


Lifting Theorems for Equality

Bruno Loff 

INESC-TEC and University of Porto, Porto, Portugal
bruno.loff@gmail.com

Sagnik Mukhopadhyay 

Computer Science Institute of Charles University, Prague, Czech Republic
sagnik@kam.mff.cuni.cz

Abstract

We show a *deterministic simulation (or lifting) theorem* for composed problems $f \circ \text{Eq}_n$ where the inner function (the gadget) is Equality on n bits. When f is a total function on p bits, it is easy to show via a rank argument that the communication complexity of $f \circ \text{Eq}_n$ is $\Omega(\deg(f) \cdot n)$. However, there is a surprising counter-example of a partial function f on p bits, such that any completion f' of f has $\deg(f') = \Omega(p)$, and yet $f \circ \text{Eq}_n$ has communication complexity $O(n)$. Nonetheless, we are able to show that the communication complexity of $f \circ \text{Eq}_n$ is at least $D(f) \cdot n$ for a complexity measure $D(f)$ which is closely related to the AND-query complexity of f and is lower-bounded by the logarithm of the leaf complexity of f . As a corollary, we also obtain lifting theorems for the set-disjointness gadget, and a lifting theorem in the context of parity decision-trees, for the NOR gadget.

As an application, we prove a tight lower-bound for the deterministic communication complexity of the communication problem, where Alice and Bob are each given p -many n -bit strings, with the promise that either all of the strings are distinct, or all-but-one of the strings are distinct, and they wish to know which is the case. We show that the complexity of this problem is $\Theta(p \cdot n)$.

2012 ACM Subject Classification Theory of computation \rightarrow Circuit complexity; Theory of computation \rightarrow Communication complexity; Theory of computation \rightarrow Oracles and decision trees

Keywords and phrases Communication complexity, Query complexity, Simulation theorem, Equality function

Digital Object Identifier 10.4230/LIPIcs.STACS.2019.50

Related Version <https://eccc.weizmann.ac.il/report/2018/175/>

Funding *Bruno Loff*: The research leading to these results has received funding from the Foundation for Science and Technology (FCT), Portugal, grant number SFRH/BPD/116010/2016. This work is partially funded by the ERDF through the COMPETE 2020 Programme within project POCI-01-0145-FEDER-006961, and by National Funds through the FCT as part of project UID/EEA/50014/2013.

Sagnik Mukhopadhyay: Most of the work is done while the author was a post-doctoral researcher at KTH Royal Institute of Technology, Stockholm. The author is now supported by European Research Council under the European Union's Seventh Framework Programme (FP/2007-2013)/ERC Grant Agreement n. 616787.

Acknowledgements We are thankful to Suhail Sherif, Mark Vinyals, and Susanna de Rezende for many helpful discussions, and Or Meir for pointing out an important bug in an earlier draft of the paper. We also thank the anonymous referees whose insights improved the paper by a substantial amount. We owe an extraordinary debt to Arkadev Chattopadhyay, an outstanding companion of many tea-break conversations on the subject of this paper.



© Bruno Loff and Sagnik Mukhopadhyay;

licensed under Creative Commons License CC-BY

36th International Symposium on Theoretical Aspects of Computer Science (STACS 2019).

Editors: Rolf Niedermeier and Christophe Paul; Article No. 50; pp. 50:1–50:19

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany



1 Introduction

In the same paper of Karchmer and Wigderson [40], where the notion of formula depth was shown to be equivalent to the communication complexity of their since-homonymous games, was also the first proof separating monotone NC_2 from monotone NC_1 . Although not formulated explicitly in this way, their separation of these two circuit classes can be nowadays be presented as a two-part argument: (I) one first shows that the monotone Karchmer–Wigderson game for connectivity on $n^{\Theta(1)}$ -node graphs is equivalent to a composition problem in communication complexity, namely $\text{Switch}_n \circ \text{Ind}_n$, the composition of the Switch relation on n bits with the Indexing gadget on $\log n$ bits (given to Alice) and n bits (given to Bob); and (II) one then shows lower-bounds for $\text{Switch}_n \circ \text{Ind}_n$ by lifting an $\Omega(\log n)$ adversarial lower-bound against decision trees trying to solve the Switch_n relation, into an $\Omega((\log n)^2)$ adversarial lower-bound against communication protocols for $\text{Switch}_n \circ \text{Ind}_n$. Formally, a composed function $f \circ g$ consisting of f on p -bits and g on n bits is defined on $p \cdot n$ bit long input $x = \langle x_1, \dots, x_p \rangle$ (where each x_i is n bit long) as follows: $(f \circ g)(x) = f(g(x_1), \dots, g(x_p))$.

Their seminal paper led to the following general approach for proving lower-bounds against a given complexity measure. One first (I) finds a composed problem $f \circ g$ whose communication complexity is upper-bounded by the given complexity measure, and (II) one then proves a lower-bound for the communication complexity of $f \circ g$ by arguing that a lower-bound for f in a simple model (such as decision trees) will *lift* to a lower-bound against protocols for $f \circ g$.

Complexity theory has profited greatly from this approach. It appears in the celebrated Raz-McKenzie separation of the monotone NC hierarchy, [57] but also in the best known lower-bounds on monotone formula depth and monotone span programs [59, 54]. Several lower-bounds on the length of proofs in various proof systems were first established using this approach [14, 54, 19], and it is the only known way of proving various separations between complexity classes in communication complexity [27, 26, 25, 24, 23, 68]. It may even be used for proving lower-bounds against data-structure schemes [13], and lower-bounds on the extension complexity of linear programs [42, 46, 22].

Owing partly to this long list of discoveries, and partly to the Karchmer-Raz-Wigderson approach [39] for proving lower-bounds against (non-monotone) NC_1 [30, 17, 21, 15], the lower-bounds community developed a specific interest in understanding the computational complexity of composition, and devoted a large effort to understanding composition problems. Under this heading we should include Sherstov’s pattern matrix method [61], and the closely related block-composition method of Shi and Zhu [65], which were developed further in [10, 47, 11, 63, 64, 55], and resulted in many different applications. The problem of understanding the communication complexity of XOR functions [56, 66, 31] is another example of a composition problem, and particularly pertinent to our case since Equality is itself an XOR function, $\text{Eq}_n = \text{NOR}_n \circ \text{XOR}_2$. It is conjectured that the communication complexity of a composition $g \circ \text{XOR}_2$ is approximately equal to the parity decision-tree complexity of g , and in fact this has been shown to hold up to a polynomial if g is a total function [31]. From this conjectured connection, it would follow that the communication complexity of a composition with Equality, $f \circ \text{Eq}_n$, should equal the parity decision-tree complexity of the composition with the NOR function, $f \circ \text{NOR}_n$.

Work on the direct-sum and direct-product problems [35, 2, 29, 33, 16, 53, 34, 36, 1, 5, 6, 7, 4, 41, 32] is also a study of composition, where the outer function f in $f \circ g$ is the hardest possible: the identity function; even this case remains unsolved in various settings.

The complexity of composition is a difficult problem – not just because, generally speaking, lower-bounds are hard to establish, but also because the composition of two hard problems is sometimes not as hard as one may expect: sometimes there is a “collapse” of hardness. A classic example is the case of direct sum in communication complexity: a near-perfect direct sum result holds in the non-deterministic case [49, 38], but fails to hold in the deterministic model [52, 18], and is still an open problem in the randomized model. The following recent example is also of great interest. In the case of deterministic decision-trees, the depth-complexity of $f \circ g$ is the product of the complexities of f and g ; this both intuitive and easy to establish, and holds whether f is a total function, a partial function, or relation of any kind. But already if we look into *randomized* decision-trees, Gavinsky *et al.* [20] and Sanyal [60] show that the depth-complexity of the composition $f \circ g$ will be as high as the product of the complexity of f with the *square-root* of the complexity of g ; and, surprisingly, [20] exhibit a *relation* f and a function g for which this bound is tight. This “collapse” of hardness when composing relations or partial functions seems to make such problems difficult to understand. As we will see, composition with Equality provides another instance of this phenomenon.

1.1 A tea-break puzzle

Alice and Bob, two renowned complexity theorists, get together during the conference’s tea break: *Communication complexity is the most successful area in complexity theory* – Alice says – *at least the natural examples of functions are really well understood*. Bob raises his eyebrows – *do you mean total functions, like Equality, or partial functions, like Gap-Hamming-distance?* – *Both* – replies Alice – *Equality has been well understood since the invention of the field [70], and even Gap-Hamming-Distance is at this point understood for every gap – the constant gap case is a simple result [69], and even $\frac{1}{\sqrt{n}}$ fraction gap was eventually understood [9, 67, 62].*

Ok – Bob replied, wryly – *how about the “ $n, (n - 1)$ -Equality-Gap”? Suppose you are given p -many n -bit strings x_1, \dots, x_p , and I am given y_1, \dots, y_p , and we are promised that either all of the (x_i, y_i) pairs are different or exactly one of the (x_i, y_i) pairs is equal... show me that we need to communicate $\Omega(n \cdot p)$ bits in order to know which is the case...*

Alice thinks for a while – *I know, we can do it via a rank argument. Your “ $n, (n - 1)$ -Equality-Gap” function is the composition $F \circ \text{Eq}_n$, where F is the partial function which is 1 on the all 0 string and 0 on the strings of Hamming weight 1, and Eq_n is Equality on n bits. The decision tree complexity of F is $\Omega(p)$ which can be seen by a simple adversarial argument, and by the connection between degree and decision tree complexity [8, 51], we can show that any completion F' of F has degree $\Omega(p^{1/3})$. Also, Eq_n has rank 2^n , so the rank of the communication matrix of $F' \circ \text{Eq}_n$ is $2^{\Omega(p^{1/3}n)}$ (see Lemma 6), and hence the communication complexity is $\Omega(p^{1/3}n)$. This is not tight, but it’s close to what you want.*

Bob nods – *Your argument holds true, but it only implies that any protocol for $F' \circ \text{Eq}_n$ needs $\Omega(n \cdot p^{1/3})$ bits. However, even though a protocol for $F \circ \text{Eq}_n$ does give you a completion of the partial communication matrix for $F \circ \text{Eq}_n$, this completion does not need to be in the composed form $F' \circ \text{Eq}_n$ where F' is a completion of F . So you did not answer my question, not even if I disregard the polynomial loss...*

At this point Alice does not know what to answer, and rightly so. We will see below an example of a p -bit partial function f , such that any completion of f must have degree $\Omega(p^{1/3})$, and yet the communication complexity of $f \circ \text{Eq}_n$ is $O(n)$, instead of $\Omega(n \cdot p^{1/3})$, which is what one would expect from a rank-degree argument. The protocol that shows this will precisely take advantage of the fact that a completion of $f \circ g$ does not have to be of the form $f' \circ \text{Eq}_n$ for some completion of f' of f . We will also show that such a counter-example does not exist if f is a partial function.

A solution to Bob’s tea-break puzzle appears as Corollary 18, in page 10. Using our lifting theorem (Theorem 13, page 9) the desired tight lower-bound of $\Omega(n \cdot p)$ is a 2-line argument.

Interestingly, the counter-example provided below the problem of distinguishing the case when all of the (x_i, y_i) pairs are equal, from the case when all but one of the (x_i, y_i) pairs are equal, so it is strongly related to the example Alice and Bob were discussing above. However, the communication complexity of the example is $\Omega(p \cdot n)$, but the communication complexity of the counter-example is only $O(n)$.

1.2 Composition with Equality

In this work, we answer a question pertaining to the communication complexity of composition of Boolean relations with the Equality gadget. Before stating the question and our main results, we explain the context surrounding this question. We begin with some definitions.

- Define the “Switch” relation: $\text{Switch}_p = \{(z, i) \in \{0, 1\}^p \times \{0, 1, \dots, p\} \mid z_i = 1, z_{i+1} = 0\}$, where we use $z_0 = 1$ and $z_{p+1} = 0$, *i.e.*, we are given p bits and wish to find a “switching point”, a position i where a 1-bit flips into a 0-bit. If $z = 0^p$ we must output $i = 0$ and if $z = 1^p$ we must output $i = p$.
- Let $\text{Ind}_n : [n] \times \{0, 1\}^n \rightarrow \{0, 1\}$ denote the two-player Indexing function on n -bits, so that $\text{Ind}_n(x, y) = y_x$.
- Then $\text{Switch}_p \circ \text{Ind}_n$ denotes the composed Boolean relation:

$$\text{Switch}_p \circ \text{Ind}_n = \{(\bar{x}; \bar{y}; i) \in [n]^p \times (\{0, 1\}^n)^p \times \{0, 1, \dots, p\} \mid (y_i)_{x_i} = 1, (y_{i+1})_{x_{i+1}} = 0\}.$$

- Let $\text{Eq}_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ denote two-player Equality on n -bits, so that $\text{Eq}_n(x, y) = 1$ iff $x = y$.
- Then $\text{Switch}_p \circ \text{Eq}_n$ denotes the composed Boolean relation:

$$\text{Switch}_p \circ \text{Eq}_n = \{(\bar{x}; \bar{y}; i) \in (\{0, 1\}^n)^p \times (\{0, 1\}^n)^p \times \{0, 1, \dots, p\} \mid x_i = y_i, x_{i+1} \neq y_{i+1}\}.$$

- Let $F \subseteq \mathcal{A} \times \mathcal{B} \times \mathcal{C}$ be a relation. The *deterministic communication complexity* of F , $D^{cc}(F)$, is the minimum communication cost of a protocol for solving the communication problem where Alice is given $a \in \mathcal{A}$, Bob is given $b \in \mathcal{B}$, and they wish to find c such that $(a, b, c) \in F$, whenever one such c exists (see [45], Chapter 5).
- Let $f \subseteq \{0, 1\}^p \times \mathcal{C}$ be a relation. The *deterministic query complexity* of f , $D^{dt}(f)$, is the minimum number of queries made by a deterministic decision-tree which, given query access to $z \in \{0, 1\}^p$, finds a $c \in \mathcal{C}$ such that $(z, c) \in f$, whenever one such c exists.

In STOC’88, Karchmer and Wigderson [40] presented a proof that connectivity is not in monotone NC_1 . At the heart of their result was an argument which may be reinterpreted as a proof of the following theorem:

► **Theorem 1** (Karchmer and Wigderson, [40]). $D^{cc}(\text{Switch}_p \circ \text{Ind}_n) = \Omega((\log n) \cdot \log p)$.

In Structures’91, the conference now known as CCC, Grigni and Sipser [28] provided an alternative proof that connectivity is not in monotone NC_1 . Their proof uses Eq in place of Ind , and this allows for a simpler argument:

► **Theorem 2** (Grigni and Sipser, [28]). $D^{cc}(\text{Switch}_p \circ \text{Eq}_n) = \Omega(n \cdot \log p)$.

It is not hard to see that Theorem 2 implies Theorem 1, by reducing $\text{Eq}_{\log n}$ to Ind_n . Later, in FOCS’97, Raz and McKenzie [57] separated the entire monotone NC hierarchy. At the heart of their proof was an argument for a vast generalization of Theorem 1:

► **Theorem 3** (Raz and McKenzie, [57]). *For any Boolean relation $f \subseteq \{0, 1\}^p \times \mathcal{C}$, whenever $n \geq p^{20}$, $D^{cc}(f \circ \text{Ind}_n) = \Omega((\log n) \cdot D^{dt}(f))$.*

Theorem 3 was not stated with such generality in [57], but appeared in this form in a recent work of Göös, Pitasi and Watson [26]. Theorem 3 has been the basis of several papers [26, 12, 44].

Knowing the above history, one naturally comes to the question of whether one can prove a similar generalization for Grigni and Sipser’s Theorem 2, i.e., whether we can prove the conjecture:

► **Conjecture 4.** *For any Boolean relation $f \subseteq \{0, 1\}^p \times \mathcal{C}$, $D^{cc}(f \circ \text{Eq}_n) = \Omega(n \cdot D^{dt}(f))$.*

Very general lifting theorems may be proven using rank arguments, and the current state of the art [59, 54] is a lifting of the *Nullstellensatz degree* of any CNF-relation¹ f to the rank of $f \circ g$, which works for a large class of gadgets g having a certain algebraic property². The equality gadget does possess the required property, however our lower-bound technique will work for any relation, and not just CNF-relations.

In the case when f is a total function, however, there is an *ad-hoc* degree-to-rank lifting theorem which works for the equality gadget, and which is in the same spirit as [59, 54]. It uses the following characterization:

► **Proposition 5** ([3]). *If h is a Boolean function and F is the communication matrix of $h \circ \text{XOR}_2$, then $\text{rank}(F) = \|h\|_0$.*

Above, $\text{rank}(F)$ is the real rank of the communication matrix of F , and $\|h\|_0$ is the Fourier sparsity (the number of non-zero Fourier coefficients) of h . We can view $f \circ \text{Eq}_n$ as an XOR_2 function, $f \circ \text{NOR}_n \circ \text{XOR}_2$. The following observation is easy to prove, but the proof is omitted due to space constraints (see the ECC version [48] for the proof).

► **Lemma 6.** *For every $f : \{+1, -1\}^p \rightarrow \{+1, -1\}$ with $\deg(f) \geq 1$, and every $g : \{+1, -1\}^n \rightarrow \{+1, -1\}$, we have $\|f \circ g\|_0 \geq (\|g\|_0 - 1)^{\deg(f)}$.*

Lemma 6 implies that $\|f \circ \text{NOR}_n\|_0 = \Omega(2^{\deg(f) \cdot n})$, since $\|\text{NOR}_n\|_0 = 2^n$. By the rank-lower bound for communication complexity, we thus have $D^{cc}(f \circ \text{Eq}) \geq \Omega(\deg(f) \cdot n)$. Now we can use the following connection between $\deg(f)$ and $D^{dt}(f)$, which improves upon a theorem of Nisan and Smolensky theorem [8].

► **Proposition 7** ([51]). *$\deg(f) = \Omega(D^{dt}(f)^{1/3})$.*

Combining the three above facts, we get that when f is a total Boolean function, then $D^{cc}(f \circ \text{Eq}_n) = \Omega(D^{dt}(f)^{1/3} \cdot n)$. This easy-to-prove result is similar to Conjecture 4, except for the $1/3$ loss in the exponent, and works for all total functions. But surprisingly, when allow f to be a partial function, Conjecture 4 is false! The following counter-example was given to us by Arkadev Chattopadhyay, Suhail Sherif, and Mark Vinyals. Let $f \subseteq \{0, 1\}^p \times \{0, 1\}$ be the relation

$$f = \{(z, 1) \mid |z| = p \text{ or } |z| < p - 1\} \cup \{(z, 0) \mid |z| = p - 1 \text{ or } |z| < p - 1\},$$

¹ A CNF-relation $f_\phi \subseteq \{0, 1\}^n \times [m]$ is defined for a given unsatisfiable CNF ϕ on n variables and m clauses, by $(x, i) \in f_\phi$ if x falsifies the i -th clause. Such relations appear prominently in the study of monotone Karchmer–Wigderson games.

² These results are explained in Robert Robere’s excellent PhD thesis [58]. The mentioned algebraic property appears in Section 5.1.

i.e., we are given a Boolean string $z \in \{0, 1\}^p$, and wish to distinguish the case when z has Hamming weight p from the case when z has Hamming weight $p - 1$. It is easy to show that $D^{dt}(f) \geq p$: an adversary keeps answering 1 to all queries, and $f(z)$ will remain unknown until the very last query. This adversary also shows that $D^{dt}(f') \geq p$ for any “completion” of f , i.e. any total function $f' : \{0, 1\}^p \rightarrow \{0, 1\}$ which agrees with f on the inputs with Hamming weight p or $p - 1$; and hence $\deg(f') = \Omega(p^{1/4})$ for any such f' , by Proposition 7. So one might mistakenly hope, like Alice did in Section 1.1, that a rank/degree argument would serve to prove a lower-bound of $\Omega(p^{1/4} \cdot n)$ for $f \circ \text{Eq}_n$.

However, a protocol for $f \circ \text{Eq}_n(x_1, \dots, x_p; y_1, \dots, y_p)$ may proceed as follows. Think of each of Alice and Bob’s inputs for $f \circ \text{Eq}_n$ as a matrix with p rows and n columns. Then let $a \in \{0, 1\}^n$ be the XOR of each column of Alice’s input, and $b \in \{0, 1\}^n$ be the XOR of each column of Bob’s input. Then Alice sends a to Bob, and Bob replies whether $a = b$. Now, if every x_i equals the corresponding y_i , then clearly $a = b$; and if every x_i equals y_i , except for a single value of $i \in [p]$, then there must exist a $j \in [n]$ such that $a_j \neq b_j$. It then holds that $D^{cc}(f \circ \text{Eq}_n) \leq n + 1$, and so Conjecture 4 is false. Remarkably, this seems to suggest that rank/degree arguments will fail to hold.

This counter-example also shows that $\text{Eq}_{\log n}$ behaves differently from Ind_n , when used as the inner function in a composition – indeed Theorem 3 implies that $D^{cc}(f \circ \text{Ind}_n) \geq p \log n$, which is strictly higher when $p = \omega(1)$. The difference between Equality and Indexing may be further explained with the help of a recent paper of Chattopadhyay, Koucký, and the authors [12]. There it is shown that a theorem like Conjecture 4 will hold for any inner function g , in place of Eq_n , which admits certain *hitting distributions*³. As it turns out, all gadgets for which we could prove a deterministic simulation theorem, namely, Indexing [57], Inner-product and gap-Hamming [12], and several others [44], all admit such hitting distributions. But it may be seen that although Equality has a 0-hitting distribution, it fails to have any 1-hitting distribution.

The existence of such a counter-example was surprising to us, because in the case of the Switch relation, the Karchmer–Wigderson theorem and Grigni–Sipser theorem behave the same way (by lifting a decision-tree adversary for the Switch relation). The main purpose of this work was to understand what is happening.

1.3 Almost Conjecture 4

We will be able to prove a simulation theorem for composition with Equality, but for a notion different than decision-tree depth. In order to avoid long preliminaries for now, we postpone the full list of our results until the end of Section 2. However, one of our results is sufficiently close to what was already discussed, that it may be easily stated in the present section, and may thus serve as motivation for the remainder.

For a given relation $f \subseteq \{0, 1\}^p \times \mathcal{C}$, let $L^{dt}(f)$ denote the smallest number of leaves of any deterministic decision-tree which, given query access to $z \in \{0, 1\}^p$, finds a $c \in \mathcal{C}$ such that $(z, c) \in F$, whenever such a c exists. Notice that $D^{dt}(f) \geq \log L^{dt}(f)$, and so if Conjecture 4 were true, a consequence would be that $D^{cc}(f \circ \text{Eq}_n) = \Omega(n \cdot \log L^{dt}(f))$. The following theorem, thus, may be considered a weak variant of Conjecture 4:

³ A (δ, h) -hitting rectangle-distribution (for $\delta \in (0, 1)$ and $h \in \mathbb{N}$) is a distribution over rectangles such that a random rectangle from this distribution will intersect any 2^{-h} -large rectangle with probability $\geq 1 - \delta$. By a Boolean function g having (δ, h) -hitting monochromatic rectangle-distributions, we mean that there are two (δ, h) -hitting rectangle-distributions σ_0 and σ_1 , such that σ_c only samples rectangles which are c -monochromatic with respect to g .

► **Theorem 8** (Lifting for $\log L^{dt}$). *For any Boolean relation $f \subseteq \{0, 1\}^p \times \mathcal{C}$, whenever $n \geq 100 \cdot \log p$,*

$$D^{cc}(f \circ \text{Eq}_n) = \Omega\left(n \cdot \frac{\log L^{dt}(f)}{\log p}\right).$$

1.4 Organization

In Section 2 we state the definitions required to understand the statements of our results, and then state all our results in full; in this section we give the first new concept required by our results, namely the notion of 0-query complexity. In Section 3, we introduce the combinatorial invariants required to prove our main result, including the notion of *thickness*, which comes from Raz and McKenzie [57, 26, 12], but also the notion of *square*, which is the second new concept required by our proofs. In Section 4 we prove a *projection lemma* – the crucial lemma required to prove the simulation theorem – which is then proven in Section 5.

2 Preliminaries, and precise statements of our results

In this section we provide basic notations and precise statements of all our results.

We will assume the reader is familiar with various basic concepts pertaining to complexity of Boolean functions, namely: decision trees, query complexity, leaf complexity, protocol trees, communication complexity, combinatorial rectangles, and Fourier analysis of Boolean functions. See [45, 37] for reference.

We will be studying the decision-tree complexity of relations. A *Boolean relation* f is a subset of $\{0, 1\}^p \times \mathcal{C}$ where \mathcal{C} is a finite set; associated with f is the search problem where we are given a string $z \in \{0, 1\}^p$, and wish to find an element $c \in \mathcal{C}$ such that $(z, c) \in f$, if such an element exists.⁴ If to each z corresponds exactly one c , we call f a *total Boolean function*.

For a given Boolean relation, we let $D^{dt}(f)$, called the *query complexity* of f , be the minimum height of T , taken over deterministic decision-trees T which solve the search problem associated with f . We let $L^{dt}(f)$, called the *leaf complexity* of f , be the minimum number of leaves of T , again taken over deterministic decision-trees T which solve the search problem associated with f .

We will also be interested in the communication complexity of relations. A *two-player relation* F is a subset $F \subseteq \mathcal{A} \times \mathcal{B} \times \mathcal{C}$ where $\mathcal{A}, \mathcal{B}, \mathcal{C}$ are finite sets; associated with F is the communication problem where Alice is given $a \in \mathcal{A}$, Bob is given $b \in \mathcal{B}$, and they wish to find $c \in \mathcal{C}$ such that $(a, b, c) \in F$, if one such c exists. If $g \subseteq \mathcal{A} \times \mathcal{B} \times \{0, 1\}$ is a two-player relation such that to each pair $(a, b) \in \mathcal{A} \times \mathcal{B}$ corresponds exactly one $c \in \{0, 1\}$ with $(a, b, c) \in g$, we call g a *gadget*. The Equality and Indexing function defined in page 4 are examples of gadgets. A third example is the *Set-disjointness function* $\text{Disj}_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$, where $\text{Disj}_n(x, y) = 0$ iff $x_i = y_i = 1$ for some $i \in [n]$.

For a given two-player relation $F \subseteq \mathcal{A} \times \mathcal{B} \times \mathcal{C}$, we let $D^{cc}(F)$, called the *communication complexity* of F , be the height of the shortest deterministic protocol-tree for solving the communication problem associated with F .

⁴ Although when considering functions the difference between a total function and a partial function (a promise problem) is very important, this distinction is irrelevant when thinking more generally about relations, at least in computational models which are guaranteed to produce an output. Indeed, a partial Boolean relation $f \subseteq \{0, 1\}^n \times \mathcal{C}$ may be replaced by the total Boolean relation $f' = f \cup \{(x, c) \in \{0, 1\}^n \times \mathcal{C} \mid (x, c') \notin f \text{ for any } c' \in \mathcal{C}\}$, meaning if the input is outside the promise we allow the algorithm to output anything.

50:8 Lifting Theorems for Equality

The *composition* of a Boolean relation $f \subseteq \{0, 1\}^p \times \mathcal{C}$ with a gadget $g : \mathcal{A} \times \mathcal{B} \rightarrow \{0, 1\}$ is the two-player relation $f \circ g \subseteq \mathcal{A}^p \times \mathcal{B}^p \times \mathcal{C}$, given by

$$f \circ g = \{(a_1, \dots, a_p; b_1, \dots, b_p; c) \mid (g(a_1, b_1) \dots g(a_p, b_p), c) \in f\}.$$

The following definition is crucial to our result and, to our knowledge, has not been used prior to this work:

► **Definition 9.** *Given a deterministic decision-tree T over $\{0, 1\}^p$, the 0-depth of T is the maximum number of queries which are answered 0, in any root-to-leaf path of T . The 0-query complexity of f , denoted $D_0^{dt}(f)$, to be the smallest 0-depth of T , taken over deterministic decision-trees T which solve the search problem associated with f .*

It is unusual to make a query complexity notion depend on the specific outcome of the queries, instead of just the number of queries. However, the above notion is closely related to a notion analogous to parity decision-trees. Indeed, we may define AND decision-trees to be like parity decision-trees, but where the algorithm is allowed the query an AND of the input bits, instead of a parity of the input bits:

► **Definition 10.** *An AND decision-tree over $\{0, 1\}^p$ is a rooted tree where each internal node v is labeled by a set of variables $Q_v \subseteq [p]$ and each edge is labeled 0 or 1. As in the case of deterministic decision-tree, the execution of T on an input $z \in \{0, 1\}^p$ traces a path in this tree: at each internal node v the execution is given the value of the conjunction $q = \bigwedge_{i \in Q_v} z_i$, and follows the edge labeled q into one of v 's children. With each node v of the tree we may associate the set $S_v \subseteq \{0, 1\}^p$ of those inputs whose execution follows the path down to the node v ; the set S_v is given by a system of conjunctive equations.*

An AND decision-tree over $\{0, 1\}^p$ is said to solve the search problem associated with a Boolean relation $f \subseteq \{0, 1\}^p \times \mathcal{C}$ if, for every leaf v , there exists a choice of $c \in \mathcal{C}$ such that $(z, c) \in f$ for every $z \in S_v$.

Then, the AND-query complexity of f , denoted $D_{\text{AND}}^{dt}(f)$, is defined as the minimum depth of T , taken over AND decision-trees T which solve the search problem associated with f .

We are then able to establish the following relationship:

► **Lemma 11.** *Let $f \subseteq \{0, 1\}^p \times \mathcal{C}$ be any Boolean relation. Then*

$$D_{\text{AND}}^{dt}(f) \geq D_0^{dt}(f) \geq \frac{D_{\text{AND}}^{dt}(f)}{\lceil \log(p+1) \rceil}$$

Since these measures are within a $\log p$ factor of each other, it is possible to think of the more natural $D_{\text{AND}}^{dt}(f)$ as a proxy for $D_0^{dt}(f)$. The proof is simple, but is omitted due to space constraints (it appears in the full version of the paper [48]).

There is also a simple relation between 0-query complexity and leaf complexity. If a decision-tree over p bits never makes more than d zero-queries, each root-to-leaf path may be specified by the positions of the 0-answers along that path, so there are fewer than $\binom{p}{\leq d} \leq 2^{(d+1)\log p}$ leaves. Hence it follows:

► **Lemma 12.** *Let $f \subseteq \{0, 1\}^p \times \mathcal{C}$ be any Boolean relation. Then*

$$D_0^{dt}(f) \geq \frac{\log L^{dt}(f)}{\log p} - 1.$$

If $\log L^{dt}(f) = \Omega(p)$, we have $\binom{p}{\leq d} \geq 2^{\Omega(H_2(d/p) \cdot p)}$, and so $D_0^{dt}(f) = \Omega(p)$ also.

Lifting theorems for Equality. Our main result is a simulation theorem which lifts 0-query complexity of a Boolean relation $f \subseteq \{0, 1\}^p \times \mathcal{C}$ to the communication complexity $f \circ \text{Eq}_n$:

► **Theorem 13** (Lifting for D_0^{dt}). *Let $f \subseteq \{0, 1\}^p \times \mathcal{C}$ be any Boolean relation. Then, whenever $n \geq 100 \cdot \log p$,*

$$D^{cc}(f \circ \text{Eq}_n) = \Omega(n \cdot D_0^{dt}(f)).$$

The proof of Theorem 13 uses the notion of thickness from Raz-McKenzie [57], and a new invariant, called a *square*, which is inspired by Grigni-Sipser [28]. These notions are presented in Section 3.

Our proof is similar in flavor to Or Meir’s lower-bound for the direct-sum of the universal relation [50], although for that problem a rank argument will work [43].⁵

► **Remark 14.** It is not hard to verify that $D_0^{dt}(f) = 1$ when f is the counter-example to Conjecture 4, which we described in Section 1.2: a decision tree for f queries coordinates one at a time until it finds the first 0. Then it follows from Theorem 13 that the protocol for $f \circ \text{Eq}_n$ appearing in page 5 is optimal, up to constant factors.

Theorem 8 follows from Theorem 13 and Lemma 12. Theorem 13 and Lemma 11 give us the following:

► **Corollary 15** (Lifting for D_{AND}^{dt}). *Let $f \subseteq \{0, 1\}^p \times \mathcal{C}$ be any Boolean relation. Then, whenever $n \geq 100 \cdot \log p$, $D^{cc}(f \circ \text{Eq}_n) = \Omega\left(n \cdot \frac{D_{\text{AND}}^{dt}(f)}{\log p}\right)$.*

Lifting theorems for Set-disjointness. By a simple reduction, we are also able to show the first lifting theorem known for set-disjointness. Indeed, we may reduce an instance of Eq_n to an instance of Disj_{2n} . Alice maps each of her bits x_i into the pair of bits $a_i = (1 - x_i)x_i$, and Bob maps each of his bits y_i into $b_i = y_i(1 - y_i)$; it now holds that $x_i = y_i$ iff a_i and b_i are disjoint, and hence $\text{Eq}_n(x, y) = \text{Disj}_{2n}(a, b)$. As a corollary, we find:

► **Corollary 16** (Lifting for disjointness). *Let $f \subseteq \{0, 1\}^p \times \mathcal{C}$ be a Boolean relation and $n \geq 100 \cdot \log p$. Then $D^{cc}(f \circ \text{Disj}_n) = \Omega(n \cdot D_0^{dt}(f))$.*

Naturally, Theorem 8 and Corollary 15 will hold for Set-disjointness.

Lifting theorems for parity decision-trees. A composition with Equality, $f \circ \text{Eq}_n$, is a XOR function $f \circ \text{NOR}_n \circ \text{XOR}_2$. It is well known and easy to see that $D^{cc}(F \circ \text{XOR}_2) \leq D_{\oplus}^{dt}(F)$ [31], where $D_{\oplus}^{dt}(F)$ is the parity-query complexity of F . Hence a consequence of our lifting theorem for Equality in communication complexity is also a lifting theorem for the NOR function, with respect to parity decision-trees:

► **Corollary 17.** *For any Boolean relation $f \subseteq \{0, 1\}^p \times \mathcal{C}$, whenever $n \geq 100 \cdot \log p$, $D_{\oplus}^{dt}(f \circ \text{NOR}_n) = \Omega(n \cdot D_0^{dt}(f))$.*

It may be seen that $D_0^{dt}(f)$ cannot be replaced by $D^{dt}(f)$, by the same counter-example f of page 5.

⁵ Or Meir’s proof is similar to what one would obtain if one were to carry out our proof when f is the identity function, so our technique can be seen as a generalization of Meir’s. Of course in our case composition with identity would be just a larger equality, so the lower-bound follows trivially, whereas in the case of the universal relation the result is not trivial.

A solution to the tea-break puzzle. A lifting theorem such as Theorem 13 is a powerful tool for proving lower-bounds in communication complexity. The theorem is very general and many such results may be proven, but let us here give an example of lower-bound for a concrete problem in communication complexity.

Consider the Bob's example $F \circ \text{Eq}_n$ from the tea-break puzzle where Alice and Bob are each given p -many n -bit strings, with the promise that either all strings are different, or exactly one pair of strings is equal, and they wish to know which is the case.

We have $F(z) = 1$ when its input, z , has Hamming weight 0, and $F(z) = 0$ when z has Hamming weight 1. This is a partial function, so we may not use Lemma 6 to prove a lower-bound on it. However (this is the two-line proof): an adversary may answer 0 $p - 1$ times before fixing $F(z)$; hence $D_0^{dt}(F) \geq p - 1$, and it follows immediately from Theorem 13:

► **Corollary 18.** *Whenever $n \geq 100 \cdot \log p$, $D^{cc}(F \circ \text{Eq}_n) = \Omega(n \cdot p)$.*

To the best of our knowledge, there is currently no other way to establish this lower-bound.

3 Thickness and squares

Notation . If p is a natural number, we write $[p]$ for the set $\{1, \dots, p\}$. For sets A and B , we use $A \rightarrow B$ to denote the set of total functions from A to B . We write $f : A \rightarrow B$ to mean $f \in (A \rightarrow B)$. We also use B^A to denote the set of total functions from A to B , but in this case we think of them as A -indexed sequences of elements from B , and if we first write $f \in B^A$, instead of $f : A \rightarrow B$, we will later write f_a instead of $f(a)$. If $f : A \rightarrow B$ (or $f \in B^A$) and $A' \subseteq A$, then $f|_{A'}$ is the restriction of f to A' . A disjoint union is denoted by \sqcup , i.e. $A \sqcup B$ denotes the union of two disjoint sets A and B .

We will look at sets $A \subseteq (\{0, 1\}^n)^{[p]}$, and we will often want to think of some set of coordinates $I \subseteq [p]$ as being *alive*, and the corresponding complement $D = [p] \setminus I$ will be the set of *dead* coordinates. We will be working with partial assignments of elements from $(\{0, 1\}^n)^{[p]}$, which can be encoded as total functions from I to $\{0, 1\}^n$. Hence the following two definitions will be helpful.

► **Definition 19 (Join).** *Let $n \geq 1$ and $p \geq 2$ be integers, $\emptyset \neq I \subsetneq [p]$ and $D = [p] \setminus I$.*

If $s' \in (\{0, 1\}^n)^I$ and $s'' : (\{0, 1\}^n)^D$, then their join $s' \times s'' \in (\{0, 1\}^n)^{[p]}$ is given by:

$$(s' \times s'')_i = \begin{cases} s'_i & \text{if } i \in I \\ s''_i & \text{if } i \in D. \end{cases}$$

This notation is extended to subsets of $(\{0, 1\}^n)^I$ and $(\{0, 1\}^n)^D$ in the natural way.

If $i \in I \subseteq [p]$, $s' \in \{0, 1\}^n$ and $s'' \in (\{0, 1\}^n)^{I \setminus \{i\}}$, then their join at i is the sequence $s' \times_i s'' \in (\{0, 1\}^n)^I$ with $(s' \times_i s'')_i = s'$, and $\forall j \in I \setminus \{i\}$ $(s' \times_i s'')_j = s''_j$.

► **Definition 20.** *Let $n \geq 1$ and $p \geq 2$ be integers, $I \subseteq [p]$, $i \in I$ and $S \subseteq (\{0, 1\}^n)^I$. We define the projections: $S_i = \{s_i \mid s \in S\} \subseteq \{0, 1\}^n$ and $S_{\neq i} = \{s|_{I \setminus \{i\}} \mid s \in S\} \subseteq (\{0, 1\}^n)^{I \setminus \{i\}}$.*

Likewise if $\emptyset \neq E \subset I$, we define $S_E = \{s|_E \mid s \in S\} \subseteq (\{0, 1\}^n)^E$ and, for each $s'' \in (\{0, 1\}^n)^{I \setminus E}$, the extensions of s'' in S is the set $\text{Ext}_S(s'') = \{s' \in (\{0, 1\}^n)^E \mid s' \times s'' \in S\}$.

For a subset $U \subseteq \{0, 1\}^n$, the restriction of S to U at coordinate i is the set $S^{i,U} = \{s \in S \mid s(i) \in U\}$. We will also write $S_{\neq i}^{i,U}$ for the set $(S^{i,U})_{\neq i}$ (i.e. we first restrict the i -th coordinate then project onto the remaining coordinates in I): $S_{\neq i}^{i,U} = \{s|_{I \setminus \{i\}} \mid s \in S, s_i \in U\}$.

3.1 Thickness and its properties

The notion of *thickness* was first used by Raz and McKenzie in [57], and is by now a well-known notion. But whereas previously the notion of thickness was only looked at with respect to all coordinates simultaneously, we will be interested in the notion of thickness with respect to a subset of coordinates. This difference is non-essential, and all the relevant properties are proven mutatis mutandis. Due to space constraints, the proofs are omitted (but appear in the full version of the paper [48]).

► **Definition 21** (Aux graph, average and min-degrees). *Let $n \geq 1, p \geq 2$ be integers, $I \subseteq [p]$, and $S \subseteq (\{0, 1\}^n)^I$. For each $i \in I$, the aux graph $G(S, i)$ is the bipartite graph with left-side vertices S_i , right-side vertices $S_{\neq i}$ and edges corresponding to the set S , i.e., (s', s'') is an edge iff $s' \times_i s'' \in S$.*

We define the average degree of $G(S, i)$ to be the average right-degree: $d_{\text{avg}}(S, i) = \frac{|S|}{|S_{\neq i}|}$, and the min-degree of $G(S, i)$, to be the minimum right-degree: $d_{\text{min}}(S, i) = \min_{s'' \in S_{\neq i}} |\text{Ext}_S(s'')|$.

► **Definition 22** (Thickness and average thickness). *Let $n \geq 1, p \geq 2$ be integers, $\emptyset \neq F \subseteq I \subseteq [p]$, and $S \subseteq (\{0, 1\}^n)^I$. Then S is called τ -thick on F if $d_{\text{min}}(S, i) \geq \tau \cdot 2^n$ for all $i \in F$. (By convention an empty set S is τ -thick.) Similarly, S is called φ -average-thick on F if $d_{\text{avg}}(S, i) \geq \varphi \cdot 2^n$ for all $i \in F$. For $p = 1$, set S is τ -thick if $|S| \geq \tau \cdot 2^n$.*

We will need the following two lemmas. The proofs are similar to the analogous lemmas in [26].

► **Lemma 23** (Average thickness implies thickness). *Let $n \geq 1, p \geq 2$ be integers, $\emptyset \neq F \subseteq I \subseteq [p]$, and $S \subseteq (\{0, 1\}^n)^I$. If S is φ -average-thick on F , then for every $\delta \in (0, 1)$ there is a subset $S' \subseteq S$ which is $\frac{\delta}{p}\varphi$ -thick on F and has $|S'| \geq (1 - \delta) \cdot |S|$.*

A recent example by Kozachinskiy [44] shows that the $\frac{1}{p}$ loss in Lemma 23 is needed. This loss is the core reason why we need the gadget to have size $n = \Omega(\log p)$ in Theorem 13.

► **Lemma 24**. *Let $n \geq 1, p \geq 2$ be integers, $i \in F \subseteq I \subseteq [p]$, and $S \subseteq (\{0, 1\}^n)^I$ be τ -thick on F . Then for any set $U \subseteq \{0, 1\}^n$, $S_{\neq i}^{i, U}$ will also be τ -thick on $F \setminus \{i\}$, and $S_{\neq i}^{i, U}$ will be empty iff $U \cap S_i$ is empty.*

3.2 Squares

We will be interested in rectangles $R = A \times B$, where A, B both are subsets of $(\{0, 1\}^n)^{[p]}$, and which have a certain “square-like” structure. Such a “square-like” rectangle appears in our proofs, and will always be a sub-rectangle of the rectangle induced by a protocol.

A “square-like” rectangle $R = A \times B$, is one for which we have a set $I \subseteq [p]$ of *live* coordinates, with a corresponding set $D = [p] \setminus I$ of *dead* coordinates, and also a family $S \subseteq (\{0, 1\}^n)^I$, for which one can do the following:

*For any $s \in S$, there exist $\alpha(s), \beta(s) \in (\{0, 1\}^n)^D$, such that
 A is exactly the set of all $s \times \alpha(s)$ and B is exactly the set of all $s \times \beta(s)$,
and, furthermore, $\alpha(s)_i \neq \beta(t)_i$ for every $s, t \in S, i \in D$.*

i.e., given any s in S , which is a way of filling the live coordinates, there are two ways of filling the dead coordinates, $\alpha(s)$ and $\beta(s)$, such that the various $s \times \alpha(s)$ will be Alice’s side of the rectangle, and the various $s \times \beta(s)$ will be Bob’s side of the rectangle; furthermore, $\alpha(s)_i \neq \beta(t)_i$ always holds. We will call such a configuration a *square*:

50:12 Lifting Theorems for Equality

► **Definition 25 (Square).** A square is a tuple $\mathcal{S} = \langle n, p, R = A \times B, I, S, \alpha, \beta \rangle$ where:

- $n \geq 1, p \geq 2$ are integers;
- $R = A \times B$ where $A, B \subseteq (\{0, 1\}^n)^{[p]}$;
- $\emptyset \neq I \subseteq [p]$ is a non-empty set of so-called live coordinates, and
- $D = [p] \setminus I$ is the corresponding set of dead coordinates;
- $S \subseteq (\{0, 1\}^n)^I$;
- $\alpha : S \rightarrow (\{0, 1\}^n)^D$ and $\beta : S \rightarrow (\{0, 1\}^n)^D$ are such that $A = \{s \times \alpha(s) \mid s \in S\}$ and $B = \{s \times \beta(s) \mid s \in S\}$;
- for every $s \in S, t \in S, i \in D$, we have $\alpha(s)_i \neq \beta(t)_i$.

► **Definition 26.** The density of square $\mathcal{S} = \langle n, p, R = A \times B, I, S, \alpha, \beta \rangle$ is given by $\text{Density}(\mathcal{S}) = \frac{|S|}{2^{n|I|}}$.

► **Definition 27.** We say a square $\mathcal{S} = \langle n, p, R = A \times B, I, S, \alpha, \beta \rangle$ is τ -thick on $F \subseteq I$ if S is τ -thick on F , and is φ -average-thick on F if S is φ -average-thick on F .

One may justify the name *square* by the observation that a square $\mathcal{S} = \langle n, p, R = A \times B, I, S, \alpha, \beta \rangle$ induces a bijection between A and B , where $s \times \alpha(s) \in A$ corresponds to $s \times \beta(s) \in B$.

4 The projection lemma

The main technical lemma of our simulation theorem is a *projection lemma*, which allow us to constrain coordinates of a square while preserving thickness, in such a way that $\alpha(s)_i \neq \beta(t)_i$ always holds.

► **Lemma 28.** Let $\mathcal{S} = \langle n, p, R = A \times B, I, S, \alpha, \beta \rangle$ be a square and $\tau, \varphi \in [0, 1]$ be real numbers. Suppose that $p \leq \frac{1}{12} \cdot 2^{\tau \cdot 2^n}$. Suppose also that \mathcal{S} is τ -thick, but not φ -average-thick, on $F \subseteq I$.

Then, for any $z \in \{0, 1\}^F$, there exists a non-empty set $E = E(z) \subseteq F$ such that, letting $E_0 = \{i \in E \mid z_i = 0\}$, we may construct a square $\mathcal{S}' = \mathcal{S}'(z) = \langle n, p, R' = A' \times B', I', S', \alpha', \beta' \rangle$, where:

- (i) $A' \subseteq A$ and $B' \subseteq B$;
- (ii) $I' = I \setminus E_0$;
- (iii) $\text{Density}(\mathcal{S}') \geq (\frac{1}{2\varphi})^{|E_0|} \cdot \text{Density}(\mathcal{S})$; and
- (iv) \mathcal{S}' is $\frac{1}{2}\varphi$ -average-thick on $F \setminus E$.

Furthermore, the set $E = E(z) \subseteq F$ is obtained by a query procedure on the string z , and is exactly the set of positions queried by this procedure.

Proof. We will explain the projection procedure in three steps. The entire procedure is achieved by running Procedure 1, 2 and 3 one after another (see below).

To begin with, \mathcal{S} is not φ -average-thick on F , and so we are assured we will add at least one coordinate to E . Every time we add an index i to E we have, immediately prior to this, that $\frac{|S_{I \setminus E_0}|}{|S_{I \setminus (E_0 \cup \{i\})}|} \leq \varphi \cdot 2^n$, and hence $|S_{I \setminus (E_0 \cup \{i\})}| \geq \frac{|S_{I \setminus E_0}|}{\varphi \cdot 2^n}$. This means that if $z_i = 0$ and we then add i to E_0 , we will have $|S_{I \setminus E_0}|$ grow by a factor of $\varphi \cdot 2^n$. By the end of this process, $S_{I \setminus E_0}$ must be φ -average-thick on $F \setminus E$ (otherwise we would add another coordinate to E), and furthermore $|S_{I \setminus E_0}| \geq \frac{|S|}{(\varphi \cdot 2^n)^{|E_0|}}$, which is to say

$$\frac{|S_{I \setminus E_0}|}{2^{|I \setminus E_0| \cdot n}} \geq \frac{1}{\varphi^{|E_0|}} \cdot \frac{|S|}{2^{|I| \cdot n}}. \quad (*)$$

This will later ensure our density increase.

► **Procedure 1.** Choosing E .

- We start by letting $E = \emptyset$.
- As long as $S_{I \setminus E_0}$ is not φ -average-thick on $F \setminus E$, there exists some $i \in F \setminus E$ such that

$$\frac{|S_{I \setminus E_0}|}{|S_{I \setminus (E_0 \cup \{i\})}|} \leq \varphi \cdot 2^n.$$

- We will then add i to E and query z_i (to know if $i \in E_0$ or not).

► **Procedure 2.** Choosing $W = (U_i, V_i)_{i \in E_0}$, X and Y .

- Independently for each $i \in E_0$, choose a partition $\{0, 1\}^n = U_i \cup V_i$, so that each string $x \in \{0, 1\}^n$ is placed in U_i with probability $\frac{1}{2}$, and is placed in V_i otherwise. Let us use $W = (U_i, V_i)_{i \in E_0}$ to denote all the partitions chosen in this step.
- Now let us start by letting $X = Y = S$.
- Then for each index $i \in E_0$ in turn, we change X to $X_{\neq i}^{i, U_i}$ and change Y to $Y_{\neq i}^{i, V_i}$.

Now consider the Procedure 2. At the end of its execution, we have both $X, Y \subseteq S_{I \setminus E_0}$. Now we may ask how much of $S_{I \setminus E_0}$ survived inside both X and Y . Let us first consider the difficult case when $|E_0| \geq 1$. We make the following claim:

▷ **Claim 29.** If $|E_0| \geq 1$, then for some choice of the partitions $(U_i, V_i)_{i \in E_0}$ we will have $|X \cap Y| \geq \frac{1}{2} \cdot |S_{I \setminus E_0}|$.

Before proving this claim, let us see why it is enough to give us our new square \mathcal{S}' . Let $U \subseteq (\{0, 1\}^n)^{E_0}$ be the product of the various U_i sets, for $i \in E_0$, and likewise let $V \subseteq (\{0, 1\}^n)^{E_0}$ be the product of the various V_i sets, for $i \in E_0$. The square \mathcal{S}' is chosen thus:

► **Procedure 3.** Choosing the square \mathcal{S}' .

- We set $\mathcal{S}' = X \cap Y$.
- For each $s' \in \mathcal{S}'$, we choose a string $u(s') \in U \cap \text{Ext}_{\mathcal{S}}(s') \subseteq (\{0, 1\}^n)^{E_0}$; such a $u(s')$ exists because of how X was constructed; letting $s = s' \times u(s') \in \mathcal{S}$, for each $i \in [p] \setminus I' = ([p] \setminus I) \cup E_0$, set

$$\alpha'(s')_i = \begin{cases} u(s')_i & \text{if } i \in E_0, \\ \alpha(s)_i & \text{if } i \in [p] \setminus I. \end{cases}$$

- We proceed symmetrically to choose $\beta'(s')$.
- A' and B' are simply the images of \mathcal{S}' under α' and β' .

For any $s \in \mathcal{S}$, $t \in \mathcal{S}$ and $i \in ([p] \setminus I) \cup E_0$, we have $\alpha(s)_i \neq \beta(t)_i$. This follows, on coordinates $i \in E_0$ because U_i and V_i are disjoint, and on coordinates $i \in [p] \setminus I$ because square \mathcal{S} has the same property for α and β .

Properties (i) and (ii) are by construction. Property (iii) is a calculation using Claim 29 and (*):

$$\text{Density}(\mathcal{S}') = \frac{|\mathcal{S}'|}{2^{|I'| \cdot n}} \stackrel{\text{Claim 29}}{\geq} \frac{\frac{1}{2} \cdot |S_{I \setminus E_0}|}{2^{|I \setminus E_0| \cdot n}} \stackrel{\text{Using (*)}}{\geq} \frac{1}{2} \cdot \frac{1}{\varphi^{|E_0|}} \cdot \frac{|\mathcal{S}|}{2^{|I| \cdot n}} = \frac{1}{2} \cdot \frac{1}{\varphi^{|E_0|}} \cdot \text{Density}(\mathcal{S}).$$

50:14 Lifting Theorems for Equality

Now Property (iii) follows using the fact that $|E_0| \geq 1$. Property (iv) follows by Claim 29, because $S_{I \setminus E_0}$ is φ -average-thick on $F \setminus E$, and S' is a subset of $S_{I \setminus E_0}$ with $|S'| \geq \frac{1}{2} \cdot |S_{I \setminus E_0}|$.

In the simple case when $|E_0| = 0$, we have $X = Y = S$, and so we set S' to be exactly S . Properties (i) and (ii) are easy to check, and Property (iii) is trivial, and property (iii) holds even without the $1/2$ factor loss, by our choice of E .

Now to prove Claim 29. Let $\delta = 2^{-\tau \cdot 2^n}$. Let us think of a matrix M where the rows are indexed by the various possible $s' \in S_{I \setminus E_0}$ and the columns are indexed by the different possible choices $W = (U_i, V_i)_{i \in E_0}$. The entry $M(s', W)$ equals 1 if $s' \in X$, where X is obtained from S and $(U_i)_{i \in E_0}$ by Procedure 2. In other words, again denoting by U the product of the various sets U_i , we have $M(s', W) = 1$ iff $U \cap \text{Ext}_S(s') \neq \emptyset$.

Now fix some $s' \in S_{I \setminus E_0}$, and let us estimate the probability that $M(s', W) = 1$, i.e. that $s' \in X$, over the randomized choice of W . At the beginning of Procedure 2, we have $X = S$, and X is τ -thick on F . Then for each index $i \in E_0 \subseteq F$ in turn, we will change X to $X_{\neq i}^{i, U_i}$. Before we do this for the first time, s' will have at least one extension $s \in \text{Ext}_X(s') \subseteq (\{0, 1\}^n)^{E_0}$; at this point X is τ -thick on F , and so, taking any extension $s'' \in \text{Ext}_{X_{\neq i}}(s') \subseteq (\{0, 1\}^n)^{E \setminus \{i\}}$, there will be at least $\tau \cdot 2^n$ strings $s''' \in \{0, 1\}^n$ such that $(s' \times s'') \times_i s''' \in S$. Each of these strings s''' is placed in U_i with probability $1/2$; hence the probability that $(s' \times s'') \in X_{\neq i}^{i, U_i}$ is at least $1 - 2^{-\tau \cdot 2^n} = 1 - \delta$, i.e., some extension s'' of s' survived with at least $1 - \delta$ probability over the choice of this first U_i . By Lemma 24, changing X to $X_{\neq i}^{i, U_i}$ gives us a set which is again thick on $F \setminus \{i\}$. Hence we may apply the same reasoning to the next index in E_0 .

Changing X in this way $|E_0|$ times, we conclude that, in the end, $\Pr[M(s', W) = 1] = \Pr[s' \in X] \geq (1 - \delta)^{|E_0|} \geq 1 - |E_0|\delta$, where the probability is with respect to the distribution of W given by the above process. Now call a certain choice of W X -good if the W -column of M has at least a $1 - 3|E_0|\delta$ fraction of the rows $s' \in S_{I \setminus E_0}$ with $M(s', W) = 1$. Then, by a standard averaging argument, we must have $\Pr[W \text{ is } X\text{-good}] > 1/2$ (where again the probability is with respect to the distribution of W).

Arguing in the same way with respect to Y , we conclude that the probability that W is Y -good will also be more than $\frac{1}{2}$. Hence there must exist a choice of W which is both X -good and Y -good. For this choice of W we will have both $|X|, |Y| \geq (1 - 3|E_0|\delta)|S_{I \setminus E_0}|$, and given that $X, Y \subseteq S_{I \setminus E_0}$, this implies that $|X \cap Y| \geq (1 - 6|E_0|\delta) \cdot |S_{I \setminus E_0}| \geq (1 - 6p\delta) \cdot |S_{I \setminus E_0}|$. This is at least $\frac{1}{2}|S_{I \setminus E_0}|$ by our assumed bound on p . The claim is thus proven. \blacktriangleleft

► Lemma 30. *Let $S = \langle n, p, R = A \times B, I, S, \alpha, \beta \rangle$ be a square which is τ -thick on $F \subseteq I$, and let $z \in \{0, 1\}^p$ be such that $z_i = 1$ for every $i \in I \setminus F$, and $z_i = 0$ for every $i \in [p] \setminus I$. Then there exists some $(x, y) \in A \times B$ with $\text{Eq}^p(x, y) = z$.*

Proof. This is proven very similarly to Lemma 28. Instead of using Procedure 1 to choose E and E_0 , we choose them directly based on z .

If there are no $i_0 \in I$ with $z_{i_0} = 0$, then any $s \in S$ will give $\text{Eq}^p(s \times \alpha(s), s \times \beta(s)) = z$. Otherwise, let $E = F \setminus \{i_0\}$, so that $E_0 = \{i \in I \mid i \neq i_0, z_i = 0\}$. We may then use Procedure 2 to construct sets X and Y such that $X, Y \subseteq S_{I \setminus E_0}$. Note now that Claim 29 will still hold, because it only requires that S be thick on F . We may then use Procedure 3 to construct S' , and Properties (i) and (ii) will hold as before. S' is a square on coordinates $I \setminus E_0 = \{i \mid z_i = 1\} \cup \{i_0\}$. By Lemma 24, we know that S' is τ -thick on $\{i_0\}$ and thus there are two strings $s \in S'$ and $t \in S'$ with $s_{i_0} \neq t_{i_0}$ but $s_i = t_i$ for all $i \in I' \setminus \{i_0\}$. Then $x = s \times \alpha(s)$ and $y = t \times \beta(t)$ give us $\text{Eq}^p(x, y) = z$. \blacktriangleleft

5 Lifting 0-query complexity

We now prove our main simulation theorem (Theorem 13). Suppose $p \leq 2^{n/100}$, and let us fix $\tau = 2^{-n/10}$ and $\varphi = 2^{-n/20}$. Suppose we are given a C -bit communication protocol π for $f \circ \text{Eq}_n$. We will then construct a decision-tree τ for f . On input $z \in \{0, 1\}^p$, τ will find a leaf v of the protocol-tree of π , such that the associated rectangle R_v has some $(x, y) \in R_v$ with $\text{Eq}^p(x, y) = z$. The label of such a leaf then equals $f(\text{Eq}^p(x, y)) = f(z)$. We now present an informal description of τ , and in Algorithm 1 below we provide pseudocode for τ . We will then show that the algorithm for τ is correct, i.e. that it is always able to find such a leaf v , and then show that the number of 0-queries that τ makes is $O(\frac{C}{n})$, which completes the proof of Theorem 13.

Given an input $z \in \{0, 1\}^p$, τ starts traversing a path from the root of the protocol tree of π . A variable v is maintained, indicating the node of the protocol tree of π which is the current-node during the ongoing simulation; associated with v is the rectangle R_v of inputs which cause the protocol to reach node v . The decision-tree τ , when traversing node v , maintains a rectangle $R = A \times B$ and a square $\mathcal{S} = \langle n, p, R = A \times B, I = F \cup O, \mathcal{S}, \alpha, \beta \rangle$, such that R is a sub-rectangle of R_v . The set F corresponds to coordinates of the input z that were not queried yet, and O is set of coordinates i which have been queried and found to have $z_i = 1$. Throughout the execution of the algorithm, it is maintained as an invariant that the square \mathcal{S} is τ -thick in the coordinates F . At the beginning, $I = F = [p]$, $O = \emptyset$, and $A = B = (\{0, 1\}^n)^{[p]}$, so the invariant is trivially true.

In each iteration of the simulation, the algorithm checks whether \mathcal{S} is φ -average-thick on F . If this fails to hold, the algorithm will use the projection lemma (Lemma 28) and change \mathcal{S} to ensure this requirement, as follows. Using Procedure 1 of Lemma 28, it chooses the set $E \subseteq F$; this requires querying z_i for $i \in E$, and gives us the set $E_0 \subseteq E$ of coordinates where $z_i = 0$, and the set $E_1 = E \setminus E_0$ of coordinates where $z_i = 1$. The algorithm then uses Procedure 3 of Lemma 28 to construct a square \mathcal{S}' . Lemma 28 guarantees that \mathcal{S}' is $\frac{\varphi}{2}$ -average-thick on $F \setminus E$, and that $\text{Density}(\mathcal{S}')$ grows by a factor of $(2\varphi)^{-|E_0|}$. If E_0 is non-empty, i.e. if we have made some 0 queries, the density will grow significantly; otherwise the density will not change. The algorithm proceeds with $\mathcal{S} = \mathcal{S}'$, $I = I \setminus E_0$, $O = O \cup E_1$, and $F = F \setminus E$.

Now the algorithm is promised to have a square \mathcal{S} which is at least $\frac{1}{2}\varphi$ -average-thick. The algorithm then proceeds to a child v_c of v which has at least $1/2$ fraction of the density of \mathcal{S} , as follows. Suppose Alice communicated in v , and for each $c \in \{0, 1\}$, let $R_{v_c} = A_{v_c} \times B_{v_c}$ be the rectangle which π associates with v_c . We then fix a choice $c \in \{0, 1\}$ such that $|R \cap R_{v_c}| \geq |R|/2$. Now consider the set $S' = \{s \in \mathcal{S} \mid s \times \alpha(s) \in A_{v_c}\}$. This set is still $\frac{1}{4}\varphi$ -average-thick. We may then apply Lemma 23, with $\delta = \frac{1}{2}$, to S' , which gives us a subset $S'' \subseteq S'$ which is τ -thick on F . The new square \mathcal{S} is then given by restricting α and β to the set S'' . By changing \mathcal{S} in this way, we have preserved a $\frac{1}{4}$ fraction of the density.

Eventually, when we reach a leaf node v of the protocol tree, we are left with a square \mathcal{S} which is τ -thick on F . The algorithm outputs the labeling of R_v in π , and we will now argue that this must equal $f(z)$.

Correctness. Because π correctly solves $f \circ \text{Eq}^n$, then for each leaf v of π we have $(x, y, \pi(v)) \in f$ for all $(x, y) \in R_v$; the rectangle R obtained at the termination of Algorithm 1 is a sub-rectangle of R_v for a leaf of π , hence $(x, y, \pi(v)) \in f$ for all $(x, y) \in R$. On the other hand, we have preserved a square $\mathcal{S} = \langle n, p, R = A \times B, I, \mathcal{S}, \alpha, \beta \rangle$ which is τ -thick on $F \subseteq I$, and such that $z_i = 1$ for every $i \in O = I \setminus F$, and $z_i = 0$ for every $i \in [p] \setminus I$. Then Corollary 30 tells us that some pair $(x, y) \in R$ is such that $\text{Eq}^p(x, y) = z$; hence $(z, \pi(v)) \in f$.

- 7 Joshua Brody, Harry Buhrman, Michal Koucký, Bruno Loff, Florian Speelman, and Nikolay Vereshchagin. Towards a reverse Newman's theorem in interactive information complexity. In *Proceedings of the 28th CCC*, pages 24–33, 2013.
- 8 Harry Buhrman and Ronald de Wolf. Complexity measures and decision tree complexity: a survey. *Theoretical Computer Science*, 288(1):21–43, 2002.
- 9 Amit Chakrabarti and Oded Regev. An Optimal Lower Bound on the Communication Complexity of Gap-Hamming-Distance. *SIAM Journal on Computing*, 41(5):1299–1317, 2012.
- 10 Arkadev Chattopadhyay. Discrepancy and the Power of Bottom Fan-in in Depth-three Circuits. In *Proceedings of the 48th FOCS*, pages 449–458, 2007.
- 11 Arkadev Chattopadhyay and Anil Ada. Multiparty Communication Complexity of Disjointness. Technical Report TR08-002, ECCC, 2008.
- 12 Arkadev Chattopadhyay, Michal Koucký, Bruno Loff, and Sagnik Mukhopadhyay. Simulation Theorems via Pseudorandom Properties. *CoRR*, abs/1704.06807, 2017.
- 13 Arkadev Chattopadhyay, Michal Koucký, Bruno Loff, and Sagnik Mukhopadhyay. Simulation beats richness: new data-structure lower bounds. In *Proceedings of the 50th STOC*, pages 1013–1020. ACM, 2018.
- 14 Susanna F. de Rezende, Jakob Nordström, and Marc Vinyals. How Limited Interaction Hinders Real Communication. In *Proceedings of the 56th FOCS*, 2016.
- 15 Irit Dinur and Or Meir. Toward the KRW Composition Conjecture: Cubic Formula Lower Bounds via Communication Complexity. *Computational Complexity*, 27(3):375–462, 2018.
- 16 Andrew Drucker. Improved direct product theorems for randomized query complexity. *Computational Complexity*, 21(2):197–244, 2012.
- 17 Jeff Edmonds, Russell Impagliazzo, Steven Rudich, and Jirí Sgall. Communication complexity towards lower bounds on circuit depth. *Computational Complexity*, 10(3):210–246, 2001.
- 18 Tomás Feder, Eyal Kushilevitz, Moni Naor, and Noam Nisan. Amortized Communication Complexity. *SIAM Journal on Computing*, 24(4):736–750, 1995.
- 19 Ankit Garg, Mika Göös, Pritish Kamath, and Dmitry Sokolov. Monotone circuit lower bounds from resolution. In *Proceedings of the 50th STOC*, pages 902–911, 2018.
- 20 Dmitry Gavinsky, Troy Lee, and Miklos Santha. On the randomised query complexity of composition. *CoRR*, abs/1801.02226, 2018.
- 21 Dmitry Gavinsky, Or Meir, Omri Weinstein, and Avi Wigderson. Toward better formula lower bounds: an information complexity approach to the KRW composition conjecture. In *Proceedings of the 46th STOC*, pages 213–222, 2014.
- 22 Mika Göös, Rahul Jain, and Thomas Watson. Extension complexity of independent set polytopes. *SIAM Journal on Computing*, 47(1):241–269, 2018.
- 23 Mika Göös, TS Jayram, Toniann Pitassi, and Thomas Watson. Randomized Communication versus Partition Number. In *Proceedings of the 44th ICALP*, 2017.
- 24 Mika Göös, Pritish Kamath, Toniann Pitassi, and Thomas Watson. Query-to-communication Lifting for P^{NP} . In *Proceedings of the 32nd CCC*, 2017.
- 25 Mika Göös, Shachar Lovett, Raghu Meka, Thomas Watson, and David Zuckerman. Rectangles are nonnegative juntas. In *Proceedings of the 47th STOC*, pages 257–266. ACM, 2015.
- 26 Mika Göös, Toniann Pitassi, and Thomas Watson. Deterministic communication vs. partition number. In *Proceedings of the 56th FOCS*, 2015.
- 27 Mika Göös, Toniann Pitassi, and Thomas Watson. The landscape of communication complexity classes. *Computational Complexity*, pages 1–60, 2015.
- 28 Michelangelo Grigni and Michael Sipser. Monotone Separation of Logspace from NC. In *Proceedings of the 6th Annual Structure in Complexity Theory Conference*, pages 294–298, 1991.
- 29 Prahladh Harsha, Rahul Jain, David McAllester, and Jaikumar Radhakrishnan. The communication complexity of correlation. In *Proceedings of the 22nd CCC*, pages 10–23, 2007.
- 30 Johan Håstad and Avi Wigderson. Composition of the Universal Relation. In *Proceedings of the DIMACS Workshop*, pages 119–134, 1990.

- 31 Hamed Hatami, Kaave Hosseini, and Shachar Lovett. Structure of Protocols for XOR Functions. *SIAM Journal on Computing*, 47(1):208–217, 2018.
- 32 Rahul Jain. New strong direct product results in communication complexity. *Journal of the ACM*, 62(3):20, 2015.
- 33 Rahul Jain, Hartmut Klauck, and Ashwin Nayak. Direct product theorems for classical communication complexity via subdistribution bounds. In *Proceedings of the 40th STOC*, pages 599–608, 2008.
- 34 Rahul Jain, Attila Pereszlényi, and Penghui Yao. A direct product theorem for the two-party bounded-round public-coin communication complexity. In *Proceedings of the 53rd FOCS*, pages 167–176, 2012.
- 35 Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A direct sum theorem in communication complexity via message compression. In *Proceedings of the 20th ICALP*, pages 300–315, 2003.
- 36 Rahul Jain and Penghui Yao. A strong direct product theorem in terms of the smooth rectangle bound. *CoRR*, abs/1209.0263, 2012.
- 37 Stasys Jukna. *Boolean Function Complexity - Advances and Frontiers*. Springer, 2012.
- 38 Mauricio Karchmer, Eyal Kushilevitz, and Noam Nisan. Fractional Covers and Communication Complexity. *SIAM Journal on Discrete Mathematics*, 8(1):76–92, 1995.
- 39 Mauricio Karchmer, Ran Raz, and Avi Wigderson. Super-Logarithmic Depth Lower Bounds Via the Direct Sum in Communication Complexity. *Computational Complexity*, 5(3/4):191–204, 1995.
- 40 Mauricio Karchmer and Avi Wigderson. Monotone Circuits for Connectivity Require Super-Logarithmic Depth. *SIAM Journal on Discrete Mathematics*, 3(2):255–265, 1990.
- 41 Iordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jérémie Roland, and David Xiao. Lower bounds on information complexity via zero-communication protocols and applications. *SIAM Journal on Computing*, 44(5):1550–1572, 2015.
- 42 Pravesh K Kothari, Raghu Meka, and Prasad Raghavendra. Approximating rectangles by juntas and weakly-exponential lower bounds for LP relaxations of CSPs. In *Proceedings of the 49th STOC*, pages 590–603. ACM, 2017.
- 43 Alexander Kozachinskiy. Comment on Meir’s paper The Direct Sum of Universal Relations. Available at the address <https://eccc.weizmann.ac.il/report/2017/128/comment/1/download/>.
- 44 Alexander Kozachinskiy. From Expanders to Hitting Distributions and Simulation Theorems. In *Proceedings of the 43rd MFCS*, pages 4:1–4:15, 2018.
- 45 Eyal Kushilevitz and Noam Nisan. *Communication complexity*. Cambridge University Press, 1997.
- 46 James Lee, Raghu Meka, and Thomas Vidick. (Less) heavy lifting: from conic junta degree to non-negative rank. Presented in the workshop *Hardness Escalation in Communication Complexity and Query Complexity*, FOCS 2017.
- 47 Troy Lee, Adi Shraibman, and Robert Spalek. A Direct Product Theorem for Discrepancy. In *Proceedings of the 23rd CCC*, pages 71–80, 2008.
- 48 Bruno Loff and Sagnik Mukhopadhyay. Lifting Theorems for Equality. *Electronic Colloquium on Computational Complexity (ECCC)*, 25:175, 2018.
- 49 László Lovász. On the ratio of optimal integral and fractional covers. *Discrete mathematics*, 13(4):383–390, 1975.
- 50 Or Meir. The direct sum of universal relations. *Information Processing Letters*, 136:105–111, 2018.
- 51 Gatis Midrijanis. Exact quantum query complexity for total Boolean functions. *CoRR*, abs/quant-ph/0403168, 2004.
- 52 Alon Orlitsky. Worst-case interactive communication. I. Two messages are almost optimal. *IEEE Transactions on Information Theory*, 36(5):1111–1126, 1990.
- 53 Denis Pankratov. Direct sum questions in classical communication complexity. Master’s thesis, University of Chicago, 2012.

- 54 Toniann Pitassi and Robert Robere. Lifting nullstellensatz to monotone span programs over any field. In *Proceedings of the 50th STOC*, pages 1207–1219, 2018.
- 55 Anup Rao and Amir Yehudayoff. Simplified Lower Bounds on the Multiparty Communication Complexity of Disjointness. In *Proceedings of the 30th CCC*, pages 88–101, 2015.
- 56 Ran Raz. Fourier analysis for probabilistic communication complexity. *Computational Complexity*, 5(3-4):205–221, 1995.
- 57 Ran Raz and Pierre McKenzie. Separation of the Monotone NC Hierarchy. *Combinatorica*, 19(3):403–435, 1999.
- 58 Robert Robere. *Unified Lower Bounds for Monotone Computation*. PhD thesis, University of Toronto, 2018.
- 59 Robert Robere, Toniann Pitassi, Benjamin Rossman, and Stephen A Cook. Exponential lower bounds for monotone span programs. In *Proceedings of the 57th FOCS*, pages 406–415, 2016.
- 60 Swagato Sanyal. A Composition Theorem via Conflict Complexity. *CoRR*, abs/1801.03285, 2018. [arXiv:1801.03285](https://arxiv.org/abs/1801.03285).
- 61 Alexander A Sherstov. The pattern matrix method. *SIAM Journal on Computing*, 40(6):1969–2000, 2011.
- 62 Alexander A. Sherstov. The Communication Complexity of Gap Hamming Distance. *Theory of Computing*, 8(1):197–208, 2012.
- 63 Alexander A. Sherstov. The multiparty communication complexity of set disjointness. In *Proceedings of the 44th STOC*, pages 525–548, 2012.
- 64 Alexander A. Sherstov. Communication lower bounds using directional derivatives. In *Proceedings of the 45th STOC*, pages 921–930, 2013.
- 65 Yaoyun Shi and Yufan Zhu. Quantum communication complexity of block-composed functions. *Quantum Information & Computation*, 9(5):444–460, 2009.
- 66 Hing Yin Tsang, Chung Hoi Wong, Ning Xie, and Shengyu Zhang. Fourier Sparsity, Spectral Norm, and the Log-Rank Conjecture. In *Proceedings of the 54th FOCS*, pages 658–667, 2013.
- 67 Thomas Vidick. A concentration inequality for the overlap of a vector on a large set, with application to the communication complexity of the Gap-Hamming-Distance problem. *Chicago Journal of Theoretical Computer Science*, 2013, 2013.
- 68 Thomas Watson. A ZPP^{NP} Lifting Theorem. *Unpublished preprint*, 2017.
- 69 David P. Woodruff. *Efficient and private distance approximation in the communication and streaming models*. PhD thesis, Massachusetts Institute of Technology, 2007.
- 70 Andrew Chi-Chih Yao. Some Complexity Questions Related to Distributive Computing (Preliminary Report). In *Proceedings of the 11h STOC*, pages 209–213, 1979.