Open Problems Column
Edited by William Gasarch

1 This Issues Column!

This issue's Open Problem Column is by William Gasarch and is *Make Multiparty Communication Complexity FUN Again*.

2 Request for Columns!

I invite any reader who has knowledge of some area to contact me and arrange to write a column about open problems in that area. That area can be (1) broad or narrow or anywhere inbetween, and (2) really important or really unimportant or anywhere inbetween.

Make Multiparty Communication Complexity FUN Again
By William Gasarch

3 Introduction

The following problem sounds like a FUN problem to tell my relative Olivia who is a freshman math and CS major (or she would be if she wasn't fictional).

Def 3.1 The $\text{EXACT}_3(n)$ problem is as follows. Alice, Bob, and Carol each have a number between 0 and $2^n - 1$ on their forehead, written in binary; so everyone has exactly n bits on their forehead. Everyone can see the two numbers that are NOT on their own forehead. Call the three numbers a, b, c. They wish to determine if $a + b + c = 2^{n+1} - 1$ (so $1 \cdots 1$ in binary where there are $n + 1$ 1's). At the end of the protocol they should all know if $a + b + c = 2^{n+1} - 1$ or not. Each player can shout information so the others hear them. Let $d_3(n)$ be the number of bits shouted.

The following easy protocol shows $d_3(n) \leq n + 1$.

1. Alice shouts b. (So now Bob knows b.)
2. Bob computes $a + b + c$.
3. If $a + b + c = 2^{n+1} - 1$ then Bob shouts YES, else NO.

Is there a protocol with a smaller value of $d_3(n)$?

Would Olivia find this fun?

1. *Good News.* Chandra, Furst, and Lipton [2] showed that $d_3(n) \leq O(\sqrt{n})$. Thats good news since if $d_3(n) \geq n$ then Olivia would be disappointed.

2. *Bad News.* The $O(\sqrt{n})$ protocol uses 3-free sets. While fans of Ramsey Theory (I am one) may find this fun, alas, Olivia would not.

Question Is there an *elementary protocol* that shows $d_3(n) \leq \alpha n$ for some $\alpha < 1$?

In Section 4 we present an *elementary protocol*, due to Dean Foster, that shows $d_3(n) \leq \frac{n}{2} + O(1)$ and ask if there is a better *elementary protocol*. In Section 5 we present a generalization of the problem. In Section 6 we summarize what is known.

4 A FUN Solution

The following is due to Dean Foster.

Theorem 4.1 *There is an elementary protocol that shows* $d_3(n) \leq \frac{n}{2} + O(1)$.

Proof: We assume n is even. We leave it to the reader to modify the proof for the case where n is odd.

Here is the protocol.

1. Alice's forehead has $a = a_{n-1} \cdots a_0$.

   Bob's forehead has $b = b_{n-1} \cdots b_0$.

   Carol's forehead has $c = c_{n-1} \cdots c_0$.

2. Alice shouts the following sequence of bits:

$$b_{n-1} \oplus c_0, b_{n-2} \oplus c_1, \cdots, b_{n/2} \oplus c_{n/2-1}.$$

   Comments

   (a) Alice shouts $n/2$ bits.

   (b) Since Bob knows all of the c_i's he now knows $b_{n/2}, \ldots, b_{n-1}$.

   (c) Since Carol knows all of the b_i's she now knows $c_0, \ldots, c_{n/2-1}$.

3. Carol knows $a_0, \ldots, a_{n/2-1}$, $b_0, \ldots, b_{n/2-1}$, $c_0, \ldots, c_{n/2-1}$. Hence she can compute

$$a_{n/2-1}a_{n/2-1} \cdots a_0 + b_{n/2-1}b_{n/2-1} \cdots b_0 + c_{n/2-1}c_{n/2-1} \cdots c_0$$

   If the answer is not $2^n - 1$ (which is $1 \cdots 1$ with n 1's) then she shouts NO and the protocol is over. They all know that $a + b + c \neq 2^{n+1} - 1$. If the answer is $2^n - 1$ then she shouts YES and then the carry bit.

   Note that Carol shouts at most 2 bits.

4. (If the protocol go to this step then Carol shouted YES and the carry bit.) Bob knows $a_{n/2}, \ldots, a_{n-1}$, $b_{n/2}, \ldots, b_{n-1}$, $c_{n/2}, \ldots, c_{n-1}$ and the carry bit. Hence Bob can compute $a+b+c$. If the answer is $2^{n+1}-1$ then he shouts NO. Otherwise he shouts YES.

   Note that Bob shouts 1 bit.

5. Whatever Bob shouted is the answer and they now all know it.

∎

Open Problem 4.2

1. Give an *elementary protocol* that shows $d_3(n) \leq \alpha n$ bits for some $\alpha < \frac{1}{2}$.

2. It is possible that there is such elementary protocol. It would be good to be able to prove that (or prove some lower bound on how well elementary protocols can do). However, there is a problem with this problem. The notion of *elementary protocol* is not well defined. So the open problem is to come up with a framework to prove that there is no elementary protocol. It is likely that such a framework would not be FUN for Olivia. It is possible that there is no such framework. I am not going to state an open problem about proving that *proving that there is no elementary protocol is hard* is hard since that would not be FUN for anyone.

5 What About Alice, Bob, Carol, Donna, ..., Zelda?

Def 5.1 Let $k \geq 3$. The $\text{EXACT}_k(n)$ problem is as follows. X_1, ..., X_k are people. Each person has a number between 0 and 2^n-1 on their forehead, written in binary; so everyone has exactly n bits on their forehead. Everyone can see the $k-1$ numbers that are NOT on their own forehead. Call the k numbers $x_1, \ldots, x_k$. They wish to determine if $x_1+\cdots+x_k = 2^{n+1}-1$ (so $1\cdots1$ in binary where there are $n+1$ 1's). At the end of the protocol they should all know if $x_1 + \cdots + x_k = 2^{n+1}-1$ or not. Each player can shout information so the others hear them. Let $d_k(n)$ be the number of bits shouted.

There is an easy protocol that shows $d_k(n) \leq n+1$, similar to the easy protocol for $\text{EXACT}_3(n)$. We leave it to the reader to show that there is an an elementary protocol which establishes $d_k(n) \leq \frac{n}{k-1} + O(1)$, similar to the protocol by Dean Foster for $d_3(n) \leq \frac{n}{2} + O(1)$ (Dean Foster may have also come up with this protocol).

Open Problem 5.2

1. Give an elementary protocol that shows $d_k(n) \leq \alpha n$ bits for some $\alpha < \frac{1}{k-1}$.

2. Devise a framework for lower bounds on elementary protocols (see Open Problem 4.2) for what this means.

6 What is the Best Known

I write this section somewhat reluctantly since I want you to focus on getting better *elementary* protocols. However, for the sake of completeness, I list what is known.

Chandra, Furst, and Lipton [2] showed the following:

1. $d_3(n) \leq O(\sqrt{n})$.
2. For all $k \geq 1$, $d_3(n) \geq \Omega(1)$. (This is what they really cared about since they used this lower bound to prove superlinear lower bounds on the length of some branching programs.)

Beigel, Gasarch, and Glenn [1] showed the following.

1. $d_3(n) \geq \Omega(\log \log n)$.
2. $d_k(n) \leq O(n^{1/(\log_2(k-1)+1)})$.

The proofs of both the upper and lower bounds use Ramsey theory. I have asked Ramsey theorists (1) what they think is true, and (2) when will it be known. The consensus is

1. The upper bounds for $d_3(n)$ and $d_k(n)$ are the likely answer.
2. There will be no improvement on the lower bounds for a long time, possibly never.

With that in mind, I urge my readers to try to get better *elementary* protocols rather than try to tighten the real upper and lower bounds.

References

[1] R. Beigel, W. Gasarch, and J. Glenn. The multiparty communication complexity of exact-t: improved bounds and new problems. In *Proceedings of the 31th International Symposium on Mathematical Foundations of Computer Science 2001,* Stara Lesna, Slovakia, pages 146–156, 2006.

[2] A. Chandra, M. Furst, and R. Lipton. Multiparty protocols. In *Proceedings of the Fifteenth Annual ACM Symposium on the Theory of Computing,* Boston MA, pages 94–99, 1983. `http://portal.acm.org/citation.cfm?id=808737`.