Multiparty quantum communication complexity

Harry Buhrman,[1,*] Wim van Dam,[2,1,†] Peter Høyer,[3,‡] and Alain Tapp[4,§]
[1]*Quantum Computing and Advanced Systems Research, Centrum voor Wiskunde en Informatica, P.O. Box 94079, 1090 GB Amsterdam, The Netherlands*
[2]*Centre for Quantum Computation, Clarendon Laboratory, Department of Physics, University of Oxford, Parks Road, Oxford OX1 3PU, United Kingdom*
[3]*BRICS, Department of Computer Science, University of Aarhus, Ny Munkegade, Building 540, DK-8000 Aarhus C, Denmark*
[4]*Département d'Informatique et de Recherche Opérationnelle, Université de Montréal, Code Postal 6128, Succursale Centre-Ville, Montréal, Québec, Canada H3C 3J7*

(Received 22 October 1997; revised manuscript received 31 March 1999)

Quantum entanglement cannot be used to achieve direct communication between remote parties, but it can reduce the communication needed for some problems. Let each of k parties hold some partial input data to some fixed k-variable function f. The communication complexity of f is the minimum number of classical bits required to be broadcasted for every party to know the value of f on their inputs. We construct a function G such that for the one-round communication model and three parties, G can be computed with $n+1$ bits of communication when the parties share prior entanglement. We then show that without entangled particles, the one-round communication complexity of G is $(3/2)n+1$. Next we generalize this function to a function F. We show that if the parties share prior quantum entanglement, then the communication complexity of F is exactly k. We also show that, if no entangled particles are provided, then the communication complexity of F is roughly $k \log_2 k$. These two results prove communication complexity separations better than a constant number of bits. [S1050-2947(99)05209-9]

PACS number(s): 03.67.Hk

I. INTRODUCTION

Suppose each of k parties holds some data that is unknown to the others, and they want to evaluate some fixed k-variable function on those data. If the function is nontrivial, then this cannot be done unless the parties communicate.

In Ref. [1], Cleve and Buhrman raised the question of whether or not less communication is needed if the parties possess entangled particles. They demonstrated that, for a specific problem, prior quantum entanglement decreases the need for communication by one bit from three to two bits. A one-bit saving was also obtained by Buhrman, Cleve, and van Dam in Ref. [2] for another problem where each party initially holds a two-bit input-string. In both of these problems, there are three parties ($k=3$). They left open the important question if a separation larger than one bit is possible. In particular, is a separation in an asymptotic setting possible? In this article we show that this is indeed the case.

Let f be a k-variable Boolean function whose inputs are n-bit binary strings (that is, f: $X^k \rightarrow \{0,1\}$ where $X = \{0,1\}^n$). There are k parties, denoted $P_1, \ldots, P_k$, where party P_i holds input data x_i ($i=1,\ldots,k$). Initially, party P_i only knows x_i, so, to evaluate f, the parties have to communicate with each other. The communication is done by broadcasting classical bits, where, each time, a party broadcasts one bit to everybody, on the total cost of one bit of communication.

We are interested in determining the minimum number of bits required to be broadcasted in the worst case for every party to know the value of f. This number is called the *communication complexity of* f and is denoted $C(f,k,n)$. We want to compare this number with $Q(f,k,n)$, the communication complexity of f *with* prior quantum entanglement. That is, the situation where we allow the parties to share a set of entangled particles before they learn their inputs [1,2].

For example, with this terminology, the separation obtained in [2] reads: there exists a three-variable ($k=3$) Boolean function g whose inputs are two-bit strings ($n=2$), and for which $C(g,3,2)=3$, but $Q(g,3,2)=2$. For some functions, no separation at all is possible. For example, Cleve *et al.* [3] showed that prior quantum entanglement does not help in computing the so-called inner product function.

References [1,2] left open the very interesting question of whether a separation in an asymptotic setting is possible. This question can be phrased more formally as: Does there exists a function f for which $C(f,k,n)$ grows in k or n, and for which the ratio between $C(f,k,n)$ and $Q(f,k,n)$ is bounded from below by some constant larger than 1?

In this paper, we first study the case where the number of parties is three ($k=3$). In this setting we consider the *one-round* communication model where each party is allowed to communicate at most once. We construct a Boolean function G for which $C(G,3,n)=(3/2)n+1$ whereas $Q(G,3,n)=n+1$. This gives a separation by a factor of 3/2 in terms of the number of bits hold by each of the three parties.

Next we relax the requirement that only one round of communication be allowed and consider an arbitrary number of parties. To this end we generalize the communication

[*] Electronic address: Harry.Buhrman@cwi.nl
[†] Electronic address: wimvdam@qubit.org
[‡] Electronic address: hoyer@brics.dk
[§] Electronic address: tappa@iro.umontreal.ca

function G to F. We demonstrate that the communication complexity of F with prior quantum entanglement is exactly k [that is, $Q(F,k,n)=k$], but that, if $n\geqslant\log_2 k$, then without quantum entanglement it is roughly $k\log_2 k$ [that is, $C(F,k,n)\approx k\log_2 k$]. We prove this by giving upper and lower bounds in both cases. This implies a separation by a logarithmic factor in k, the number of parties.

This paper thus presents a function with a separation by a constant factor in terms of the number of bits, and a function with a separation by a logarithmic factor in terms of the number of parties. Very recently, much more impressive separations have been obtained in terms of the number of bits. Buhrman, Cleve, and Wigderson [4], Ambainis *et al.* [5], and Raz [6] have all found two-party computational problems for which an exponential separation holds.

II. MODULO-4 SUM PROBLEM

In this section, we fix the number of parties to three ($k=3$). As is common, we name the parties Alice, Bob, and Carol.

In Ref. [2], Buhrman, Cleve, and van Dam considered the *modulo-4 sum problem* defined as follows. Alice, Bob, and Carol receive x, y, and z, respectively, where $x,y,z\in U=\{0,1,2,3\}$, and they are promised that

$$(x+y+z)\bmod 2=0. \tag{1}$$

The common goal is for every party to learn the value of the function

$$f(x,y,z)=\frac{1}{2}[(x+y+z)\bmod 4]. \tag{2}$$

We say that $(x,y,z)\in U\times U\times U$ is a *valid* input if Eq. (1) holds. The function $f{:}U\times U\times U\rightarrow\{0,1\}$ can be viewed as computing the second-least significant bit in the sum of x, y, and z. Note that for all inputs $y,z\in U$ to Bob and Carol, there exists a unique input $x\in U$ for Alice such that (x,y,z) is a valid input and $f(x,y,z)=1$.

For every integer $m\geqslant 1$, we generalize f to $G_m{:}U^m\times U^m\times U^m\rightarrow\{0,1\}$ by setting

$$G_m(\mathbf{x},\mathbf{y},\mathbf{z})=1 \text{ if and only if for all}$$

$$1\leqslant i\leqslant m \quad \text{we have } f(x_i,y_i,z_i)=1,$$

where $\mathbf{x}=(x_1,\ldots,x_m)$, $\mathbf{y}=(y_1,\ldots,y_m)$, and $\mathbf{z}=(z_1,\ldots,z_m)$, and with the condition that

$$(x_i+y_i+z_i)\bmod 2=0 \quad (1\leqslant i\leqslant m). \tag{3}$$

Thus, we give Alice, Bob, and Carol m valid instances of f, all at the same time, and ask if they all evaluate to 1. Again, we say that $(\mathbf{x},\mathbf{y},\mathbf{z})$ is a *valid* input if Eq. (3) holds.

Buhrman *et al.* [2] showed that *with* prior entanglement, function f can be solved with one-round communication using 3 bits. In their protocol, Bob and Carol each broadcast one bit, where after Alice is capable of computing the value of f and then broadcasting the resulting bit. (See Sec. III A for a direct generalization of their protocol.) Their protocol therefore immediately yields a $2m+1$ bits protocol for G_m.

Theorem 1. With prior quantum entanglement G_m can be solved with one-round communication using $2m+1$ bits.

In Sec. II B below, we prove the following lower bound for the case in which we do not allow quantum entanglement.

Theorem 2. Without quantum entanglement, there is no one-round protocol for G_m that uses less than $3m+1$ bits of communication.

For one-round protocols we thus archive a separation of $2m+1$ bits against $3m+1$ bits. We do not know the classical communication complexity of computing G_m without any restriction on the number of rounds.

A. Classical upper bound

The lower bound in theorem 2 is tight as there is a straightforward one-round protocol that computes G_m with $3m+1$ bits of communication. It is instructive for understanding the proof of our lower bound, first to understand that protocol.

Consider an input $\mathbf{x}\in U^m$ to Alice. We can think of $\mathbf{x}=(x_1,\ldots,x_m)$ as consisting of two parts, the high bits and the low bits. That is, we identify $\mathbf{x}$ with the pair $(\mathbf{x}_{\text{high}},\mathbf{x}_{\text{low}})$, where the ith coordinate in $\mathbf{x}_{\text{high}}\in\{0,1\}^m$ is $(x_i \operatorname{div} 2)$, and where the ith coordinate in $\mathbf{x}_{\text{low}}\in\{0,1\}^m$ is $(x_i \bmod 2)$. We think of Bob's input $\mathbf{y}=(y_1,\ldots,y_m)$ and Carol's input $\mathbf{z}=(z_1,\ldots,z_m)$ in a similar manner.

The $3m+1$ one-round protocol works as follows: First Bob broadcasts all $2m$ bits of his input $(\mathbf{y}_{\text{high}},\mathbf{y}_{\text{low}})$. Then Carol broadcasts the m high bits $\mathbf{z}_{\text{high}}$ of her input. Now Alice is capable of computing the value of f on all m instances, that is, she can compute $f(x_i,y_i,z_i)$ for all $1\leqslant i\leqslant m$. Due to the promise that $(x_i+y_i+z_i)\bmod 2=0$, she does not need the low bits $\mathbf{z}_{\text{low}}$ of Carol's input. Finally Alice checks if $f(x_i,y_i,z_i)=1$ for all $1\leqslant i\leqslant m$. If so, $G_m(\mathbf{x},\mathbf{y},\mathbf{z})=1$ and Alice therefore broadcasts 1, otherwise she broadcasts 0.

Intuitively, Alice has to have all of Bob's m high bits, all of Carol's m high bits, but just m of the $2m$ low bits. Hence, *intuitively*, if there exists a protocol for G_m in which Bob broadcasts s_B bits and Carol broadcasts s_C bits, then s_B should be at least m, s_C at least m, and s_B+s_C at least $3m$. It is the result of the following subsection that this intuition is valid.

B. Classical lower bound

We now prove our lower bound stated in theorem 2. Since we only consider one-round protocols, we can without loss of generality assume that any protocol computing G_m is made up of the following three parts.

(1) Bob (knowing only his input $\mathbf{y}$) broadcasts the message $\sigma_B=\sigma_B(\mathbf{y})$.

(2) Carol (knowing her input $\mathbf{z}$ and Bob's message σ_B) broadcasts the message $\sigma_C=\sigma_C(\mathbf{z},\sigma_B)$.

(3) Alice (knowing $\mathbf{x}$, σ_B, and σ_C) computes the answer $\sigma_A(\mathbf{x},\sigma_B,\sigma_C)\in\{0,1\}$ which she then broadcasts to Bob and Carol. Since this protocol computes G_m, we can without loss of generality assume that $\sigma_A=G_m$ on all valid inputs.

In agreement with our intuition described above, the following key lemma explicitly specifies 2^{3m} different inputs on which Bob and/or Carol have to send different messages. Theorem 2 is immediate.

Lemma 1. Consider the above one-round protocol for computing G_m. Let σ_B and σ_C denote Bob's and Carol's messages on inputs $\mathbf{y}=(\mathbf{y}_{\text{high}},\mathbf{y}_{\text{low}})$ and $\mathbf{z}=(\mathbf{z}_{\text{high}},\mathbf{y}_{\text{low}})$, respectively. Let σ_B' and σ_C' denote Bob's and Carol's messages on inputs $\mathbf{y}'=(\mathbf{y}_{\text{high}}',\mathbf{y}_{\text{low}}')$ and $\mathbf{z}'=(\mathbf{z}_{\text{high}}',\mathbf{y}_{\text{low}}')$, respectively. Then the following holds.

(i) If $\mathbf{y}_{\text{high}}\neq\mathbf{y}_{\text{high}}'$ and $\mathbf{y}_{\text{low}}=\mathbf{y}_{\text{low}}'$, then $\sigma_B\neq\sigma_B'$.

(ii) If $\mathbf{z}_{\text{high}}\neq\mathbf{z}_{\text{high}}'$ and $\mathbf{y}_{\text{low}}=\mathbf{y}_{\text{low}}'$, then $\sigma_C\neq\sigma_C'$.

(iii) If $\mathbf{y}_{\text{low}}\neq\mathbf{y}_{\text{low}}'$, then $\sigma_B\neq\sigma_B'$ or $\sigma_C\neq\sigma_C'$.

We first prove (i) by contradiction. Assume $\mathbf{y}_{\text{high}}\neq\mathbf{y}_{\text{high}}'$, $\mathbf{y}_{\text{low}}=\mathbf{y}_{\text{low}}'$, and $\sigma_B=\sigma_B'$. Let $\mathbf{x}$ be the unique input to Alice such that $G_m(\mathbf{x},\mathbf{y},\mathbf{z})=1$. Then $(\mathbf{x},\mathbf{y}',\mathbf{z})=(\mathbf{x},(\mathbf{y}_{\text{high}}',\mathbf{y}_{\text{low}}),\mathbf{z})$ is a valid input on which G_m takes the value 0. But, since $\sigma_B=\sigma_B'$, we also have $\sigma_C(\mathbf{z},\sigma_B)=\sigma_C'(\mathbf{z},\sigma_B')$, and hence Alice incorrectly outputs the same answer $\sigma_A(\mathbf{x},\sigma_B,\sigma_C)=\sigma_A(\mathbf{x},\sigma_B',\sigma_C')$ in both cases. Thus, the assumption is wrong and (i) holds. The proof of (ii) is almost identical to the proof of (i), and we therefore omit it.

We also prove (iii) by contradiction. Assume $\mathbf{y}_{\text{low}}\neq\mathbf{y}_{\text{low}}'$, $\sigma_B=\sigma_B'$, and $\sigma_C=\sigma_C'$. Let $\mathbf{x}=(\mathbf{x}_{\text{high}},\mathbf{0})$ be the unique input to Alice such that $G_m(\mathbf{x},\mathbf{y},\mathbf{z})=1$. Since the protocol correctly computes G_m, then Alice must answer 1 on the input $(\mathbf{x},\mathbf{y},\mathbf{z})$. But then $(\mathbf{x},\mathbf{y}',\mathbf{z}')$ is also a valid input on which Alice answers 1. Further, let $\mathbf{x}'=(\mathbf{x}_{\text{high}}',\mathbf{x}_{\text{low}}')$ be the unique input to Alice such that $G_m(\mathbf{x}',\mathbf{y}',\mathbf{z})=1$. Since the protocol correctly computes G_m, then Alice must answer 1 on the input $(\mathbf{x}',\mathbf{y}',\mathbf{z})$. But then $(\mathbf{x}',\mathbf{y},\mathbf{z}')$ is also a valid input on which Alice answers 1.

Thus, Alice answers 1 on all of these 4 valid inputs: $(\mathbf{x},\mathbf{y},\mathbf{z})$, $(\mathbf{x},\mathbf{y}',\mathbf{z}')$, $(\mathbf{x}',\mathbf{y}',\mathbf{z})$, and $(\mathbf{x}',\mathbf{y},\mathbf{z}')$. But, since $\mathbf{y}_{\text{low}}\neq\mathbf{y}_{\text{low}}'$, then (as we show in the next paragraph) G_m takes the value 0 on at least one of the valid inputs $(\mathbf{x},\mathbf{y}',\mathbf{z}')$ and $(\mathbf{x}',\mathbf{y},\mathbf{z}')$, and thus the protocol incorrectly computes G_m. Hence, the assumption is wrong and (iii) follows.

To see that G_m has to take the value 0 on at least one of the valid inputs $(\mathbf{x},\mathbf{y}',\mathbf{z}')$ and $(\mathbf{x}',\mathbf{y},\mathbf{z}')$, assume otherwise. Let $1\leqslant i\leqslant m$ be a coordinate where $\mathbf{y}_{\text{low}}$ and $\mathbf{y}_{\text{low}}'$ differ. For ease of notation, we let y_{low} denote the ith coordinate (bit) of $\mathbf{y}_{\text{low}}\in\{0,1\}^m$, and we use similar notation for the ith coordinate of the other vectors. Since $G_m(\mathbf{x},\mathbf{y},\mathbf{z})=1$, then

$$(x_{\text{high}}+y_{\text{high}}+z_{\text{high}}+y_{\text{low}})\bmod 2=0.$$

Since $G_m(\mathbf{x}',\mathbf{y}',\mathbf{z})=1$, then

$$(x_{\text{high}}'+y_{\text{high}}'+z_{\text{high}}+1)\bmod 2=0.$$

Since $G_m(\mathbf{x},\mathbf{y}',\mathbf{z}')=1$, then

$$(x_{\text{high}}+y_{\text{high}}'+z_{\text{high}}'+y_{\text{low}}')\bmod 2=0.$$

Since $G_m(\mathbf{x}',\mathbf{y},\mathbf{z}')=1$, then

$$(x_{\text{high}}'+y_{\text{high}}+z_{\text{high}}'+1)\bmod 2=0.$$

But all of these four equations cannot hold at the same time, and thus the assumption that G_m takes the value 1 on $(\mathbf{x},\mathbf{y}',\mathbf{z}')$ and $(\mathbf{x}',\mathbf{y},\mathbf{z}')$ is wrong. This completes our proof of lemma 1, from which theorem 2 immediately follows.

It is worthy noticing that, by lemma 1, for Alice to correctly output the value of G_m, she has to be able to correctly compute f on every one of the m instances of f. This is in general not so, and it is a deep open question in communication complexity to characterize the functions that possess this property.

III. MULTIROUNDS AND MULTIPARTIES

We now generalize f defined in Eq. (2) to a function F which we shall use to prove a separation in terms of the number of parties. There are k parties, where party P_i obtains input data $x_i\in V=\{0,\ldots,2^n-1\}$ $(i=1,\ldots,k)$. We say that an input $\mathbf{x}=(x_1,\ldots,x_k)$ is *valid* if it satisfies that

$$\left(\sum_{i=1}^{k}x_i\right)\bmod 2^{n-1}=0. \tag{4}$$

Let F: $V^k\rightarrow\{0,1\}$ denote the Boolean function on the valid inputs defined by

$$F(\mathbf{x})=\frac{1}{2^{n-1}}\left[\left(\sum_{i=1}^{k}x_i\right)\bmod 2^n\right]. \tag{5}$$

We say that a valid input $\mathbf{x}$ is *b-valid* if $F(\mathbf{x})=b$ $(b=0,1)$. The function F can be viewed as computing the nth least significant bit of the sum of the x_i's.

We first show that with prior quantum entanglement, k bits of communication are necessary and sufficient for every party to evaluate F. That is, for all $k\geqslant 2$ and $n\geqslant 1$,

$$Q(F,k,n)=k. \tag{6}$$

Then, we show how the parties can evaluate F with roughly $k\log_2 k$ bits of communication without using any entangled particles. Specifically, for all $k\geqslant 2$ and $n\geqslant 1$,

$$C(F,k,n)\leqslant(k-1)\{\lceil\log_2(k-1)\rceil+1\}+1. \tag{7}$$

Finally, we prove that this is optimal up to low order terms by showing that, for all $k\geqslant 2$ and $n\geqslant\log_2 k$,

$$C(F,k,n)>k\log_2(k)-k. \tag{8}$$

By comparing the bounds of Eqs. (6) and (8), we see that we have established a separation by a factor of $\log_2(k/2)$.

A. With entanglement

We first show that if the parties share entangled particles, then in a straightforward manner, the k parties can evaluate F using only one bit of communication each. This is obtained by a direct generalization of the idea used both in Sec. 2.1 of Ref. [2] (which itself is based on the work of Mermin [7]) and in Ref. [8]. The prior quantum entanglement shared by the k parties is the cat state $|q_1\ldots q_k\rangle=(|0\ldots0\rangle+|1\ldots1\rangle)/\sqrt{2}$, where party P_i holds qubit q_i $(i=1,\ldots,k)$.

Each party P_i uses the following procedure. First party P_i applies a phase-change operator $\phi(x_i)$ defined by $|0\rangle\mapsto|0\rangle$ and $|1\rangle\mapsto\exp(2\pi x_i\sqrt{-1}/2^n)|1\rangle$ on her qubit q_i. Thanks to the promise on the inputs, these phase rotations add up so that the resulting state is $(|0\ldots0\rangle + (-1)^{F(\mathbf{x})}|1\ldots1\rangle)/\sqrt{2}$. Then she applies the Walsh-Hadamard transform that maps $|0\rangle$ to $(|0\rangle+|1\rangle)/\sqrt{2}$, and $|1\rangle$ to $(|0\rangle-|1\rangle)/\sqrt{2}$. Finally, she measures her qubit q_i in the computational basis $\{|0\rangle,|1\rangle\}$ and broadcasts the outcoming bit.

Let b_i be the outcome of party P_i's measurement. Simple calculations show that $b_1\oplus\cdots\oplus b_k$ equals $F(x_1,\ldots,x_k)$, where $\oplus$ denotes addition in modulo-2 arithmetic. It follows that every party can compute the value of F from the k communicated bits. On the other hand, k bits of communication are necessary since if one of the parties does not broadcast any bits, then none of the others can determine the value of F. To see this, note that if we toggle the most significant bit of any one of the inputs, then the value of F changes. Equation (6) follows.

B. Without entanglement

The simplest way to evaluate the function F is for all but one of the parties to broadcast their inputs. The last party then evaluates $F(x_1,\ldots,x_k)$ and communicates the resulting bit to the others. Hence, the communication complexity (without entanglement) is at most $(k-1)n+1$.

Now, consider that all but one of the parties broadcast the d most significant bits of their inputs, for some integer $d \geqslant 1$. The last party, say P_k, then computes the sum $(\Sigma_{i=1}^k x_i)-\delta$, where

$$\delta=\sum_{i=1}^{k-1}(x_i \bmod 2^{n-d}).$$

Suppose $n\geqslant d$ where $d=1+\lceil\log_2(k-1)\rceil$. Then

$$0\leqslant\delta\leqslant(k-1)(2^{n-d}-1)<2^{n-1},$$

so party P_k knows the value of the sum $\Sigma_{i=1}^k x_i$ up to an additional non-negative term strictly smaller than 2^{n-1}. Since the sum is divisible by 2^{n-1} for all valid inputs, party P_k can determine it exactly and thus compute the value of F. It follows that $(k-1)d+1$ bits of communication suffice, as stated as Eq. (7).

A good method to prove lower bounds for the communication complexity of functions comes from a combinatorial view on the protocol for the communication. Consider the space V^k of all possible inputs, where $V=\{0,\ldots,2^n-1\}$. A *rectangle* in V^k is a subset $R\subseteq V^k$ such that $R=R_1\times\cdots\times R_k$ for some $R_i\subseteq V$ $(i=1,\ldots,k)$. If a rectangle contains no 0-valid inputs or no 1-valid inputs, then it is said to be *F-monochromatic*.

We now use the observation that every deterministic and errorless communication protocol corresponds to a covering of all the valid inputs in V^k by F-monochromatic rectangles (see Ref. [9]). Without increasing the communication complexity, such a protocol can always be transformed into a protocol that uses a partitioning that covers all of V^k, and for which each monochromatic rectangle contains at least one valid input. By proving that every such partition requires at least t rectangles, we also prove that the communication complexity of F is at least $\log_2 t$ [9]. Hence, upper bounds on the cardinality of the possible F-monochromatic rectangles imply a lower bound on the communication complexity of F.

In the Appendix, we prove that if a rectangle $R\subseteq V^k$ is F-monochromatic and if R contains a valid input, then its cardinality is upper bounded by a value r, for which

$$r=\left(\frac{2^n-2}{k}+1\right)^k. \tag{9}$$

Since there are 2^{nk} input values to be covered, this bound on the size of the rectangles shows that we need at least $t=2^{nk}/r$ rectangles to partition V^k in the above described fashion.

If $n\geqslant\log_2 k$ and $k\geqslant2$, then basic algebra gives that

$$\log_2 t=\log_2\left(\frac{2^{nk}}{r}\right)>k\log_2(k)-k.$$

From this, the lower bound on the communication complexity of Eq. (8) follows.

ACKNOWLEDGMENTS

We are grateful to Lucien Hardy for pointing out an error in an earlier version of this paper, and to Richard Cleve and Andrew Landahl for discussions. H. B. thanks Ricard Gavaldà for stimulating conversations. W. v.D. has been supported by the European TMR Research Network EPR-4061 PL95-1412, Hewlett-Packard, and the Institute for Logic, Language, and Computation in Amsterdam, The Netherlands. P. H. has been supported in part by the ESPRIT Long Term Research Program of the EU under Project No. 20244 (ALCOM-IT). A.T. has been supported in part by Canada's NSERC. Parts of this research were carried out while P.H. was at the Laboratoire d'Informatique Théorique et Quantique at the Université de Montréal, and during the 1997 Elsag-Bailey–ISI Foundation research meeting on quantum computation.

APPENDIX: UPPER BOUND ON THE CARDINALITY OF A MONOCHROMATIC RECTANGLE

Equip the set $V=\{0,\ldots,2^n-1\}$ with the natural addition operation, denoted $\oplus$ and given by $x\oplus y=(x+y)\bmod 2^n$. Then $V=\langle V,\oplus\rangle$ is a cyclic group of order 2^n.

Let $R\subseteq V^k$ be a fixed rectangle. By definition, $R=R_1\times\cdots\times R_k$ for some subsets $R_i\subseteq V$, $i=1,\ldots,k$. For any two subsets $A,B\subseteq V$, define $A\oplus B=\{a\oplus b|a\in A,b\in B\}$. We now define a family of subsets of V. Set $S_0=\{0\}\subset V$ and $S_i=S_{i-1}\oplus R_i$ for $i=1,\ldots,k$. Then for each element $(x_1,\ldots,x_k)\in R$, the value $(\Sigma_{i=1}^k x_i)\bmod 2^n$ is in S_k. We shall use Kneser's theorem [10] to give an upper bound on the cardinality of R.

Kneser's theorem. Let $G=\langle G,\oplus\rangle$ be an Abelian group with finite subsets A and B. Then there exists a subgroup H of G such that

$$A\oplus B\oplus H=A\oplus B$$

and

$$|A\oplus B|\geqslant|A\oplus H|+|B\oplus H|-|H|.$$

Let H_i be the largest subgroup of V for which $S_i = S_i \oplus H_i$, $(i=0,\ldots,k)$. Since $\oplus$ is associative, then $H_{i-1} \subseteq H_i$ for all $1 \leqslant i \leqslant k$.

Suppose R is a monochromatic rectangle that contains a valid input. Without loss of generality, assume that it is a 0-valid input, that is, that $0 \in S_k$. Then H_i is the trivial subgroup $\{0\}$ for all i, since otherwise we have that $2^{n-1} \in H_i \subseteq H_k$ and hence R would not be monochromatic. This shows that if we identify $A = S_{i-1}$ and $B = R_i$ in Kneser's theorem, it follows that H is the trivial subgroup. We therefore have that $|S_i| \geqslant |S_{i-1}| + |R_i| - 1$, so

$$|S_k| \geqslant \sum_{i=1}^{k} |R_i| - (k-1).$$

Since $2^{n-1} \notin S_k$, then $|S_k| \leqslant 2^n - 1$, so

$$\sum_{i=1}^{k} |R_i| \leqslant 2^n - 2 + k,$$

and therefore

$$|R| = \prod_{i=1}^{k} |R_i| \leqslant \left(\frac{2^n - 2}{k} + 1 \right)^k.$$

It follows that the right hand side of Eq. (9) is an upper bound on the cardinality of any F-monochromatic rectangle that contains a valid input.

[1] R. Cleve and H. Buhrman, Phys. Rev. A **56**, 1201 (1997).

[2] H. Buhrman, R. Cleve, and W. van Dam, e-print quant-ph/9705033.

[3] R. Cleve, W. van Dam, M. Nielsen, and A. Tapp, in *Proceedings of the first NASA International Conference on Quantum Computing and Quantum Communications*, Lecture Notes in Computer Science Vol. 1509 (Springer-Verlag, Berlin, 1999), p. 61.

[4] H. Buhrman, R. Cleve, and A. Wigderson, in *Proceedings of the 29th Annual ACM Symposium on Theory of Computing*, Dallas, Texas (The Association for Computing Machinery, New York, 1998), p. 63.

[5] A. Ambainis, L. Schulman, A. Ta-Shma, U. Vazirani, and A. Wigderson, in *Proceedings of the 30th Annual Symposium on Foundations of Computer Science*, Palo Alto, California (IEEE Computer Society Press, Los Alamitos, CA, 1998), p. 342.

[6] R. Raz, in *Proceedings of the 31st Annual ACM Symposium on Theory of Computing*, Atlanta, Georgia (The Association for Computing Machinery, New York, 1999), p. 358.

[7] N. D. Mermin, Phys. Today **43**, 9 (1990).

[8] L. K. Grover, e-print quant-ph/9704012.

[9] E. Kushilevitz and N. Nisan, *Communication Complexity* (Cambridge University Press, Cambridge, England, 1997), see pages 3–10 of the first introductory chapter. Corollary 1.17 states the fact for two parties only: If every partition of V^2 into f-monochromatic rectangles requires t or more rectangles, then the communication complexity of f is at least $\log_2 t$. It is an easy exercise to generalize this result to any number of parties $(k \geqslant 2)$. The question of additivity is discussed in section 4.1, open problem 4.2. A lower bound for partial functions via monochromatic rectangles is stated as proposition 5.4 in section 5.

[10] M. Kneser, Math. Z. **58**, 459 (1953); H. B. Mann, *Addition Theorems: The Addition Theorems of Group Theory and Number Theory* (Wiley, New York, 1965), p. 6.