



# ON PUBLIC-COIN ZERO-ERROR RANDOMIZED COMMUNICATION COMPLEXITY

BEN DAVIS, HAMED HATAMI, WILLIAM PIRES, RAN TAO, AND HAMZA USMANI

**ABSTRACT.** Improving the exponential bound of [HHH21], we show that the largest possible gap between the deterministic communication complexity and the public-coin zero-error randomized communication complexity is at most polynomial. Previously, such a bound was known only in the private-coin model. The proof combines the approach of Gavinsky and Lovett [GL14] with new ideas.

**Keywords:** Zero-error, average case, communication complexity, Las Vegas

## 1. INTRODUCTION

The field of communication complexity studies the amount of communication required to solve the problem of computing discrete functions when the input is split between two or more parties. In the most commonly studied framework, there are two parties, often called Alice and Bob, and a communication problem is defined by a Boolean function  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$ . An input  $x \in \mathcal{X}$  is given to Alice, and an input  $y \in \mathcal{Y}$  is given to Bob. Together, they should both compute the entry  $f(x, y)$  by exchanging bits of information in turn, according to a previously agreed-on protocol. There is no restriction on their computational power; the only measure we care to minimize is the number of exchanged bits.

A deterministic protocol  $\pi$  specifies for each of the two players, the bit to send next, as a function of their input and history of the communication so far. It naturally corresponds to a binary tree as follows. Every internal node is associated with either Alice or Bob. If an internal node  $v$  is associated with Alice, then it is labeled with a function  $a_v : \mathcal{X} \rightarrow \{0, 1\}$ , which prescribes the bit sent by Alice at this node as a function of her input. After this bit was sent, the players move to the corresponding child of  $v$ : they move to the left child if the bit is 0, and to the right child if the bit is 1. Similarly, Bob's nodes are labeled with Boolean functions on  $\mathcal{Y}$ . Each leaf is labeled by 0 or 1, which corresponds to the output of the protocol. The *cost* of the protocol on an input  $(x, y)$ , denoted by  $\text{cost}(\pi(x, y))$ , is the number of bits exchanged on this input. The cost of the protocol is the maximum of  $\text{cost}(\pi(x, y))$  over all inputs  $(x, y)$ . The *deterministic communication complexity* of  $f$ , denoted by  $D(f)$ , is the smallest cost of a protocol that computes  $f$  correctly on all inputs.

Next, we discuss randomized communication complexity. Randomness can be introduced in two different ways: private randomness or public randomness.

A *private-coin randomized protocol* assumes that each player has access to his or her independent random bits and can use them to decide which bit to send next. More precisely, Alice and Bob have access to random strings  $R_A$  and  $R_B$ , respectively. These two strings are chosen independently, each according to some probability distribution described by the protocol. The bit sent by Alice at a node  $v$  is now determined as a function of both  $x$  and  $R_A$ . Similarly, the bits sent by Bob are determined as functions of  $y$  and  $R_B$ .

On the other hand, in the *public-coin* model, it is assumed that the players have access to a shared source of randomness. In other words, Alice and Bob are both given the same random string  $R$ . The public-coin model is stronger than the private-coin model as the former can simulate the latter by using  $R = (R_A, R_B)$  as the public random string.

In this article, we are interested in *zero-error* randomized communication protocols. There are two commonly used definitions for these protocols: one uses average communication complexity, and the other allows inconclusive outputs. The two definitions are equivalent up to a multiplicative constant. We will use the second definition since it is more convenient for our purposes: the output of a zero-error protocol is 0, 1, or  $\perp$ , where  $\perp$  indicates a failure to compute  $f(x, y)$ . The protocol must never output 0 or 1 erroneously;

---

HH was supported by an NSERC Discovery Grant.

however, on every input, it is allowed to output  $\perp$  with probability at most  $\frac{1}{2}$ . The cost of such a protocol is the maximum number of bits exchanged over all inputs and choices of randomness.

The private-coin zero-error randomized communication complexity of a function  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$ , denoted by  $R_0^{\text{prv}}(f)$ , is the infimum cost over all private-coin randomized protocols that compute  $f$  with zero error. The public-coin zero-error randomized communication complexity is defined similarly using public randomness and is denoted by  $R_0^{\text{pub}}(f)$ .

We have the trivial relations

$$R_0^{\text{pub}}(f) \leq R_0^{\text{prv}}(f) \leq D(f).$$

The quantity  $R_0^{\text{prv}}(f)$  is very well-understood (see [Für87]), but in this article, our focus is  $R_0^{\text{pub}}(f)$ . In particular, how small can  $R_0^{\text{pub}}(f)$  be compared to  $R_0^{\text{prv}}(f)$  and  $D(f)$ ?

Every function  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$  naturally corresponds to an  $\mathcal{X} \times \mathcal{Y}$  matrix with the  $xy$ -entries given by  $f(x, y)$ . A fundamental fact in communication complexity is that the leaves of every deterministic protocol computing  $f$  partitions this matrix into rectangles (a rectangle is a set  $S \times T \subseteq \mathcal{X} \times \mathcal{Y}$ ) such that the value of  $f$  is constant on each rectangle. Such rectangles are called *monochromatic*. Hence, every deterministic protocol of cost  $c$  provides a partition of  $\mathcal{X} \times \mathcal{Y}$  into at most  $2^c$  monochromatic rectangles, and since the rank (as a real matrix) of a monochromatic rectangle is at most one, we obtain the classical lower-bound

$$(1) \quad D(f) \geq \log \text{rk}(f),$$

where  $\text{rk}(f)$  denotes the rank of the matrix of  $f$  over the reals, and here and throughout the paper logarithms are in base 2.

Let  $N(f)$  denote the logarithm of the minimum number of monochromatic rectangles required to *cover*  $\mathcal{X} \times \mathcal{Y}$ . It follows from the above discussion that  $N(f) \leq D(f)$ , and furthermore as it is shown in [AUY83] (see also the proof of [KN97, Theorem 2.11]) the gap can be at most quadratic:

$$(2) \quad D(f) \leq 4N(f)^2.$$

The quantity  $N(f)$  can also be used to lower-bound  $R_0^{\text{prv}}(f)$ . Indeed, a zero-error private-coin protocol can be interpreted as a deterministic protocol (with three possible outputs  $\{0, 1, \perp\}$ ) where Alice's input is  $(x, R_A)$  and Bob's input is  $(y, R_B)$ . Hence the leaves of such a protocol provide a *partition*  $\mathcal{P}$  of  $(\mathcal{X} \times \Omega_A) \times (\mathcal{Y} \times \Omega_B)$  into monochromatic combinatorial rectangles, where  $\Omega_A$  and  $\Omega_B$  are the supports of the random strings  $R_A$  and  $R_B$ , respectively. We shall ignore the  $\perp$ -monochromatic rectangles, and focus on the set  $\mathcal{P}' \subseteq \mathcal{P}$  of 0- and 1-monochromatic rectangles in  $\mathcal{P}$ . For every such rectangle  $S \times T \in \mathcal{P}'$ , define  $\widehat{S} \times \widehat{T} \subseteq \mathcal{X} \times \mathcal{Y}$  as

$$\widehat{S} = \{x \in \mathcal{X} : \exists r_A \in \Omega_A, (x, r_A) \in S\}, \quad \widehat{T} = \{y \in \mathcal{Y} : \exists r_B \in \Omega_B, (y, r_B) \in T\}.$$

Since the protocol is of zero-error, every such  $\widehat{S} \times \widehat{T}$  is monochromatic, and moreover, every  $(x, y) \in \mathcal{X} \times \mathcal{Y}$  belongs to at least one such  $\widehat{S} \times \widehat{T}$ . Hence the set of all  $\widehat{S} \times \widehat{T}$  for  $S \times T \in \mathcal{P}'$  provides a cover of  $\mathcal{X} \times \mathcal{Y}$  with at most  $2^c$  monochromatic rectangles. Thus  $N(f) \leq \log 2^c = R_0^{\text{prv}}(f)$ . Combining this with Equation (2) yields

$$(3) \quad R_0^{\text{prv}}(f) = \Omega(\sqrt{D(f)}).$$

Furthermore, as it is shown by Fürer [Für87], there are examples for which this quadratic gap is necessary.

## 2. MAIN RESULT

Next, we turn our attention to the public-coin model, which is the main focus of this article. In general, private-coin and public-coin communication complexities of a function can behave very differently. For example, it is known [KN97, Lemma 3.8] that for every error-probability  $0 \leq \epsilon < \frac{1}{2}$ ,

$$R_\epsilon^{\text{prv}}(f) \leq D(f) \leq 2^{R_\epsilon^{\text{prv}}(f)} \left( \log_2 \left( \frac{1}{2} - \epsilon \right)^{-1} + R_\epsilon^{\text{prv}}(f) \right).$$

In contrast, the example of the equality function shows that for every  $\epsilon > 0$ , there are functions with  $R_\epsilon^{\text{pub}}(f) = O(1)$  that have arbitrarily large  $D(f)$ . *Can a similar gap hold for the case of zero-error?* The answer is negative. In [HHH21, Theorem 3], a Ramsey theoretic approach is used to prove that there is a dimension-free relation between  $R_0^{\text{pub}}(f)$  and  $D(f)$ , that is,

$$\Omega(\log D(f)) \leq R_0^{\text{pub}}(f) \leq D(f).$$

To be more precise, [HHH21, Theorem 3] states that  $\Omega(\log \text{rk}(f)) \leq R_0^{\text{pub}}(f)$ , which combined with the well-known upper bound  $D(f) \leq \text{rk}(f) + 1$  (see [RY20, Theorem 2.2]) yields the above lower bound.

In this article, we establish an improved polynomial relation between these two parameters.

**Theorem 2.1** (Main Theorem). *For every  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$  we have*

$$R_0^{\text{pub}}(f) = \Omega(D(f)^{\frac{1}{4}}).$$

### 3. PROOF OF THEOREM 2.1

Perhaps the most famous result relating public-coin and private-coin models is Newman's lemma [New91], which in the zero-error case (see [KN97, Exercise 3.15]) states

$$(4) \quad R_0^{\text{prv}}(f) \leq O(R_0^{\text{pub}}(f) + \log \log |\mathcal{X} \times \mathcal{Y}|).$$

To prove Theorem 2.1, it is tempting to apply Newman's lemma to replace  $R_0^{\text{prv}}(f)$  with  $R_0^{\text{pub}}(f)$  in Equation (3). However, this will not result in a dimension-free bound since  $\log \log |\mathcal{X} \times \mathcal{Y}|$  can be the dominant term in Equation (4).

The key insight for proving Theorem 2.1 is to consider the relation between  $\text{rk}(f)$  and  $D(f)$ . If  $\log \text{rk}(f)$  is small, then by applying a classical result of Nisan and Wigderson [NW95], one can deduce that  $D(f)$  cannot be much larger than  $R_0^{\text{pub}}(f)$ .

On the other hand, if  $\log \text{rk}(f)$  is large, then by Equation (1) one can consider a full-rank submatrix of  $f$  whose deterministic communication complexity is large as well. Since this submatrix is of full-rank, its dimensions are equal to its rank, and thus one can successfully apply Newman's lemma (the  $\log \log(\cdot)$  term will be small in Equation (4)) to obtain a strong lower-bound on its public-coin zero-error communication complexity.

The following lemma follows from the work of Nisan and Wigderson [NW95]. In the statement, for a rectangle  $A \subseteq \mathcal{X} \times \mathcal{Y}$ , we denote by  $|A|$  its set-theoretic cardinality.

**Lemma 3.1.** [NW95] *Let  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$  be a Boolean function, and  $\delta > 0$  a real number. Assume that for every rectangle  $A_1 \subseteq \mathcal{X} \times \mathcal{Y}$ , there exists a sub-rectangle  $A_2 \subseteq A_1$  such that  $A_2$  is monochromatic and  $|A_2| \geq \delta|A_1|$ . Then*

$$D(f) \leq O(\log(1/\delta) \log \text{rk}(f) + \log^2 \text{rk}(f)).$$

*Proof.* Denote  $r = \text{rk}(f)$ . Without loss of generality, we may assume that  $f$  has no repeated rows or columns, which in particular implies  $|\mathcal{X} \times \mathcal{Y}| \leq 2^{2r}$ .

By applying the assumption to  $A_1 = \mathcal{X} \times \mathcal{Y}$ , we find a monochromatic rectangle  $R \subseteq \mathcal{X} \times \mathcal{Y}$  of size at least  $\delta|\mathcal{X} \times \mathcal{Y}|$ . Consider the partition of the matrix of  $f$  as

$$f = \begin{bmatrix} R & S \\ P & Q \end{bmatrix}.$$

Since  $R$  is monochromatic, we have  $\text{rk}(R) \leq 1$ , and thus  $\text{rk}(S) + \text{rk}(P) \leq r + 1$ . Without loss of generality, we assume that  $\text{rk}(S) \leq r/2 + 1$ , as otherwise, we can switch the roles of the rows and columns. The row player sends one bit, indicating whether the input  $x$  is in the top part or in the bottom part of the matrix. If it is in the top part, then the rank decreases to  $\text{rk}([R \ S]) \leq \text{rk}(R) + \text{rk}(S) \leq \frac{r}{2} + 2$ . If it is in the bottom part, the size of the matrix reduces to at most  $(1 - \delta)|\mathcal{X} \times \mathcal{Y}|$ .

We construct a partial protocol tree by iterating the above process recursively and stopping as soon as the rank drops to  $\leq \frac{r}{2} + 2$ . Note that for every internal node, we immediately stop on one of the children, and decrease the size of the matrix by a factor of  $(1 - \delta)$  on the other child. Since for  $k = \frac{\log(|\mathcal{X} \times \mathcal{Y}|)}{\delta} \leq \frac{2r}{\delta}$ , we have  $(1 - \delta)^k |\mathcal{X} \times \mathcal{Y}| \leq e^{-\delta k} |\mathcal{X} \times \mathcal{Y}| \leq 1$ , this partial tree has at most  $O(\frac{2r}{\delta})$  leaves.

We constructed a partial protocol tree with  $O(\frac{2r}{\delta})$  leaves such that the rank of the sub-matrix corresponding to each leaf is at most  $\frac{r}{2} + 2$ . Applying this process recursively for  $O(\log(r))$  times decreases the rank to  $O(1)$  resulting in a deterministic communication protocol for  $f$  with  $(2r/\delta)^{O(\log(r))}$  leaves. In particular, the matrix of  $f$  can be partitioned into  $(2r/\delta)^{O(\log(r))}$  monochromatic rectangles. Now we can apply a standard tree-balancing procedure (i.e., [KN97, Lemma 2.8]) to conclude that

$$D(f) \leq \log \left( (2r/\delta)^{O(\log(r))} \right) = O(\log(1/\delta) \log r + \log^2 r).$$

□

In the following simple corollary, we observe that  $f$  satisfies the assumption of [Lemma 3.1](#) with  $\delta = 2^{-2R_0^{\text{pub}}(f)-1}$ .

**Corollary 3.2.** *There exists a universal constant  $c \geq 1$  such that every  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$  satisfies*

$$D(f) \leq cR_0^{\text{pub}}(f) \log \text{rk}(f) + c \log^2 \text{rk}(f).$$

*Proof.* Let  $\pi_R$  be a zero-error public-coin communication protocol of cost  $R_0^{\text{pub}}(f)$  for  $f$ . Here,  $R$  denotes the public randomness, and any fixation of  $R$  to a string  $r$  leads to a deterministic protocol  $\pi_r$  with three possible outputs  $\{0, 1, \perp\}$ . Since  $\Pr_R[\pi_R(x, y) \neq \perp] \geq \frac{1}{2}$  for every  $(x, y)$ , there exists a fixation of  $R$  to  $r$  such that

$$\Pr_{(x, y) \in A_1} [\pi_r(x, y) \neq \perp] \geq \frac{1}{2}.$$

In other words, the 0-leaves and 1-leaves of the protocol  $\pi_r$  contain at least half of the points in  $A_1$ . Since there are at most  $2^{-R_0^{\text{pub}}(f)}$  such leaves, one of them must contain at least  $2^{-R_0^{\text{pub}}(f)-1}|A_1|$  points in  $A_1$ . Thus  $f$  satisfies the assumption of [Lemma 3.1](#) with  $\delta = 2^{-2R_0^{\text{pub}}(f)-1}$ . □

To optimize our bound, instead of applying Newman's lemma, we apply the next lemma from [[DW07](#), Corollary 3.6], whose proof is almost identical to the proof of Newman's lemma.

**Lemma 3.3.** *Every Boolean function  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$  satisfies*

$$N(f) \leq R_0^{\text{pub}}(f) + \log \log |\mathcal{X}||\mathcal{Y}| + 1.$$

*Proof.* Let  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$  be a Boolean function and  $R_0^{\text{pub}}(f) = t$ , witnessed by a zero-error randomized protocol  $\pi_R$ .

Let  $\ell = \log(|\mathcal{X}||\mathcal{Y}|) + 1$  so that  $2^\ell > |\mathcal{X} \times \mathcal{Y}|$ , and consider  $\ell$  independent executions of  $\pi_R$  by considering  $\ell$  independent copies  $R_1, \dots, R_\ell$  of  $R$ . For every  $(x, y)$ , we have

$$\Pr_{R_1, \dots, R_\ell} [\forall i, \pi_{R_i}(x, y) = \perp] \leq \frac{1}{2^\ell} < \frac{1}{|\mathcal{X} \times \mathcal{Y}|}.$$

Hence there exists a choice of  $r_1, \dots, r_\ell$  such that for every  $(x, y) \in \mathcal{X} \times \mathcal{Y}$ , at least one  $i \in \{1, \dots, \ell\}$  satisfies  $\pi_{r_i}(x, y) \neq \perp$ . Since the protocol does not make errors  $\pi_{r_i}(x, y) = f(x, y)$ .

To obtain the desired bound on  $N(f)$ , observe that each  $\pi_{r_i}$  is a deterministic protocol with communication cost at most  $t$ , and thus provides a partition of the points  $(x, y)$  with  $\pi_{r_i}(x, y) \neq \perp$  into at most  $2^t$  monochromatic rectangles. Consequently, there exists a collection of  $\ell 2^t$  monochromatic rectangles whose union is all of  $\mathcal{X} \times \mathcal{Y}$ , or in other words,

$$N(f) \leq \log(\ell 2^t) = R_0^{\text{pub}}(f) + \log \log |\mathcal{X} \times \mathcal{Y}| + 1.$$

□

*Proof of [Theorem 2.1](#).* Let  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$  be a Boolean function, and let  $c \geq 1$  be the constant from [Corollary 3.2](#). We consider two cases.

**Case I:** In this case we assume

$$\log \text{rk}(f) \leq \frac{1}{2c} \sqrt{D(f)}.$$

By [Corollary 3.2](#), we have

$$D(f) \leq \frac{1}{2} R_0^{\text{pub}}(f) \sqrt{D(f)} + \frac{D(f)}{4},$$

which simplifies to

$$\sqrt{D(f)} \leq R_0^{\text{pub}}(f).$$

**Case II:** In this case we assume

$$\log \text{rk}(f) > \frac{1}{2c} \sqrt{D(f)}.$$

Denote  $m = 2^{\frac{1}{2c}\sqrt{D(f)}}$ . By the assumption,  $f$  contains a full-rank  $m \times m$  submatrix  $A$ . By [Equation \(2\)](#) and [Lemma 3.3](#), we have

$$\frac{\sqrt{D(A)}}{2} \leq N(A) \leq R_0^{\text{pub}}(f) + \log \log(m^2) + 1 \leq R_0^{\text{pub}}(f) + \log \log m + 2.$$

Combining this with the rank lower-bound (see [Equation \(1\)](#))

$$D(A) \geq \log \text{rk}(A) \geq \log m,$$

yields

$$\frac{\sqrt{\log m}}{2} - \log \log m - 2 \leq R_0^{\text{pub}}(f).$$

Substituting  $m = 2^{\frac{1}{2c}\sqrt{D(f)}}$ , we obtain

$$R_0^{\text{pub}}(f) = \Omega(D(f)^{1/4}).$$

□

#### 4. CONCLUDING REMARKS AND OPEN PROBLEMS

- We suspect that the bound in [Theorem 2.1](#) can be improved. Is it true that similar to private-coin model, for every function  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$ ,

$$(5) \quad R_0^{\text{pub}}(f) = \Omega(\sqrt{D(f)})?$$

Note that by Fürer's result [[Für87](#)] there are functions  $f$  for which  $R_0^{\text{pub}}(f) = \Theta(\sqrt{D(f)})$ , and thus [Equation \(5\)](#) is the strongest bound one can hope for.

- We are not aware of any examples separating  $N(f)$ ,  $R_0^{\text{prv}}(f)$ , and  $R_0^{\text{pub}}(f)$ . To the best of our knowledge, it could be the case that these parameters are within constant factors of each other. See also [[KN97](#), Problem 3.11].
- In the case where protocols are allowed to make error, the gap between the public-coin and private-coin randomized communication complexities can be arbitrarily large. For example, for the  $N \times N$  identity matrix  $\mathbf{I}_N$ , allowing an error probability of  $\frac{1}{3}$ , we have

$$R_{1/3}^{\text{pub}}(\mathbf{I}_N) = O(1), \quad R_{1/3}^{\text{prv}}(\mathbf{I}_N) = \Theta(\log \log N), \quad D(\mathbf{I}_N) = \Theta(\log N).$$

- [Corollary 3.2](#) shows that if  $\text{rk}(f)$  is small, then  $D(f)$  can be bounded from above by a function of  $R_0^{\text{pub}}(f)$ . Gavinsky and Lovett [[GL14](#)] show that this can be generalized to a similar bound for  $R_{1/3}^{\text{pub}}(f)$ , albeit with slightly worse parameters:

$$D(f) = O(R_{1/3}^{\text{pub}}(f) \log^2 \text{rk}(f)).$$

Acknowledgement. We wish to thank Manuel Stoeckl for pointing to us an error in an earlier version of this article. We thank the anonymous referee for the helpful comments and constructive remarks on this manuscript.

#### REFERENCES

- [AUY83] Alfred V. Aho, Jeffrey D. Ullman, and Mihalis Yannakakis. On notions of information transfer in vlsi circuits. In *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*, STOC '83, page 133–139, 1983.
- [DW07] Martin Dietzfelbinger and Henning Wunderlich. A characterization of average case communication complexity. *Information Processing Letters*, 101(6):245–249, 2007.
- [Für87] Martin Fürer. The power of randomness for communication complexity. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, STOC '87, page 178–181, 1987.
- [GL14] Dmitry Gavinsky and Shachar Lovett. En route to the log-rank conjecture: new reductions and equivalent formulations. In *Automata, languages, and programming. Part I*, volume 8572 of *Lecture Notes in Comput. Sci.*, pages 514–524. Springer, Heidelberg, 2014.
- [HHH21] Lianna Hambardzumyan, Hamed Hatami, and Pooya Hatami. Dimension-free bounds and structural results in communication complexity. *Israel J. Math.*, 2021. To appear.
- [KN97] Eyal Kushilevitz and Noam Nisan. *Communication complexity*. Cambridge University Press, Cambridge, 1997.

- [New91] Ilan Newman. Private vs. common random bits in communication complexity. *Inform. Process. Lett.*, 39(2):67–71, 1991.
- [NW95] Noam Nisan and Avi Wigderson. On rank vs. communication complexity. *Combinatorica*, 15(4):557–565, 1995.
- [RY20] Anup Rao and Amir Yehudayoff. *Communication Complexity: and Applications*. Cambridge University Press, 2020.

SCHOOL OF COMPUTER SCIENCE, MCGILL UNIVERSITY, MONTREAL, QC  
*Email address:* `benjamin.davis2@mail.mcgill.ca`

SCHOOL OF COMPUTER SCIENCE, MCGILL UNIVERSITY, MONTREAL, QC  
*Email address:* `hatami@cs.mcgill.ca`

SCHOOL OF COMPUTER SCIENCE, MCGILL UNIVERSITY, MONTREAL, QC  
*Email address:* `william.pires@mail.mcgill.ca`

DEPARTMENT OF MATHEMATICS AND STATISTICS, MCGILL UNIVERSITY, MONTREAL, QC  
*Email address:* `ran.tao6@mail.mcgill.ca`

SCHOOL OF COMPUTER SCIENCE, MCGILL UNIVERSITY, MONTREAL, QC  
*Email address:* `hamza.usmani@mail.mcgill.ca`