The Communication Complexity of the Exact-N Problem Revisited

William Gasarch[1], James Glenn[2], and Andre Utis[3]

[1] University of Maryland
Department of Computer Science
College Park, MD, 20742, USA
gasarch@cs.umd.edu
[2] Dept. of Computer Science,
Loyola College in Maryland, 4501 N. Charles St,
Baltimore, MD 21210.
jglenn@cs.loyola.edu
[3] Institute of Author3, Department of Author3
Address ZIP, Town, Street, Country
author3@inst3
[4] University of Maryland
Department of Computer Science
College Park, MD, 20742, USA
utis@cs.umd.edu

Abstract. If Alice has x, y, Bob has x, z and Carol has y, z can they determine if $x + y + z = N$? They can if (say) Alice broadcasts x to Bob and Carol; can they do better? Chandra, Furst, and Lipton studied this problem and showed sublinear upper bounds. They also had matching (up to an additive constant) lower bounds. We give an exposition of their result with some attention to what happens for particular values of N.

Keywords. Communication Complexity, Exact-N problem, Arithmetic Sequences

1 Introduction

Consider the following function f.

Definition 1. *Let $L, N \in \mathsf{N}$ and let $n = 2^L - 1$. We view elements of $\{0,1\}^L$ as numbers in $\{0, \ldots, n\}$ Let $f : \{0,1\}^L \times \{0,1\}^L \times \{0,1\}^L \to \{0,1\}$ be defined as*

$$f(x, y, z) = \begin{cases} 1 & \text{if } x + y + z = N; \\ 0 & \text{otherwise.} \end{cases} \tag{1}$$

We will refer to f as the Exact-N Problem.

Dagstuhl Seminar Proceedings 04421
Algebraic Methods in Computational Complexity
http://drops.dagstuhl.de/opus/volltexte/2005/102

Assume Alice has x, y, Bob has x, z, and Carol has y, z. Is there a protocol such that, at the end of it, they all know $f(x, y, z)$? (See [6] for the rigorous definition of a protocol.) We assume that they can each broadcast information to the other two. One protocol is (1) Alice broadcasts x, (2) Carol determines if $x + y + z = N$ or not, and then (3) Carol broadcasts 1 (for YES) or 0 (for NO). This takes $L + 1$ bits. Is there a protocol that uses $<< L$ bits?

Definition 2. *Let f be any function from $\{0,1\}^L \times \{0,1\}^L \times \{0,1\}^L$ to $\{0,1\}$. Assume Alice has x, y, Bob has x, z, and Carol has y, z. Let $d(f)$ be the number of bits transmitted in the optimal deterministic protocol for f. This is called the multiparty communication complexity of f. Note that there is always the $L+1$-bit protocol of (1) Alice broadcasts x, (2) Carol computes $f(x, y, z)$ and (3) Carol broadcasts $f(x, y, z)$. The cases of interest are when f can be computed with substantially fewer than L bits.*

Chandra, Furst, and Lipton [3] (see also [6]) exhibit matching (up to an addtive constant) upper and lower sublinear bounds on $d(f)$ for f the Exact-N Problem. The bound they get is related to a concept in combinatorics called *3-free sets* (see below), and hence is not explicit. Their motivation was that the results gave lower bounds on branching programs.

We present their proofs with several additions.

1. A recent paper of Gasarch and Glenn [4] has tables of sizes of 3-free sets. Those tables, together with this exposition, which tracks constants carefully, enables us to see, for what values of L, N, and n the protocol is sublinear.
2. The lower bound in [3] is only valid when $n \geq N$. One of the main points of their paper is that, in this case, the lower bound is not constant. If $n < N/3$ and Alice, Bob, and Carol all know this, then there is a 0-bit protocol: they all know that $x+y+z \neq N$. We give a lower bound that shows what happens when $n = \alpha N + \beta$, where $\frac{1}{3} \leq \alpha \leq 1$.
3. Chandra, Furst, and Lipton[3] actually looked at the Exact-N problem with k people and k inputs $x_1, \ldots, x_k$, where person i knows all inputs except for x_i. The solution to this problem depends on k-free sets. Large k-free sets are known and can be used to give an upper bound for the protocol. This appears to be a new result.

Definition 3.

1. *Let $[n]$ denote the set $\{1, \ldots, n\}$.*
2. *A set $A \subseteq [n]$ is 3-free if there do not exist $x, y, z \in A$ such that x, y, z form an arithmetic progression of length 3.*
3. *Let $sz(n)$ be the size of the largest 3-free set of $[n]$.*

2 The Upper Bound

2.1 The Upper Bound for any N

Theorem 1. *Let f be the Exact-N problem. Then*

$$d(f) \leq 2 + \left\lceil \lg\left(\frac{9N \ln(3N)}{\mathrm{sz}(3N)} + 1\right) \right\rceil .$$

(Note that this bound is independent of n and L. However, it is not of interest when the players know that $n \le N/3$ since $f(x, y, z) = 0$ and $d(f) = 0$.)

We prove the upper bound by a series of statements.

Definition 4. *Let $c, N \in \mathsf{N}$.*

1. *Let S_N be the set of all (x, y, z) such that $x, y, z \ge 0$ and $x + y + z = N$.*
2. *A proper c-coloring of S_N is a function $COL : S_N \to [c]$ such that there does not exist $x, y, z, \in [N]$ and $\lambda \in \mathsf{Z} - \{0\}$ such that $x + y + z + \lambda = N$ and*

$$COL(x + \lambda, y, z) = COL(x, y + \lambda, z) = COL(x, y, z + \lambda).$$

3. *Let $\chi(N)$ be the least c such that there is a proper c-coloring of S_N.*

The next theorem gives two protocols for the Exact-N problem, and hence two different upper bounds. The first one is smaller; however, the second one will be useful later.

Theorem 2. *Let f be the Exact-N problem.*

1. *$d(f) \le 2 + \lceil \lg(\chi(N) + 1) \rceil$.*
2. *$d(f) \le 5 + \lceil \lg(\chi(2N/3) + 1) \rceil$.*

Proof. 1) Let COL be a proper c-coloring of S_N where $c = \chi(N)$. We represent elements of $[c]$ by bit strings; however, we do not allow $0 \cdots 0$ to represent a color. Hence we need $\lceil \lg(\chi(N) + 1) \rceil$ bits. We denote $\lceil \lg(\chi(N) + 1) \rceil$ by g. Alice, Bob, and Carol will all know COL ahead of time. We present the protocol and then discuss why it works.

1. Alice has x, y, Bob has x, z, and Carol has y, z.
2. In this step all three players compute internally but do not broadcast.
   (a) Alice computes $z' = N - x - y$. (Note that $x + y + z' = N$ so $COL(x, y, z')$ exists so long as $z' \ge 0$.) If $z' \ge 0$ then Alice computes $COL(x, y, z') = a_1 \cdots a_g$. Otherwise $a_1 \cdots a_g = 0^g$.
   (b) Bob computes $y' = N - x - z$. (Note that $x + y' + z = N$ so $COL(x, y', z)$ exists so long as $y' \ge 0$.) If $y' \ge 0$ then Bob computes $COL(x, y', z) = b_1 \cdots b_g$. Otherwise $b_1 \cdots b_g = 0^g$.
   (c) Carol computes $x' = N - y - z$. (Note that $x' + y + z = N$ so $COL(x', y, z)$ exists so long as $x' \ge 0$.) If $z' \ge 0$ then Carol computes $COL(x', y, z) = c_1 \cdots c_g$. Otherwise $c_1 \cdots c_g = 0^g$.
3. Alice broadcasts $a_1 a_2 a_3 \cdots a_g$. (Note that this is exactly g bits.) If she broadcasts all 0's then everyone knows $f(x, y, z) = 0$ and the protocol terminates.
4. If $(\forall i)[b_i = a_i]$ then Bob broadcasts 1. Otherwise he broadcasts 0.
5. If $(\forall i)[c_i = a_i]$ then Carol broadcasts 1. Otherwise she broadcasts 0.
6. If both Bob and Carol broadcast a 1 then they all know $f(x, y, z) = 1$. If either of them broadcasts a 0 then they all know $f(x, y, z) = 0$.

Claim 1: If $f(x,y,z)=1$ then in the last three steps of the protocol Bob and Carol broadcast 1.

Proof. If $f(x,y,z)=1$ then $x'=x$, $y'=y$, and $z'=z$. Hence $(\forall i)[a_i=b_i=c_i]$.
(End of proof of Claim 1).

Claim 2: If in the last three steps of the protocol Bob and Carol broadcast 1 then $f(x,y,z)=1$.

Proof. Assume that at the end of the protocol Bob and Carol broadcast 1. Then

$$COL(x',y,z)=COL(x,y',z)=COL(x,y,z').$$

Recall that

$$x'=N-y-z,$$

$$y'=N-x-z,$$

and

$$z'=N-x-y.$$

Hence

$$COL(N-y-z,y,z)=COL(x,N-x-z,z)=COL(x,y,N-x-y).$$

Let $\lambda=(N-x-y-z)$. We have

$$COL(x+\lambda,y,z)=COL(x,y+\lambda,z)=COL(x,y,z+\lambda).$$

Since the coloring is proper we must have $\lambda=0$ so $x+y+z=N$.
(End of proof of Claim 2).

2) We present an alternative protocol. We assume N is divisible by 3.

1. Alice broadcasts 1 if $x \geq N/3$ and 0 otherwise,
2. Bob broadcasts 1 if $z \geq N/3$ and 0 otherwise.
3. Carol broadcasts 1 if $y \geq N/3$ and 0 otherwise.
4. There are four cases depending on how many of them broadcast a 1.
   (a) None of them broadcast a 1. Then $x+y+z \neq N$ and they are done. This took 3 bits.
   (b) Exactly one of them broadcasts a 1. We assume it is Alice (the other cases are identical). Alice and Bob set $x^- = x - N/3$. Then Alice, Bob, and Carol execute the protocol in part 1 to determine if $x^- + y + z = 2N/3$. This takes $2+\lceil \lg(\chi(2N/3)+1)\rceil$. Hence the total number of bits used is $5+\lceil \lg(\chi(2N/3)+1)\rceil$.

(c) Exactly two of them broadcast a 1. We assume they are Alice and Bob (the other cases are identical). Alice and Bob set $x^- = x - N/3$. Bob and Carol set $z^- = z - N/3$. Then Alice, Bob, and Carol execute the protocol in part 1 to determine if $x^- + y + z^- = N/3$. This takes $2 + \lceil \lg(\chi(N/3) + 1) \rceil$. Hence the total number of bits used is $5 + \lceil \log(\chi(N/3) + 1) \rceil$.

(d) All three of them broadcast a 1. Alice broadcasts a 1 if either $x > N/3$ or $y > N$, and a 0 otherwise. Bob broadcasts a 1 if $z > N/3$ and a 0 otherwise. If either of them broadcasts a 1 then $x+y+z \neq N$, otherwise $x + y + z = N$. This takes 2 bits so the total number of bits is 5.

We relate $\chi(N)$ with other combinatorial concepts.

Definition 5.

1. *A* 3*-AP is an arithmetic sequence of length* 3.
2. *Let $C(N)$ be the minimum number of colors needed to color $[N]$ such that there are no monochromatic 3-AP's.*

Lemma 1.

1. $\chi(N) \leq C(3N)$.
2. $C(M) \leq \frac{3M \ln M}{\mathrm{sz}(M)}$.
3. $\chi(N) \leq \frac{9N \ln(3N)}{\mathrm{sz}(3N)}$. *(This follows from 1 and 2.)*

Proof. 1) Assume that $C(3N) = c$. Let COL be a c-coloring of $[3N]$ with no monochromatic 3-AP's. We use this to construct a proper c-coloring COL' of S_N.

$$COL'(x, y, z) = COL(x + 2y + 3z).$$

We show that COL' is proper. Assume that there exists x, y, z, λ such that $x + y + z + \lambda = N$ and

$$COL'(x + \lambda, y, z) = COL'(x, y + \lambda, z) = COL'(x, y, z + \lambda).$$

Then

$$COL(x + 2y + 3z + \lambda) = COL(x + 2y + 3z + 2\lambda) = COL(x + 2y + 3z + 3\lambda).$$

Since COL has no monochromatic 3-AP's we must have $\lambda = 0$. Hence COL' is proper.

2) Let $A \subseteq [M]$ be a set of size $C(M)$ with no 3-APs. We use A to obtain a coloring of $[M]$. The main idea is that we use randomly chosen translations of A to cover all of $[M]$.

Let $x \in [M]$. Pick a translation of A by picking $t \in [-M, M]$. The probability that $x \in A + t$ is $\frac{|A|}{2M}$. Hence the probability that $x \notin A + t$ is $1 - \frac{|A|}{2M}$. If we pick

s translations $t_1, \ldots, t_s$ at random (s to be determined later) then the expected number of x that are not covered by any $A + t_i$ is

$$M\left(1 - \frac{|A|}{2M}\right)^s \leq Me^{-s\frac{|A|}{2M}}.$$

We need to pick s such that this quantity is < 1. We take $s = \frac{3M \ln M}{|A|}$ which yields

$$Me^{-s\frac{|A|}{2M}} = Me^{(-3/2)\ln M} = M^{-1/2} < 1.$$

(We could have taken $s = \frac{(2+\epsilon)\ln M}{|A|}$ which works for large M, but we wanted a value of s that works for all M.)

We color $[M]$ by coloring each of the s translates a different color. If a number is in two translates then we color it by one of them arbitrarily. Clearly this coloring has no monochromatic 3-APs. Note that it uses $\frac{3M \ln M}{|A|} = \frac{3M \ln M}{\mathrm{sz}(M)}$ colors.

We now restate and prove the main theorem.

Theorem 3. *Let f be the Exact-N problem. Then*

$$d(f) \leq 3 + \left\lceil \lg \frac{9N \ln(3N)}{\mathrm{sz}(3N)} \right\rceil.$$

Proof. By Theorem 2 we have

$$d(f) \leq 2 + \lceil \lg(\chi(N) + 1) \rceil.$$

By Lemma 1

$$\chi(N) \leq \frac{9N \ln(3N)}{\mathrm{sz}(3N)}.$$

Hence

$$d(f) \leq 2 + \left\lceil \lg(\frac{9N \ln(3N)}{\mathrm{sz}(3N)} + 1) \right\rceil.$$

3 What is the Complexity

Theorem 2 gives an upper bound that we will later see is very close to the lower bound. Theorem 1 gives an upper bound as well. Neither theorem tells us if $d(f)$ is sublinear. In this section we establish that $d(f)$ is sublinear and, for some actual values of n, give upper bounds on $d(f)$.

If $n < N/3$, and Alice, Bob, and Carol all know this, then there is an O(1) protocol: since $x + y + z < N$ they all, without any communication, know that $f(x, y, z) = 0$. Hence we are interested in the case when $n \geq N/3$. For definitiveness we will look at the case of $n = N$. Note that the trivial protocol of Alice broadcasting x of length $L = \lg n$ is the one we want to beat.

We will refer the the protocol from Theorem 1 as 'the CFL protocol' in honor of the authors Chandra, Furst, and Lipton.

3.1 What Happens for Large N

Corollary 1. *Let f be the Exact-N problem. The CFL-protocol shows $d(f) \le O(\sqrt{\log N})$. When $N = n$ we get $O(\sqrt{\log n}) = O(\sqrt{L})$. (Note that this is sublinear.)*

Proof.

$$d(f) \le 3 + \left\lceil \lg \frac{9n \ln(3n)}{\mathrm{sz}(3n)} \right\rceil = O\left(\log \frac{n \log n}{\mathrm{sz}(3n)} \right).$$

Behrends ([1] but see also [4]) showed that that there exists a c such that $\mathrm{sz}(m) \ge me^{-c\sqrt{\log m}}$. It is easy to see that there exists a (possibly different) constant c such that $\mathrm{sz}(3m) \ge me^{-c\sqrt{\log m}}$. Hence

$$\frac{N \log N}{\mathrm{sz}(3N)} \le \frac{N \log N}{Ne^{-c\sqrt{\log N}}} = \frac{\log N}{e^{-c\sqrt{\log N}}} \le (\log N)(e^{c\sqrt{\log N}}) \le e^{c\sqrt{\log n} + \log\log n}.$$

Hence we have

$$d(f) = O\left(\log \left(\frac{N \log N}{\mathrm{sz}(3N)} \right) \right) = O(\log(e^{c\sqrt{\log N} + \log\log N})) = O(\sqrt{\log N}).$$

If $n = N$ then

$$d(f) = O(\sqrt{\log N}) = O(\sqrt{\log} n) = O(\sqrt{L}).$$

3.2 What Happens for Particular Values of n?

Gasarch and Glenn [4] survey several constructions of 3-free sets and use them to produce actual 3-free sets. The following table uses the values of $\mathrm{sz}(n)$ presented there. The table gives n, $\mathrm{sz}(n)$, $L = \lg n$, and $d(f) = 3 + \left\lceil \lg \frac{9n\ln(3n)}{\mathrm{sz}(n)} \right\rceil$. We use $\mathrm{sz}(n)$ instead of $\mathrm{sz}(3n)$ since this is the data we had. Since $3\mathrm{sz}(n) \ge \mathrm{sz}(3n) \ge \mathrm{sz}(n)$, and we end up taking logarithms, this will make our table at most 2 bits more than the actual protocol. We also give the ratio of $d(f)$ to $\sqrt{L}$ since $O(\sqrt{L})$ is what the analysis gives. Note the following.

1. The lowest value where we know that the CFL protocol beats the trivial one is around 10^6. Since larger 3-free sets may be possible this might be improved in the future.
2. At $n = 10^{18}$, $d(f) = L/2$. At $n = 10^{36}$, $d(f) = L/3$. At $n = 10^{60}$, $d(f) = L/4$. Hence the degree to which the CFL protocol is better than the trivial one seems to increase with n.
3. The ratio of $d(f)$ to $\sqrt{L}$ (roughly) decreases from 4 to 3.5 in our data. It is not clear if a limit exists.

n	$sz(n)$	df	L	$\lceil\sqrt{L}\rceil$	ratio
10^1	5.00×10^0	5	4	2	2.50
10^2	2.40×10^1	10	7	3	3.78
10^3	1.05×10^2	12	10	4	3.79
10^4	5.12×10^2	13	14	4	3.47
10^5	2.04×10^3	15	17	5	3.64
10^6	8.19×10^4	13	20	5	2.91
10^7	3.28×10^4	18	24	5	3.67
10^8	1.31×10^5	20	27	6	3.85
10^9	5.73×10^5	21	30	6	3.83
10^{10}	2.74×10^6	22	34	6	3.77
10^{11}	1.56×10^7	23	37	7	3.78
10^{12}	9.81×10^7	24	40	7	3.79
10^{13}	5.27×10^8	25	44	7	3.77
10^{14}	3.51×10^9	26	47	7	3.79
10^{15}	2.10×10^{10}	26	50	8	3.68
10^{16}	1.33×10^{11}	27	54	8	3.67
10^{17}	8.25×10^{11}	28	57	8	3.71
10^{18}	5.68×10^{12}	29	60	8	3.74
10^{19}	3.78×10^{13}	29	64	8	3.62
10^{20}	2.39×10^{14}	30	67	9	3.67
10^{21}	1.63×10^{15}	31	70	9	3.71
10^{22}	1.22×10^{16}	31	74	9	3.60
10^{23}	7.65×10^{16}	32	77	9	3.65
10^{24}	5.17×10^{17}	32	80	9	3.58
10^{25}	3.67×10^{18}	33	84	10	3.60
10^{26}	2.46×10^{19}	34	87	10	3.65
10^{27}	1.73×10^{20}	34	90	10	3.58
10^{28}	1.26×10^{21}	35	94	10	3.61
10^{29}	8.90×10^{21}	35	97	10	3.55
10^{30}	6.33×10^{22}	36	100	10	3.60

n	$sz(n)$	df	L	$\lceil\sqrt{L}\rceil$	ratio
10^{31}	4.66×10^{23}	37	103	11	3.65
10^{32}	3.35×10^{24}	38	107	11	3.67
10^{33}	2.40×10^{25}	38	110	11	3.62
10^{34}	1.73×10^{26}	39	113	11	3.67
10^{35}	1.29×10^{27}	39	117	11	3.61
10^{36}	9.63×10^{27}	40	120	11	3.65
10^{37}	7.09×10^{28}	40	123	12	3.61
10^{38}	5.24×10^{29}	41	127	12	3.64
10^{39}	3.91×10^{30}	41	130	12	3.6
10^{40}	2.94×10^{31}	42	133	12	3.64
10^{41}	2.20×10^{32}	42	137	12	3.59
10^{42}	1.66×10^{33}	42	140	12	3.55
10^{43}	1.26×10^{34}	43	143	12	3.6
10^{44}	9.63×10^{34}	43	147	13	3.55
10^{45}	7.31×10^{35}	44	150	13	3.59
10^{46}	5.59×10^{36}	44	153	13	3.56
10^{47}	4.26×10^{37}	45	157	13	3.59
10^{48}	3.27×10^{38}	45	160	13	3.56
10^{49}	2.53×10^{39}	45	163	13	3.52
10^{50}	1.96×10^{40}	46	167	13	3.56
10^{51}	1.52×10^{41}	46	170	14	3.53
10^{52}	1.18×10^{42}	47	173	14	3.57
10^{53}	9.13×10^{42}	47	177	14	3.53
10^{54}	7.15×10^{43}	47	180	14	3.50
10^{55}	5.60×10^{44}	48	183	14	3.55
10^{56}	4.39×10^{45}	48	187	14	3.51
10^{57}	3.45×10^{46}	48	190	14	3.48
10^{58}	2.71×10^{47}	49	193	14	3.53
10^{59}	2.12×10^{48}	49	196	14	3.50
10^{60}	1.69×10^{49}	50	200	15	3.54
10^{61}	1.34×10^{50}	50	203	15	3.51
10^{62}	1.07×10^{51}	50	206	15	3.48
10^{63}	8.48×10^{51}	51	210	15	3.52
10^{64}	6.73×10^{52}	51	213	15	3.49
10^{65}	5.33×10^{53}	51	216	15	3.47

4 Lower Bounds

Chandra, Furst and Lipton [3] showed that if $n \geq N$, then $d(f) \geq 1 + \lg \chi(N)$.

Theorem 4. *If f is restricted to $x, y, z \in \{0, \ldots, N\}$ then $d(f) \geq \log \chi(N)$. (Note that in this case the upper bound and lower bound differ by an additive constant of at most 2.)*

Proof. Let P be a protocol for Exact-N. We use this protocol to create a proper coloring of S_N.

Let x, y, z be such that $x + y + z = N$.

$COL(x, y, z)$ = *the transcript of communication if* (x, y, z) *is fed into the protocol.*

We first claim that this is a proper coloring. Note that if

$$COL(x + \lambda, y, z) = COL(x, y + \lambda, z) = COL(x, y, z + \lambda)$$

then the transcripts of $(x + \lambda, y, z)$, $(x, y + \lambda, z)$, and $(x, y, z + \lambda)$ are identical. By a standard result in communication complexity (see [6]) the transcript for (x, y, z) will be identical to this transcript. Since $x + y + z = N$ we have that the protocol says 1 on $(x + \lambda, y, z)$. Hence $x + \lambda + y + z = N$ so $\lambda = 0$.

Therefore the number of possible transcripts that lead to a YES is at least $\chi(N)$. Note that the number of transcripts that lead to a NO is at least 1. By a standard result in communication complexity (see[6]) we obtain $d(f)$ is at least the lg of the number of transcripts. Hence $d(f) \geq 1 + \lg \chi(N)$.

We present a lower bound that covers cases close to $n \leq N/3$.

Theorem 5. *Let* $0 \leq \alpha < 1$ *and* $\beta \in \mathsf{N}$. *If* f *is restricted to* $x, y, z \in \{0, \ldots, \alpha N + \beta\}$ *then* $d(f) \geq \log \chi(\frac{3\alpha-1}{2}N + \beta)$.

Proof. Let f be be the Exact-N problem restricted to $x, y, z \in \{0, \ldots, \alpha N + \beta\}$. We proceed by reducing an easier problem to our problem.

Fix an integer $0 \leq m \leq \alpha N$. Let f^m be the Exact-N problem where the inputs are restricted by

$$x, y \in \{m, \ldots, \alpha N + \beta\} \text{ and } z \in \{0, \ldots, \alpha N + \beta\}.$$

This problem is clearly easier than the original problem. Hence $d(f^m) \leq d(f)$.

Since m is a fixed positive parameter of the problem, each party can independently subtract m from x and y, and add $2m$ to z. The sum will remain the same and all the inputs will remain non-negative, i.e. we will get a problem $f^{m'}$ with the inputs restricted by

$$x, y \in \{0, \ldots, \alpha N - m + \beta\} \text{ and } z \in \{2m, \ldots, \alpha N + 2m + \beta\}$$

which is equivalent to f^m. Hence $d(f^{m'}) = d(f^m) \leq d(f)$.

Let $m = \frac{1-\alpha}{2}N$. Note that $m > 0$ since $\alpha < 1$. Denote $f^{m'}$ with this value of m by f'. So f' is the Exact-N problem with $x, y \in \{0, \ldots, \frac{3\alpha-1}{2}N + \beta\}$ and $z \in \{(1-\alpha)N, \ldots, N+\beta\}$. We can further make this problem easier by narrowing the range of z to be $\{\frac{3(1-\alpha)}{2}N, \ldots, N + \beta\}$. Let f'' be this problem. Note that $x + y + z = N$ iff $x + y + (z - \frac{3(1-\alpha)}{2}N + \beta) = \frac{3\alpha-1}{2}N + \beta$.

Let $M = \frac{3\alpha-1}{2}N + \beta$. Let f''' be the Exact-M problem restricted to $x, y, z \in \{0, \ldots, M\}$. By the above iff statement we have that $d(f'') = d(f''')$. We can apply Theorem 4 to f''' and hence $d(f''') \geq \log \chi(M) = \log \chi(\frac{3\alpha-1}{2}N + \beta)$.

We can use Theorems 1, and the fact that $\chi(N)$ is not constant (see [3]), and another protocol to establish a sharp cutoff between where $d(f)$ is constant and where it is not.

Theorem 6.

1. *Let* $0 \le \alpha \le \frac{1}{3}$ *and* $\beta \in \mathsf{N}$. *If* f *is restricted to* $x, y, z \in \{0, \ldots, \alpha N + \beta\}$ *then* $d(f) = O(1)$.
2. *Let* $\alpha > \frac{1}{3}$. *If* f *is restricted to* $x, y, z \in \{0, \ldots, \alpha N\}$ *then* $d(f)$ *is not constant.*

Proof. 1) We describe a protocol for this case.

1. Alice broadcasts 1 if $x \ge N/3$ and 0 otherwise. Bob broadcasts 1 if $z \ge N/3$ and 0 otherwise. Carol broadcasts 1 if $y \ge N/3$ and 0 otherwise.
2. There are four cases depending on how many of them broadcast a 1.
   (a) None of them broadcast a 1. Then $x + y + z \ne N$ and they are done. This took 3 bits.
   (b) Exactly one of them broadcasts a 1. We assume it is Alice (the other cases are identical). Bob broadcasts 1 if $z \ge \frac{N}{3} - \beta$ and 0 otherwise. Carol broadcasts 1 if $y \ge \frac{N}{3} - \beta$ and 0 otherwise.
   (c) If either broadcasts 0 then $x + y + z \ne N$ and they are done. If both broadcast 1 then (1) Alice and Bob set $x^- = x - \frac{N}{3}$, (2) Bob and Carol set $z^- = z - D$, (3) Alice and Carol set $y^- = y - D$, and (4) Alice, Bob and Carol use the protocol from Theorem 1.1 to determine if $x^- + y^- + z^- = \beta$. This will take $3 + \log \chi(\beta)$ bits, a constant.
3. Exactly two of them broadcasts a 1. We assume they are Alice and Bob (the other cases are identical). Carol broadcasts 1 if $y \ge \frac{N}{3} - 2\beta$ and 0 otherwise. If she broadcasts 0 then $x + y + z \ne N$ and they are done. If she broadcasts 1 then (1) Alice and Bob set $x^- = x - N/3$, (2) Bob and Carol set $z^- = z - N/3$, (3) Alice and Carol set $y^- = y - D$, and (4) Alice, Bob and Carol use the protocol from Theorem 1 to determine if $x' + y' + z' = 2\beta$. This takes $3 + \lg(\chi(\beta))$ bits, a constant.
4. All three of them broadcasts a 1. Alice broadcasts a 0 if either $x > N/3$ or $y \ge N/3$ and a 1 otherwise. If she broadcasts a 0 then $x + y + z \ne N$ so they are done. If she broadcasts a 1 then Carol broadcasts 0 if $z > N/3$ and 1 otherwise. If she broadcasts a 1 then $x + y + z = N$, otherwise $x + y + z \ne N$. In either case they are done. This took 5 bits total.

2) By Theorem 5 $d(f) \ge \log \chi(\frac{3\alpha-1}{2} N + \beta)$. Since $\alpha > \frac{1}{3}$ there is a constant γ such that $d(f) \ge \lg(\chi(\gamma N))$. It is known that $\chi(\gamma)$ is not constant. One can prove this from Gallai's Theorem, as was done in [3], or from van der Waerden's Theorem, which we leave as an exercise.

In the case where $n \le \alpha n + \beta$ we have a lower bound of $\lg \chi(\frac{3\alpha-1}{2} N + \beta)$ and an upper bound of $3 + \lg(\chi(N))$ or $5 + \lg(\chi(2N/3))$ How do these bounds compares?

We first need a lemma about the behavior of $\lg(\chi(N))$. Note that it is purely combinatorial lemma proven using the upper and lower bounds on the Exact-N problem.

Lemma 2. *For any $\gamma > 0$ there is a constant c such that $\lg(\chi(N)) \le c + \lg(\chi(\gamma N))$.*

Proof. Let f be the Exact-N problem with no restrictions on the input. By Theorem 4 $\lg(\chi(N)) \le d(f)$. By Theorem 2.2 $d(f) \le 5 + \lg(\chi(2N/3))$ Hence we have $\lg(\chi(N)) \le d(f) \le 5 + \lg(\chi(2N/3))$. We can iterate this p times to obtain

$$\lg(\chi(N)) \le 5p + \lg(\chi((\frac{2}{3})^p N)).$$

Let p be the least integer such that $(\frac{2}{3})^p < \gamma$. Clearly

$$\lg(\chi(N)) \le 5p + \lg(\chi((\frac{2}{3})^p N)) \le 5p + \lg(\chi(\gamma N)).$$

Theorem 7. *Let $\alpha > 1/3$ and $\beta \in \mathsf{N}$. Let f be be the Exact-N problem restricted to $x, y, z \in \{0, \ldots, \alpha N + \beta\}$. Then the upper and lower bounds for $d(f)$ from Theorems 5 and Theorem 2 differ by an additive constant (which depends on α).*

Proof. We express the lower bound on $d(f)$ from Theorem 5 as $\lg(\chi(\gamma N))$ where $\gamma > 0$. Hence we have $\lg(\chi(\gamma N)) \ge d(f)$.

By Theorem 2 we have $d(f) \le \lg(\chi(N))$. By Lemma 2 these upper and lower bounds differ by an additive constant.

5 What Else is Known

Chandra, Furst, and Lipton [3] actually proved a generalization of what we have presented here.

Consider the following function f.

Definition 6. *Let $k, L, N \in \mathsf{N}$ and let $n = 2^L - 1$. We view elements of $\{0,1\}^L$ as numbers in $\{0, \ldots, n\}$ Let $f_k : \{0,1\}^L \times \cdots \times \{0,1\}^L \to \{0,1\}$ (there are k inputs to f_k) be defined as*

$$f_k(x_1, \ldots, x_k) = \begin{cases} 1 & \text{if } \sum_{i=1}^{k} x_i = N; \\ 0 & \text{otherwise.} \end{cases} \qquad (2)$$

We refer to f_k as the Exact-N problem for k players.

The following lemmas and theorem can be proven by the same techniques for the $k = 3$ case.

Definition 7. *Let $c, N \in \mathsf{N}$.*

1. *Let S_N^k be the set of all $(x_1, \ldots, x_k)$ such that $\sum_{i=1}^{k} x_i = N$.*

2. *A proper c-coloring of* S_N^k *is a function* $COL : S_N^k \to [c]$ *such that there does not exist* $x_1, \ldots, x_k \in [N]$ *and* $\lambda \in \mathsf{Z} - \{0\}$ *such that* $x_1 + \cdots + x_k + \lambda = N$ *and*

$$c(x_1 + \lambda, x_2, \ldots, x_k) = c(x_1, x_2 + \lambda, \ldots, x_k) = c(x_1, x_2, \ldots, x_k + \lambda).$$

3. *Let* $\chi_k(N)$ *be the least c such that there is a proper c-coloring of* S_N^k.

Theorem 8. *Let* f_k *be the Exact-N problem for k players.*

1. $d(f_k) \leq k + \lceil \lg \chi_k(N) \rceil$.
2. $d(f_k) \leq 2k + \left\lceil \lg \chi_k(\frac{k-1}{k}N) \right\rceil$.

Definition 8.

1. *If* $k \in \mathsf{N}$ *then a k-AP is an arithmetic sequence of length k.*
2. *Let* $C_k(N)$ *be the minimum number of colors needed to color* $[n]$ *such that there are no monochromatic k-AP's.*
3. $\mathrm{sz}_k(n)$ *is the size of the largest k-free set of* $[n]$.

Lemma 3.

1. $\chi_k(N) \leq C_k(kN)$.
2. $C_k(M) \leq \frac{3M \ln M}{\mathrm{sz}_k(M)}$.
3. $\chi_k(N) \leq \frac{9N \ln(3N)}{\mathrm{sz}_k(3N)}$. *(This follows from 1 and 2.)*

Theorem 9. *Let* f_k *be the Exact-N problem for k players. Then*

$$d(f_k) \leq k + \left\lceil \lg \frac{9N \ln(3N)}{\mathrm{sz}_k(3N)} \right\rceil.$$

The following bound on k-free sets is known ([8] but see also [7]).

Theorem 10. $\mathrm{sz}_k(M) \geq M e^{-c(\log M)^{1/(k+1)}}$.

Combining Theorems 9 and 10 yields the following result. This result appears here for the first time. It seems that Chandra, Furst, and Lipton were unaware of the bounds from [8] and hence could not obtain an explicit upper bound for $d(f_k)$.

Theorem 11. *Let* f_k *be the Exact-N problem for k players. Then*

$$d(f_k) \leq O((\log N)^{1/(k+1)}).$$

Theorem 12. *Let* $0 \leq \alpha < 1$ *and* $\beta \in \mathsf{N}$. *If* f_k *is restricted to* $x_1, x_2, \ldots, x_k \in \{0, \ldots, \alpha N + \beta\}$ *then* $d(f_k) \geq \log \chi(\frac{k\alpha - 1}{k-1}N + \beta)$.

Theorem 13. *Let* $t \in \mathsf{N}$. *If* f_k *is restricted to* $x_1, \ldots, x_k \in \{0, \ldots, \frac{N}{t}\}$ *then* $d(f_k) \geq \log \chi(\frac{N}{2}(\frac{k}{t} - 1))$.

6 Open Problems

1. The upper bound on $d(f)$ depends on the size of large 3-free sets. Larger 3-free sets will imply lower upper bounds on $d(f)$. It is an open problem to obtain $\mathrm{sz}(m) >> ne^{-c\sqrt{\log m}}$. It is known that $\mathrm{sz}(m) < O(m\sqrt{\frac{\log\log m}{\log m}})$ ([2] but see also [5]). If $\mathrm{sz}(m) = \Theta(m\sqrt{\frac{\log\log m}{\log m}})$ then in the $n = N$ case $d(f) \le O(\log\log n) = O(\log L)$.
2. The estimates on the lower bound on $d(f)$ are far from those on the upper bounds. Any improvement on lower bounds on $\chi(N)$ would help here.
3. Similar open problems to those above apply for $d(f_k)$.
4. There has been no empirical work on 4-free sets or k-free sets (except for [9] which deals with very small numbers). Empirical work on 4-free sets would enable us to show where the protocol for $d(f_4)$ is really sublinear, and also when it is substantially better than the protocol for $d(f_3)$.

References

1. F. Behrend. On set of integers which contain no three in arithmetic progression. *Proc. of the National Acadamy of Science (USA)*, 23:331–332, 1946.
2. J. Bourgain. On triples in arithmetic progression. *Geometric and Functional Analysis*, 9:968–984, 1999.
3. A. Chandra, M. Furst, and R. Lipton. Multiparty protocols. In *Proc. of the 15th ACM Sym. on Theory of Computing*, pages 94–99, 1983.
4. W. Gasarch and J. Glenn. Finding large sets without arithmetic progressions of length three: An empirical view, 2004. Email him at gasarch@cs.umd.edu for a copy. Not ready enough to be on website.
5. B. Green. On triples in arith. prog., 1999. www.dpmms.cam.ac.uk/˜bjg23/papers/bourgain.pdf.
6. E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 1997.
7. I. Laba and M. T. Lacey. On sets of integers not containing long arithmetic progressions, 2001. Website arxiv.org/pdf/math.CO/0108155 or www.math.ubc.ca/ ilaba/preprints.
8. R. Rankin. Sets of integers containing not more than a given number of terms in an arithmetic progression, 1960—1961.
9. S. Wagstaff. On k-free sequences of integers. *Mathematics of Computation*, pages 767–771, 1972.