finite, hence P is well-defined. Moreover, by definition, P is a nonzero polynomial. Choose $X_0 \in U$ such that $P(X_0) \neq 0$; such a point exists because a nonzero polynomial cannot vanish on a nonempty Euclidean open set.

Let $\pi = (v_1,\ldots,v_\ell)$ be the path followed by (X_0,X_0). For each $i \in [\ell]$ with $\widetilde{P}_{v_i} \not\equiv 0$, continuity gives an open ball B_i containing X_0 on which $\widetilde{P}_{v_i}$ has the same sign as at X_0 over $\mathbb{R}$, or remains nonzero over $\mathbb{C}$. If $\widetilde{P}_{v_i} \equiv 0$, set $B_i = \mathbb{F}^n$. Then

$$W = U \cap \bigcap_{i=1}^{\ell} B_i$$

is a nonempty Euclidean open subset of U, since π is finite and U and every B_i are open sets containing X_0. Every (X,X), with $X \in W$, takes the same branch as (X_0,X_0) at each node and therefore it follows π. Finally, π is accepting because $(X_0,X_0) \in V(X-Y)$. □

Let $a_1,\ldots,a_s \in \mathbb{F}[X]$ and $b_1,\ldots,b_t \in \mathbb{F}[Y]$ be the transcript messages along π. Define

$$A_\pi(X) = \left(a_1(X),\ldots,a_s(X)\right), \qquad B_\pi(X) = \left(b_1(X),\ldots,b_t(X)\right).$$

Next we show that the common path forces each of these maps to distinguish all inputs in W.

Lemma 3.6. *Let W and π be given by Lemma 3.5. The maps $A_\pi : W \to \mathbb{F}^s$ and $B_\pi : W \to \mathbb{F}^t$ are injective.*

Proof. Suppose that $X, X' \in W$ and $A_\pi(X) = A_\pi(X')$. Along π, the cross-input (X,X') produces the same transcript as (X',X'): Alice's messages agree by assumption, and Bob has input X' in both instances. Thus (X,X') reaches the same accepting leaf. Since $(X,X') \in U \times U$ and C recognizes equality on this domain, $X = X'$, and hence A_π is injective on W.

If $B_\pi(X) = B_\pi(X')$, then (X,X') produces the same transcript as (X,X) and is likewise accepted. Therefore $X = X'$, so B_π is also injective on W. □

We now have all the ingredients for the lower bound.

Theorem 3.7 (Strengthened restatement of Theorem 1.4)**.** *For every $n \geq 1$, $\mathbb{F} \in \{\mathbb{R},\mathbb{C}\}$, and nonempty Euclidean open set $U \subseteq \mathbb{F}^n$, the deterministic communication complexity of recognizing $V(X-Y)$ under the promise $X,Y \in U$ is $2n$. Consequently, the deterministic communication complexity of $V(X-Y)$ is $2n$.*

Proof. Broadcasting all coordinates of X and Y gives a deterministic protocol of cost $2n$.

Conversely, let $U \subseteq \mathbb{F}^n$ be a nonempty Euclidean open set, and let C be any deterministic protocol deciding equality under the promise $X,Y \in U$. By Lemma 3.5, the diagonal inputs from some nonempty open set $W \subseteq U$ follow one accepting path π. Let s and t be the numbers of Alice- and Bob-messages along π. By Lemma 3.6, the corresponding polynomial maps $A_\pi : W \to \mathbb{F}^s$ and $B_\pi : W \to \mathbb{F}^t$ are injective. By Proposition 2.4, this gives $s \geq n$ and $t \geq n$. Hence π contains at least $s + t \geq 2n$ messages, so the depth of C is at least $2n$. Taking $U = \mathbb{F}^n$ gives the claimed complexity of $V(X-Y)$. □

By restricting the inputs, the tight lower bound for $V(X-Y)$ can be lifted to $V(\mathsf{UEQ}_n)$ defined in Eq. (3.3).

Theorem 3.8. *For every $n \geq 1$ and $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$,*

$$\mathrm{DCC}_{\mathbb{F}}\left(V(\mathsf{UEQ}_n)\right) = 2n.$$

Proof. The upper bound follows from observation 3.2 and Theorem 1.4.

For the lower bound, choose pairwise disjoint nonempty open sets $U_1, \ldots, U_n \subseteq \mathbb{F}$ and set $U = U_1 \times \cdots \times U_n$. For $X, Y \in U$, if $X_i = Y_{\sigma(i)}$, then, they belong to both U_i and $U_{\sigma(i)}$, disjointness forces $\sigma(i) = i$. Thus

$$\text{For all } X, Y \in U \qquad (X, Y) \in V(\mathsf{UEQ}_n) \quad \iff \quad X = Y.$$

Thus any protocol recognizing $V(\mathsf{UEQ}_n)$ decides equality under the promise $X, Y \in U$. Since U is nonempty and Euclidean open, Theorem 3.7 gives $\mathrm{DCC}(V(\mathsf{UEQ}_n)) \geq 2n$. □

3.3 Complexity of sparse difference

Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. For integers $n \geq 1$ and $1 \leq k \leq n$, define the *k-sparse difference set over $\mathbb{F}$* by:

$$V(\mathsf{SD}_{n,k}) \coloneqq \{(X, Y) \in \mathbb{F}^n \times \mathbb{F}^n \;\mid\; \#\{i \in [n] : X_i \neq Y_i\} \leq k\}.$$

We start with the observation that any set-recognition protocol for $V(\mathsf{SD}_{n+k,k})$ would give an equally efficient protocol for $V(X-Y)$.

Observation 3.9 (Equality reduces to sparse difference)**.** *For every $n \geq 1$ and $k \geq 1$,*

$$\mathrm{DCC}_{\mathbb{F}}\left(V(X-Y)\right) \leq \mathrm{DCC}_{\mathbb{F}}\left(V(\mathsf{SD}_{n+k,k})\right) \qquad \textit{and} \qquad \mathrm{PCC}_{\mathbb{F}}\left(V(X-Y)\right) \leq \mathrm{PCC}_{\mathbb{F}}\left(V(\mathsf{SD}_{n+k,k})\right).$$

Proof. Given $(X, Y) \in \mathbb{F}^n \times \mathbb{F}^n$, define

$$\widehat{X} = \left(X_1, \ldots, X_n, \underbrace{0, \ldots, 0}_{k}\right) \qquad \text{and} \qquad \widehat{Y} = \left(Y_1, \ldots, Y_n, \underbrace{1, \ldots, 1}_{k}\right).$$

The appended coordinates contribute exactly k disagreements, and hence

$$\left|\left\{i \in [n+k] \;\mid\; \widehat{X}_i \neq \widehat{Y}_i\right\}\right| = k + \left|\{i \in [n] \;\mid\; X_i \neq Y_i\}\right|.$$

Therefore,

$$X = Y \quad \iff \quad \left(\widehat{X}, \widehat{Y}\right) \in V(\mathsf{SD}_{n+k,k}).$$

□

Together with the deterministic lower bound for equality, this reduction gives the following lower bound for sparse difference:

Theorem 3.10 (Deterministic lower bound for $V(\mathsf{SD}_{n,k})$)**.** *For every $n \geq 1$, $1 \leq k \leq n$, and $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$,*

$$\mathrm{DCC}_{\mathbb{F}}\left(V(\mathsf{SD}_{n,k})\right) \geq 2(n-k).$$

Proof. For $k = n$, the claim is immediate. For $k < n$, apply Observation 3.9 with equality on $\mathbb{F}^{n-k}$. By Theorem 1.4,

$$\mathrm{DCC}\left(V(\mathsf{SD}_{n,k})\right) = \mathrm{DCC}\left(V(\mathsf{SD}_{(n-k)+k,\,k})\right) \geq \mathrm{DCC}\left(V(X-Y)\right) = 2(n-k).$$

□

In the next theorem, we show that $V(\mathsf{SD}_{n,k})$ admits an efficient probabilistic protocol. For the correctness of the protocol, we will need the following standard evaluation-rank criterion:

Proposition 3.11 ([Kay11, Claim 7])**.** *Let $f_1, \ldots, f_\ell \in \mathbb{F}[t]$. Then, the matrix*

$$\begin{pmatrix} f_1(\alpha_1) & \cdots & f_\ell(\alpha_1) \\ \vdots & & \vdots \\ f_1(\alpha_\ell) & \cdots & f_\ell(\alpha_\ell) \end{pmatrix}$$

has nonzero determinant as a polynomial in $\alpha_1, \ldots, \alpha_\ell$ if and only if $f_1, \ldots, f_\ell$ are linearly independent over $\mathbb{F}$.

We now apply this criterion to obtain an efficient probabilistic protocol for recognizing $V(\mathsf{SD}_{n,k})$.

Theorem 3.12 (Probabilistic protocol for $V(\mathsf{SD}_{n,k})$)**.** *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. For $n \geq 1$ and $1 \leq k \leq n$, let*

$$V(\mathsf{SD}_{n,k}) = \{(X, Y) \in \mathbb{F}^n \times \mathbb{F}^n \;\mid\; \#\{i \in [n] : X_i \neq Y_i\} \leq k\}.$$

Then,

$$\mathrm{PCC}_{\mathbb{F}}\left(V(\mathsf{SD}_{n,k})\right) \leq 2k + 2.$$

In particular, for fixed k, the probabilistic communication complexity is independent of n.

Proof. **Setup.** For inputs $X, Y \in \mathbb{F}^n$, define

$$q_X(t) = \sum_{i=1}^{n} X_i t^i, \qquad q_Y(t) = \sum_{i=1}^{n} Y_i t^i, \qquad q_{\mathrm{diff}}(t) = q_X(t) - q_Y(t).$$

Let

$$D = (k+1)n\binom{n}{k}.$$

Choose a finite set $A \subseteq \mathbb{F}$ with $|A| \geq 3D$. Choose

$$\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_{k+1}) \in A^{k+1}.$$

uniformly at random.

For a set $S = \{s_1, \ldots, s_k\} \subseteq [n]$ of size k,

$$M_S(\boldsymbol{\alpha}) = \begin{pmatrix} \alpha_1^{s_1} & \cdots & \alpha_1^{s_k} & q_{\mathrm{diff}}(\alpha_1) \\ \vdots & & \vdots & \vdots \\ \alpha_{k+1}^{s_1} & \cdots & \alpha_{k+1}^{s_k} & q_{\mathrm{diff}}(\alpha_{k+1}) \end{pmatrix}.$$

The sampled value of $\boldsymbol{\alpha}$ determines the following deterministic protocol $T_{\boldsymbol{\alpha}}$.

Protocol. Alice broadcasts $q_X(\alpha_j)$ and Bob broadcasts $q_Y(\alpha_j)$ for every $j \in [k+1]$. All intermediate testing polynomials are constant. At the final node, the protocol computes the transcript differences

$$q_{\mathrm{diff}}(\alpha_j) = q_X(\alpha_j) - q_Y(\alpha_j) \qquad (j \in [k+1]).$$

Define the testing polynomial

$$P(\boldsymbol{\alpha}) = \prod_{S \in \binom{[n]}{k}} \mathsf{Det}\, M_S(\boldsymbol{\alpha}).$$

This is a polynomial in the transcript values $q_X(\alpha_j), q_Y(\alpha_j)$, and the protocol accepts exactly when it evaluates to zero. Thus each $T_{\boldsymbol{\alpha}}$ has depth $2k+2$.

Correctness. The input $(X, Y) \in V(\mathsf{SD}_{n,k})$ if and only if q_{diff} has at most k nonzero coefficients. Then, for some $S \in \binom{[n]}{k}$ the support of q_{diff} is contained in S. Indeed, if the support has fewer than k elements, we may extend it to a k-element subset of $[n]$. For this S, the last column of $M_S(\boldsymbol{\alpha})$ is a linear combination of the first k columns. Hence, $P(\boldsymbol{\alpha}) = 0$ for every choice of $\boldsymbol{\alpha}$, so the sampled protocol always accepts.

Conversely, suppose $(X, Y) \notin V(\mathsf{SD}_{n,k})$. Then, q_{diff} has more than k nonzero coefficients. For every $S = \{s_1, \ldots, s_k\}$, the polynomials

$$t^{s_1}, \ldots, t^{s_k}, q_{\text{diff}}(t)$$

are linearly independent, since q_{diff} has a nonzero coefficient in a degree outside S. By Proposition 3.11, each $\mathsf{Det}\, M_S(\boldsymbol{\alpha})$ is a nonzero polynomial in $\boldsymbol{\alpha}$; hence, their product is nonzero. Moreover,

$$\deg \mathsf{Det}\, M_S(\boldsymbol{\alpha}) \le n + \sum_{s \in S} s \le (k+1)n,$$

and therefore $\deg P \le D$. By Lemma 2.5,

$$\Pr\left[T_{\boldsymbol{\alpha}} \text{ accepts } (X, Y)\right] = \Pr_{\boldsymbol{\alpha} \in A^{k+1}}\left[P(\boldsymbol{\alpha}) = 0\right] \le \frac{D}{|A|} \le \frac{1}{3}.$$

Thus the protocol rejects with probability at least $2/3$. Alice and Bob each communicate $k+1$ values, so the total cost is $2k+2$. □

3.4 Complexity of bilinear forms

Let $A \in \mathbb{F}^{n \times n}$ be a fixed public matrix known to both Alice and Bob, and let $X = (X_1, \ldots, X_n)$ and $Y = (Y_1, \ldots, Y_n)$ be vectors of variables. The matrix A defines the bilinear form

$$\mathsf{BF}_{n,A}(X, Y) = X^T A Y.$$

Consider the real threshold set for a fixed $A \in \mathbb{R}^{n \times n}$

$$S(\mathsf{BF}_{n,A}) = \left\{(X, Y) \in \mathbb{R}^n \times \mathbb{R}^n \;\middle|\; \mathsf{BF}_{n,A}(X, Y) \le 0\right\}.$$

Over $\mathbb{C}$, we consider the zero set for a fixed $A \in \mathbb{C}^{n \times n}$

$$V(\mathsf{BF}_{n,A}) = \left\{(X, Y) \in \mathbb{C}^n \times \mathbb{C}^n \;\middle|\; \mathsf{BF}_{n,A}(X, Y) = 0\right\}.$$

Recall the notation for the inner product problems from Theorem 1.1. Taking $A = I_n$ gives $\mathsf{BF}_{n,I_n} = \mathsf{IP}_n$. Thus, the family of set-recognition problems for bilinear-form threshold sets includes the inner-product problem. Moreover, we observe the following equivalence in the complexity of these two problems.

Observation 3.13 (Equivalence with inner product)**.** *Let $A \in \mathbb{R}^{n\times n}$ and $r = \operatorname{rank}_{\mathbb{R}}(A) \geq 1$. Then,*

$$\mathrm{DCC}_{\mathbb{R}}\left(S(\mathsf{BF}_{n,A})\right) = \mathrm{DCC}_{\mathbb{R}}\left(S(\mathsf{IP}_r)\right), \qquad \mathrm{PCC}_{\mathbb{R}}\left(S(\mathsf{BF}_{n,A})\right) = \mathrm{PCC}_{\mathbb{R}}\left(S(\mathsf{IP}_r)\right).$$

For the complex case, let $A \in \mathbb{C}^{n\times n}$ and $r = \operatorname{rank}_{\mathbb{C}}(A) \geq 1$. Then,

$$\mathrm{DCC}_{\mathbb{C}}\left(V(\mathsf{BF}_{n,A})\right) = \mathrm{DCC}_{\mathbb{C}}\left(V(\mathsf{IP}_r)\right), \qquad \mathrm{PCC}_{\mathbb{C}}\left(V(\mathsf{BF}_{n,A})\right) = \mathrm{PCC}_{\mathbb{C}}\left(V(\mathsf{IP}_r)\right).$$

Proof. First, let us assume that $\mathbb{F} = \mathbb{R}$. Choose $P, Q \in \mathrm{GL}_n(\mathbb{R})$ such that

$$P^T A Q = \begin{pmatrix} I_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}.$$

Let $\widetilde{X} \in \mathbb{R}^r$ and $\widetilde{Y} \in \mathbb{R}^r$ be the truncations of $P^{-1}X$ and $Q^{-1}Y$, respectively, to their first r coordinates. Then,

$$\begin{aligned} \mathsf{BF}_{n,A}(X,Y) &= \left(P^{-1}X\right)^T P^T A Q \left(Q^{-1}Y\right) \\ &= \left(P^{-1}X\right)^T \begin{pmatrix} I_r & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \left(Q^{-1}Y\right) \\ &= \widetilde{X}^T\widetilde{Y} \quad = \quad \mathsf{IP}_r\left(\widetilde{X},\widetilde{Y}\right). \end{aligned}$$

Consequently,

$$(X,Y) \in S(\mathsf{BF}_{n,A}) \quad \Longleftrightarrow \quad (\widetilde{X},\widetilde{Y}) \in S(\mathsf{IP}_r).$$

By a similar argument for $\mathbb{F} = \mathbb{C}$ we also get the following:

$$(X,Y) \in V(\mathsf{BF}_{n,A}) \quad \Longleftrightarrow \quad (\widetilde{X},\widetilde{Y}) \in V(\mathsf{IP}_r).$$

Here Alice computes $\widetilde{X}$ from X, while Bob computes $\widetilde{Y}$ from Y, so this transformation is local.

Conversely, let $(\widetilde{X},\widetilde{Y}) \in \mathbb{F}^r \times \mathbb{F}^r$ be an input to the inner product problem, where $\mathbb{F} \in \{\mathbb{R},\mathbb{C}\}$. Alice and Bob locally construct

$$X = P\left(\widetilde{X}, \mathbf{0}_{n-r}\right), \qquad Y = Q\left(\widetilde{Y}, \mathbf{0}_{n-r}\right).$$

Then,

$$\mathsf{BF}_{n,A}(X,Y) = \left(\widetilde{X}, \mathbf{0}_{n-r}\right)^T P^T A Q \left(\widetilde{Y}, \mathbf{0}_{n-r}\right) = \widetilde{X}^T\widetilde{Y} = \mathsf{IP}_r\left(\widetilde{X},\widetilde{Y}\right).$$

Thus, a protocol for the bilinear-form problem can recognize inner product with the same cost and error probability. Together with the forward reduction, this proves the claimed equivalences. □

The observation transfers communication bounds for r-dimensional inner product directly to bilinear forms of rank r. In particular, after proving the inner product lower bound in Section 6.3, we use it to obtain the same $2r-4$ lower bound for both the real threshold set $S(\mathsf{BF}_{n,A})$ and the complex zero set $V(\mathsf{BF}_{n,A})$.

4 Communication complexity via mixed Hessian rank

We now return to the communication complexity of computing a polynomial, as defined in Definition 2.6; see Example 2.7 for the basic example. Abelson [Abe80] proved that such a computation is constrained by the rank of the matrix of mixed second partial derivatives.

Definition 4.1 (Mixed Hessian matrix)**.** *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. For a polynomial $g \in \mathbb{F}[X, Y]$, its $n \times n$* mixed Hessian matrix $\mathsf{H}_{X|Y}(g)$ *is defined by*

$$[\mathsf{H}_{X|Y}(g)]_{ij} \quad = \quad \frac{\partial^2 g}{\partial X_i \partial Y_j}.$$

The rank of the mixed Hessian matrix defined above is a lower bound on the communication complexity of computing a polynomial.

Lemma 4.2 ([Gri08, Lemma 2.2])**.** *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$, and let $g \in \mathbb{F}[X, Y]$. Suppose that*

$$g(X, Y) = Q(a_1(X), \ldots, a_{r_1}(X), b_1(Y), \ldots, b_{r_2}(Y))$$

is a minimum-size representation of g, where $a_1, \ldots, a_{r_1} \in \mathbb{F}[X]$ and $b_1, \ldots, b_{r_2} \in \mathbb{F}[Y]$. Then $\operatorname{rank} \mathsf{H}_{X|Y}(g) \leq \min\{r_1, r_2\}$ *and*

$$c(g) = r_1 + r_2 \geq 2 \cdot \operatorname{rank} \mathsf{H}_{X|Y}(g).$$

Here the rank of a polynomial matrix is taken over $\mathbb{F}(X, Y)$.

For completeness, we give the proof of the lemma in Section A. The rank lemma can be used to obtain tight bounds for communication complexity of computing the inner product polynomial.

Example 4.3 (Tightness for inner product)**.** *Recall from Example 2.7 that the inner product polynomial*

$$\mathsf{IP}_n(X, Y) = \sum_{i=1}^{n} X_i Y_i$$

satisfies $c(\mathsf{IP}_n) \leq 2n$. Clearly, $\mathsf{H}_{X|Y}(\mathsf{IP}_n)$ is the identity matrix, hence, $\operatorname{rank} \mathsf{H}_{X|Y}(\mathsf{IP}_n) = n$*. By Lemma 4.2, $c(\mathsf{IP}_n) \geq 2n$. Therefore, $c(\mathsf{IP}_n) = 2n$.*

Grigoriev observed that the rank of the mixed Hessian matrix is dictated by the irreducible factors of the polynomial. The following lemma generalizes [Gri08, Lemma 2.4].

Lemma 4.4 (Rank of multiples)**.** *Over a field $\mathbb{F}$ of characteristic zero*[5]*, let $p \in \mathbb{F}[X, Y]$ be irreducible, and let r be an integer with $1 \leq r \leq n$. Suppose that some $r \times r$ minor of $\mathsf{H}_{X|Y}(p)$ is not divisible by p. Let*

$$g = p^m h, \qquad m \geq 1, \qquad p \nmid h.$$

Then,

$$\operatorname{rank} \mathsf{H}_{X|Y}(g) \geq r - 2.$$

[5] Over arbitrary fields $\mathbb{F}$, we require $\operatorname{char}(\mathbb{F}) \nmid m$

Proof. For each $i, j \in [n]$, we first differentiate with respect to Y_j and then with respect to X_i, following the convention in Definition 4.1. Differentiating $g = p^m h$ and grouping the rank-one terms gives

$$\begin{aligned}\mathsf{H}_{X|Y}(g) = mp^{m-1}h\,\mathsf{H}_{X|Y}(p) + p^m\mathsf{H}_{X|Y}(h) \\ + m(\nabla_X p)\left(\nabla_Y(p^{m-1}h)\right)^T + mp^{m-1}(\nabla_X h)(\nabla_Y p)^T.\end{aligned}$$

After factoring out the common scalar p^{m-1} from the first two terms, the main matrix is

$$\begin{aligned}M &= mh\,\mathsf{H}_{X|Y}(p) + p\,\mathsf{H}_{X|Y}(h) \\ &\equiv mh\,\mathsf{H}_{X|Y}(p) \pmod{p}.\end{aligned}$$

Let μ be an $r \times r$ minor of $\mathsf{H}_{X|Y}(p)$ that is not divisible by p, and let μ_M be the corresponding minor of M. Then

$$\mu_M \equiv (mh)^r \mu \pmod{p}.$$

Since p is irreducible, it is prime in the unique factorization domain $\mathbb{F}[X, Y]$. Also, m is a nonzero scalar in $\mathbb{F}$ and hence a unit. Together with the assumptions $p \nmid h$ and $p \nmid \mu$, this gives $p \nmid (mh)^r \mu$. Thus, $\mu_M \neq 0$, so M, and hence $p^{m-1}M$, has rank at least r.

The remaining terms in $\mathsf{H}_{X|Y}(g)$ are two matrices of rank at most one:

$$\mathsf{H}_{X|Y}(g) = p^{m-1}M + m(\nabla_X p)\left(\nabla_Y(p^{m-1}h)\right)^T + mp^{m-1}(\nabla_X h)(\nabla_Y p)^T,$$

By the inequality $\operatorname{rank}(A + B) \geq \operatorname{rank}(A) - \operatorname{rank}(B)$, adding a rank-one matrix can decrease the rank by at most one. Thus the two rank-one terms can decrease the rank of $p^{m-1}M$ by at most two. Therefore

$$\operatorname{rank}\mathsf{H}_{X|Y}(g) \geq r - 2.$$

□

In the following lemma, we observe that under stronger assumptions we get full mixed Hessian rank for powers of irreducible polynomials.

Lemma 4.5 (Full-rank criterion for powers)**.** *Over a field $\mathbb{F}$ of characteristic zero, let $p \in \mathbb{F}[X, Y]$ be irreducible, and define the determinant of $(n+1) \times (n+1)$ matrix*

$$R_p \quad := \quad \mathsf{Det}\begin{pmatrix}\mathsf{H}_{X|Y}(p) & \nabla_X p \\ (\nabla_Y p)^T & 0\end{pmatrix}.$$

Suppose that $p \nmid R_p$. Then, for every

$$g = p^m h, \qquad m \geq 2, \qquad p \nmid h,$$

we have

$$\operatorname{rank}\mathsf{H}_{X|Y}(g) = n.$$

Proof. Let $\boldsymbol{x} = \nabla_X p$, and $\boldsymbol{y} = \nabla_Y p$. Following again the convention in Definition 4.1, differentiating $g = p^m h$ and factoring out p^{m-2} gives

$$\begin{aligned}\mathsf{H}_{X|Y}(g) &= p^{m-2}\left(\underbrace{m(m-1)h}_{\lambda}\,\boldsymbol{x}\boldsymbol{y}^T + p\left(\underbrace{mh\mathsf{H}_{X|Y}(p) + m\boldsymbol{x}\left(\nabla_Y h\right)^T + m\left(\nabla_X h\right)\boldsymbol{y}^T + p\mathsf{H}_{X|Y}(h)}_{M}\right)\right) \\ &= p^{m-2}\left(\lambda\boldsymbol{x}\boldsymbol{y}^T + pM\right).\end{aligned}$$

The matrix determinant lemma gives

$$\mathsf{Det}\left(\lambda \boldsymbol{x}\boldsymbol{y}^T + pM\right) \quad = \quad -p^{n-1}\,\mathsf{Det}\begin{pmatrix} M & \lambda\boldsymbol{x} \\ \boldsymbol{y}^T & -p \end{pmatrix} \quad = \quad p^{n-1}Q, \tag{4.6}$$

where

$$Q \quad = \quad -\,\mathsf{Det}\begin{pmatrix} M & \lambda\boldsymbol{x} \\ \boldsymbol{y}^T & -p \end{pmatrix}.$$

Modulo p, the term $p\mathsf{H}_{X|Y}(h)$ in M vanishes. Therefore computing Q modulo p gives

$$\begin{aligned} Q &\equiv -\lambda\,\mathsf{Det}\begin{pmatrix} mh\mathsf{H}_{X|Y}(p) + m\boldsymbol{x}\left(\nabla_Y h\right)^T + m\left(\nabla_X h\right)\boldsymbol{y}^T & \boldsymbol{x} \\ \boldsymbol{y}^T & 0 \end{pmatrix} \\ &\equiv -\lambda\,\mathsf{Det}\begin{pmatrix} mh\mathsf{H}_{X|Y}(p) & \boldsymbol{x} \\ \boldsymbol{y}^T & 0 \end{pmatrix} \end{aligned}$$

For the second equality, subtract $m \cdot (\partial h/\partial Y_j)$ times the last column from the jth column, and then subtract $m \cdot (\partial h/\partial X_i)$ times the last row from the ith row. Thus,

$$\begin{aligned} Q &\equiv -\lambda(mh)^{n-1}R_p \\ &\equiv -m^n(m-1)h^nR_p \pmod{p}. \end{aligned}$$

Since p is irreducible, it is prime in the unique factorization domain $\mathbb{F}[X,Y]$. Hence, if p does not divide h then it does not divide h^n. Since it divides neither h^n nor R_p, it does not divide h^nR_p. Thus, the right-hand side of the preceding congruence is not divisible by p, and consequently $Q \neq 0$. By Eq. (4.6),

$$\mathsf{Det}\,\mathsf{H}_{X|Y}(g) = p^{n(m-2)+n-1}Q \neq 0.$$

Therefore, $\operatorname{rank}\mathsf{H}_{X|Y}(g) = n$. □

The full-rank criterion extends from polynomials to rational functions; we prove this generalization in Section 8.2.

Remark 4.7. The assumption $m \geq 2$ causes no loss in lower-bound applications. Indeed, if $g = p^m h$ with $m \geq 1$ and $p \nmid h$, then $g^2 = p^{2m}h^2$, where $2m \geq 2$ and $p \nmid h^2$. Thus, Lemmas 4.2 and 4.5 give $c(g^2) \geq 2n$. Moreover, any protocol computing g also computes g^2 at the same cost by squaring its output, so $c(g^2) \leq c(g)$. Hence, $c(g) \geq 2n$ as well.

5 Framework for probabilistic lower bounds

In this section, we present a general framework for proving algebraic communication lower bounds. The framework is designed by providing sufficient conditions that make the set-recognition problem hard for the communication model. The recipe is similar whether we are working over the reals or complex numbers. However, due to the topological differences between $\mathbb{R}$ and $\mathbb{C}$, the proofs are substantially different. We will start with the case $\mathbb{F} = \mathbb{R}$.

5.1 Over the real numbers

Recall from Lemma 4.5 that, for an irreducible polynomial $p \in \mathbb{F}[X,Y]$, we define determinant of $(n+1) \times (n+1)$ matrix

$$R_p = \mathsf{Det}\begin{pmatrix} \mathsf{H}_{X|Y}(p) & \nabla_X p \\ \left(\nabla_Y p\right)^T & 0 \end{pmatrix}.$$

Theorem 5.1. *Let $S \subseteq \mathbb{R}^n \times \mathbb{R}^n$ be a semialgebraic set and let $F \in \mathbb{R}[X_1, ..., X_n, Y_1, ..., Y_n]$ satisfying:*

1. *F is irreducible over $\mathbb{R}$*
2. *$\partial S \cap V(F)$ has dimension $2n - 1$*
3. *$F \nmid R_F$.*

Then $\mathrm{PCC}_{\mathbb{R}}(S) \geq 2n$

Proof. Let $\mathcal{C}$ be a probabilistic communication protocol recognizing S. By definition, $\mathcal{C}$ is a family of deterministic protocols $\{C_1, ..., C_N\}$, where each deterministic protocol C_i is chosen with probability $p_i \geq 0$ such that $\sum_{i \in [N]} p_i = 1$. Let d denote the maximum depth of any deterministic protocol tree in the finite support of $\mathcal{C}$ (i.e., the communication complexity of $\mathcal{C}$).

For each C_i and a node v in C_i, let $g_{i,v}$ be a testing polynomial at node v. We define $G_i = \prod g_{i,v}$, where the product ranges over the nodes v of C_i. We will assume that our protocols are minimal. That is, the protocol has been pruned such that there are no unreachable nodes and any node whose composed testing polynomial is identically zero has been contracted. We will first prove the following lemma about the boundary of S. Recall that, if a point lies in the boundary of S, namely ∂S, then for any ball around u, there is at least one point in S and one point outside S.

Claim 5.2. *For any $u \in \partial S$, there exists at least one $i \in [N]$ such that $G_i(u) = 0$, i.e.,*

$$\partial S \subseteq \bigcup_{i=1}^{N} V(G_i).$$

Proof of the claim. Assume, for contradiction, that there exists $u \in \partial S$ such that $G_i(u) \neq 0$, for all $i \in [N]$. Then, no testing polynomial in any C_i vanishes on u, meaning u is in the *finite* intersection, (recall that $D(q)$ denotes the nonzero set of q)

$$u \in \bigcap_{\substack{C \in \mathcal{C} \\ q \in C}} D(q) =: \mathcal{A},$$

where, the intersection ranges over the (nonzero) testing polynomials $q \in C_i$ and across all $C_i \in \mathcal{C}$.

But, since $\mathcal{A}$ is a Zariski open set (thus, a Euclidean open set), as it is defined by polynomials, there exists some ball B_u around u such that every testing polynomial across every protocol has constant sign across the elements of B_u, and, by extension, all C_i are constant functions on B_u.

To see this, first observe that for every $i \in [N]$, $G_i(u) \neq 0$. This means that, on input u, the protocol traverses only along > 0 or < 0 tests, and reaches a leaf (l_i in protocol C_i). Assume that the output at this leaf is $o_i \in \{\text{accept, reject}\}$. That is, C_i outputs o_i on u. Then, by continuity of the polynomials in the protocol, there is a ball of radius δ_i around u, denoted by $B_u(\delta_i)$, such that every point $z \in B_u(\delta_i)$, $C_i(z) = o_i$. Let $\delta_0 = \min_{i \in [N]} \delta_i$. Then, we know that for every point $z \in B_u(\delta_0)$, and every $i \in [N]$, $C_i(z) = C_i(u)$.

Now, for any $z \in B_u(\delta_0)$,

$$\begin{aligned} \Pr[\mathcal{C} \text{ accepts } z] &= \sum_{i \in [N]} p_i \times \mathbb{1}[C_i \text{ accepts } z] \\ &= \sum_{i \in [N]} p_i \times \mathbb{1}[C_i \text{ accepts } u] \\ &= \Pr[\mathcal{C} \text{ accepts } u], \end{aligned} \tag{5.3}$$

where $\mathbb{1}[C_i \text{ accepts } z]$ is 1 if C_i accepts z and 0 otherwise. The second equality comes from our argument above and the fact that $z \in B_u(\delta_0)$.

But, u is in the boundary of S. This means that in any ball around u, and, hence specifically in $B_u(\delta_0)$, we have two points $z_{\text{in}} \in S$ and $z_{\text{out}} \notin S$. Thus, we know that $\Pr[\mathcal{C} \text{ accepts } z_{\text{in}}] \geq 2/3$ and $\Pr[\mathcal{C} \text{ accepts } z_{\text{out}}] \leq 1/3$. Thus, $2/3 \leq Pr[C_i \text{ accepts } z_{\text{in}}] = Pr[C_i \text{ accepts } z_{\text{out}}] \leq 1/3$, which is a contradiction. ◇

We use the above claim and the following fact to complete the proof of Theorem 5.1.

Fact 5.4. *[Hen07] If F is irreducible, $\dim(V(F)) = 2n-1$ and $F \nmid G$ then*

$$\dim(V(F) \cap V(G)) \leq 2n-2$$

At an intuitive level, the above fact says that, given a set of zeroes of an irreducible polynomial F, if we impose an additional non-trivial constraint $G = 0$ on the set, then the codimension of the intersection must be at least 1, i.e., the dimension must drop by at least 1. Note that, the assumption $\dim V(F) = 2n-1$ ensures that the real zero set of F contains a genuine hypersurface piece.[6]

Using the above fact, we will first show that F must divide some G_i. Suppose it does not. Then, for any $i \in [N]$, not all the roots of F can be roots of G_i. Thus, if F did not divide any G_i, then we would have $\dim(V(F) \cap V(G_i)) \leq 2n-2$ for all $i \in [N]$ and so

$$\dim\left(\bigcup_{i=1}^{N} (V(F) \cap V(G_i))\right) \leq 2n-2. \tag{5.5}$$

By Claim 5.2, we have $\partial S \cap V(F) \subseteq \bigcup_{i=1}^{N} (V(F) \cap V(G_i))$, so Eq. (5.5) implies that

$$\dim(\partial S \cap V(F)) \leq \dim\left(\bigcup_{i=1}^{N} (V(F) \cap V(G_i))\right) \leq 2n-2, \tag{5.6}$$

which contradicts Assumption *2*.

Thus, F must divide some G_i. Since F is irreducible (in particular prime), it must divide some individual testing polynomial, G, occurring in the tree C_i. That is, $G = F^m \cdot H$, where $m \geq 1$ and $F \nmid H$. The polynomial F being irreducible also means that $G^2 = F^{2m} \cdot H^2 = F^{m'} \cdot H^2$, where $m' \geq 2$ and $F \nmid H^2$. From our assumption in Theorem 5.1, we also know that $F \nmid R_F$.

We now apply Lemma 4.5 to G^2 and obtain that $c(G^2) \geq 2\,\text{rank}(\mathsf{H}_{X|Y}(G^2)) = 2n$. Next, notice that $c(G) \geq c(G^2)$: suppose $c(G) = s$, it implies that $G(X,Y) = g(a_1(X), \ldots, a_{s_1}(X), b_1(Y), \ldots, b_{s_2}(Y))$, where $s_1 + s_2 = s$. Then, $G^2(X,Y)$ is computed by simply squaring g. Thus, $c(G^2) \leq s$. Together with the lower bound on $c(G^2)$, we get $c(G) \geq 2n$ and hence, the communication complexity of recognizing S, i.e. the depth of the protocol, which is at least $c(G)$, is at least $2n$. □

Remark 5.7. The condition that $\dim(\partial S \cap V(F)) = 2n-1$ is crucial and cannot be made weaker. Indeed, if $\dim(\partial S \cap V(F)) \leq 2n-2$ then Eq. (5.6) would not be a contradiction. In other words, we need dimension $2n-1$ so that the boundary is too large to lie inside $V(F) \cap V(G)$ unless $F \mid G$.

A weaker mixed Hessian assumption gives a correspondingly weaker lower bound. If some $r \times r$ minor of $\mathsf{H}_{X|Y}(F)$ is not divisible by F, then Lemma 4.4 can be used in the final step of the preceding proof to obtain a lower bound of $2(r-2)$.

[6] In particular, it excludes polynomials such as $x^2 + y^2$, whose real zero set has smaller dimension.

Theorem 5.8. *Let $S \subseteq \mathbb{R}^n \times \mathbb{R}^n$ be a semialgebraic set and let $F \in \mathbb{R}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$, and let $1 \leq r \leq n$. Suppose that*

1. *F is irreducible over $\mathbb{R}$;*
2. *$\partial S \cap V(F)$ has dimension $2n-1$; and*
3. *some $r \times r$ minor of $\mathsf{H}_{X|Y}(F)$ is not divisible by F.*

Then $\mathrm{PCC}_{\mathbb{R}}(S) \geq 2(r-2)$.

We now derive the main result stated in the introduction by specializing S in Theorem 5.1 to the threshold set $S(F)$.

Theorem 1.5 (Restated)**.** *Let $F \in \mathbb{R}[X, Y]$ be irreducible, and let $S(F) = \{(X, Y) \in \mathbb{R}^n \times \mathbb{R}^n \mid F(X, Y) \leq 0\}$. If there exists $u \in \mathbb{R}^n \times \mathbb{R}^n$ such that*

$$F(u) = 0 \qquad \text{and} \qquad R_F(u) \neq 0,$$

then, the probabilistic communication complexity of $S(F)$ over $\mathbb{R}$ is $\geq 2n$, i.e., $\mathrm{PCC}_{\mathbb{R}}(S(F)) \geq 2n$.

Proof. Let $(z_1, ..., z_{2n}) = (X, Y)$. It suffices to verify Conditions 2 and 3 of Theorem 5.1. Condition 3 follows immediately: if $F \mid R_F$, then $V(F) \subseteq V(R_F)$, contradicting $F(u) = 0$ and $R_F(u) \neq 0$.

It remains to verify Condition 2, namely,

$$\dim(\partial S(F) \cap V(F)) = 2n - 1.$$

Since $R_F(u) \neq 0$, neither the last row nor the last column is zero. Hence,

$$\nabla_X F(u) \neq 0 \qquad \text{and} \qquad \nabla_Y F(u) \neq 0,$$

so $\nabla F(u) \neq 0$. We may therefore fix $i \in [2n]$ such that $\partial F / \partial z_i(u) \neq 0$. By continuity, there exists an open ball B_u around u such that $\partial F / \partial z_i$ has constant sign on B_u. Since u is non-singular, by the Implicit Function Theorem, intersecting $V(F)$ with a sufficiently small ball around u preserves its dimension. Hence, shrinking B_u further if necessary, we get by Proposition 2.3,

$$\dim(V(F) \cap B_u) = 2n - 1. \tag{5.9}$$

Now, fix $z = (z_1, ..., z_{2n}) \in V(F) \cap B_u$. Since we assumed $\partial F / \partial z_i$ has constant nonzero sign on B_u, we get that F is strictly monotone in the z_i-direction. Thus, for sufficiently small $\varepsilon > 0$, we have

$$F(z_1, ..., z_i - \varepsilon, ..., z_{2n}) < F(z_1, ..., z_i, ..., z_{2n}) = 0 < F(z_1, ..., z_i + \varepsilon, ..., z_{2n})$$

if increasing and with the inequalities reversed if decreasing. In either case the two points

$$(z_1, ..., z_i - \varepsilon, ..., z_{2n}) \qquad \text{and} \qquad (z_1, ..., z_i + \varepsilon, ..., z_{2n})$$

lie on opposite sides of $S(F)$ and so we conclude that $z \in \partial S(F)$. Thus, since z was arbitrary, we have

$$V(F) \cap B_u \subseteq \partial S(F) \tag{5.10}$$

Finally, Eq. (5.10) together with Eq. (5.9) gives us

$$2n - 1 = \dim(V(F) \cap B_u) \leq \dim(\partial S(F) \cap V(F)) \leq 2n - 1.$$

Hence, $\dim(\partial S(F) \cap V(F)) = 2n - 1$, as desired. □

Remark 5.11. The same proof works for the stricter threshold set,

$$S_{<0}(F) = \{(X, Y) \in \mathbb{R}^n \times \mathbb{R}^n \mid F(X, Y) < 0\}.$$

All results regarding weak threshold sets thus remain true after replacing it with a strict threshold set.

5.2 Over the complex numbers

We now prove the complex analogue of the real framework. The real framework is formulated using the Euclidean boundary, whereas, over $\mathbb{C}$, we express the corresponding condition using Zariski closure.

Theorem 5.12. *Let $S \subseteq \mathbb{C}^n \times \mathbb{C}^n$ be a constructible set of dimension $2n-1$ and let $F \in \mathbb{C}[X_1, ..., X_n, Y_1, ..., Y_n]$ satisfy*

1. *F is irreducible over $\mathbb{C}$*
2. *$V(F) \subseteq \overline{S}$, where $\overline{S}$ is the Zariski closure of S.*
3. *$F \nmid R_F$.*

Then, $\mathrm{PCC}_{\mathbb{C}}(S) \geq 2n$.

Proof. Let $U = V(F)$ and note that almost every point of U lies in S.[7]

Let $\mathcal{C} = \{C_1, ..., C_N\}$ be a probabilistic communication protocol recognizing S, and let $\mu_1, \ldots, \mu_N$ be the corresponding probability distribution. The following claim identifies a single protocol C_k that is correct on a constant fraction of the points both inside and outside U.

Claim 5.13. *There exists $C_k \in \mathcal{C}$ that accepts at least $1/3$ of the points in U and rejects at least $1/3$ of the points outside U.*

Proof of the claim. For each $j \in [N]$, let A_j be the fraction of points in U accepted by C_j and let B_j be the fraction of points outside U rejected by C_j. By the correctness of the probabilistic protocol,[8]

$$\sum_{j \in [N]} \mu_j A_j \geq \frac{2}{3} \qquad \text{and} \qquad \sum_{j \in [N]} \mu_j B_j \geq \frac{2}{3}.$$

Therefore,

$$\sum_{j \in [N]} \mu_j (A_j + B_j) \geq \frac{4}{3},$$

so there exists $k \in [N]$ such that $A_k + B_k \geq 4/3$. Since $A_k, B_k \leq 1$, both A_k and B_k are at least $1/3$. ◇

Let $T_1, ..., T_m$ be the polynomials along the path π in C_k, in which all decisions are $T_i(X, Y) \neq 0$. Take the product

$$G_k = \prod_{i=1}^{m} T_i.$$

First, we will show that π as defined above is a rejecting path in C_k. We will use this fact to deduce that $F | G_k$. Once we have that $F | G_k$, then the proof is similar to the proof of Theorem 5.1.

Claim 5.14. *Let π and G_k as defined above. Then any $u \in D(G_k)$, i.e., any input that ends up at the leaf of π, is rejected by C_k.*

[7] U is irreducible and has dimension $2n-1$. Since $U \subseteq \overline{S}$ and $\dim \overline{S} = \dim S = 2n-1$, U is an irreducible component of $\overline{S}$ and so $S \cap U$ contains a dense Zariski-open subset of U, since S is constructible.

[8] By the previous footnote, almost every point of U belongs to S. Moreover, almost every point outside U lies outside S.

Proof of the claim. Let π' be some path other than π and let $T'_1, \cdots, T'_{m'}$ be the testing polynomials encountered along π'. Since π' differs from π, the points, (X', Y'), which follow π' must have $T'_i(X', Y') = 0$ for some $i \in [m']$. Since T'_i is nonzero, $V(T'_i)$ is either empty or a finite union of hypersurfaces of dimension $2n-1$, by Proposition 2.3. Hence the set of inputs following π', being contained in $V(T'_i)$, has dimension at most $2n-1$.

Thus, π is the only path for which a full dimensional subset follows. Furthermore, the space of points we wish to reject, $(\mathbb{C}^n \times \mathbb{C}^n) \setminus S$, is full dimensional, since S has dimension $2n-1$ and constructible. By Claim 5.13, 1/3 of points of $(\mathbb{C}^n \times \mathbb{C}^n) \setminus S$ are correctly rejected and this can only be the case if π is a rejecting path. ◇

Claim 5.15. $F \mid G_k$

Proof of the claim. Suppose, for contradiction, that $F \nmid G_k$. As F is irreducible, using Fact 5.4, we get that

$$\dim(E) \leq 2n-2, \qquad \text{where} \qquad E = U \cap V(G_k).$$

Furthermore, for every $u \in U \setminus E$ we have $G_k(u) \neq 0$ and so C_k rejects u. Thus

$$B = \{u \in U \mid C_k(u) = \text{accept}\} \subseteq E.$$

Hence, C_k only accepts points from a dimension $2n-2$ set, which is a zero fraction of the points of U. But C_k was chosen to accept 1/3 of points from U. This is a contradiction. ◇

We can now write $G_k = F^m \cdot H$, where $m \geq 1$ and $F \nmid H$. We know that F is irreducible. This means that $G_k^2 = F^{2m} \cdot H^2 = F^{m'} \cdot H^2$, where $m' \geq 2$ and $F \nmid H^2$. From our assumption in Theorem 5.12, we also know that $F \nmid R_F$. The rest of the proof is identical to the proof of Theorem 5.1, which shows that $c(G_k) \geq 2n$ and hence, the communication complexity of recognizing S is at least $2n$, i.e. the depth of the protocol, which is at least $c(G_k)$, is at least $2n$. □

As in the real case, a weaker assumption on the mixed Hessian gives a correspondingly weaker lower bound. Using a non-divisible $r \times r$ minor together with Lemma 4.4 yields the following complex analogue of Theorem 5.8.

Theorem 5.16 (Mixed Hessian framework over $\mathbb{C}$)**.** *Let $S \subseteq \mathbb{C}^n \times \mathbb{C}^n$ be a constructible set of dimension $2n-1$, let $F \in \mathbb{C}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$, and let $1 \leq r \leq n$. Suppose that*

1. *F is irreducible over $\mathbb{C}$;*
2. *$V(F) \subseteq \overline{S}$, where $\overline{S}$ is the Zariski closure of S; and*
3. *some $r \times r$ minor of $\mathsf{H}_{X|Y}(F)$ is not divisible by F.*

Then

$$\mathrm{PCC}_{\mathbb{C}}(S) \geq 2(r-2).$$

In the complex case we do not have threshold sets, but the natural analogue would be the hypersurface-membership problem:

Theorem 1.6 (Restated)**.** *Let $F \in \mathbb{C}[X, Y]$ be irreducible and let $V(F) = \{(X, Y) \in \mathbb{C}^n \times \mathbb{C}^n \mid F(X, Y) = 0\}$. If there exists $u \in \mathbb{C}^n \times \mathbb{C}^n$ such that*

$$F(u) = 0 \qquad \text{and} \qquad R_F(u) \neq 0,$$

then $\mathrm{PCC}_{\mathbb{C}}(V(F)) \geq 2n$.

Proof. Clearly $V(F)$ is a constructible set of dimension $2n-1$, so we need only verify that Conditions 2 and 3 of Theorem 5.12 are satisfied. First observe that Condition 2 is trivial since $V(F)$ is already Zariski closed, so $V(F) = \overline{V(F)}$. Next, Condition 3, that $F \nmid R_F$, is also easy to see. If $F \mid R_F$ then $V(F) \subseteq V(R_F)$ which contradicts the existence of u. □

6 New probabilistic lower bounds

We now apply the framework developed in the previous section to prove probabilistic communication lower bounds for several natural set-recognition problems over both $\mathbb{R}$ and $\mathbb{C}$.

6.1 The ε-equality set

For $\varepsilon > 0$, define[9]

$$\mathsf{EQ}_n(X,Y) = \sum_{i=1}^{n} (X_i - Y_i)^2, \qquad \mathsf{EQ}_{n,\varepsilon} = \mathsf{EQ}_n - \varepsilon \tag{6.1}$$

and

$$S(\mathsf{EQ}_{n,\varepsilon}) = \left\{(X,Y) \in \mathbb{R}^n \times \mathbb{R}^n \mid \mathsf{EQ}_{n,\varepsilon}(X,Y) \leq 0\right\}.$$

Thus, $S(\mathsf{EQ}_{n,\varepsilon})$ consists of pairs of vectors whose squared Euclidean distance is at most ε. We first prove that the defining polynomial is irreducible.

Lemma 6.2 (Irreducibility of $\mathsf{EQ}_{n,\varepsilon}$)**.** *For every $n \geq 2$ and $\varepsilon > 0$, the polynomial $\mathsf{EQ}_{n,\varepsilon}(X,Y)$ defined in Eq. (6.1) is irreducible over both $\mathbb{R}$ and $\mathbb{C}$.*

Proof. Set $d_i = X_i - Y_i$. Since the map $(X_i, Y_i) \mapsto (X_i - Y_i, Y_i)$ is an invertible linear change of variables, it suffices to prove that

$$q(d) = \sum_{i=1}^{n} d_i^2 - \varepsilon$$

is irreducible over $\mathbb{C}$. Its homogenization is

$$Q(d,z) = \sum_{i=1}^{n} d_i^2 - \varepsilon z^2.$$

Since Q is a quadratic form of rank $n+1 \geq 3$, it is irreducible over $\mathbb{C}$ (see [Tve64]). If q had a non-trivial factorization, homogenizing its factors would give a non-trivial factorization of Q. Hence q, and therefore $\mathsf{EQ}_{n,\varepsilon}$, is irreducible over $\mathbb{C}$, and consequently over $\mathbb{R}$.

□

We now prove the communication complexity of the real threshold set $S(\mathsf{EQ}_{n,\varepsilon})$ and of the corresponding complex hypersurface.

Theorem 6.3 (Communication complexity of $\mathsf{EQ}_{n,\varepsilon}$)**.** *Let $n \geq 2$ and $\varepsilon > 0$, and set*

$$\mathsf{EQ}_n(X,Y) = \sum_{i=1}^{n} (X_i - Y_i)^2, \qquad \mathsf{EQ}_{n,\varepsilon} = \mathsf{EQ}_n - \varepsilon,$$

[9]The polynomial EQ_n exactly captures equality of vectors over $\mathbb{R}$, but not over $\mathbb{C}$ when $n \geq 2$. Nevertheless, we retain the notation for consistency.

$$S(\mathsf{EQ}_{n,\varepsilon}) = \left\{(X,Y) \in \mathbb{R}^n \times \mathbb{R}^n \mid \mathsf{EQ}_{n,\varepsilon}(X,Y) \le 0\right\}.$$

Then,

$$\mathrm{PCC}_{\mathbb{R}}\left(S(\mathsf{EQ}_{n,\varepsilon})\right) = \mathrm{DCC}_{\mathbb{R}}\left(S(\mathsf{EQ}_{n,\varepsilon})\right) = 2n.$$

Moreover,

$$\mathrm{PCC}_{\mathbb{C}}\left(V(\mathsf{EQ}_{n,\varepsilon})\right) = \mathrm{DCC}_{\mathbb{C}}\left(V(\mathsf{EQ}_{n,\varepsilon})\right) = 2n.$$

Proof. By Lemma 6.2, the polynomial $\mathsf{EQ}_{n,\varepsilon}$ is irreducible over both $\mathbb{R}$ and $\mathbb{C}$. Let $u \in \mathbb{R}^n \times \mathbb{R}^n \subseteq \mathbb{C}^n \times \mathbb{C}^n$ be any point satisfying

$$X - Y = \left(\sqrt{\varepsilon}, 0, \ldots, 0\right).$$

Then, $\mathsf{EQ}_{n,\varepsilon}(u) = 0$. Writing $d = X - Y$, we have

$$\nabla_X \mathsf{EQ}_{n,\varepsilon} = 2d, \qquad \nabla_Y \mathsf{EQ}_{n,\varepsilon} = -2d, \qquad \mathsf{H}_{X|Y}(\mathsf{EQ}_{n,\varepsilon}) = -2I_n,$$

and hence

$$R_{\mathsf{EQ}_{n,\varepsilon}}(u) = 4(-2)^{n-1} d^T d = 4(-2)^{n-1}\varepsilon \neq 0.$$

Therefore, Theorem 1.5 gives $\mathrm{PCC}_{\mathbb{R}}\left(S(\mathsf{EQ}_{n,\varepsilon})\right) \ge 2n$. The same point u also satisfies the hypotheses of Theorem 1.6, so

$$\mathrm{PCC}_{\mathbb{C}}\left(V(\mathsf{EQ}_{n,\varepsilon})\right) \ge 2n.$$

For the matching upper bounds, Alice and Bob broadcast their coordinates, using $2n$ messages in total, after which the testing polynomial evaluates $\mathsf{EQ}_{n,\varepsilon}(X,Y)$. Over $\mathbb{R}$, the protocol accepts when this value is nonpositive; over $\mathbb{C}$, it accepts when the value is zero. Thus, both deterministic protocols have depth $2n$, completing the proof. □

6.2 The ε-hypercube set

For $\varepsilon > 0$, define

$$\mathsf{HC}_n(X,Y) = \sum_{i=1}^{n} \left((X_i - Y_i)^2 - 1\right)^2, \qquad \mathsf{HC}_{n,\varepsilon} = \mathsf{HC}_n - \varepsilon \tag{6.4}$$

and

$$S(\mathsf{HC}_{n,\varepsilon}) = \left\{(X,Y) \in \mathbb{R}^n \times \mathbb{R}^n \mid \mathsf{HC}_{n,\varepsilon}(X,Y) \le 0\right\}.$$

The set $S(\mathsf{EQ}_{n,\varepsilon})$ can be viewed as recognizing whether a point $Z \in \mathbb{R}^n$ is close to the origin, when Z is distributed between the two parties and presented as $Z = X - Y$. We can generalize this to sets recognizing whether a distributed point $Z = X - Y$ is close to some point in a finite structured set. Taking this structured set to be the vertices $\{-1,1\}^n$ of the Boolean hypercube, we obtain $S(\mathsf{HC}_{n,\varepsilon})$, which we call the ε-hypercube problem.

We first prove that its defining polynomial is irreducible.

Lemma 6.5 (Irreducibility of $\mathsf{HC}_{n,\varepsilon}$)**.** *For every $n \ge 3$ and $\varepsilon \ge 0$, the polynomial $\mathsf{HC}_{n,\varepsilon}(X,Y)$ defined in Eq. (6.4) is irreducible over $\mathbb{C}$.*

Remark 6.6. For $n = 2$, it can be proved that $\mathsf{HC}_{2,\varepsilon}$ is irreducible over $\mathbb{R}$ whenever $\varepsilon \neq 1$.

Proof of Lemma 6.5. Let $d_i = X_i - Y_i$. Since this is an invertible linear change of variables, it suffices to prove irreducibility in the variables $d_1, \dots, d_n$. The highest-degree homogeneous part of

$$\mathsf{HC}_{n,\varepsilon} = \sum_{i=1}^{n} (d_i^2 - 1)^2 - \varepsilon$$

is $A = \sum_{i=1}^{n} d_i^4$, which is irreducible over $\mathbb{C}$ when $n \geq 3$ (see [Tve64]). If $\mathsf{HC}_{n,\varepsilon} = gh$ were a non-trivial factorization, then the highest-degree homogeneous parts of g and h would give a non-trivial factorization of A, a contradiction. Thus $\mathsf{HC}_{n,\varepsilon}$ is irreducible over $\mathbb{C}$, and hence over $\mathbb{R}$. □

Having proved the irreducibility of $\mathsf{HC}_{n,\varepsilon}$, we compute the mixed Hessian needed to apply the lower-bound framework.

Lemma 6.7 (Mixed Hessian of $\mathsf{HC}_{n,\varepsilon}$)**.** *Let $d_i = X_i - Y_i$. Then*

$$\mathsf{H}_{X|Y}(\mathsf{HC}_{n,\varepsilon}) = -\operatorname{diag}(12d_1^2 - 4, \dots, 12d_n^2 - 4).$$

In particular,

$$\Delta_{n,\varepsilon} := \mathsf{Det}\, \mathsf{H}_{X|Y}(\mathsf{HC}_{n,\varepsilon}) = (-1)^n \prod_{i=1}^{n} (12d_i^2 - 4).$$

Proof. Each summand of $\mathsf{HC}_{n,\varepsilon}$ depends on only one d_i, so the mixed derivative vanishes when $i \neq j$. For $i = j$,

$$\frac{\partial \mathsf{HC}_{n,\varepsilon}}{\partial X_i} = 4d_i(d_i^2 - 1), \qquad \frac{\partial^2 \mathsf{HC}_{n,\varepsilon}}{\partial X_i \partial Y_i} = -4(3d_i^2 - 1) = -(12d_i^2 - 4). \tag{6.8}$$

The two formulas follow. □

We now determine the communication complexity of the real threshold set $S(\mathsf{HC}_{n,\varepsilon})$ and of the corresponding complex hypersurface.

Theorem 6.9 (Communication complexity of $\mathsf{HC}_{n,\varepsilon}$)**.** *Let $\varepsilon > 0$ and $n \geq 3$, and set*

$$\mathsf{HC}_n(X, Y) = \sum_{i=1}^{n} \Big((X_i - Y_i)^2 - 1 \Big)^2, \quad S(\mathsf{HC}_{n,\varepsilon}) = \{(X, Y) \in \mathbb{R}^n \times \mathbb{R}^n \mid \mathsf{HC}_{n,\varepsilon}(X, Y) \leq 0\},$$

where $\mathsf{HC}_{n,\varepsilon} = \mathsf{HC}_n - \varepsilon$. Then

$$\mathrm{PCC}_{\mathbb{R}}\left(S(\mathsf{HC}_{n,\varepsilon})\right) = \mathrm{DCC}_{\mathbb{R}}\left(S(\mathsf{HC}_{n,\varepsilon})\right) = 2n.$$

Moreover,

$$\mathrm{PCC}_{\mathbb{C}}\left(V(\mathsf{HC}_{n,\varepsilon})\right) = \mathrm{DCC}_{\mathbb{C}}\left(V(\mathsf{HC}_{n,\varepsilon})\right) = 2n.$$

Proof. By Lemma 6.5, the polynomial $\mathsf{HC}_{n,\varepsilon}$ is irreducible over the relevant field under the stated assumptions. Choose $u \in \mathbb{R}^n \times \mathbb{R}^n \subseteq \mathbb{C}^n \times \mathbb{C}^n$ such that, with $d = X - Y$,

$$d_1^2 = 1 + \sqrt{\varepsilon}, \qquad d_2 = \cdots = d_n = 1.$$

Then $\mathsf{HC}_{n,\varepsilon}(u) = 0$. Let $v = \nabla_X \mathsf{HC}_{n,\varepsilon}(u)$. From Eq. (6.8)

$$v_i = 4d_i(d_i^2 - 1),$$

we have $v_1 = 4d_1\sqrt{\varepsilon} \neq 0$ and $v_i = 0$ for $i \geq 2$. By Lemma 6.7, the last $n-1$ diagonal entries of $\mathsf{H}_{X|Y}(\mathsf{HC}_{n,\varepsilon})(u)$ are all -8. Moreover, $\nabla_Y \mathsf{HC}_{n,\varepsilon} = -\nabla_X \mathsf{HC}_{n,\varepsilon}$, and hence

$$R_{\mathsf{HC}_{n,\varepsilon}}(u) = \mathsf{Det}\begin{pmatrix} \mathsf{H}_{X|Y}(\mathsf{HC}_{n,\varepsilon})(u) & v \\ -v^T & 0 \end{pmatrix} = v_1^2(-8)^{n-1} \neq 0.$$

Applying Theorem 1.5 gives

$$\mathrm{PCC}_{\mathbb{R}}\left(S(\mathsf{HC}_{n,\varepsilon})\right) \geq 2n,$$

while Theorem 1.6 gives

$$\mathrm{PCC}_{\mathbb{C}}\left(V(\mathsf{HC}_{n,\varepsilon})\right) \geq 2n.$$

For the upper bound, Alice broadcasts $h_i = X_i$ and Bob broadcasts $h_{n+i} = Y_i$ for every $i \in [n]$. The final testing polynomial is

$$\sum_{i=1}^{n}\Big((h_i - h_{n+i})^2 - 1\Big)^2 - \varepsilon.$$

Over $\mathbb{R}$, the protocol accepts when this value is nonpositive. Over $\mathbb{C}$, it accepts when the value is zero. This gives deterministic protocols of depth $2n$ for $S(\mathsf{HC}_{n,\varepsilon})$ and $V(\mathsf{HC}_{n,\varepsilon})$, respectively. Together with the two lower bounds, this proves both equalities. □

6.3 Inner product

Grigoriev proved a lower bound of $2(n-3)$ for the inner product set-recognition problems [Gri08, Proposition 3.1]. Using our framework together with the mixed Hessian rank bound of Lemma 4.4 (instead of Lemma 4.5), we improve this bound to be $2(n-2)$.

Recall that

$$\mathsf{IP}_n(X,Y) = \sum_{i=1}^{n} X_i Y_i.$$

Over $\mathbb{R}$, we consider the threshold set $S(\mathsf{IP}_n)$, while over $\mathbb{C}$, we consider the zero set $V(\mathsf{IP}_n)$.

Theorem 6.10 (Probabilistic lower bound for inner product)**.** *For every $n \geq 3$,*

$$\mathrm{PCC}_{\mathbb{R}}\left(S(\mathsf{IP}_n)\right) \geq 2(n-2) \qquad \textit{and} \qquad \mathrm{PCC}_{\mathbb{C}}\left(V(\mathsf{IP}_n)\right) \geq 2(n-2).$$

Consequently, the same lower bound holds for $\mathrm{DCC}_{\mathbb{R}}\left(S(\mathsf{IP}_n)\right)$ *and* $\mathrm{DCC}_{\mathbb{C}}\left(V(\mathsf{IP}_n)\right)$.

Proof. The polynomial IP_n is irreducible over both $\mathbb{R}$ and $\mathbb{C}$. Over $\mathbb{R}$, consider the point $u = ((1,0,\ldots,0),0) \in V(\mathsf{IP}_n)$. Since $\nabla \mathsf{IP}_n(u) = (0,(1,0,\ldots,0)) \neq 0$, Proposition 2.3 gives $\dim V(\mathsf{IP}_n) = 2n-1$.

Claim 6.11. $\partial S(\mathsf{IP}_n) = V(\mathsf{IP}_n)$.

Proof of the claim. First, let $(X,Y) \notin V(\mathsf{IP}_n)$. Then $\mathsf{IP}_n(X,Y)$ is either strictly positive, or strictly negative. By continuity, the same strict inequality holds throughout some open ball around (X,Y). This ball is therefore either contained in $S(\mathsf{IP}_n)$, or disjoint from it, so $(X,Y) \notin \partial S(\mathsf{IP}_n)$. Hence

$$\partial S(\mathsf{IP}_n) \subseteq V(\mathsf{IP}_n).$$

For the reverse inclusion, fix $(X,Y) \in V(\mathsf{IP}_n)$ and an arbitrary open ball $B_r(X,Y)$. We construct within this ball one point where IP_n is negative and another where it is positive.

Suppose first that $X \neq 0$. For every $t > 0$,

$$\mathsf{IP}_n(X, Y + tX) = t\sum_{i=1}^{n} X_i^2 > 0, \qquad \mathsf{IP}_n(X, Y - tX) = -t\sum_{i=1}^{n} X_i^2 < 0,$$

where we used the bilinearity of IP_n and the fact that $\mathsf{IP}_n(X, Y) = 0$. Choosing $t < r/\|X\|$ places both points in $B_r(X, Y)$.

If $X = 0$ and $Y \neq 0$, the same argument applies after perturbing the first input:

$$\mathsf{IP}_n(tY, Y) = t\sum_{i=1}^{n} Y_i^2 > 0, \qquad \mathsf{IP}_n(-tY, Y) = -t\sum_{i=1}^{n} Y_i^2 < 0.$$

Again, both points lie in $B_r(X, Y)$ for sufficiently small $t > 0$.

Finally, if $X = Y = 0$, then for sufficiently small $t > 0$ the points $((t, 0, \ldots, 0), (t, 0, \ldots, 0))$ and $((t, 0, \ldots, 0), (-t, 0, \ldots, 0))$ lie in $B_r(0, 0)$, while

$$\mathsf{IP}_n((t, 0, \ldots, 0), (t, 0, \ldots, 0)) = t^2 > 0, \qquad \mathsf{IP}_n((t, 0, \ldots, 0), (-t, 0, \ldots, 0)) = -t^2 < 0.$$

Thus every open ball centered at (X, Y) meets both $S(\mathsf{IP}_n)$ and its complement. Therefore $(X, Y) \in \partial S(\mathsf{IP}_n)$, proving the reverse inclusion. ◇

We have

$$\mathsf{H}_{X|Y}(\mathsf{IP}_n) = I_n.$$

Hence $\mathsf{Det}\,\mathsf{H}_{X|Y}(\mathsf{IP}_n) = 1$, which is not divisible by IP_n. Together with the claim and $\dim V(\mathsf{IP}_n) = 2n - 1$, this verifies the hypotheses of Theorem 5.8 with $r = n$. Therefore,

$$\mathrm{PCC}_{\mathbb{R}}\left(S(\mathsf{IP}_n)\right) \geq 2(n - 2).$$

Over $\mathbb{C}$, Proposition 2.3 gives $\dim V(\mathsf{IP}_n) = 2n - 1$. Moreover, $V(\mathsf{IP}_n)$ is Zariski closed and hence equals its Zariski closure. Thus, the hypotheses of Theorem 5.16 are satisfied with $r = n$, and

$$\mathrm{PCC}_{\mathbb{C}}\left(V(\mathsf{IP}_n)\right) \geq 2(n - 2).$$

□

We now return to the bilinear-form threshold and zero-set problems introduced in Section 3.4.

Corollary 6.12 (Communication bounds for bilinear forms)**.** *Let $A \in \mathbb{R}^{n\times n}$ and $r = \mathrm{rank}_{\mathbb{R}}(A) \geq 1$. Then*

$$2r - 4 \leq \mathrm{PCC}_{\mathbb{R}}\left(S(\mathsf{BF}_{n,A})\right) \leq \mathrm{DCC}_{\mathbb{R}}\left(S(\mathsf{BF}_{n,A})\right) \leq 2r.$$

For the complex case, let $A \in \mathbb{C}^{n\times n}$ and $r = \mathrm{rank}_{\mathbb{C}}(A) \geq 1$. Then

$$2r - 4 \leq \mathrm{PCC}_{\mathbb{C}}\left(V(\mathsf{BF}_{n,A})\right) \leq \mathrm{DCC}_{\mathbb{C}}\left(V(\mathsf{BF}_{n,A})\right) \leq 2r.$$

Proof. The upper bounds follow from observation 3.13 and the protocol in which Alice and Bob each broadcast their r coordinates. For $r \leq 2$, the lower bounds are immediate. For $r \geq 3$, Theorem 6.10 gives the lower bound $2(r - 2)$ in both cases, and the result follows from observation 3.13. □

6.4 The ε-SI set

The set-intersection problem asks whether two input vectors, viewed as sets, share a common element; that is, whether $X_i = Y_j$ for some $i, j \in [n]$. Grigoriev proved probabilistic communication lower bounds of n over $\mathbb{R}$ and $n/2$ over $\mathbb{C}$ for this problem (see [Gri08, Corollary 5.5]). We consider the following perturbed variant. Let

$$\mathsf{SI}_n(X,Y) = \prod_{i=1}^{n}\prod_{j=1}^{n}(X_i - Y_j), \qquad \mathsf{SI}_{n,\varepsilon}(X,Y) = \mathsf{SI}_n(X,Y) - \varepsilon, \tag{6.13}$$

where $\varepsilon > 0$, and define

$$S(\mathsf{SI}_{n,\varepsilon}) = \{(X,Y) \in \mathbb{R}^n \times \mathbb{R}^n \;\mid\; \mathsf{SI}_{n,\varepsilon}(X,Y) \le 0\}.$$

We first prove the irreducibility of the ε-SI polynomial [10].

Lemma 6.14. *For every $n \ge 2$ and $\varepsilon \in \mathbb{R}\backslash\{0\}$, the polynomial $\mathsf{SI}_{n,\varepsilon}$ defined in Eq. (6.13) is irreducible over both $\mathbb{R}$ and $\mathbb{C}$.*

Proof. It suffices to prove irreducibility over $\mathbb{C}$. Set $d = n^2$. The homogenization of $\mathsf{SI}_{n,\varepsilon}$ is

$$\mathsf{SI}_n(X,Y) - \varepsilon Z^d.$$

The polynomials $X_i - Y_j$ are irreducible, and no two are nonzero constant multiples of one another. Hence, every irreducible factor of $\mathsf{SI}_n/\varepsilon$ occurs with multiplicity one, whereas its multiplicity in a qth power would be divisible by q; thus, $\mathsf{SI}_n/\varepsilon$ is not a qth power in $\mathbb{C}(X,Y)$ for any prime $q \mid d$. Therefore, by the binomial irreducibility criterion, the homogenization is irreducible when regarded as a polynomial in Z over $\mathbb{C}(X,Y)$. By Gauss's lemma [GG13, Section 6.2], the homogenization is therefore irreducible in $\mathbb{C}[X,Y,Z]$. If $\mathsf{SI}_{n,\varepsilon}$ admitted a non-trivial factorization over $\mathbb{C}$, homogenizing its factors would give a non-trivial factorization of $\mathsf{SI}_n(X,Y) - \varepsilon Z^d$. Hence $\mathsf{SI}_{n,\varepsilon}$ is irreducible over $\mathbb{C}$, and therefore also over $\mathbb{R}$. □

For the mixed Hessian rank we use the following identity of Borchardt.

Proposition 6.15 (Borchardt's identity [Bor57, Equation 2])**.** *Let C and $C^{(2)}$ be the $n \times n$ matrices defined by*

$$C_{ij} = \frac{1}{X_i - Y_j}, \qquad C^{(2)}_{ij} = \frac{1}{(X_i - Y_j)^2}.$$

Then

$$\mathsf{Det}\, C^{(2)} \;=\; \mathsf{Det}(C)\,\mathsf{Perm}(C) \;=\; \frac{\displaystyle\prod_{1\le i<j\le n}(X_j - X_i)(Y_i - Y_j)}{\displaystyle\prod_{i=1}^{n}\prod_{j=1}^{n}(X_i - Y_j)}\,\mathsf{Perm}(C),$$

where $\mathsf{Perm}(C)$ denotes the permanent of C. Moreover, $\mathsf{Perm}(C)$ is a nonzero rational function. Consequently, $\mathsf{Det}\, C^{(2)} \neq 0$, and $C^{(2)}$ has rank n over $\mathbb{F}(X,Y)$ for $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$.

Lemma 6.16 (Mixed Hessian of the SI polynomial)**.** *For every $n \ge 2$ and $\varepsilon \neq 0$, there exists a nonzero $(n-1)\times(n-1)$ minor M of $\mathsf{H}_{X|Y}(\mathsf{SI}_{n,\varepsilon})$ such that*

$$\mathsf{SI}_{n,\varepsilon} \nmid M.$$

[10] We will show that $\mathsf{SI}_{n,\varepsilon}$ is irreducible over all $\varepsilon \neq 0$. However, we will use it when $\varepsilon > 0$.

Proof. Since $\mathsf{SI}_{n,\varepsilon} = \mathsf{SI}_n - \varepsilon$, it has the same mixed Hessian as SI_n. We perform the following calculation in the rational function field $\mathbb{F}(X, Y)$. Clearing denominators then gives the corresponding polynomial identity. We compute $\mathsf{H}_{X|Y}(\mathsf{SI}_n)$ using logarithmic differentiation. The first derivatives are:

$$\frac{\partial \mathsf{SI}_n}{\partial X_i} = \mathsf{SI}_n \sum_{b=1}^{n} \frac{1}{X_i - Y_b}, \qquad \frac{\partial \mathsf{SI}_n}{\partial Y_j} = -\mathsf{SI}_n \sum_{a=1}^{n} \frac{1}{X_a - Y_j}$$

Taking the mixed second derivative and applying the product rule gives

$$\begin{aligned}
\frac{\partial^2 \mathsf{SI}_n}{\partial X_i \partial Y_j} &= \frac{\partial}{\partial X_i}\left(-\mathsf{SI}_n \sum_{a=1}^{n} \frac{1}{X_a - Y_j}\right) \\
&= -\frac{\partial \mathsf{SI}_n}{\partial X_i}\left(\sum_{a=1}^{n} \frac{1}{X_a - Y_j}\right) - \mathsf{SI}_n \cdot \frac{\partial}{\partial X_i}\left(\sum_{a=1}^{n} \frac{1}{X_a - Y_j}\right) \\
&= -\mathsf{SI}_n \left(\sum_{b=1}^{n} \frac{1}{X_i - Y_b}\right)\left(\sum_{a=1}^{n} \frac{1}{X_a - Y_j}\right) + \mathsf{SI}_n \frac{1}{(X_i - Y_j)^2}
\end{aligned}$$

We can express this system over all $i, j \in [n]$ as a matrix equation. Let $C^{(2)}$ be the $n \times n$ matrix with entries $C^{(2)}_{i,j} = \frac{1}{(X_i - Y_j)^2}$. Let u and v be column vectors defined by $u_i = \sum_{b=1}^{n} \frac{1}{X_i - Y_b}$ and $v_j = \sum_{a=1}^{n} \frac{1}{X_a - Y_j}$. We can now write the mixed Hessian as

$$\mathsf{H}_{X|Y}(\mathsf{SI}_n) = \mathsf{SI}_n \cdot \left(C^{(2)} - uv^T\right).$$

Thus $\operatorname{rank} \mathsf{H}_{X|Y}(\mathsf{SI}_n) = \operatorname{rank}(C^{(2)} - uv^T)$.

By Proposition 6.15, $C^{(2)}$ has rank n, while uv^T has rank at most one. Hence

$$\operatorname{rank} \mathsf{H}_{X|Y}(\mathsf{SI}_n) \geq n - 1.$$

Therefore $\mathsf{H}_{X|Y}(\mathsf{SI}_{n,\varepsilon})$ has a nonzero $(n-1) \times (n-1)$ minor M. Every entry of this mixed Hessian is homogeneous of degree $n^2 - 2$, so M is homogeneous. Since $\mathsf{SI}_{n,\varepsilon}$ is not homogeneous due to its nonzero constant term, it cannot divide the nonzero homogeneous polynomial M. □

We obtain the probabilistic lower bound by the same framework used for the inner product set.

Theorem 6.17 (Probabilistic lower bound for the ε-SI set)**.** *For every $n \geq 2$ and $\varepsilon > 0$*[11]*,*

$$\mathrm{PCC}_{\mathbb{R}}\left(S(\mathsf{SI}_{n,\varepsilon})\right) \geq 2(n-3) \qquad \text{and} \qquad \mathrm{PCC}_{\mathbb{C}}\left(V(\mathsf{SI}_{n,\varepsilon})\right) \geq 2(n-3).$$

Consequently, the same lower bounds hold for the corresponding deterministic communication complexities.

Proof. By Lemma 6.14, $\mathsf{SI}_{n,\varepsilon}$ is irreducible over both $\mathbb{R}$ and $\mathbb{C}$.

Claim 6.18. $\partial S(\mathsf{SI}_{n,\varepsilon}) = V(\mathsf{SI}_{n,\varepsilon})$.

Proof of the claim. Continuity gives $\partial S(\mathsf{SI}_{n,\varepsilon}) \subseteq V(\mathsf{SI}_{n,\varepsilon})$. Conversely, let $z \in V(\mathsf{SI}_{n,\varepsilon})$. Since SI_n is homogeneous of degree n^2, Euler's theorem of homogeneous polynomials gives

$$\sum_{i=1}^{n} X_i \frac{\partial \mathsf{SI}_n}{\partial X_i} + \sum_{j=1}^{n} Y_j \frac{\partial \mathsf{SI}_n}{\partial Y_j} = n^2 \mathsf{SI}_n.$$

[11] For $n \in \{2, 3\}$, these lower bounds are vacuous.

Then $\mathsf{SI}_n(z) = \varepsilon$, so evaluating Euler's identity at z shows that $\nabla \mathsf{SI}_{n,\varepsilon}(z) \neq 0$. Moving a sufficiently small distance from z in the two opposite gradient directions therefore gives points where $\mathsf{SI}_{n,\varepsilon}$ has opposite signs. Hence $z \in \partial S(\mathsf{SI}_{n,\varepsilon})$, proving the reverse inclusion. ◇

Let $u \in \mathbb{R}^n \times \mathbb{R}^n$ be given by

$$X_i = \varepsilon^{1/n^2}, \qquad Y_i = 0 \qquad (i \in [n]).$$

Then $\mathsf{SI}_n(u) = \varepsilon$, so $u \in V(\mathsf{SI}_{n,\varepsilon})$. Moreover,

$$\frac{\partial \mathsf{SI}_{n,\varepsilon}}{\partial X_1}(u) = n\varepsilon^{1-1/n^2} \neq 0,$$

so $\nabla \mathsf{SI}_{n,\varepsilon}(u) \neq 0$. By Proposition 2.3,

$$\dim V(\mathsf{SI}_{n,\varepsilon}) = 2n - 1.$$

Together with the claim, this gives

$$\dim \left(\partial S(\mathsf{SI}_{n,\varepsilon}) \cap V(\mathsf{SI}_{n,\varepsilon})\right) = 2n - 1.$$

By Lemma 6.16, an $(n-1) \times (n-1)$ minor of $\mathsf{H}_{X|Y}(\mathsf{SI}_{n,\varepsilon})$ is not divisible by $\mathsf{SI}_{n,\varepsilon}$. Applying Theorem 5.8 with $r = n - 1$ gives

$$\mathrm{PCC}_{\mathbb{R}}\left(S(\mathsf{SI}_{n,\varepsilon})\right) \geq 2(n-3).$$

Over $\mathbb{C}$, Proposition 2.3 gives $\dim V(\mathsf{SI}_{n,\varepsilon}) = 2n - 1$. The set $V(\mathsf{SI}_{n,\varepsilon})$ is Zariski closed, and hence equals its Zariski closure. Together with Lemmas 6.14 and 6.16, this verifies the hypotheses of Theorem 5.16 with $r = n - 1$, which gives

$$\mathrm{PCC}_{\mathbb{C}}\left(V(\mathsf{SI}_{n,\varepsilon})\right) \geq 2(n-3).$$

□

7 Applications of communication lower bounds

In this section, we provide an application of our communication complexity lower bounds to an algorithmic setting. To the best of our knowledge, this algorithmic model has not been considered in the literature before. But very similar models have been studied in different settings such as of one-pass algorithms, streams over $\mathbb{N}$, and turnstile models [AMS99; LNW14; Mut05].

Informally, the setup is as follows. The input is a string $(\alpha_1, \ldots, \alpha_n) \in \mathbb{F}^n$. The algorithm reads the string, after reading each

coordinate, it may write a polynomial function of that coordinate into its memory and optionally query a testing polynomial with the current contents of its memory. The decisions in the following steps are based on the result of the tests ($=, \neq$ in the case of $\mathbb{C}$ and $<, >, =$ in the case of $\mathbb{R}$). The underlying algorithm may be deterministic or probabilistic. In the latter case, the probability of error is bounded by 1/3. The formal definition follows.

Definition 7.1 (Algebraic Scanner)**.** *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$. An algebraic scanner is an algorithm that, on input $\overline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}^n$, scans the input from left to right. It has a memory register which is initially empty, that is, $M^{(0)} = \perp$. At each step (i), it may perform the following operations.*

- *Append the memory with a new value $f_i(\alpha_i)$: $M^{(i)} = \left(M^{(i-1)}, f_i(\alpha_i)\right)$, where $f_i \in \mathbb{F}[z]$. The memory stays unchanged, i.e., $M^{(i)} = M^{(i-1)}$, if nothing is appended in step i.*
- *Ask a tester query about the content of the memory at that step: Is $Q_i(M^{(i)})$ $\mathtt{op}$ 0?, where $Q_i \in \mathbb{F}[z_1, \ldots, z_{\ell_i}]$, ℓ_i is the number of items in the memory and $\mathtt{op} \in \{\neq, =\}$ if $\mathbb{F} = \mathbb{C}$ and $\mathtt{op} \in \{<, >, =\}$, if $\mathbb{F} = \mathbb{R}$.*
- *At each step, at most 1 memory append operation can happen and at most one query is performed. The result of the query may be used to decide the choice of polynomials f's and Q's in the following steps.*

At the end of step (n), the algorithm either accepts or rejects.

We will say that $S \subseteq \mathbb{F}^n$ is accepted by an (ℓ, t)-scanner, if there is an algebraic scanner that uses at most ℓ items in the memory and at most t query polynomials and accepts $a \in \mathbb{F}^n$ if and only if $a \in S$. We say the cost of the scanner is $\ell + t$.

A probabilistic scanner is defined as a finite-support distribution over deterministic scanners. We say that $S \subseteq \mathbb{F}^n$ is accepted by an (ℓ, t)-probabilistic scanner, if there is an algebraic probabilistic scanner that uses at most ℓ items in the memory and at most t query polynomials. For $a \in \mathbb{F}^n$, if $a \in S$, it accepts a with probability at least $2/3$ and, if $a \notin S$, it rejects with probability at least $2/3$.

Theorem 7.2. *Let $S \subseteq \mathbb{F}^n \times \mathbb{F}^n$ and let $\widetilde{S} = \{X \circ Y \in \mathbb{F}^{2n} \mid (X, Y) \in S\}$, where $X \circ Y$ denotes concatenation of X and Y. If $\mathrm{PCC}_{\mathbb{F}}(S) \geq r$, then any (ℓ, t)-probabilistic scanner for $\widetilde{S}$ is such that $\ell + t \geq r$.*

Proof. We prove the contrapositive. Suppose we have an (ℓ, t)-probabilistic scanner for $\widetilde{S}$, where $\ell + t < r$. Then given input X to Alice and Y to Bob, Alice runs the scanner on her input. When she finishes processing her input, Bob starts processing his input. Each stored value from Alice's half becomes an Alice message; each stored value from Bob's half becomes a Bob message; the referee simulates all tests.

Notice that every time something is written in the memory, it becomes a possible input to the query polynomial at subsequent steps. Thus, the query polynomial receives at most ℓ inputs. Second, every time a test is performed, the protocol branches and increases the depth of the protocol. As there are at most t tests and ℓ memory storage steps, we get that $r \geq \ell + t$, which contradicts our assumption. □

Using the above theorem and the lower bounds on the communication complexity from Section 6, we obtain lower bounds on algebraic scanners for the following problems.

> ε-ℓ_2-**distance**:
> Given: vectors $\alpha, \beta \in \mathbb{R}^n$
> Check: $\ell_2(\alpha, \beta) \leq \varepsilon$

> **bichromatic collision**:
> Given: n green points $\alpha \in \mathbb{F}^n$ followed by n red points $\beta \in \mathbb{F}^n$
> Check: Is there a pair of points of different colors that have the same value?

Corollary 7.3. *Let $n \geq 2$ and let $\varepsilon > 0$. Any algebraic probabilistic scanner over $\mathbb{R}$ for ε-ℓ_2-**distance** has cost at least $2n$ and over $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$ for **bichromatic collision** has cost $\Omega(n)$.*

Proof. Note that for $(\alpha, \beta) \in \mathbb{R}^n \times \mathbb{R}^n$, $\ell_2(\alpha, \beta) \leq \varepsilon$ if and only if $(\alpha, \beta) \in S(\mathsf{EQ}_{n,\varepsilon^2})$. Also, note that $\alpha \in \mathbb{F}^n$ and $\beta \in \mathbb{F}^n$ have a bichromatic collision if and only if $(\alpha, \beta) \in V(\mathsf{SI}_n)$ Thus, using the probabilistic communication complexity lower bounds on $S(\mathsf{EQ}_{n,\varepsilon^2})$ and $V(\mathsf{SI}_n)$ and by Theorem 7.2 we get the corollary. □

We also obtain lower bounds for two algebraic problems. To define these two problems, we introduce some notation. For the sake of this discussion, we will assume $\mathbb{F} = \mathbb{C}$.

Notation. A univariate monic[12] polynomial of degree n may be represented either by its coefficients or by its roots. For example, consider $f(t) = t^2 - 4t + 3$. Here, we can represent it by the coefficient vector (1, -4, 3). But suppose we rewrite $f(t) = (t-1)(t-3)$, then we can represent it in terms of the multiset of roots, i.e., by $\{1, 3\}$. Here, we will assume the latter representation for univariate monic polynomials. We will denote this representation by $\mathsf{roots}(f(t)) = \{\alpha_1, \ldots, \alpha_n\}$. This means, $f(t) = \prod_{i \in [n]} (t - \alpha_i)$.

> **GCD**:
> Given: $\mathsf{roots}(f(t))$ followed by $\mathsf{roots}(g(t))$, where $f(t)$ and $g(t)$ are univariate monic polynomials.
> Check: Is $\gcd(f(t), g(t)) \neq 1$?

> **Resultant**:
> Given: $\mathsf{roots}(f(t))$ followed by $\mathsf{roots}(g(t))$, where $f(t)$ and $g(t)$ are univariate monic polynomials.
> Check: Is $\text{Resultant}(f(t), g(t)) = \varepsilon$?

Corollary 7.4. *Let $n \geq 2$ and $\varepsilon > 0$. Any algebraic probabilistic scanner over $\mathbb{C}$ for both GCD and Resultant has cost $\Omega(n)$.*

Proof. Note that resultant of $f(t)$ and $g(t)$ is equal to

$$\prod_{i \in [n]} \prod_{j \in [n]} (\alpha_i - \beta_j).$$

And this is 0 if and only if their gcd is non-trivial, i.e., it is not equal to 1 [CLO05, Chapter 3, Section 1].

Thus, by lower bounds on the communication complexity of $V(\mathsf{SI}_n)$ and $V(\mathsf{SI}_{n,\varepsilon})$ and by Theorem 7.2, we get the corollary. □

8 Extension to bounded-time BSS machines

In this section we generalize the communication model and prove that our framework for proving probabilistic lower bounds can be adapted in this general model. Our more general model is inspired by the well-known Blum–Shub–Smale model of computation [Blu+98].

[12] A univariate monic polynomial is a polynomial in one variable whose leading coefficient is 1

8.1 Bounded-time BSS machines

In this general model, Alice, Bob, and the referee are allowed to compute more general classes of functions. Implicitly, they are allowed to use computation defined by the following computational model:

Definition 8.1 (Bounded-time BSS machine)**.** *A* bounded-time BSS machine *is a finite computation tree consisting of*

- ***Input nodes*** *that read input from* $\mathbb{R}$ *into specified registers,* $(R_1, ..., R_n)$*, together with finitely many additional registers initialized to fixed real constants*
- ***Computation nodes*** *that execute* $R_i \leftarrow R_j * R_k$*, where* $* \in \{+, -, \times, /\}$*, where division by zero is disallowed.*
- ***Branch nodes*** *that branch according to* $R_i > 0$ *or* $R_i = 0$ *or* $R_i < 0$*.*
- ***Output leaves*** *that outputs a single real-valued number.*

Remark 8.2. Usually, in a standard BSS model, the output leaf writes out the (vector-valued) contents of the registers. However, since the communication model we consider is single-valued, we will only be considering BSS machines with single-valued output.

Note that BSS machines are usually directed graphs, not trees, but by assuming every input halts within a uniform finite time bound we may unravel the BSS machine to a (potentially exponential sized) tree as defined above.

Now if we just follow one path, τ in this tree then by regarding the inputs as variables, the output is a rational function, which we denote as $M^\tau(X) \in \mathbb{R}(X)$. Hence, globally, the output of the BSS machine, $M(X)$, is just a piecewise rational function. We assume these rational function have *no* poles on their corresponding pieces.

Furthermore, the set of points which travel along τ is given by a semialgebraic set. Indeed, each branching along τ is given by the sign of a rational function which can be described by (in)equalities of polynomials.[13]

Thus, a bounded-time BSS machine induces a finite partition of $\mathbb{R}^n$ into semialgebraic sets, one for each feasible computation path, and on each such set its output agrees with a rational function.

8.2 Extension of the full-rank mixed Hessian criterion to rational functions

We start by generalizing Lemma 4.5 to work for rational functions. This will play a critical role in Theorem 8.6.

Lemma 8.3 (Fractional full-rank criterion for powers)**.** *Let* $\mathbb{F}$ *be a field of characteristic zero, let* $p \in \mathbb{F}[X, Y]$ *be irreducible, and define determinant of* $(n+1) \times (n+1)$ *matrix*

$$R_p \quad := \quad \mathsf{Det} \begin{pmatrix} \mathsf{H}_{X|Y}(p) & \nabla_X p \\ (\nabla_Y p)^T & 0 \end{pmatrix}.$$

Suppose that $p \nmid R_p$*. Then for every*

$$g = p^m \frac{a}{b}, \qquad m \geq 2, \qquad p \nmid a, \qquad p \nmid b$$

with $a, b \in \mathbb{F}[X, Y] \setminus \{0\}$*, we have*

$$\operatorname{rank} \mathsf{H}_{X|Y}(g) = n.$$

[13] Since if $Q(X) = A(X)/B(X)$ then $Q(X) = 0 \iff A(X) = 0$ and $Q(X) > 0 \iff A(X)B(X) > 0$ and $Q(X) < 0 \iff A(X)B(X) < 0$. (Assuming $B(X) \neq 0$).

Proof. Let

$$A = \mathbb{F}[X,Y]_{\langle p\rangle} = \left\{ \frac{c}{d} : c,d \in \mathbb{F}[X,Y],\ d \neq 0,\ p \nmid d \right\}, \qquad h = \frac{a}{b}.$$

First, h is a unit in A, since $p \nmid a$ and hence $h^{-1} = b/a \in A$. Second, A is closed under differentiation: if $r/s \in A$, then

$$\frac{\partial}{\partial Z}\left(\frac{r}{s}\right) = \frac{s\,\partial_Z r - r\,\partial_Z s}{s^2} \in A,$$

since $p \nmid s^2$. Finally, since $\mathbb{F}[X,Y]$ is a unique factorization domain and p is irreducible, $\langle p\rangle$ is prime. Hence, A is a local domain with maximal ideal pA, so A/pA is a field. The images of both h and R_p in this field are nonzero: the former because h is a unit and the latter because $p \nmid R_p$.

These are precisely the properties of h and reduction modulo p used in the proof of Lemma 4.5. Hence, the same calculation applies over A and gives

$$\mathsf{Det}\,\mathsf{H}_{X|Y}(g) = p^{n(m-2)+n-1}Q, \qquad Q \equiv -m^n(m-1)h^n R_p \not\equiv 0 \pmod{pA}.$$

Here, the nonvanishing follows from $m \geq 2$, $\mathrm{char}(\mathbb{F}) = 0$, and the preceding observations about h and R_p. Therefore, $Q \neq 0$ and $\mathsf{Det}\,\mathsf{H}_{X|Y}(g) \neq 0$. Since the fraction field of A is $\mathbb{F}(X,Y)$, it follows that

$$\mathrm{rank}_{\mathbb{F}(X,Y)}\,\mathsf{H}_{X|Y}(g) = n.$$

□

Remark 8.4. The above is a *strict* generalization of Lemma 4.5, since we retrieve the result by simply setting $b = 1$.

8.3 Framework for BSS probabilistic lower bounds

We now consider the extension of Definition 2.8 and Definition 2.9 given by replacing every polynomial with bounded-time BSS machine. I.e. the protocol is exactly the same but the local computations and the branching are now done by bounded-time BSS machines. Furthermore, the communication complexity, $c(g)$, in this new model is defined exactly as in Definition 2.6 but with $a_1,...,a_{r_1}$, $b_1,...,b_{r_2}$ and P and g all given by bounded-time BSS machines.

Surprisingly, it turns out that even with this general model we can get the exact same framework for lower bounds of semialgebraic set-recognition! This result seems to hint that increasing the local power of the model does not result in greater computational power for set-recognition of semialgebraic sets.

Before we state and prove the main theorem, we need a generalization of Lemma 4.2, since path-specific computations of bounded-time BSS machines are rational functions rather than polynomial functions. This generalizes [Gri08] whose result is inspired by the much more general result, [Abe80, Theorem 2].

Lemma 8.5 (Mixed Hessian bound for rational computations)**.** *Let $\mathbb{F} \in \{\mathbb{R},\mathbb{C}\}$, and let $g \in \mathbb{F}(X,Y)$ be a rational function. Suppose that*

$$g(X,Y) = Q(a_1(X),...,a_{r_1}(X),b_1(Y),...,b_{r_2}(Y)),$$

is a minimum-size representation of g, where $a_1,...,a_{r_1} \in \mathbb{F}(X)$, $b_1,...,b_{r_2} \in \mathbb{F}(Y)$ and $Q \in \mathbb{F}(A_1,...,A_{r_1},B_1,...,B_{r_2})$ are all rational functions. Then $\mathrm{rank}\,\mathsf{H}_{X|Y}(g) \leq \min\{r_1,r_2\}$ and consequently

$$c(g) = r_1 + r_2 \geq 2 \cdot \mathrm{rank}\,\mathsf{H}_{X|Y}(g),$$

where the rank is taken over $\mathbb{F}(X,Y)$.

Proof. In the following all derivatives are formal derivatives and the calculations can be done over any open subset of $\mathbb{F}^n \times \mathbb{F}^n$ on which the denominators are non-zero.

Let $a = (a_1, ..., a_{r_1})$ and $b = (b_1, ..., b_{r_2})$. All the considered functions at least of regularity $\mathcal{C}^2$ (as we are dealing with quotients of polynomials), so Schwartz's theorem can be applied (and the partial derivatives can be swapped). By the same calculation as in the proof of Lemma 4.2 we have that

$$\mathsf{H}_{X|Y}(g) = J_X(a)\mathsf{H}_{A|B}(Q)(a,b)J_Y(b)^T,$$

where $J_X(a)$ is the $n \times r_1$ Jacobian matrix and $J_Y(b)$ is the $n \times r_2$ Jacobian matrix. Thus

$$\operatorname{rank} \mathsf{H}_{X|Y}(g) \leq \min\{r_1, r_2\}.$$

and so

$$c(g) = r_1 + r_2 \geq 2 \operatorname{rank} \mathsf{H}_{X|Y}(g)$$

as desired. □

Theorem 8.6. *Let $S \subseteq \mathbb{R}^n \times \mathbb{R}^n$ be a semialgebraic set and let $F \in \mathbb{R}[X, Y]$ satisfy*

1. *F is irreducible over $\mathbb{R}$*
2. *$\partial S \cap V(F)$ has dimension $2n - 1$*
3. *$F \nmid R_F$*

Then S has BSS-probabilistic communication complexity at least $2n$.

This proof is a lift of the proof of Theorem 5.1, so while it can mostly stand on its own, it is essentially simply a modification of Theorem 5.1.

Proof. Throughout this proof we only consider paths through trees which are realizable; i.e. paths for which there exists some input that follows the given path. Furthermore, throughout this proof, all fractions are in reduced form.

Let $\mathcal{C}$ be a probabilistic communication protocol recognizing S.

Note that a protocol C consists of a computation tree of computation trees: Indeed, we have an outer tree which branches based on the results of BSS machines which themselves are computation trees.

Thus we define a *trace*, τ, of a protocol C to consist of

- A path through the outer tree.
- A path through every communication BSS machine encountered on that outer path. This could be either Alice's machine or Bob's machine.
- A path through every transcript-testing BSS machine encountered on that outer path. This is the referee's BSS machine.

and we denote by $\operatorname{Tr}(C)$ the set of traces of C.

Along such a τ, the communicated values are rational functions and all testing functions are conducted by rational functions. Therefore, we see that any branch test occurring along τ has the form

$$G_{C,\tau,i}(X, Y) = \frac{N_{C,\tau,i}(X, Y)}{D_{C,\tau,i}(X, Y)}$$

where i indexes the branch tests.

Then, we define (assuming without loss of generality that $N_{C,\tau,i} \not\equiv 0$):

$$P_{C,\tau} = \prod_i N_{C,\tau,i}$$

which is a finite product, since every path is finite. Furthermore, the set

$$\mathcal{P} = \{P_{C,\tau} \mid C \in \mathcal{C}, \tau \in \mathrm{Tr}(C)\}$$

is finite since there are only finitely many protocols in $\mathcal{C}$ and since we consider only *bounded-time* BSS machines, there are only finitely many traces, τ, in C.

Claim 8.7.

$$\partial S \subseteq \bigcup_{C\in\mathcal{C}} \bigcup_{\tau\in\mathrm{Tr}(C)} V(P_{C,\tau}) =: \mathcal{V}$$

Proof of the claim. Suppose, for contradiction, that there exists $u \in \partial S$ such that $u \notin \mathcal{V}$. So $P_{C,\tau}(u) \neq 0$ for all $P_{C,\tau} \in \mathcal{P}$.

For each $C \in \mathcal{C}$ we denote by τ_C the unique trace followed by u. Since we disallow division by zero in BSS machines, every denominator along the trace encountered is nonzero. Moreover, since $u \notin \mathcal{V}$ every numerator encountered is also nonzero. Since the nonzero set of these numerators and denominators is an open set it follows that there exists an open neighborhood B_C around u. Moreover, by continuity the signs of the numerators and denominators are unchanged on B_C. Thus every element of B_C follows the trace, τ_C, and outputs the same value as u. Hence, the *finite* intersection of open neighborhoods,

$$B_u = \bigcap_{C\in\mathcal{C}} B_C,$$

is itself an open neighborhood of u on which the protocol, $\mathcal{C}$, has constant output.

More precisely this observation shows that, on B_u, we have

$$\Pr[\mathcal{C} \text{ accepts } z] = \Pr[\mathcal{C} \text{ accepts } u]$$

and so is constant on B_u.

But, u is on the boundary of S and so B_u must contain two points $z_{\text{in}} \in S$ and $z_{\text{out}} \notin S$ and by definition we must have $\Pr[\mathcal{C} \text{ accepts } z_{\text{in}}] \geq 2/3$ and $\Pr[\mathcal{C} \text{ accepts } z_{\text{out}}] \leq 1/3$. This gives us the desired contradiction:

$$2/3 \leq \Pr[\mathcal{C} \text{ accepts } z_{\text{in}}] = \Pr[\mathcal{C} \text{ accepts } z_{\text{out}}] \leq 1/3$$

since $z_{\text{in}}, z_{\text{out}} \in B_u$ and $\Pr[\mathcal{C} \text{ accepts } z]$ is constant on B_u. ◇

Assume now for contradiction that $F \nmid P_{C,\tau}$ for all C and τ. By Claim 8.7 and by Fact 5.4 we see that

$$\dim(\partial S \cap V(F)) \leq \dim\left(\bigcup_{C\in\mathcal{C}} \bigcup_{\tau\in\mathrm{Tr}(C)} (V(P_{C,\tau}) \cap V(F))\right) \leq 2n-2$$

which contradicts assumption 2.

Thus, F divides some P_{C_0,τ_0} and since F is irreducible (in particular prime) F must divide some numerator, $N_{C_0,\tau_0,0}$.

Claim 8.8. *$N_{C_0,\tau_0,0}$ comes from a transcript test. (In particular not from any private computation done by Alice or Bob).*

Proof of the claim. Assume it came from a private computation, say from Alice. Then $N_{C_0,\tau_0,0}$ would only depend on X:

$$N_{C_0,\tau_0,0}(X,Y) = A(X).$$

But then $F(X,Y) \mid A(X)$ and so F would only depend on X and be independent of Y. This would imply that $\nabla_Y F = 0$ and in particular $R_F = 0$ which means $F \mid R_F$. This contradicts $F \nmid R_F$ and so $N_{C_0,\tau_0,0}$ must come from a transcript test. ◇

Let $Q(X,Y)$ be the rational function such that (written in reduced representation)

$$Q(X,Y) = \frac{N_{C_0,\tau_0,0}(X,Y)}{D_{C_0,\tau_0,0}(X,Y)}$$

What we have shown so far is that by Claim 8.8, $Q(X,Y)$ is the result of a transcript test and so

$$Q(X,Y) = \hat{Q}(a_1(X),...,a_{r_A}(X),b_1(Y),...,b_{r_B}(Y)) = \frac{N_{C_0,\tau_0,0}(X,Y)}{D_{C_0,\tau_0,0}(X,Y)}$$

with

$$F \mid N_{C_0,\tau_0,0}$$

and since Q was written in reduced form we have $\gcd(N_{C_0,\tau_0,0}, D_{C_0,\tau_0,0}) = 1$ so we also have

$$F \nmid D_{C_0,\tau_0,0}$$

We may therefore write $N_{C_0,\tau_0,0} = F^m \hat{N}$ with $m \geq 1$ and $F \nmid \hat{N}$. This, in turn, gives

$$Q^2 = F^{2m}\left(\frac{\hat{N}}{D_{C_0,\tau_0,0}}\right)^2$$

with $2m \geq 2$ and $F \nmid \hat{N}^2$ and $F \nmid D^2_{C_0,\tau_0,0}$. Thus, we now apply the fractional full-rank criterion, Lemma 8.3, to get that

$$c(Q^2) \geq 2\,\mathrm{rank}(\mathsf{H}_{X|Y}(Q^2)) = 2n$$

where the first inequality is from Lemma 8.5. Finally, by the same observation in the proof of Theorem 5.1 we get

$$c(Q) \geq c(Q^2) \geq 2n$$

as desired. □

Remark 8.9. One can define *complex* bounded-time BSS machines, that is, BSS machines when the underlying field $\mathbb{F}$ is $\mathbb{C}$, wherein we branch only on $=$ or $\neq$. With this model one should be able to get a BSS analogue of the complex framework Theorem 5.12.

Indeed, if we consider all the rational functions, $T_1,...,T_m$ along the trace in following $\neq 0$ and take their product to be G_k. Then, in reduced form, we would have that

$$G_k = \frac{N_k}{D_k}$$

and, by the same argument as Claim 5.14 and Claim 5.15, we may conclude that

$$F \mid N_k \qquad \text{and} \qquad F \nmid D_k.$$

Furthermore, by the same argument as in Claim 8.8 it must be the case that a factor of N_k comes from the numerator of a transcript test.

The proof then follows exactly as in Theorem 8.6 to conclude that

$$c(G_k) \geq c(G_k^2) \geq 2n,$$

i.e. the depth of the protocol, which is at least $c(Q)$, is at least $2n$.

Acknowledgements

We thank the organizers and participants of the Bellairs Complexity Workshop 2026 in Barbados and the WAVE Workshop 2025 in Copenhagen for the stimulating environments and discussions that helped shape this work.

References

[Abe80] Harold Abelson. "Lower Bounds on Information Transfer in Distributed Computations". In: *J. ACM* 27.2 (1980), pp. 384–392 (cited on pages 3, 4, 9, 21, 40).

[AMS99] Noga Alon, Yossi Matias, and Mario Szegedy. "The Space Complexity of Approximating the Frequency Moments". In: *J. Comput. Syst. Sci.* 58.1 (1999), pp. 137–147 (cited on pages 9, 36).

[App+22] Benny Applebaum, Amos Beimel, Oded Nir, Naty Peter, and Toniann Pitassi. "Secret Sharing, Slice Formulas, and Monotone Real Circuits". In: *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*. Ed. by Mark Braverman. Vol. 215. Leibniz International Proceedings in Informatics (LIPIcs). Dagstuhl, Germany: Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022, 8:1–8:23 (cited on page 10).

[Ben83] Michael Ben-Or. "Lower bounds for algebraic computation trees". In: *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*. STOC '83. New York, NY, USA: Association for Computing Machinery, 1983, pp. 80–86 (cited on page 10).

[BV08] Markus Bläser and Elias Vicari. "Distributed Algorithmic Mechanism Design and Algebraic Communication Complexity". In: *Algorithmic Game Theory, First International Symposium, SAGT 2008, Paderborn, Germany, April 30-May 2, 2008. Proceedings*. Vol. 4997. Lecture Notes in Computer Science. Springer, 2008, pp. 206–217 (cited on pages 3, 4, 7, 9, 10).

[Blu+98] Lenore Blum, Felipe Cucker, Michael Shub, and Steve Smale. *Complexity and real computation*. Springer, 1998 (cited on pages 5, 38).

[BCR98] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy. *Real Algebraic Geometry*. Vol. 36. Ergebnisse der Mathematik und ihrer Grenzgebiete (3). Berlin, Heidelberg: Springer-Verlag, 1998 (cited on page 11).

[Bor57] Carl Wilhelm Borchardt. "Bestimmung der symmetrischen Verbindungen vermittelst ihrer erzeugenden Function". In: *Journal für die reine und angewandte Mathematik* 53 (1857), pp. 193–198 (cited on page 34).

[CLO05] David A. Cox, John Little, and Donal O'Shea. *Using Algebraic Geometry*. Graduate Texts in Mathematics. Springer New York, 2005 (cited on page 38).

[DL78] Richard A. DeMillo and Richard J. Lipton. "A Probabilistic Remark on Algebraic Program Testing". In: *Information Processing Letters* 7.4 (1978), pp. 193–195 (cited on page 11).

[GG13] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. 3rd ed. Cambridge University Press, 2013 (cited on page 34).

[Gri08] Dima Grigoriev. "Probabilistic Communication Complexity Over The Reals". In: *Computational Complexity* 17.4 (2008), pp. 536–548 (cited on pages 3–5, 7–9, 12, 21, 32, 34, 40).

[Hen07] Martin Henk. "Polynomdarstellungen von Polyedern". In: *Jahresberichte der DMV* 109 (2007), pp. 51–69 (cited on page 25).

[HP17] Pavel Hrubes and Pavel Pudlák. "A note on monotone real circuits". In: *Electron. Colloquium Comput. Complex.* TR17 (2017). ECCC: TR17-048 (cited on page 9).

[KW90] Mauricio Karchmer and Avi Wigderson. "Monotone Circuits for Connectivity Require Super-Logarithmic Depth". In: *SIAM J. Discret. Math.* 3.2 (1990), pp. 255–265 (cited on page 9).

[Kay11] Neeraj Kayal. "Efficient Algorithms for Some Special Cases of the Polynomial Equivalence Problem". In: *Proceedings of the Twenty-Second Annual ACM-SIAM Symposium on Discrete Algorithms*. SODA '11. SIAM, 2011, pp. 1409–1421 (cited on page 18).

[Kra98] Jan Krajícek. "Interpolation by a Game". In: *Math. Log. Q.* 44 (1998), pp. 450–458 (cited on page 9).

[KN97] Eyal Kushilevitz and Noam Nisan. *Communication complexity*. Cambridge University Press, 1997 (cited on page 3).

[LNW14] Yi Li, Huy L. Nguyen, and David P. Woodruff. "Turnstile streaming algorithms might as well be linear sketches". In: *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*. Ed. by David B. Shmoys. ACM, 2014, pp. 174–183 (cited on page 36).

[LN96] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. 2nd ed. Vol. 2.1. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1996 (cited on pages 11, 45).

[LT93] Zhi-Quan Luo and John N. Tsitsiklis. "On the Communication Complexity of Distributed Algebraic Computation". In: *J. ACM* 40.5 (1993), pp. 1019–1047 (cited on page 9).

[Mut05] S. Muthukrishnan. *Data Streams: Algorithms and Applications*. Foundations and trends in theoretical computer science. Now Publishers, 2005 (cited on pages 3, 9, 36).

[Ore22] Øystein Ore. "Über höhere Kongruenzen (German) [About higher congruences]". In: *Norsk Mat. Forenings Skrifter* 1.7 (1922). See also [LN96, Theorem 6.13], p. 15 (cited on page 11).

[Pud97] Pavel Pudlák. "Lower Bounds for Resolution and Cutting Plane Proofs and Monotone Computations". In: *J. Symb. Log.* 62.3 (1997), pp. 981–998 (cited on page 9).

[RY20] Anup Rao and Amir Yehudayoff. *Communication Complexity and Applications*. Cambridge University Press, 2020 (cited on page 3).

[Sch80] Jacob T. Schwartz. "Fast Probabilistic Algorithms for Verification of Polynomial Identities". In: *Journal of the ACM* 27.4 (1980), pp. 701–717 (cited on page 11).

[Spi65] Michael Spivak. *Calculus on Manifolds: A Modern Approach to Classical Theorems of Advanced Calculus*. New York: W. A. Benjamin, 1965 (cited on page 11).

[Tao14] Terence Tao. *Hilbert's Fifth Problem and Related Topics*. Vol. 153. Graduate Studies in Mathematics. American Mathematical Society, 2014 (cited on page 11).

[Tve64] Helge Tverberg. "A Remark on Ehrenfeucht's Criterion for Irreducibility of Polynomials". In: *Prace Matematyczne* 8 (1963/64), pp. 117–118 (cited on pages 29, 31).

[Vic08] Elias Vicari. "On Locality and Related Problems: Communicating, Computing, Exploring". Diss. ETH No. 17937. PhD thesis. Zurich, Switzerland: ETH Zurich, 2008 (cited on page 14).

[Yao79] Andrew Chi-Chih Yao. "Some Complexity Questions Related to Distributive Computing (Preliminary Report)". In: *Proceedings of the 11th Annual ACM Symposium on Theory of Computing, April 30 - May 2, 1979, Atlanta, Georgia, USA*. Ed. by Michael J. Fischer, Richard A. DeMillo, Nancy A. Lynch, Walter A. Burkhard, and Alfred V. Aho. ACM, 1979, pp. 209–213 (cited on page 3).

[Zip79] Richard Zippel. "Probabilistic Algorithms for Sparse Polynomials". In: *Symbolic and Algebraic Computation: EUROSAM '79*. Vol. 72. Lecture Notes in Computer Science. Springer, 1979, pp. 216–226 (cited on page 11).

A Proof of the mixed Hessian rank bound

Lemma 4.2 (Restated)**.** *Let $\mathbb{F} \in \{\mathbb{R}, \mathbb{C}\}$, and let $g \in \mathbb{F}[X, Y]$. Suppose that*

$$g(X, Y) = Q(a_1(X), \dots, a_{r_1}(X), b_1(Y), \dots, b_{r_2}(Y))$$

is a minimum-size representation of g, where $a_1, \dots, a_{r_1} \in \mathbb{F}[X]$ and $b_1, \dots, b_{r_2} \in \mathbb{F}[Y]$. Then $\operatorname{rank} \mathsf{H}_{X|Y}(g) \leq \min\{r_1, r_2\}$ *and*

$$c(g) = r_1 + r_2 \geq 2 \cdot \operatorname{rank} \mathsf{H}_{X|Y}(g).$$

Here the rank of a polynomial matrix is taken over $\mathbb{F}(X, Y)$.

Proof. Let $i, j \in \{1, \cdots, n\}$. We use the same notations as in Definition 2.6. In the rest of the proof, all the functions are at least of regularity $\mathcal{C}^2$ (as we are dealing with polynomials), so Schwarz's theorem can be applied (and the partial derivatives can be swapped). We compute $\mathsf{H}_{X|Y}$:

$$\begin{aligned} \frac{\partial g}{\partial X_i}(X, Y) &= \frac{\partial Q(a_1(X), \cdots, a_{r_1}(X), b_1(Y), \cdots, b_{r_2}(Y))}{\partial X_i}(X, Y) \\ \text{(chain rule)} \quad &= \sum_{p=1}^{r_1} \frac{\partial Q(a_1(X), \cdots, a_{r_1}(X), b_1(Y), \cdots, b_{r_2}(Y))}{\partial a_p(X)} \frac{\partial a_p(X)}{\partial X_i} \end{aligned}$$

Hence,

$$\frac{\partial^2 g}{\partial X_i \partial Y_j}(X,Y) = \sum_{p=1}^{r_1} \frac{\partial^2 Q(a_1(X),\cdots,a_{r_1}(X),b_1(Y),\cdots,b_{r_2}(Y))}{\partial a_p(X)\partial Y_j}\frac{\partial a_p(X)}{\partial X_i} + \frac{\partial Q(a_1(X),\cdots,a_{r_1}(X),b_1(Y),\cdots,b_{r_2}(Y))}{\partial a_p(X)}\underbrace{\frac{\partial^2 a_p(X)}{\partial X_i \partial Y_j}}_{=0}$$

$$\text{(chain rule)} \quad = \sum_{p=1}^{r_1}\sum_{q=1}^{r_2}\left(\frac{\partial b_q(Y)}{\partial Y_j}\right)\left(\frac{\partial^2 Q(a_1(X),\cdots,a_{r_1}(X),b_1(Y),\cdots,b_{r_2}(Y))}{\partial a_p(X)\partial b_q(Y)}\right)\left(\frac{\partial a_p(X)}{\partial X_i}\right)$$

Thus,

$$\mathsf{H}_{X|Y}(g) = \begin{pmatrix} \partial a_1(X)/\partial X \\ \vdots \\ \partial a_{r_1}(X)/\partial X \end{pmatrix} \mathsf{H}_{a|b}(Q) \begin{pmatrix} \partial b_1(Y)/\partial Y \\ \vdots \\ \partial b_{r_2}(Y)/\partial Y \end{pmatrix}^T$$

where $a = (a_1,\cdots,a_{r_1})$ and $b = (b_1,\cdots,b_{r_2})$.
Thus, $\operatorname{rank}(\mathsf{H}_{X|Y}(g)) \leq \min(r_1,r_2)$ and $r_1+r_2 \geq 2\min(r_1,r_2) \geq 2\operatorname{rank}(\mathsf{H}_{X|Y}(g))$. We conclude. □

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il