DE GRUYTER
OPEN

Annales Mathematicae Silesianae **29** (2015), 93–117
Prace Naukowe Uniwersytetu Śląskiego nr 3332, Katowice
DOI: 10.1515/amsil-2015-0008

# COMMUNICATION COMPLEXITY AND LINEARLY ORDERED SETS

Mieczysław Kula, Małgorzata Serwecińska

**Abstract.** The paper is devoted to the communication complexity of lattice operations in linearly ordered finite sets. All well known techniques ([4, Chapter 1]) to determine the communication complexity of the infimum function in linear lattices disappoint, because a gap between the lower and upper bound is equal to $\mathcal{O}(\log_2 n)$, where $n$ is the cardinality of the lattice. Therefore our aim will be to investigate the communication complexity of the function more carefully. We consider a family of so called interval protocols and we construct the interval protocols for the infimum. We prove that the constructed protocols are optimal in the family of interval protocols. It is still open problem to compute the communication complexity of constructed protocols but the numerical experiments show that their complexity is less than the complexity of known protocols for the infimum function.

## 1. Introduction

The model of the communication complexity was introduced by Yao [8] in 1979 and has been studied in many papers. Let $X, Y, Z$ be finite, nonempty sets. Two players Alice and Bob, know a function $f\colon X \times Y \to Z$. Alice is given $x \in X$ and Bob is given $y \in Y$. Their goal is to compute the value of $f(x, y)$. The players are allowed to communicate with each other. They have unlimited computational power and local computations are free. The communication between Alice and Bob proceeds according to a deterministic protocol $\mathcal{P}$ which

*Received: 24.07.2014. Revised: 21.03.2015.*
(2010) Mathematics Subject Classification: 68Q17, 68Q25.
*Key words and phrases:* communication complexity, linear lattice, communication protocol, interval protocol.

depends on the function $f$. The communication complexity of the function $f$ denoted by $D(f)$ is the minimum length of $\mathcal{P}$ over all protocols $\mathcal{P}$ for $f$.

A *(communication) protocol* $\mathcal{P}$ is defined as a binary rooted tree such that every internal node $v$ is labeled either by a function $a_v\colon X \to \{0,1\}$, where $a_v(x)$ is the bit sent by Alice or by a function $b_v\colon Y \to \{0,1\}$, where $b_v(y)$ is the bit sent by Bob. Every leaf is labeled by an element $z \in Z$. For a given input $(x,y) \in X \times Y$ the players walk along the protocol tree beginning from the root and at each internal node they take the left subtree if $a_v(x) = 0$ or $b_v(y) = 0$ and the right subtree if $a_v(x) = 1$ or $b_v(y) = 1$. The protocol is terminated when the players reach a leaf. If $f\colon X \times Y \to Z$ and for every input $(x,y) \in X \times Y$ the leaf reached by the players is labeled by $f(x,y)$, then we say that $\mathcal{P}$ is a *protocol for the function* $f$.

The *length of the protocol* $\mathcal{P}$ for the function $f$, denoted by $D_{\mathcal{P}}(f)$, is defined as the height of the tree, i.e., the number of bits communicated during the course of $\mathcal{P}$ on the worst-case input $(x,y) \in X \times Y$. The *communication complexity* of $f$, denoted by $D(f)$, is the minimum length of $\mathcal{P}$, over all protocols $\mathcal{P}$ for $f$. In other words, the communication complexity of the function $f$ is the least number of bits exchanged by the players for those inputs which require the largest exchange of information. We denote the communication complexity of the function $f$ by $D(f)$. Any protocol for $f$ of the length $D(f)$ is said to be *optimal*. In general, optimal protocols are not determined uniquely.

Notice that elements of the sets $X, Y, Z$ can be encoded as binary sequences of length $\lceil \log_2 |X| \rceil$, $\lceil \log_2 |Y| \rceil$, $\lceil \log_2 |Z| \rceil$, respectively. The simplest protocol for the function $f$ on an input $(x,y)$ will be as follows: Alice sends her input $x$ to Bob - this takes $\lceil \log_2 |X| \rceil$ bits, hence Bob can evaluate $f(x,y)$ and sends the result to Alice - this takes $\lceil \log_2 |Z| \rceil$ bits. In order to optimize this protocol we assume:

- if $|X| = 1$, then Bob sends $f(x,y)$ to Alice.
- if $|Y| < |Z|$, then Bob sends $y$ instead of $f(x,y)$ to Alice.
- if $|Y| < |X|$ and $|Z| \leq |X|$, then the players change roles.

Hence, if $|X| \leq |Y|$, then

$$D(f) \leq \lceil \log_2 |X| \rceil + \min\{\lceil \log_2 |Y| \rceil, \lceil \log_2 |Z| \rceil\}.$$

This protocol is called *trivial*.

A (combinatorial) rectangle in $X \times Y$ is a subset $R \subseteq X \times Y$ such that $R = A \times B$ for some $A \subseteq X$ and $B \subseteq Y$. A subset $R \subseteq X \times Y$ is called $f$-monochromatic if $f$ restricted to $R$ is constant. Yao showed that any protocol $\mathcal{P}$ for $f$ induces a partition of $X \times Y$ into $t$ pairwise disjoint $f$-monochromatic rectangles, where $t$ is the number of leaves of $\mathcal{P}$. This fact implies the following result.

LEMMA 1.1 ([8, Theorem 1], [4, Lemma 1.16]). *If any partition of $X \times Y$ into $f$-monochromatic rectangles requires at least $t$ rectangles, then $D(f) \geq \lceil \log_2 t \rceil$.*

Finite lattices are very important combinatorial structures with many applications, so communication complication of lattice problems deserve research. Several results on communication complexity in the lattice of all subsets of a finite set can be found in the literature. This paper is motivated by [1], where the communication complexity of lattice operations is considered in general. Ahlswede, Cai and Tamm [1] studied the functions $\text{DISJ}(x, y) = 1$ if $x \wedge y = 0_{min}$ and $\text{DISJ}(x, y) = 0$, otherwise, $\text{INF}(x, y) = x \wedge y$ and $\text{RANK}(x, y) = r(x \wedge y)$, where $0_{min}$ is the minimum element of the lattice and $r$ is the rank function. In the case of geometric lattices the determined values of $D(\text{DISJ})$ and $D(\text{INF})$ are exact and $D(\text{RANK})$ is estimated up to one bit. These results are based on the trivial protocols and the rank method introduced by Mehlhorn and Schmidt in [6]. The technique developed in [1] cannot be applied to many other important lattices. For example the lattice $\Delta(n)$ of all divisors of a positive integer $n$ with $a \wedge b = \gcd(a, b)$ and $a \vee b = \text{lcm}(a, b)$ is not geometric, unless $n$ is square-free. It turns out that the existence of long linearly ordered intervals in non-geometric lattices is the main obstacle in extending the methods applied in [1] to a wider class of lattices.

It is easy to see that in the case of linearly ordered lattices $D(\text{DISJ}) = 2$ and the functions INF and RANK are equivalent. Hence it is enough to compute the communication complexity of INF. From [1, Corollary 2] we have $\lceil \log_2(2n-1) \rceil \leq D(\text{INF}) \leq 2\lceil \log_2 n \rceil$ so the difference between the lower and upper bound is equal $\mathcal{O}(\log_2 n)$, where $n$ is the cardinality of the lattice. Computing the communication complexity of the function INF will be a step to compute the communication complexity of the gcd of two integers and the intersection of two multisets. Protocols computing INF in a finite linear lattice were used in [2] for constructing algorithms with incentive compatibility in environments with self-interested players considered. The authors presented a fast protocol which establishes much better upper bound $D(\text{INF}) = \log_2 n + \mathcal{O}(\log_2 \log_2 n)$. In this paper we consider the family of so called interval protocols and we construct optimal interval protocols for the function INF. The class of interval protocols was also considered by Kushilevitz and Nisan [4, Exercise 1.18]. The numerical experiments show that the protocol presented in [2] is not optimal. The length of the interval protocol developed here is smaller than the length of the protocol of [2] (cf. Table 1).

## 2. Interval communication complexity

In this section we introduce interval protocols and review some properties of interval communication complexity of the function INF which will be helpful in building optimal protocols. We shall assume throughout that $X, Y, Z$ are all finite sets and $X, Y$ are linearly ordered.

DEFINITION 2.1. A protocol for $f\colon X \times Y \to Z$ such that the sets $a_v^{-1}(0)$, $a_v^{-1}(1)$ are intervals of $X$, and the sets $b_v^{-1}(0)$, $b_v^{-1}(1)$ are intervals of $Y$ for each node $v$, will be referred to as an *interval protocol*.

Without loss of generality we can consider only interval protocols with increasing labeling functions, i.e. if $x_1 < x_2$, then $a_v(x_1) \leq a_v(x_2)$ and if $y_1 < y_2$, then $b_v(y_1) \leq b_v(y_2)$. If a node is labeled by a decreasing function, then we swap the left and the right subtrees of this node. This operation does not change the height of the tree. It is easy to see that under some obvious assumption the trivial protocol is an interval protocol.

The *interval communication complexity* of a function $f\colon X \times Y \to Z$, denoted by $D^*(f)$, is defined as the minimum length of interval protocols for $f$. Let us note that $D^*(f) \geq D(f)$. Every interval protocol for $f$ with the smallest length will be referred to as an *optimal interval protocol*.

The aim of this paper is to study optimal interval protocols for INF in finite linearly ordered lattice $X$ which can be identified with an interval of the set of integers. To do this we need to investigate a more general case. We consider the function INF$\colon \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by INF$(x, y) = \min(x, y)$ restricted to $X \times Y$, where $X$ and $Y$ are arbitrary finite intervals of $\mathbb{Z}$. The interval communication complexity of such function will be denoted by $D^*(X, Y)$.

From now on, we assume that a protocol means an interval protocol, unless we explicitly say otherwise. Throughout the paper all intervals are assumed to be finite.

Let $A \subseteq X$, $B \subseteq Y$ and let $\mathcal{P}$ be a protocol for a function $f\colon X \times Y \to Z$. The protocol $\mathcal{P}$ induces a protocol $\mathcal{P}'$ for the function $f \restriction A \times B$, (the restriction of $f$ to $A \times B$). The labeling functions of $\mathcal{P}'$ are defined by $a'_v = a_v \restriction_A$ and $b'_v = b_v \restriction_B$. This operation may produce inaccessible nodes, which can be removed from the tree. Every node labeled by a constant function can be stick together with its unique child. These operations makes the tree simpler without affecting the values determined by the protocol. The obtained protocol $\mathcal{P}'$ will be called the *restriction of* $\mathcal{P}$ *to* $A \times B$. The protocol $\mathcal{P}$ will also be referred to as an *extension* of $\mathcal{P}'$. Obviously the length of $\mathcal{P}'$ does not exceed the length of $\mathcal{P}$.

Obviously, if $A \subseteq X$ and $B \subseteq Y$, then the restriction of an interval protocol defined for inputs in $X \times Y$ to $A \times B$ is also an interval protocol.

For a function $f\colon X \times Y \to Z$ one can define a function $f^T\colon Y \times X \to Z$ as follows $f^T(y,x) = f(x,y)$ for all $(y,x) \in Y \times X$. Similarly, given a protocol $\mathcal{P}$ for $f$, one can define a protocol $\mathcal{P}^T$ of $f^T$ by changing the roles of Alice and Bob, i.e. the labeling functions $a_v^T$ and $b_v^T$ are equal to $b_v$ and $a_v$, respectively. Obviously the protocols $\mathcal{P}$ and $\mathcal{P}^T$ have the same length. The protocol $\mathcal{P}^T$ will be called the *transposed protocol*.

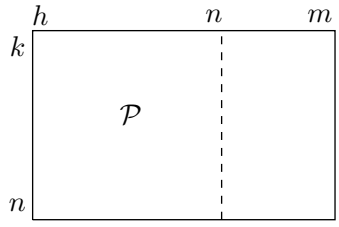
Let us observe that $\text{INF}(x,y) = \text{INF}(x-k, y-k) + k$, for any $x, y, k \in \mathbb{Z}$. Recall the notation $A + k = \{a + k \in \mathbb{Z} \ : \ a \in A\}$ for $A \subseteq \mathbb{Z}$ and $k \in \mathbb{Z}$. For a given protocol $\mathcal{P}$ for INF restricted to $X \times Y$ one can define the *shifted protocol* $\mathcal{P}^{[k]}$ for the function INF restricted to $(X+k) \times (Y+k)$. It is enough to make the following modification of the labeling functions and the labels of leaves of $\mathcal{P}$:

- if $a_v\colon X \to \{0,1\}$ is assigned to the node $v$ of $\mathcal{P}$, then the function $a_v^{[k]} : X + k \to \{0,1\}$ assigned to the node $v$ in the protocol tree $\mathcal{P}^{[k]}$ is defined by $a_v^{[k]}(x) = a_v(x-k)$;
- if $b_v\colon Y \to \{0,1\}$ is assigned to the node $v$ of $\mathcal{P}$, then the function $b_v^{[k]} : Y + k \to \{0,1\}$ assigned to the node $v$ in the protocol tree $\mathcal{P}^{[k]}$ is defined by $b_v^{[k]}(y) = b_v(y-k)$;
- the labels of leaves are increased by $k$.

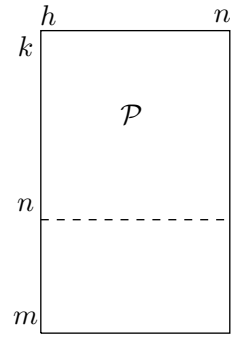
Obviously, the lengths of the protocols $\mathcal{P}$ and $\mathcal{P}^{[k]}$ are the same for all $k \in \mathbb{Z}$. Hence $D^*(X+k, Y+k) = D^*(X,Y)$.

Let us consider some properties of interval protocols which can be helpful in building optimal protocols.

LEMMA 2.2. *Let $k, h, n, m \in \mathbb{Z}$ and $k, h \le n \le m$. Every protocol for* INF *restricted to $[k,n] \times [h,n]$ can be extended without change of the length to protocols for* INF *restricted to the sets $[k,n] \times [h,m]$ and $[k,m] \times [h,n]$.*




The set of inputs of $\mathcal{Q}'$




The set of inputs of $\mathcal{Q}''$

PROOF. Let $\mathcal{P}$ be a protocol for INF restricted to $[k,n]\times[h,n]$. It is easy to see that $\text{INF}(x,y)=\text{INF}(x,n)$ for $x\in[k,n]$ and $y\in[n,m]$. The protocol $\mathcal{Q}'$ for INF restricted to $[k,n]\times[h,m]$ can be constructed in the following way:

(1) make a copy of the protocol tree $\mathcal{P}$,
(2) change the functions assigned to Bob's nodes – if the node $v$ is labeled by the function $b_v\colon[h,n]\to\{0,1\}$, then the node $v$ of the tree protocol $\mathcal{Q}'$ is labeled by the function $b'_v\colon[h,m]\to\{0,1\}$ defined as

$$b'_v(y)=\begin{cases}b_v(y) & \text{for } h\le y<n,\\ b_v(n) & \text{for } n\le y\le m.\end{cases}$$

Changing similarly the functions assigned to Alice's nodes in $\mathcal{P}$ yields the protocol $\mathcal{Q}''$ for INF restricted to $[k,m]\times[h,n]$. Obviously, the lengths of the resultant protocols are equal to the length of $\mathcal{P}$. □

The protocols $\mathcal{Q}'$ and $\mathcal{Q}''$ obtained in the above proof will be called the *natural extensions* of $\mathcal{P}$.

COROLLARY 2.3. *If the intervals $[k,m]$, $[h,n]$ of $\mathbb{Z}$ are not disjoint, then*

$$D^*([k,m],[h,n])=D^*([k,l],[h,l]),$$

*where $l=\min\{m,n\}$.*

PROOF. It is enough to notice that the intervals $[k,l]$, $[h,l]$ are nonempty and apply the above lemma. □

REMARK 2.4. If the intervals $[k,m]$, $[h,n]$ are disjoint and let us say $m<h$, then the interval $[h,l]$ is empty. It is easy to check that $D^*([k,m],[h,n])=D^*([k,m],\{m\})$.

The above lemma says that all inputs $(x,y)\in X\times Y$ such that $x$ or $y$ is greater than $\max(X\cap Y)$ can be neglected while we determine the communication complexity. This means that it is enough to consider only pairs of intervals $X,Y$ such that $\max X=\max Y$, in particular one of the interval is contained in the other one. In this case we can extend the observation made above that the communication complexity depends only on the number of elements in $X$ and $Y$. If $|X|=n$, $|Y|=m$ and $\max X=\max Y$, then we write $D^*(n,m)$ instead of $D^*(X,Y)$. Obviously, $D^*$ considered as a function of two variables is symmetric and increasing with respect to each variable separately.

The set $X\times Y=[m-n,m-1]\times[0,m-1]$ is called the *standard* $(n,m)$-*rectangle*. The function INF restricted to the standard $(n,m)$-rectangle will be denoted by $R(n,m)$. The function $R(n,m)$ will be often identified with the

matrix $[\text{INF}(x,y)]_{(x,y)\in X\times Y}$. To simplify the notation, the function $R(n,n)$ will be denoted by $S(n)$ and the interval communication complexity of $S(n)$ will be denoted by $D^*(n)$.

Let $X$ be an interval of $\mathbb{Z}$. A pair $(X_0, X_1)$ of intervals will be called a *cut* of $X$ if $X_0 \cup X_1 = X$ and $x_0 < x_1$ for all $x_i \in X_i$, $i = 0, 1$. Let $\mathcal{P}$ be an interval protocol and let the root $r$ of $\mathcal{P}$ be labeled by the function $a_r : X \to \{0,1\}$, and $X_i = a_r^{-1}(i)$ for $i = 0, 1$. Then $(X_0, X_1)$, is a cut determined by the first step of the protocol $\mathcal{P}$ and the restrictions of $\mathcal{P}$ to $(X_0, Y)$ and $(X_1, Y)$ match to the left and right subtrees of $\mathcal{P}$, respectively. It is obvious that for every cut $(X_0, X_1)$ of $X$ we have

$$D^*(X,Y) \le 1 + \max\{D^*(X_0,Y), D^*(X_1,Y)\}. \tag{1}$$

A similar inequality we have for every cut $(Y_0, Y_1)$ of $Y$.

PROPOSITION 2.5. *Let $n, m, k \in \mathbb{Z}$ and $k < m$, then*

$$D^*(n,m) \le 1 + \max\{D^*(\ell(n-k), m-k), D^*(n,k)\}$$

*where $\ell(n-k) = \max\{1, n-k\}$.*

PROOF. Let $X = [m-n, m-1]$, $Y = [0, m-1]$, $Y_0 = [0, m-k-1]$ and $Y_1 = [m-k, m-1]$. Observe that $(Y_0, Y_1)$ is a cut of $Y$. Hence from the inequality (1) for the cut $(Y_0, Y_1)$ of $Y$ we get

$$\begin{aligned} D^*(n,m) = D^*(X,Y) &\le 1 + \max\{D^*(X,Y_0), D^*(X,Y_1)\} \\ &= 1 + \max\{D^*(X,Y_0), D^*(n,k)\}. \end{aligned}$$

Observe that $X \cap Y_0 = \emptyset$ if and only if $n - k \le 0$. Hence if $n - k \le 0$ then by Remark 2.4 $D^*(X,Y_0) = D^*(1, m-k)$ else by Corollary 2.3 $D^*(X,Y_0) = D^*([m-n, m-k-1], [0, m-k-1]) = D^*(n-k, m-k)$. In the both cases we have $D^*(X,Y_0) = D^*(\ell(n-k), m-k)$. □

In Lemma 2.14 we will prove that in the above proposition the equality holds if $k$ is suitably chosen.

The following lemma slightly improves the lower bound of the communication complexity obtained from the counting monochromatic rectangles. To simplify notation we omit INF when we say about INF-monochromatic rectangles in the table of values of the function INF restricted to $X \times Y$.

LEMMA 2.6. *For every integer $n \ge 3$ we have $D^*(n) \ge 1 + \lceil \log_2(\frac{4}{3}n - 1) \rceil$. In particular, if $l \ge 3$ and $n \ge 2^l - 1$, then $D^*(n) \ge l + 2$.*

PROOF. Assume $X = [0, n-1]$. To prove the lemma, we consider any protocol $\mathcal{P}$ for INF restricted to $X \times X$. Running the protocol Alice sends her first message to Bob. The message determines a cut $(X_0, X_1)$ of $X$ where $X_0 = [0, n-k-1]$ and $X_1 = [n-k, n-1]$ for a suitable $k \in X$. Let us consider two tables of values of INF:

$$K_0 = [\mathrm{INF}(x,y)]_{(x,y)\in X_0\times X}$$
$$K_1 = [\mathrm{INF}(x,y)]_{(x,y)\in X_1\times X}.$$

It is easy to check that the number of monochromatic rectangles of $K_0$ is at least $2(n-k)-1$ and the number of monochromatic rectangles of $K_1$ is at least $n+k-1$. Hence by [4, Corollary 1.17]

$$D_{\mathcal{P}}(n) \geq 1 + \lceil \log_2 \max\{n+k-1, 2(n-k)-1\} \rceil .$$

For $k \geq \frac{n}{3}$ it holds that $n+k-1 \geq 2(n-1)$. This implies

$$\max\{n+k-1, 2(n-k)-1\} = \begin{cases} n+k-1 & \text{for } k \geq \frac{n}{3}, \\ 2(n-k)-1 & \text{for } k < \frac{n}{3}. \end{cases}$$

The sequence $(n+k-1)_{k=1,2,\ldots,n-1}$ is strictly increasing, so $n+k-1 \geq \frac{4}{3}n-1$ for $k \geq \frac{n}{3}$. The sequence $(2(n-k)-1)_{k=1,2,\ldots,n-1}$ is strictly decreasing, so $2(n-k)-1 \geq \frac{4}{3}n-1$ for $k < \frac{n}{3}$. Thus

$$D_{\mathcal{P}}(n) \geq 1 + \left\lceil \log_2 \left( \frac{4}{3}n - 1 \right) \right\rceil$$

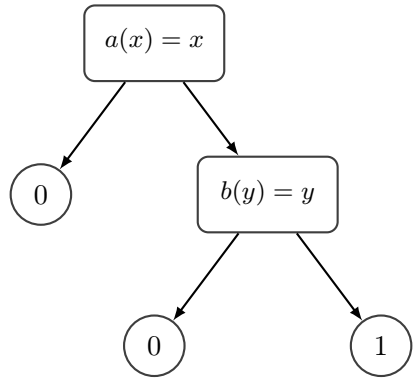
for arbitrary protocol $\mathcal{P}$, as required.

The second statement follows immediately. □

EXAMPLE 2.7. The communication complexity of

$$S(2) = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

is equal to 2. Indeed, every partition of $S(2)$ requires of at least 3 monochromatic rectangles. Hence $D^*(2) \geq D(2) \geq \lceil \log_2 3 \rceil = 2$. On the other hand, the length of the following protocol for $S(2)$ is equal to 2, so $D^*(2) = D(2) = 2$.




EXAMPLE 2.8. (a) The matrix $R(1,m)$ is equal to $\begin{bmatrix} 0 & 1 & \dots & m-1 \end{bmatrix}$. It easy to see that every partition of $R(1,m)$ consists of $m$ monochromatic rectangles. Hence $D^*(1,m) \geq \lceil \log_2 m \rceil$. On the other hand, the value of $\text{INF}(m-1,n)$ for some $n \in [0,m-1]$, can be computed by the trivial protocol. Its length is equal to $\lceil \log_2 m \rceil$. Hence $D^*(1,m) = D(1,m) = \lceil \log_2 m \rceil$.

(b) It is easy to see that the minimal number of monochromatic rectangles in the matrix $R(2,m)$ is equal to $m+1$. So $D^*(2,m) \geq \lceil \log_2(m+1) \rceil$. The trivial protocol for $R(2,2^s)$ has length $s+1$ so we have $D^*(2,2^s) = s+1$. If $2^{s-1} < m < 2^s$ then $D^*(2,m) = s$. Indeed, by the induction we have $s \leq D^*(2,m) \leq 1 + \max\{D^*(1,2^{s-1}), D^*(2,m-2^{s-1})\} = s$, as $m - 2^{s-1} < 2^{s-1}$.

LEMMA 2.9. *Let $n,m$ be positive integers with $n \geq 2$ or $m \geq 2$. Then $D^*(n+1,m+1) \leq D^*(n,m) + 1$.*

PROOF. Without loss of generality one can assume that $m \geq 2$. It is easy to see that the number of monochromatic rectangles in $R(n,m)$ is greater than or equal to $m+n-1$, so

$$D^*(n,m) \geq \lceil \log_2(m+n-1) \rceil \geq \lceil \log_2(n+1) \rceil .$$

Hence and from Example 2.8(a) we have $D^*(n+1,1) = \lceil \log_2(n+1) \rceil \leq D^*(n,m)$.

Applying Proposition 2.5 yields

$$D^*(n+1,m+1) \leq 1 + \max\{D^*(n,m), D^*(n+1,1)\} = 1 + D^*(n,m),$$

so the lemma is proved. □

The following lemma shows that the length of protocols for INF restricted to $X \times Y$ can be smaller when in the first turn the longer of the intervals $X$ and $Y$ is divided.

LEMMA 2.10. *Let $X, Y$ be intervals of $\mathbb{Z}$ and let $X \subseteq Y$. For every protocol $\mathcal{P}$ for* INF *restricted to $X \times Y$ with the root labeled by Alice's function there exists a protocol $\mathcal{Q}$ computing the same function with the root labeled by Bob's function such that $D_{\mathcal{Q}}(X, Y) \leq D_{\mathcal{P}}(X, Y)$.*

PROOF. Let $X = [m_1, m_2]$ and $Y = [n_1, n_2]$. The assumption $X \subseteq Y$ implies $n_1 \leq m_1 \leq m_2 \leq n_2$. If $m_1 = m_2$, then the lemma is obvious. Let us assume $m_1 < m_2$. First, we consider the case $m_2 = n_2$. Let $\mathcal{P}$ be a protocol for INF on $X \times Y$ such that at the first step Alice divides the interval $X$ into two disjoint intervals $X_0 = [m_1, l-1]$ and $X_1 = [l, m_2]$, where $l$ is an integer in $(m_1, m_2]$. Next, the players run the protocol $\mathcal{P}_0$ for $\text{INF}|_{X_0 \times Y}$ or $\mathcal{P}_1$ for $\text{INF}|_{X_1 \times Y}$ depending on Alice's input (Figure 1a). The protocols $\mathcal{P}_0$ and $\mathcal{P}_1$ are obtained from $\mathcal{P}$ by removing the root and distinguishing its children as the roots of the subtrees. Obviously $D_{\mathcal{P}}(X, Y) = 1 + \max\{D_{\mathcal{P}_0}(X_0, Y), D_{\mathcal{P}_1}(X_1, Y)\}$. Let $Y_0 = [n_1, l-1]$.

Denote by $\mathcal{P}'_0$ the restriction of $\mathcal{P}_0$ to $X_0 \times Y_0$ (Figure 1b). Now we construct a new protocol $\mathcal{Q}$. In the first step Bob divides the interval $Y$ into two disjoint intervals $Y_0 = [n_1, l-1]$ and $Y_1 = [l, n_2]$. Next, depending on Bob's input the players run the protocol $\mathcal{Q}_0$ for $\text{INF}|_{X \times Y_0}$ or $\mathcal{Q}_1$ for $\text{INF}|_{X \times Y_0}$ (Figure 1c) defined as follows. The protocol $\mathcal{Q}_0$ is the natural extension of $\mathcal{P}'_0$ to $X \times Y_0$. According to Lemma 2.2 we have $D_{\mathcal{Q}_0}(X, Y_0) = D_{\mathcal{P}'_0}(X_0, Y_0) \leq D_{\mathcal{P}_0}(X_0, Y)$.

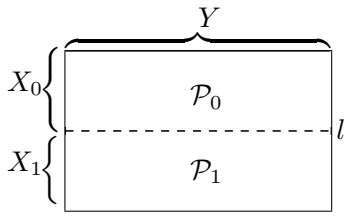



Figure 1a. The protocol $\mathcal{P}$

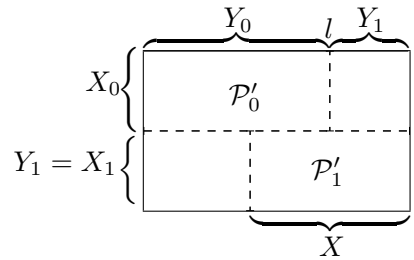



Figure 1b. Transition from $\mathcal{P}$ to $\mathcal{Q}$

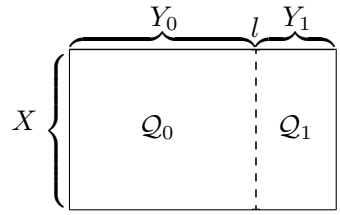



Figure 1c. The protocol $\mathcal{Q}$

Recall $Y_1 = [l, n_2] = [l, m_2] = X_1$. The transposition of $X \times Y_1$ is equal to $Y_1 \times X$ which is a subset of $X_1 \times Y$ because $X \subseteq Y$. Denote by $\mathcal{P}_1'$ the restriction of $\mathcal{P}_1$ to $[l, m_2] \times [m_1, m_2] = Y_1 \times X$ (Figure 1b).

The protocol $\mathcal{Q}_1$ is defined to be the transpose of $\mathcal{P}_1'$. Hence $D_{\mathcal{Q}_1}(X, Y_1) \leq D_{\mathcal{P}_1}(X_1, Y)$. Thus we have

$$\begin{aligned} D_{\mathcal{Q}}(X, Y) &= 1 + \max\{D_{\mathcal{Q}_0}(X, Y_0), D_{\mathcal{Q}_1}(X, Y_1)\} \\ &\leq 1 + \max\{D_{\mathcal{P}_0}(X_0, Y), D_{\mathcal{P}_1}(X_1, Y)\} = D_{\mathcal{P}}(X, Y). \end{aligned}$$

In the general case, according to Lemma 2.2 the protocol $\mathcal{Q}'$ constructed as above for the restriction of $\mathcal{P}$ to the set $X \times [n_1, m_2]$ can be extended to the protocol $\mathcal{Q}$ for INF restricted to $X \times Y$ without increasing its length. □

We shall prove two lemmata which form a basis for determining interval communication complexity. Let us recall the notation $\ell(x) = \max\{1, x\}$ for every $x \in \mathbb{Z}$.

LEMMA 2.11. *Let $k, m, n$ be positive integers such that $k, n \leq m$. If*

$$D^*(\ell(n-k), m-k) = D^*(n, k) = s - 1$$

*then $D^*(n, m) = s$.*

PROOF. Proposition 2.5 implies $D^*(n, m) \leq 1 + \max\{D^*(\ell(n-k), m-k), D^*(n, k)\} = s$. Let $X, Y$ be intervals of $\mathbb{Z}$ with $|X| = n$, $|Y| = m$, $\max X = \max Y$ and let $\mathcal{P}$ be a protocol for INF restricted to $X \times Y$. By Lemma 2.10 we can assume that Bob divides in his first turn the interval $Y$ into two disjoint subintervals $Y_0$, $Y_1$ of $m - h$, $h$ elements, respectively. Let $\mathcal{P}_0$ and $\mathcal{P}_1$ be the left and the right subtrees of the protocol $\mathcal{P}$. If $h = |Y_1| \geq k$, then $D_{\mathcal{P}_1}(X, Y_1) \geq D^*(n, h) \geq D^*(n, k) = s - 1$. If $h \leq k$, then $D_{\mathcal{P}_0}(X, Y_0) \geq D^*(X, Y_0) \geq D^*(\ell(n-h), m-h) \geq D^*(\ell(n-k), m-k) = s - 1$. Hence in both the cases we have

$$D_{\mathcal{P}}(X, Y) = 1 + \max\{D_{\mathcal{P}_0}(X, Y_0), D_{\mathcal{P}_1}(X, Y_1)\} \geq s.$$

Thus $D_{\mathcal{P}}(X, Y) \geq s$ for all the protocols, which completes the proof. □

EXAMPLE 2.12. We shall determine $D^*(3)$. Consider $X = [0, 2]$, $Y_0 = [0, 1]$, and $Y_1 = \{2\}$. We have already shown that $D^*(X, Y_0) = D^*(2) = 2$ and $D^*(X, Y_1) = D^*(3, 1) = 2$. Applying Lemma 2.11 yields $D^*(3) = D(3) = 3$.

Let $n$ be a positive integer. A positive integer $m$ such that $D^*(n, m) < D^*(n, m+1)$ will be referred to as an *$n$-threshold number*.

LEMMA 2.13. *Let $n \leq m$ be positive integers. Let $0 < k < m$ be an $n$-threshold number and $D^*(\ell(n-k), m-k) > D^*(n,k) = s-1$, then $D^*(n,m) \geq s+1$.*

PROOF. Let $X, Y$ be intervals of $\mathbb{Z}$ with $|X| = n$, $|Y| = m$, $\max X = \max Y$ and let $\mathcal{P}$ be a protocol for INF restricted to $X \times Y$. By Lemma 2.10 we can assume that in the first step of $\mathcal{P}$ Bob divides the interval $Y$ into two disjoint subintervals $Y_0$, $Y_1$ of $m-h$ and $h$ elements, respectively. Let $\mathcal{P}_0$ and $\mathcal{P}_1$ be the left and the right subtrees of the protocol $\mathcal{P}$. Then $D_{\mathcal{P}}(X,Y) = 1 + \max\{D_{\mathcal{P}_0}(X,Y_0), D_{\mathcal{P}_1}(X,Y_1)\}$.

If $h = |Y_1| > k$, then $D_{\mathcal{P}_1}(X,Y_1) \geq D^*(n,h) > D^*(n,k) = s-1$, since $k$ is an $n$-threshold number. Hence $D_{\mathcal{P}}(n,m) \geq 1 + D_{\mathcal{P}_1}(n,h) \geq s+1$. If $h \leq k$, then $D_{\mathcal{P}}(X,Y) \geq 1 + D_{\mathcal{P}_0}(X,Y_0) \geq D^*(\ell(n-k), m-k) \geq s+1$. This shows that the length of every protocol for INF restricted to $X \times Y$ is at least $s+1$, as required. □

LEMMA 2.14. *If $m, n$ are positive integers with $n \leq m$, then there exists a positive integer $k < m$ such that $D^*(\ell(n-k), m-k) \geq D^*(n,k)$ and $D^*(n,m) = 1 + D^*(\ell(n-k), m-k)$.*

PROOF. Let $X, Y$ be intervals of $\mathbb{Z}$ with $|X| = n$, $|Y| = m$ and $\max X = \max Y$. According to Lemma 2.10 we can assume that the first step of an optimal protocol $\mathcal{P}$ for INF restricted to $X \times Y$ determines a cut $(Y_0, Y_1)$ of $Y$. Let $\mathcal{P}_0$ and $\mathcal{P}_1$ be the restrictions of $\mathcal{P}$ to $X \times Y_0$ and $X \times Y_1$, respectively. Let us denote $h = |Y_1|$. Applying Proposition 2.5 we obtain

$$\begin{aligned} D^*(n,m) = D^*(X,Y) &= 1 + \max\{D_{\mathcal{P}_0}(X,Y_0), D_{\mathcal{P}_1}(X,Y_1)\} \\ &\geq 1 + \max\{D^*(X,Y_0), D^*(X,Y_1)\} \\ &= 1 + \max\{D^*(\ell(n-h), m-h), D^*(n,h)\} \geq D^*(n,m). \end{aligned}$$

If $D^*(\ell(n-h), m-h) \geq D^*(n,h)$, then $D^*(n,m) = 1 + D^*(\ell(n-h), m-h)$ and the proof is complete.

Otherwise, let us take the smallest positive integer $h'$ with $D^*(\ell(n-h'), m-h') < D^*(n,h')$. Since $h' \leq h$, we have $1 + D^*(n,h) = D^*(n,m) \leq 1 + \max\{D^*(\ell(n-h'), m-h'), D^*(n,h')\} = 1 + D^*(n,h') \leq 1 + D^*(n,h)$, so $D^*(n,m) = 1 + D^*(n,h')$. Obviously, setting $k = h' - 1$ we obtain $D^*(\ell(n-k), m-k) \geq D^*(n,k)$. Thus $1 + D^*(n,h') = D^*(n,m) \leq 1 + \max\{D^*(\ell(n-k), m-k), D^*(n,k)\} = 1 + D^*(\ell(n-k), m-k)$. Hence applying Lemma 2.9 yields $D^*(\ell(n-h'), m-h') + 1 \leq D^*(n,h') \leq D^*(\ell(n-k), m-k) = D^*(\ell(n-h'+1), m-h'+1) \leq D^*(\ell(n-h'), m-h') + 1$, which implies $D^*(n,h') = D^*(\ell(n-k), m-k)$ and $D(n,m) = 1 + D^*(n,h') = 1 + D^*(\ell(n-k), m-k)$, as required. □

Now we define some functions, which will be helpful in building optimal protocols. Let $\mathbb{N}$ denote the set of positive integers. Let us define the functions: $\tau_i\colon \mathbb{N}\to\mathbb{N}$, $\kappa_e\colon \mathbb{N}\to\mathbb{N}$ and $\mu\colon \mathbb{N}\to\mathbb{N}$ in the following way

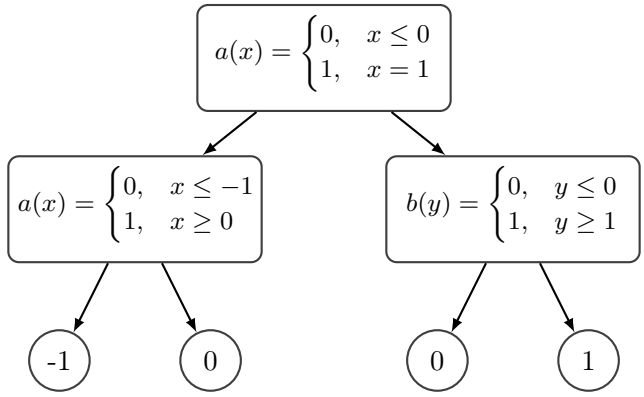
$$\tau_0(1)=2,\quad \tau_i(1)=2^i,\quad i\geq 1,$$
$$\tau_i(n)=\max\{m : D^*(n,m)=D^*(n)+i\},\quad i\geq 0,\ n\geq 2,$$
$$\mu(1)=1,\quad \mu(s)=\min\{m : D^*(m)=s\},\quad s\geq 2,$$
$$\kappa_e(2)=1,\quad \kappa_e(n)=\max\{k : D^*(k)<D^*(n-e)\wedge D^*(k)=D^*(k,n)\}\cup\{0\},$$
$$n\geq 3,\ e=0,1.$$

To simplify the notation we write $\tau(n)$ instead of $\tau_0(n)$.

It is worth noticing that $D^*(n)=s$ for all $\mu(s)\leq n<\mu(s+1)$. In other words, $n=\mu(s)$ is the least integer such that the interval communication complexity of $S(n)$ equals $s$. Although $D^*(1)=0$, assuming $\mu(1)=1$ makes many further relation true for all positive integers. Moreover $\tau_i(n)$ are $n$-threshold numbers for $i=0,1,2,\ldots$. In other words $m=\tau_i(n)$ is the greatest integer such that the interval communication complexity of $R(n,m)$ equals $i$ plus the interval communication complexity of $S(n)$.

Finally, it is easy to check that $\kappa_e(n)=\max\{k : D^*(k)<D^*(n-e)\wedge \tau(k)\geq n\}\cup\{0\}$, $n\in\mathbb{N}$, $e=0,1$. The values $\kappa_0(n),\kappa_1(n)$ play a crucial role in the protocols described in Section 3, as they determine the first step of Alice.

Example 2.15. Let us compute $\tau(2)$. The protocol tree presented in Example 2.7 can be extended to the protocol tree for $R(3,2)$ i.e., for INF restricted to $[-1,1]\times[0,1]$ in the following way.




Hence we have $2=D^*(2)\leq D^*(2,3)\leq D_{\mathcal{P}}(3,2)\leq 2$. On the other hand, the matrix $R(2,m)$ consists of at least 5 monochromatic rectangles for $m\geq 4$, so $D^*(2,m)\geq 3$. Thus $\tau(2)=3$.

By Example 2.12 we have $D^*(3,6) \geq D^*(3) = 3$. On the other hand by Proposition 2.5 we get $D^*(3,6) \leq 1 + \max\{D^*(1,4), D^*(3,2)\} = 3$. If $m > 6$ then $D^*(1,m) = \lceil \log_2 m \rceil > D^*(3,2) = 2$ and 2 is a 3-threshold number, so by Lemma 2.13 we have $D^*(3,m) \geq 4$. This shows that $\tau(3) = 6$.

LEMMA 2.16. *Let $s_0, r_0$ be positive integers such that $\tau(m_0) \geq m_0 + r_0$ for $m_0 = \mu(s_0+1) - 1$. Then $\tau(n) \geq n + r_0$ for all $n \geq \mu(s_0)$.*

PROOF. It is enough to prove $D^*(n, n+r_0) = D^*(n)$, for $n \geq \mu(s_0)$. If $\mu(s_0) \leq m \leq m_0$, then $D^*(m) = D^*(m_0)$ and $D^*(m,\tau(m_0)) \leq D^*(m_0,\tau(m_0))$. So $\tau(m) \geq \tau(m_0) \geq m_0 + r_0$. Thus $\tau(m) \geq m + (m_0 - m) + r_0 \geq m + r_0$.

Further we proceed by induction on $s$. Let us consider a positive integer $n$ such that $s = D^*(n) > s_0$. By Lemma 2.14 there is $k < n$ such that $D^*(n-k) \geq D^*(n,k)$ and $D^*(n) = 1 + D^*(n-k)$. Hence $D^*(n-k) = D^*(n) - 1 = s-1 \geq s_0$. Applying the induction hypothesis yields $\tau(n-k) \geq n-k+r_0$, i.e., $D^*(n-k) = D^*(n-k, n-k+r_0) = s-1$ and $D^*(n,k) \leq D^*(n-k) = s-1$. Applying Proposition 2.5 yields

$$s = D^*(n) \leq D^*(n, n+r_0) \leq 1 + \max\{D^*(n-k, n-k+r_0), D^*(n,k)\} = s.$$

This shows that $\tau(n) \geq n + r_0$ which completes the proof. □

REMARK 2.17. It is obvious that $\tau(1) = 2$. Assuming $s_0 = 1$ and $r_0 = 1$ in the above lemma we get $\tau(n) \geq n+1$ for all $n \geq 1$. Since $\tau(3) = 6$ by Example 2.15, so the above lemma implies $\tau(n) \geq n+3$ for all $n \geq 3$.

Now we collect several properties of the functions $\tau, \mu$ and $\kappa_e$ in the following lemma.

LEMMA 2.18. *For every integer $s \geq 1$ we have*

(1) $\tau(\mu(s)) = \mu(s) + 2^{s-1} - 1$ *for* $s \geq 2$;
(2) $D^*(\mu(s)+1, \tau(\mu(s))) \geq s+1$;
(3) $D^*(\tau(\mu(s))+1) \geq s+2$.

PROOF. (1) For $s = 2$ the claim follows from Examples 2.7 and 2.15. Assume that $s \geq 3$. Denote $n = \mu(s)$ and $m = 2^{s-1} - 1$. The definition of $\mu(s)$ combined with Lemma 2.9 implies $D^*(n) = s$ and $D^*(n-1) = s-1$. From Remark 2.17 we get $\tau(n-1) \geq n$, so $D^*(n-1, n) = s-1$. This shows that $n-1$ is an $n$-threshold number. By Example 2.8 we have $D^*(1, m+1) = s-1$. To prove that $D^*(n, n+m) = s$ it is enough to apply Lemma 2.11 with $k = n-1$. Moreover if $l > m$, then we have $D^*(1, l+1) > s-1 = D^*(n, n-1)$ and $n-1$ is an $n$-threshold number, hence by Lemma 2.13 we have $D^*(n, n+l) > s$ for $l > m$, so (1) is proved.

(2) If $s = 1$, then $\mu(1) = 1$ and $\tau(\mu(1)) = 2$, so we have $D^*(2,2) = 2 = s+1$. Let us denote $n = \mu(s)$ and $m = 2^{s-1} - 1$. The minimal number of monochromatic rectangles in $R(n+1, \tau(n))$ is equal to $(n+1) + \tau(n) - 1 = 2n + m$. This combined with Lemma 1.1 yields

$$D^*(n+1, \tau(n)) \geq \lceil \log_2(2n+m) \rceil = \begin{cases} 3 & \text{for } s = 2, \\ 4 & \text{for } s = 3, \end{cases}$$

which proves the claim for $s = 2, 3$.

Let us assume $s \geq 4$. By Remark 2.17 we have $\tau(n-1) \geq (n-1)+3 = n+2$, so $s - 1 \leq D^*(n+1, n-1) \leq D^*(n+2, n-1) = D^*(n-1) = s-1$ but $D^*(n+1, n) = s$. Thus $n-1$ is an $(n+1)$-threshold number. By Example 2.8 we have $D^*(2, m+1) = s$. Letting $k = n-1$ in Lemma 2.13 we conclude $D^*(n+1, n+m) \geq s+1$, as required.

(3) For $s = 1$ we have $D^*(\tau(\mu(1)) + 1) = D^*(3) = 3 = s+2$. For $s = 2$ Lemma 2.6 implies $D^*(\tau(\mu(2)) + 1) = D^*(4) \geq 4 = s+2$. Similarly, for $s = 3$ by Examples 2.7 and 2.12 we have $\mu(3) = 3$, so $\tau(3) = 3 + 2^2 - 1 = 6$. Hence by Lemma 2.6 we have $D^*(\tau(\mu(3)) + 1) = D^*(7) \geq 5 = s+2$.

Assume that $s \geq 4$, $n = \mu(s)$ and $m = 2^{s-1} - 1$. According to the claim (1) $\tau(\mu(s)) = n+m$. To estimate $D^*(n+m)$ we apply Lemma 2.13 for $k = n$. The definitions of $\mu$ and $\tau$ imply $D^*(n+m, k) = D^*(n+m, n) = D^*(n) = s$. From Lemma 2.6, we have $D^*(n+m-k, n+m-k) = D^*(m) \geq s+1$. The claim (2) implies that $n$ is an $(n+m)$-threshold number, hence by Lemma 2.13 we obtain (3). □

It is worth pointing out that in the proof of (3) we showed more than claimed, namely $D^*(\tau(\mu(s)) \geq s+2$, provided $s \geq 4$. Analyzing Table 1 one can conjecture that for every positive integer $i$ there is $s_i$ such that $D^*(\tau(\mu(s))) \geq s+i$ for all $s \geq s_i$.

LEMMA 2.19. *For every integer $n \geq 2$ we have*

(1) $0 < \mu(s-1) \leq \kappa_0(n) < n$ *and* $D^*(\kappa_0(n)) = s-1$, *where* $s = D^*(n)$.
(2) *If* $\mu(D^*(n)) < n$, *then* $\kappa_1(n) = \kappa_0(n)$, *else* $\kappa_1(n) < \kappa_0(n)$.
(3) $D^*(n) = D^*(n,m)$ *if and only if* $D^*(n - \kappa_0(n), m - \kappa_0(n)) < D^*(n)$ *for every integer* $m \geq n$.
(4) *If* $i = D^*(n) - D^*(n - \kappa_0(n)) - 1 \geq 0$, *then* $\tau(n) = \kappa_0(n) + \tau_i(n - \kappa_0(n))$.

PROOF. (1) The claim is obvious for $n = 2$. Assume that $n \geq 3$. Since $D^*(\kappa_0(n)) < D^*(n)$, we have $\kappa_0(n) < n$. On the other hand if $D^*(n) = s$, then $\mu(s) \leq n < \mu(s+1)$. From Lemma 2.18(3) we get $\mu(s+1) \leq \tau(\mu(s-1))+1$, hence $n \leq \tau(\mu(s-1))$ and consequently $\kappa_0(n) \geq \mu(s-1) > 0$. This yields $D^*(\kappa_0(n)) = s-1$.

(2) Assume $D^*(n) = s$ and $\mu(s) < n$. Then $D^*(n-1) = s$, so $\kappa_1(n) = \kappa_0(n)$. If $\mu(s) = n$, then $D^*(n-1) = s-1$. Thus we have $D^*(\kappa_1(n)) < s-1 = D^*(\kappa_0(n))$, so $\kappa_1(n)) < \kappa_0(n)$.

(3) Let $k = \kappa_0(n)$. Assume $D^*(n) = D^*(n,m) = s$. By Lemma 2.14 there exists a positive integer $h < m$, such that $D^*(\ell(n-h), m-h) \geq D^*(n,h)$ and $D^*(n,m) = 1 + D^*(\ell(n-h), m-h)$. If $h \geq n$, then $D^*(n,h) \geq D^*(n) = s$ which follows $D^*(n,m) \geq s+1$, a contradiction. Hence we have $h < n$, i.e., $\ell(n-h) = n-h$, so $D^*(h) \leq D^*(n,h) \leq D^*(n-h, m-h) = s-1$. By definition, $k = \kappa_0(n)$ is the greatest number such that $D^*(k) \leq s-1$ and $D^*(k) = D^*(k,n)$. So if $k < h < n$, then $D^*(h) < D^*(n,h)$ as either $D^*(h) \leq s-1$. But by the claim (1) we have $s-1 = D^*(k) \leq D^*(h) < s-1$, so we get a contradiction. Thus $h \leq k$ and $D^*(n-k, m-k) \leq D^*(n-h, m-h) = s-1$.

Conversely, if $D(n-k, m-k) \leq s-1$, then we have

$$s = D^*(n) \leq D^*(n,m) \leq 1 + \max\{D^*(n-k, m-k), D^*(n,k)\} \leq s,$$

i.e. $D^*(n,m) = s$, as required.

(4) Let $k = \kappa_0(n)$ and $s = D^*(n)$. By the above $\tau(n) = \max\{m : D^*(n-k, m-k) \leq s-1\}$. Let $i = s - D^*(n-k) - 1$ and $m_0 = \tau(n)$. Thus we have $D^*(n-k, m_0-k) \leq s-1 = D^*(n-k) + i$ and $i \geq 0$ as $n \leq m_0$. Hence $m_0 - k \leq \max\{l : D^*(n-k, l) = D^*(n-k) + i\} = \tau_i(n-k)$. This yields $\tau(n) \leq k + \tau_i(n-k)$. On the other hand, for $l_0 = \tau_i(n)$ we have $D^*(n-k, l_0) = D^*(n-k) + i = s-1$, so $D^*(n) = D^*(n, l_0+k)$, and consequently $l_0 + k \leq \tau(n)$. Thus $\tau_i(n) + k \leq \tau(n)$, which completes the proof. □

LEMMA 2.20. *If $n$ is a positive integer and $D^*(n) = s \geq 2$, then for all $i \geq 0$ we have*

(1) $\tau_{i+1}(n) = \tau_i(n) + 2^{s+i}$;
(2) $\tau_i(n) = \tau(n) + 2^s(2^i - 1)$.

PROOF. (1) Let $s = D^*(n)$ and $m = \tau_i(n)$. Hence $m \geq \tau(n)$. We have to compute the maximal integer $m'$ such that $D^*(n,m') = s+i+1$. Consider an integer $m' > m$. Notice that $m$ is an $n$-threshold number. Since $n - m \leq 0$ then Proposition 2.5 yields $D^*(n,m') \leq 1 + \max\{D^*(1, m'-m), D^*(n,m)\}$. Consequently $D^*(1, m'-m) = \lceil \log_2(m'-m) \rceil$. If $m' > m + 2^{s+i}$, then $D^*(1, m'-m) = \lceil \log_2(m'-m) \rceil > s+i = D^*(n,m)$ and by Lemma 2.13 we have $D^*(n,m') > s+i+1$. Thus $\tau_{i+1} \leq m + 2^{s+i}$.

Assuming $m' = m + 2^{s+i}$ and applying the definition of $\tau_i(n)$ we get

$$s+i+1 \leq D^*(n,m') \leq 1 + \max\{D^*(1, m'-m), D^*(n,m)\} = s+i+1.$$

This implies $\tau_{i+1}(n) = m + 2^{s+i} = \tau_i(n) + 2^{s+i}$, as required.

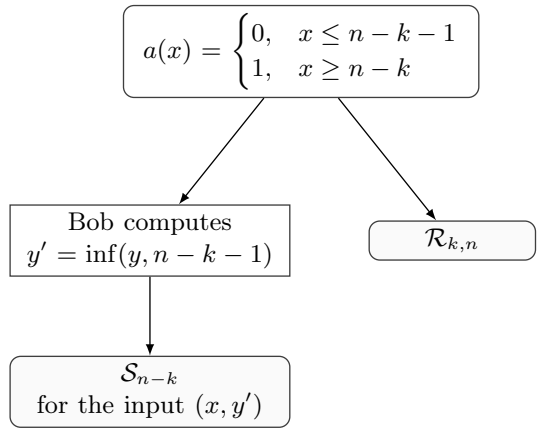
(2) follows from (1) by an easy induction. □

## 3. The construction of optimal protocols

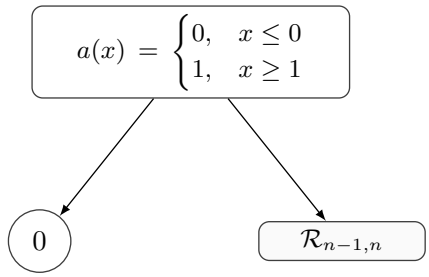
We shall construct recursively two series of optimal protocols $\mathcal{S}_l$ and $\mathcal{R}_{l,m}$ for $S(l)$ and $R(l,m)$, respectively. The protocols $\mathcal{S}_2$ and $\mathcal{R}_{1,m}$ were presented in Examples 2.7 and 2.8, respectively. Let $n \geq 3$ be an integer. Let us assume that the protocols $\mathcal{S}_l$ and $\mathcal{R}_{l,m}$ are already built for all positive integer numbers $l, m$ with $l < n$ and $l \leq m \leq n$. In particular the numbers $D^*(l)$ and $D^*(l,m)$ are known.

**The protocol $\mathcal{S}_n$ for $S(n)$.**
Input: $x \in [0, n-1]$, $y \in [0, n-1]$

(1) Alice and Bob denote $s = D^*(n-1)$ and compute $k = \kappa_1(n)$;
(2) If $D^*(n-k) < s$, then
  (a) If $x \in [0, n-k-1]$, then Alice sends 0 otherwise she sends 1.
  (b) If 0 has been sent, then Bob computes $y' = \text{INF}(y, n-k-1)$ and the players run $\mathcal{S}_{n-k}$ for the input $(x, y')$.
  (c) If 1 has been sent, then the players run the protocol $\mathcal{R}_{k,n}$.
  (d) Both players set $D^*(n) = s$.
  This part of the protocol can be illustrated as follows:




(3) If $k = 0$ or $D^*(n-k) \geq s$, then
  (a) If $x = 0$, then Alice sends 0 otherwise 1.
  (b) If 0 has been sent, then both players know $\text{INF}(x, y) = 0$, and the protocol terminates.
  (c) If 1 has been sent, then the players run the protocol $\mathcal{R}_{n-1,n}$.
  (d) Both players set $D^*(n) = s + 1$.
  This part of the protocol can be illustrated as follows:




THEOREM 3.1. *Let $n \geq 2$ be an integer. The protocol $\mathcal{S}_n$ for $S(n)$ is optimal. Moreover its length equals $D^*(n)$ specified in the protocol.*

PROOF. Example 2.7 shows that the protocol $\mathcal{S}_2$ is optimal, so let us assume that $n \geq 3$. Keep the notation above. Let us notice that $k < n$.

First we consider the case $D^*(n-k) < s$. The protocols $\mathcal{S}_{n-k}$ and $\mathcal{R}_{k,n}$ are already defined. By the definition of $k$ we have $D^*(k,n) \leq s-1$. From $D^*(n-k) < s$ it follows, that $D_{\mathcal{S}_n}(n) = 1+\max\{D_{\mathcal{S}_{n-k}}(n-k), D_{\mathcal{R}_{k,n}}(k,n)\} \leq s$. Thus we get $s = D^*(n-1) \leq D^*(n) \leq D_{\mathcal{S}_n}(n) \leq s$, so $\mathcal{S}_n$ is an optimal protocol and its length is equal to $s$.

Now we consider the case $D^*(n-k) \geq s$. Hence $D_{\mathcal{S}_n}(n) = 1+D_{\mathcal{R}_{n-1,n}}(n-1,n) = s+1$. To prove that $\mathcal{S}_n$ is an optimal protocol we have to show that $D^*(n) = s+1$. If $k = 0$, then $D^*(n) \geq D^*(n-1) = s$. Let us suppose that $D^*(n) = s$. It follows from Lemma 2.19 (1), (2) that $\kappa_1(n) = \kappa_0(n)$ and $k > 0$ which is a contradiction. This, combined with Lemma 2.9 gives $D^*(n) = s+1$.

If $k > 0$, then by the definition of $k$ we have $D^*(k,n) = D^*(k) \leq s-1$ and $D^*(k+1,n) = s$. This means that $k$ is an $n$–threshold number. By Lemma 2.13 we get $D^*(n) = s+1$. So in this case the protocol $\mathcal{S}_n$ is optimal, as well. □

Now we shall construct the optimal protocol $\mathcal{R}_{n,m}$ for $R(n,m)$ with $n,m \in \mathbb{Z}$, $1 \leq n < m$. The construction will be preceded by an auxiliary protocol $\mathcal{P}_{n,m}$ for $R(n,m)$ with $n,m \in \mathbb{Z}$, $1 \leq n < m$. The case $n = 1$ is established in Example 2.8, so we can set $\mathcal{P}_{1,m}$ to be the trivial protocol. Let us assume that $n \geq 2$ and that the optimal protocols $\mathcal{S}_h$, $\mathcal{R}_{h,l}$ and their lengths $D^*(h)$, $D^*(h,l)$ are known for all $1 \leq h \leq n$ and $h < l < m$. These combined with Lemma 2.20 allow us to determine $\tau_i(h)$ for all $i,h \in \mathbb{Z}, i \geq 0$ and $0 < h < n$. Let us consider the following protocol.

**The protocol $\mathcal{P}_{n,m}$ for $R(n,m)$**

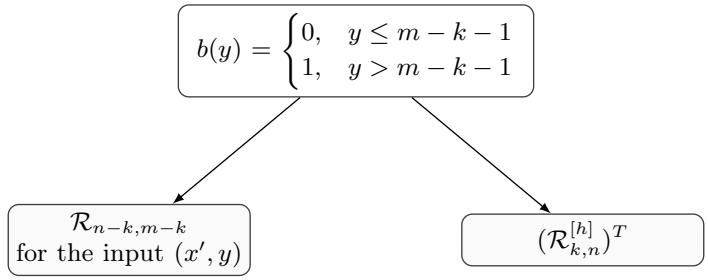
Input: $x \in [m-n, m-1]$, $y \in [0, m-1]$

(1) Knowing $\mathcal{S}_n$ Alice and Bob compute $s = D^*(n)$ and $k = \kappa_0(n)$ (local computation).

(2) If $y \in [0, m-k-1]$, then Bob sends 0 else he sends 1.

(3) If 0 has been sent, then Alice computes $x' = \text{INF}(x, m-k-1)$ and the players run $\mathcal{R}_{n-k,m-k}$ for the input $(x', y)$.
(4) If 1 has been sent, then $(x, y) \in [m-n, m-1] \times [m-k, m-1] = ([0, n-1]+h) \times ([n-k, n-1]+h)$ where $h = m-n$. Thus the players run the protocol $(\mathcal{R}_{k,n}^{[h]})^T$ which is the transpose of the protocol $\mathcal{R}_{k,n}$ shifted by $h$.

This protocol can be illustrated as follows:




The following lemma shows that $\mathcal{P}_{n,m}$ is optimal under some special assumption.

LEMMA 3.2. *Let $n \ge 2$ be an integer. If $D^*(n-\kappa_0(n), m-\kappa_0(n)) < D^*(n)$, then $\mathcal{P}_{n,m}$ is an optimal protocol for $R(n,m)$. The length of $\mathcal{P}_{n,m}$ is equal to $D^*(n)$.*

PROOF. Let us assume $s = D^*(n)$ and $k = \kappa_0(n)$. By Lemma 2.19(1) we have $0 < k < n$. Hence the protocols $\mathcal{R}_{n-k,m-k}$ and $\mathcal{R}_{k,n}$ are known. Since $s = D^*(n) \le D^*(n,m)$, the length of $\mathcal{P}_{n,m}$ is not less than $s$. On the other hand,

$$\begin{aligned} D_{\mathcal{P}_{n,m}}(n,m) &= 1 + \max\{D_{\mathcal{R}_{n-k,m-k}}(n-k, m-k), D_{\mathcal{R}_{k,n}}(k,n)\} \\ &= 1 + \max\{D^*(n-k, m-k), D^*(k,n)\} \le s, \end{aligned}$$

under the assumption $D^*(n-k, m-k) < s$. This implies $D^*(n,m) = s$, so the protocol $\mathcal{P}_{n,m}$ is optimal. □

We shall construct a general optimal protocol recursively. Let us assume that the protocols $\mathcal{R}_{n,h}$ and their lengths are known for all $n \le h < m$. These combined with Lemma 2.20 allow us to determine $\tau_i(h)$ for all $i, h \in \mathbb{Z}, i \ge 0$ and $0 < h < n$. Let us consider the following protocol.

**The protocol $\mathcal{R}_{n,m}$ for $R(n,m)$.**
Input: $x \in [m-n, m-1]$, $y \in [0, m-1]$

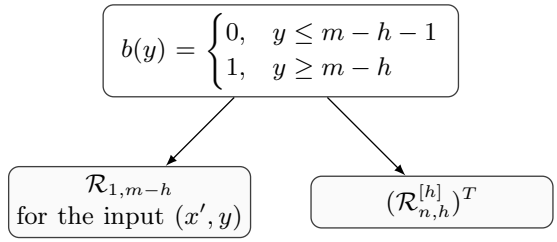
(1) Knowing $\mathcal{S}_n$ Alice and Bob compute $s = D^*(n)$ and $k = \kappa_0(n)$ (local computation).

If $D^*(n-k, m-k) < s$, then the players perform the protocol $\mathcal{P}_{n,m}$ described above.

Otherwise, Alice and Bob compute $i = D^*(n, m-1) - s$ and $l = \tau_i(n)$. Observe $m - 1 \leq l$ (cf. the proof bellow).

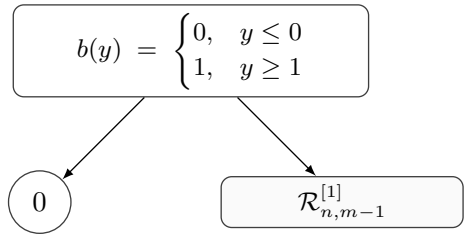
(2) If $m \leq l$, then
   (a) Alice and Bob compute $h = \tau_{i-1}(n)$.
   (b) If $y \in [0, m-h-1]$, then Bob sends 0 else he sends 1.
   (c) If 0 has been sent, then Alice denotes $x' = m-h-1$ and the players run the protocol $\mathcal{R}_{1,m-h}$ for the input $(x', y)$.
   (d) If 1 has been sent, then the players run $\mathcal{R}_{n,h}^{[m-h]}$.
   (e) The players put $D^*(n, m) = s + i$.

   This part of the protocol can be illustrated as follows.




(3) If $m = l + 1$, then
   (a) If $y = 0$, then Bob sends 0 else he sends 1.
   (b) If 0 has been sent, then both players know that $\text{INF}(x, y) = 0$.
   (c) If 1 has been sent, then the players run $\mathcal{R}_{n,m-1}^{[1]}$.
   (d) The players put $D^*(n, m) = s + i + 1$.

   This part of the protocol can be illustrated as follows:




The optimality of the protocols $\mathcal{R}_{n,m}$ is given by the following theorem.

THEOREM 3.3. *Let $n, m$ be positive integers such that $m \geq n$. The protocol $\mathcal{R}_{n,m}$ for $R(n,m)$ is optimal and its length is equal to $D^*(n,m)$ computed in the protocol.*

PROOF. By Lemma 2.19(3) we have $D^*(n-k, m-k) < s$ if and only if $m \in [n, \tau(n)]$, so $D^*(n,m) = s$. This case has already been considered in Lemma 3.2, so we assume that $m > \tau(n)$. According to the above settings we have $i + s = D^*(n, m-1) \leq D^*(n,m)$ and $m - 1 \leq \tau_i(n) = l$.

Hence we have either $\tau(n) < m \leq \tau_i(n) = l$ or $m = \tau_i(n) + 1 = l + 1$. First we assume $\tau(n) < m \leq l = \tau_i(n)$. Hence we have $i > 0$ and

$$s + i = D^*(n, m-1) \leq D^*(n,m) \leq s + i.$$

This implies that $D^*(n,m) = s + i$.

After the first step of $\mathcal{R}_{n,m}$ the interval $[0, m-1]$ is divided into two subintervals $[0, m-h-1]$ and $[m-h, m-1]$. The choice of $h$ implies $D^*(n,h) = s + i - 1$. Let us assume that $x \in [m-n, m-1]$. By Remark 2.17 we have $h \geq \tau(n) > n$. Hence $x \geq m - n > m - \tau(n) \geq m - h$. This follows that $x' = \min\{x, m-h-1\} = m - h - 1$. This proves that the step 2c is correct. Moreover, by Lemma 2.20 we have $m - h \leq 2^{s+i-1}$. This, combined with Example 2.8 yields $D^*(1, m-h) \leq s+i-1$. Hence the length of the constructed protocol equals

$$D_{\mathcal{R}_{n,m}}(n,m) = 1 + \max\{D_{\mathcal{R}_{1,m-h}}(1, m-h), D_{\mathcal{R}_{n,h}}(n,h)\} = s + i.$$

This proves that the protocol $\mathcal{R}_{n,m}$ is optimal.

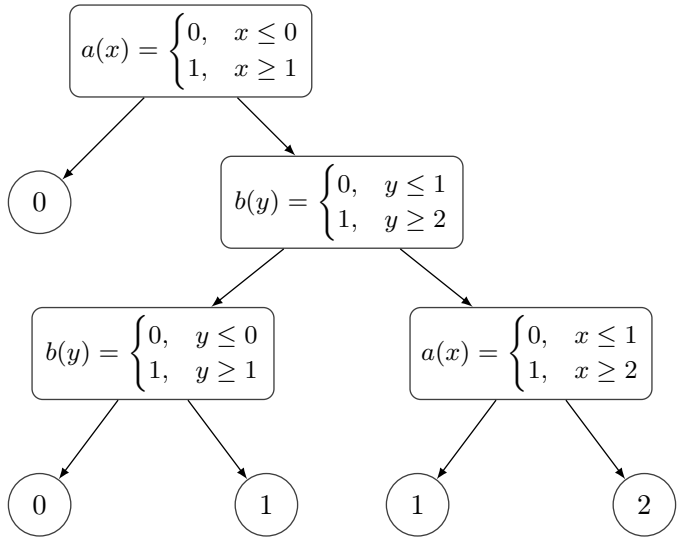
If $m = l + 1$, then $D^*(n,m) = s + i + 1$ and $D^*(n, m-1) = s + i$. On the other hand,

$$D_{\mathcal{R}_{n,m}}(n,m) = 1 + D_{\mathcal{R}_{n,m-1}}(n, m-1) = s + i + 1.$$

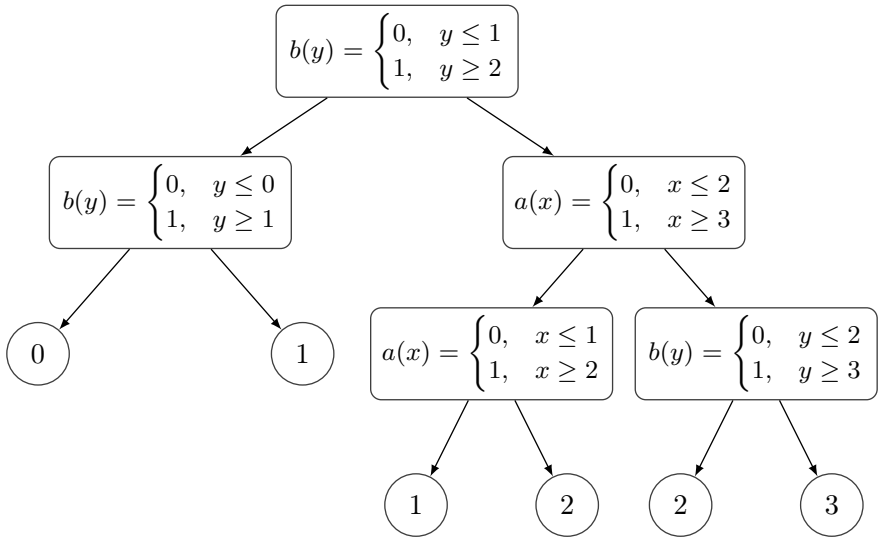
This proves that the protocol $\mathcal{R}_{n,m}$ is also optimal in this case. □

EXAMPLE 3.4. We construct the protocol $\mathcal{R}_{2,3}$ for $R(2,3)$. By definition we get $\kappa_0(2) = 1$ and from Examples 2.7 and 2.8 we have $D^*(2) = 2$ and $D^*(1,2) = 1$. Hence the condition $D^*(1,2) < D^*(2)$ is fulfilled, so we have to construct the protocol $\mathcal{P}_{2,3}$. But it is easy to see that this protocol is the transpose of the protocol from the Example 2.15 shifted by 1.

EXAMPLE 3.5. We construct the protocol $\mathcal{S}_3$ for $S(3)$. By definition $\kappa_1(3) = \max\{k : D^*(k) < D^*(2) \ \wedge \ D^*(k) = D^*(k,3)\} \cup \{0\} = 0$. So to the construction of the protocol $\mathcal{S}_3$ we need the protocol $\mathcal{R}_{2,3}$ which is constructed in the previous example. Hence we get the following protocol tree.

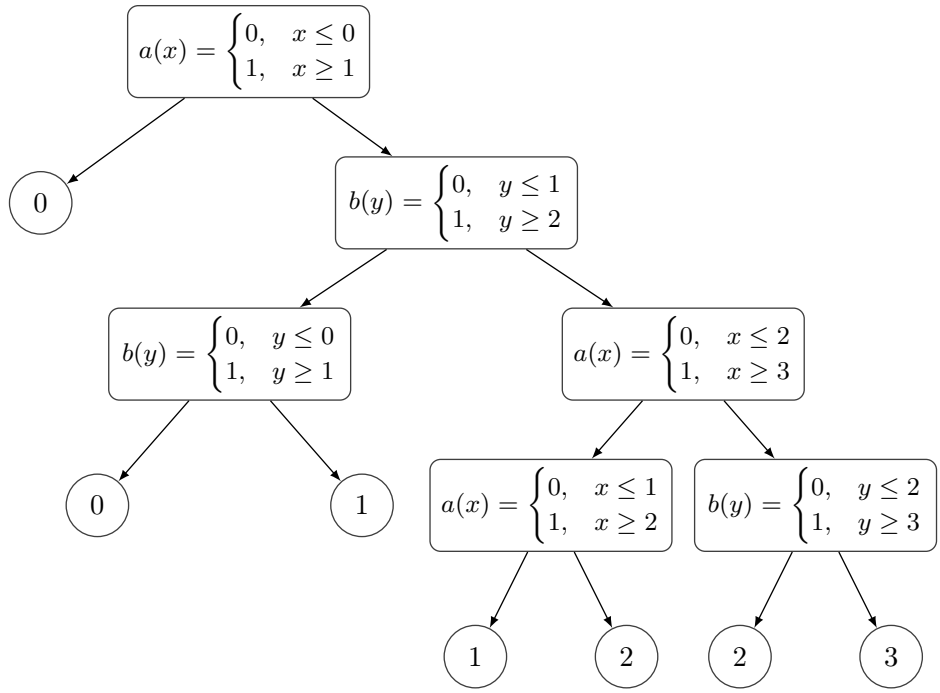



EXAMPLE 3.6. We construct the protocol $\mathcal{R}_{3,4}$ for $R(3,4)$. We already know that $D^*(3) = 3, D^*(1,2) = 1$ and we can compute that $\kappa_0(3) = 2$. Hence the condition $D^*(1,2) < D^*(3)$ is fulfilled. So we have to construct the protocol $\mathcal{P}_{3,4}$ which uses the protocols $\mathcal{R}_{1,2}$ and $(\mathcal{R}^{[1]}_{2,3})^T$. Hence we get the following protocol tree.




EXAMPLE 3.7. We construct the protocol $\mathcal{S}_4$ for $S(4)$. It is easy to see that $\kappa_1(4) = \max\{k : \ D^*(k) < D^*(3) \ \wedge \ D^*(k) = D^*(k,4)\} \cup \{0\} = 0$. So to the

construction of the protocol $\mathcal{S}_4$ we need the protocol $\mathcal{R}_{3,4}$. Hence we get the following protocol tree.




## 4. Remarks

The algorithms presented above were implemented in C++ and applied to computing $D^*(n)$ for all $n \le \mu(31) = 81\,010\,029$. The results are displayed in Table 1. The values $C(s)$ and $\lambda(\mu(s))$ will be explained below.

The determining of an analytic formula for $\mu(s)$ seems to be a hard task. Analysis of the data collected in Table 1 leads to the following conjecture on the asymptotic behaviour of the function $\mu$:

Conjecture 1. For suitable constants $c, u \in \mathbb{R}$

$$\mu(s) \approx c\frac{2^s}{s^u}.$$

Table 1. The values of $\mu(s)$, $\tau(\mu(s))$, $C(s)$ and $\lambda(\mu(s))$ for $s \leq 31$

| $s$ | $\mu(s)$ | $\tau(\mu(s))$ | $C(s)$ | $\lambda(\mu(s))$ | $s$ | $\mu(s)$ | $\tau(\mu(s))$ | $C(s)$ | $\lambda(\mu(s))$ |
|---|---|---|---|---|---|---|---|---|---|
| 2 | 2 | 3 | | | 17 | 9002 | 74537 | 1,0400 | 25 |
| 3 | 3 | 6 | 2,1296 | | 18 | 17032 | 148103 | 1,0343 | 25 |
| 4 | 4 | 11 | 2,0000 | 9 | 19 | 32286 | 294429 | 1,0298 | 25 |
| 5 | 7 | 22 | 1,4724 | 9 | 20 | 61364 | 585651 | 1,0259 | 29 |
| 6 | 11 | 42 | 1,4189 | 11 | 21 | 116978 | 1165553 | 1,0223 | 31 |
| 7 | 20 | 83 | 1,2682 | 13 | 22 | 223512 | 2320663 | 1,0189 | 31 |
| 8 | 35 | 162 | 1,2170 | 13 | 23 | 427843 | 4622146 | 1,0160 | 31 |
| 9 | 63 | 318 | 1,1718 | 16 | 24 | 820189 | 9208796 | 1,0136 | 31 |
| 10 | 114 | 625 | 1,1423 | 16 | 25 | 1574747 | 18351962 | 1,0114 | 36 |
| 11 | 210 | 1233 | 1,1148 | 16 | 26 | 3026895 | 36581326 | 1,0096 | 36 |
| 12 | 388 | 2435 | 1,0953 | 21 | 27 | 5827991 | 72936854 | 1,0078 | 36 |
| 13 | 721 | 4816 | 1,0798 | 21 | 28 | 11235235 | 145452962 | 1,0063 | 36 |
| 14 | 1351 | 9542 | 1,0656 | 21 | 29 | 21683645 | 290119100 | 1,0050 | 36 |
| 15 | 2533 | 18916 | 1,0555 | 21 | 30 | 41894301 | 578765212 | 1,0038 | 41 |
| 16 | 4767 | 37534 | 1,0471 | 25 | 31 | 81010029 | 1154751852 | 1,0028 | 41 |

If the conjecture is true, then the upper bound for the interval communication complexity is given by:

$$D^*(n) = \log_2 n + \mathcal{O}(\log_2 \log_2 n). \tag{2}$$

Obviously, this implies the same upper bound for the communication complexity (in general sense).

Let us define $C(s)$ such that

$$s = D^*(\mu(s)) = \log_2(\mu(s)) + C(s)\log_2(\log_2(\mu(s)).$$

The values of $C(s)$ for $s = 3, \ldots, 31$ displayed in the fourth (and ninth) column of Table 1 suggest that the sequence $C(s)$ is bounded (maybe $C(s)$ converges to 1).

Let $\lambda(n)$ denote the length of the protocol presented in [2] for INF restricted to $[0, n-1] \times [0, n-1]$. The upper bound for $\lambda(n)$ is similar to that of (2). Table 1 shows that $\lambda(\mu(s)) > s = D^*(\mu(s))$ for $s \leq 31$. Since $D^*(n) = s$ whenever $\mu(s) \leq n < \mu(s+1)$, so $\lambda(n) > D^*(n)$ for at least $n \leq \mu(31)$. This provides us with a heuristic argument that the bound (2) is correct.

In Lemma 2.16 we proved that $\tau(n) - n \geq r_0$ for all $n \geq \mu(s_0)$, with suitable $r_0, s_0$. Analysis of the results of numerical experiments yields more values for $r_0, s_0$.

| $s_0$ | 2 | 3 | 5 | 9 | 14 | 27 |
|---|---|---|---|---|---|---|
| $r_0$ | 1 | 3 | 5 | 11 | 27 | 107 |
| $\mu(s_0)$ | 2 | 3 | 7 | 63 | 1 351 | 5 827 991 |

It is obvious that $D^*(\tau(\mu(s))) \geq s$, so we can write $D^*(\tau(\mu(s))) = s + j_0$ for all $s \geq s_0$, with suitable $j_0, s_0$. In the proof of Lemma 2.18 we showed that $j_0 = 2$ and $s_0 = 4$. By numerical experiments we get further values for $j_0, s_0$.

| $s_0$ | 1 | 4 | 13 | 31 |
|---|---|---|---|---|
| $j_0$ | 1 | 2 | 3 | 4 |

This observation leads to the following conjecture.

Conjecture 2.

$$\lim_{n\to\infty} \tau(n) - n = \infty \text{ and } \lim_{s\to\infty} D^*(\tau(\mu(s))) - s = \infty.$$

If we could estimate how fast these sequences increase, then we probably would be able to prove the equality (2).

## References


[1] Ahlswede R., Cai N., Tamm U., *Communication complexity in lattices*, Appl. Math. Lett. **6** (1993), no. 6, 53–58.

[2] Babaioff M., Blumrosen L., Naor M., Schapira M., *Informational overhead of incentive compatibility*, in: Proc. 9th ACM Conference on Electronic Commerce, ACM, 2008, pp. 88–97.

[3] Björner A., Kalander J., Lindström B., *Communication complexity of two decision problems*, Discrete Appl. Math. **39** (1992), 161–163.

[4] Kushilevitz E., Nisan N., *Communication complexity*, Cambridge University Press, Cambridge, 1997.

[5] Lovasz L., Sachs M., *Communication complexity and combinatorial lattice theory*, J. Comput. System Sci. **47** (1993), 322–349.

[6] Mehlhorn K., Schmidt E., *Las Vegas is better than determinism in VLSI and distributed computing*, in: Proc. 14th Ann. ACM Symp. on Theory of Computing, ACM, 1982, pp. 330–337.

[7] Serwecińska M., *Communication complexity in linear ordered sets*, Bull. Sect. Logic **33** (2004), no. 4, 209–222.

[8] Yao A.C., *Some complexity questions related to distributive computing*, in: Proc. 11th Ann. ACM Symp. on Theory of Computing, ACM, 1979, pp. 209–213.



Institute of Mathematics
University of Silesia
Bankowa 14
40-007 Katowice
Poland
e-mail: mkula@us.edu.pl
e-mail: malgorzata.serwecinska@us.edu.pl