Exactly N With More Than 3 Players

University of Toronto Theory Student Seminar
(October 2022)

Lianna Hambardzumyan Toniann Pitassi
Suhail Sherif **Morgan Shirley** Adi Shraibman

Communication Complexity

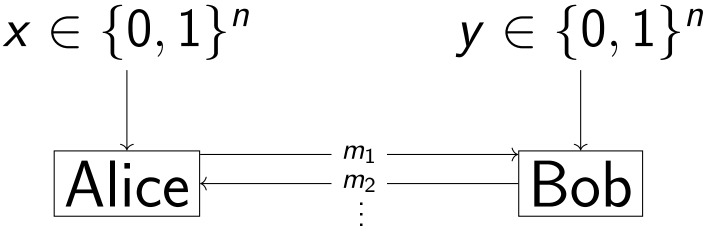
Alice

Bob

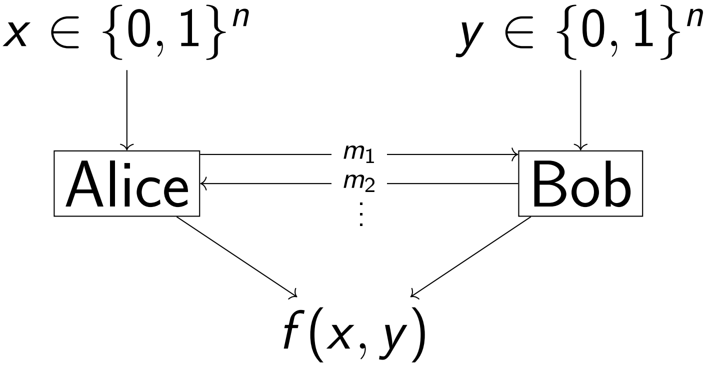
Communication Complexity

$$\begin{array}{ccc} x \in \{0,1\}^n & \qquad & y \in \{0,1\}^n \\ \downarrow & & \downarrow \\ \boxed{\text{Alice}} & & \boxed{\text{Bob}} \end{array}$$

Communication Complexity

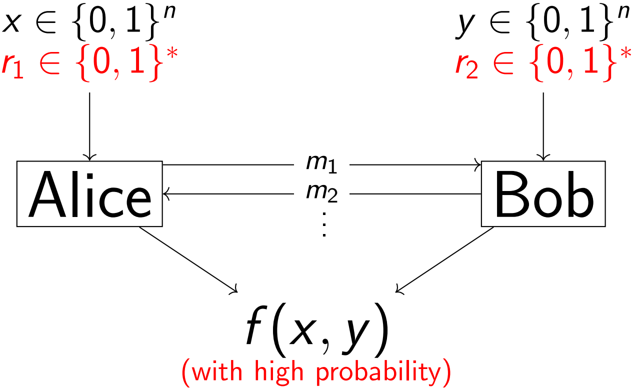


Communication Complexity



The cost of the protocol is the *number of bits exchanged*.

Randomized Communication Complexity



Classical Complexity:
P vs BPP still open

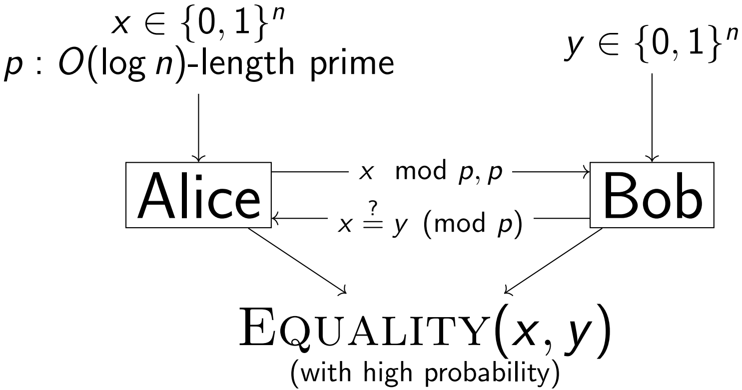
Communication Complexity:
Randomness helps!

Randomized Communication Complexity

$$\textsc{Equality}(x, y) = 1 \Leftrightarrow x = y$$

Randomized Communication Complexity

$$\textsc{Equality}(x, y) = 1 \Leftrightarrow x = y$$



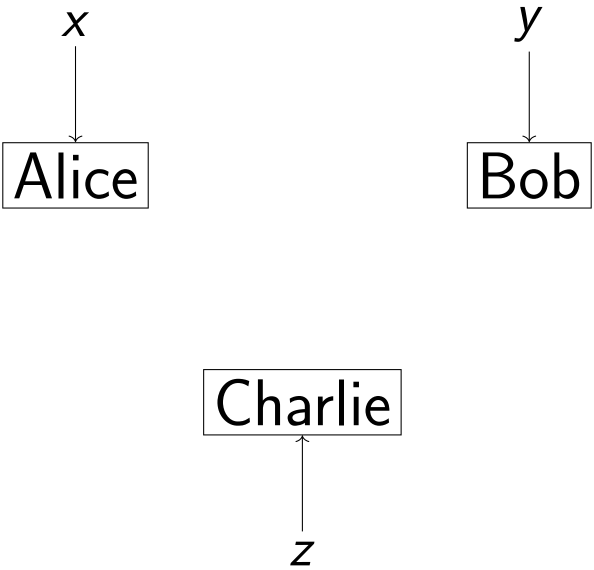
3-party communication complexity

Alice

Bob

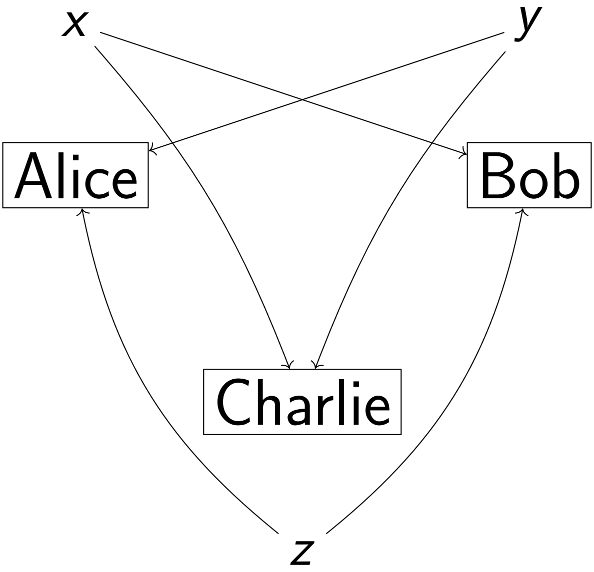
Charlie

3-party communication complexity



This is the *number-in-hand* model (NIH)

3-party communication complexity



This is the *number-on-forehead* model (NOF)

Why we care about NOF complexity

Applications to other fields!

- Strong NOF lower bounds give ACC_0 lower bounds [Y90,HG91]
- Lower bounds for Lovász-Schrijver systems in proof complexity [BPS07]
- Explicit pseudorandom generator constructions [BNS92]
- Time-space trade-offs in Turing Machines [BNS92]
- This talk: applications to **additive combinatorics**

NIH vs. NOF

NOF lower bounds seem harder to prove than NIH lower bounds.

Example: EQUALITY

Model	Det.	Rand.	Notes
2-party	Hard	Easy	Yao, folklore
NIH	Hard	Easy	by reduction to 2-party model
NOF	Easy	Easy	Charlie announces $x = y$ Bob announces $x = z$

NIH vs. NOF

NOF lower bounds seem harder to prove than NIH lower bounds.

Example: EQUALITY

Model	Det.	Rand.	Notes
2-party	Hard	Easy	Yao, folklore
NIH	Hard	Easy	by reduction to 2-party model
NOF	Easy	Easy	Charlie announces $x = y$ Bob announces $x = z$

Can we separate randomized and deterministic communication in the NOF model?

The $\textsc{Exactly}N$ function

Inputs $x_1, \ldots, x_k$ are in $\{0, \ldots, N\}$.

$\textsc{Exactly}N(x_1, \ldots, x_k) = 1$ if $\sum_{i=1}^{k} x_i = N$

$\textsc{Exactly}N$ has an easy randomized protocol

$\textsc{Exactly}N$ is a candidate hard function for deterministic NOF communication...

The $\textsc{Exactly}N$ function

Inputs $x_1, \ldots, x_k$ are in $\{0, \ldots, N\}$.

$\textsc{Exactly}N(x_1, \ldots, x_k) = 1$ if $\sum_{i=1}^{k} x_i = N$

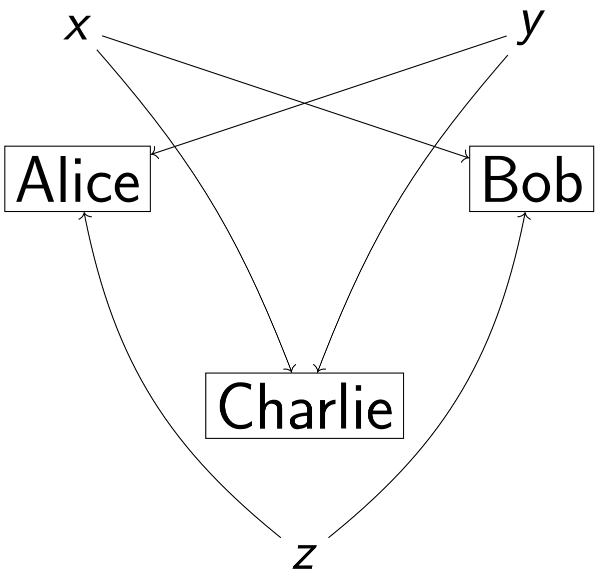
$\textsc{Exactly}N$ has an easy randomized protocol

$\textsc{Exactly}N$ is a candidate hard function for deterministic NOF communication...but it isn't maximally hard!

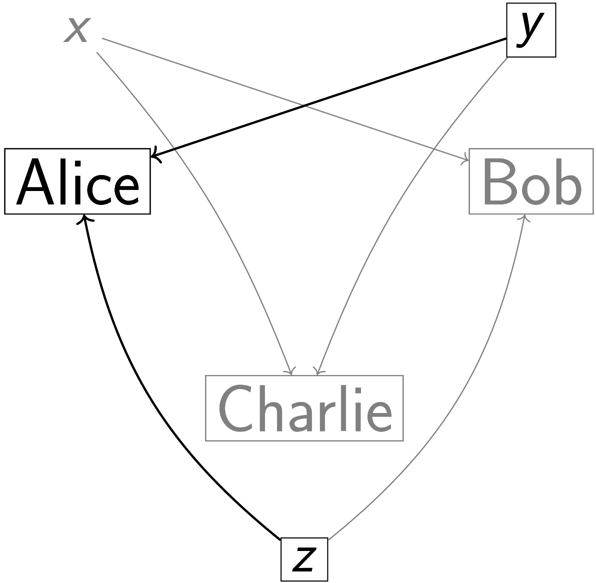
A maximally hard function would take $O(\log N)$ bits of communication.

$\textsc{Exactly}N$ can be done with less.

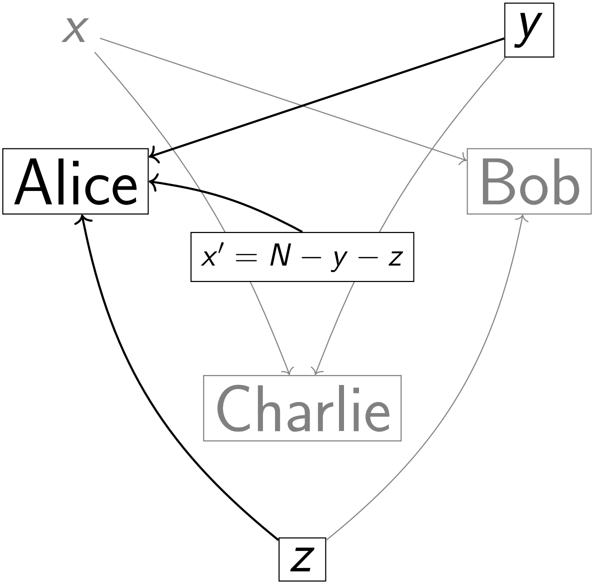
Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$



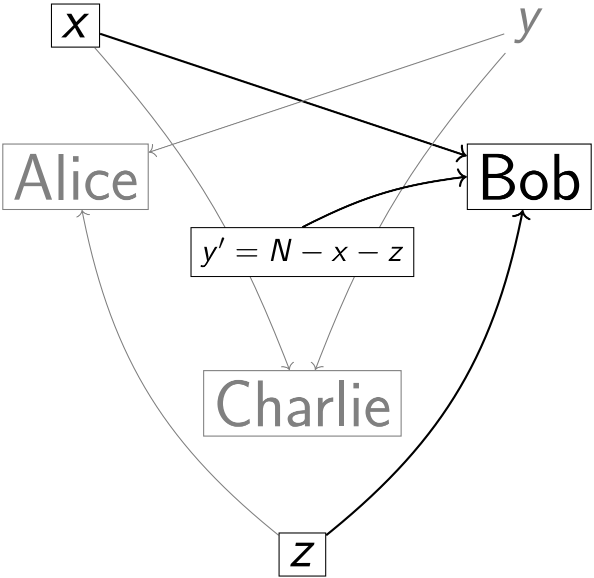
Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$



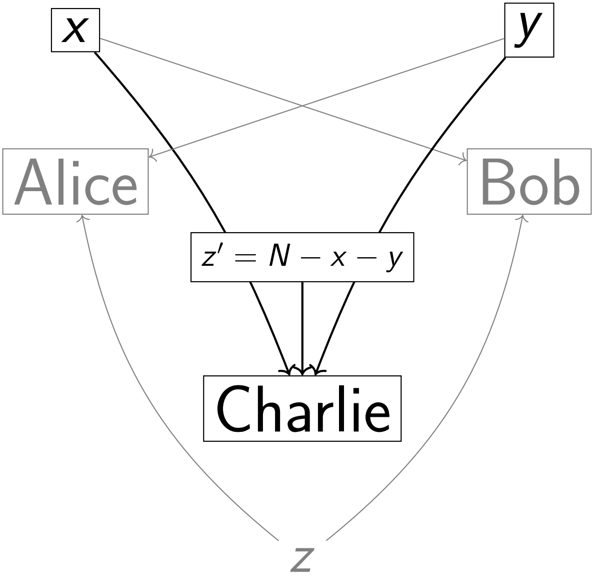
Chandra/Furst/Lipton protocol for ExactlyN



Chandra/Furst/Lipton protocol for EXACTLYN



Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$



Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$

$$\boxed{x' = N - y - z} \qquad \boxed{y' = N - x - z} \qquad \boxed{z' = N - x - y}$$

Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$

$$\boxed{x' = N - y - z} \qquad \boxed{y' = N - x - z} \qquad \boxed{z' = N - x - y}$$

Let $\Delta = N - (x + y + z)$

Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$

$\boxed{x' = N - y - z}$ $\boxed{y' = N - x - z}$ $\boxed{z' = N - x - y}$

Let $\Delta = N - (x + y + z)$

$(x' - x) = (y' - y) = (z' - z) = \Delta$

Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$

$\boxed{x' = N - y - z}$ $\boxed{y' = N - x - z}$ $\boxed{z' = N - x - y}$

Let $\Delta = N - (x + y + z)$

$(x' - x) = (y' - y) = (z' - z) = \Delta$

Define $T = x + 2y + 3z$

Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$

$\boxed{x' = N - y - z}$ $\boxed{y' = N - x - z}$ $\boxed{z' = N - x - y}$

Let $\Delta = N - (x + y + z)$

$(x' - x) = (y' - y) = (z' - z) = \Delta$

Define $T = x + 2y + 3z$

$T_x = x' + 2y + 3z$

Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$

$$\boxed{x' = N - y - z} \qquad \boxed{y' = N - x - z} \qquad \boxed{z' = N - x - y}$$

Let $\Delta = N - (x + y + z)$

$(x' - x) = (y' - y) = (z' - z) = \Delta$

Define $T = x + 2y + 3z$

$T_x = x' + 2y + 3z = T - \Delta$

Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$

$\boxed{x' = N - y - z}$ $\boxed{y' = N - x - z}$ $\boxed{z' = N - x - y}$

Let $\Delta = N - (x + y + z)$

$$(x' - x) = (y' - y) = (z' - z) = \Delta$$

Define $T = x + 2y + 3z$

$$\begin{aligned} T_x &= x' + 2y + 3z = T - \Delta \\ T_y &= x + 2y' + 3z = T - 2\Delta \\ T_z &= x + 2y + 3z' = T - 3\Delta \end{aligned}$$

T_x, T_y, T_z comprise a 3-term *arithmetic progression*

Arithmetic progressions

A k-term arithmetic progression (k-AP) is a set of the form

$$\{a, a+b, \ldots, a+(k-1)b\}.$$

A k-AP is *trivial* if $b = 0$ (i.e. if it is a singleton).

Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$

$$
\begin{aligned}
T_x &= x' + 2y + 3z = T - \Delta \\
T_y &= x + 2y' + 3z = T - 2\Delta \\
T_z &= x + 2y + 3z' = T - 3\Delta
\end{aligned}
$$

T_x, T_y, T_z comprise a 3-AP that is trivial $\Leftrightarrow \Delta = 0$.

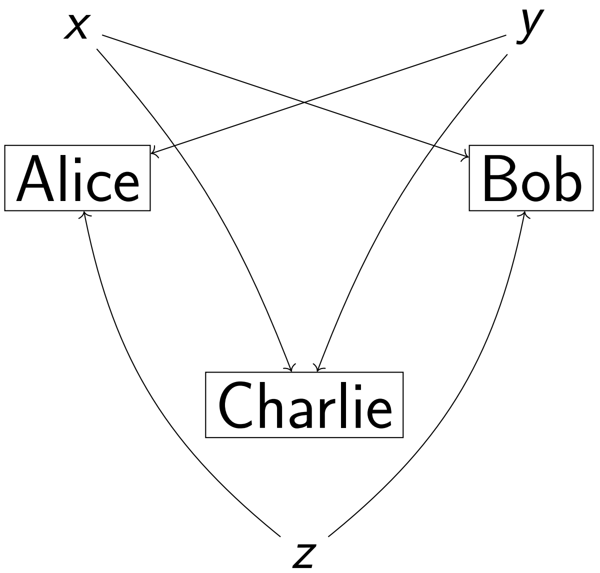
Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$

$$
\begin{aligned}
T_x &= x' + 2y + 3z = T - \Delta \\
T_y &= x + 2y' + 3z = T - 2\Delta \\
T_z &= x + 2y + 3z' = T - 3\Delta
\end{aligned}
$$

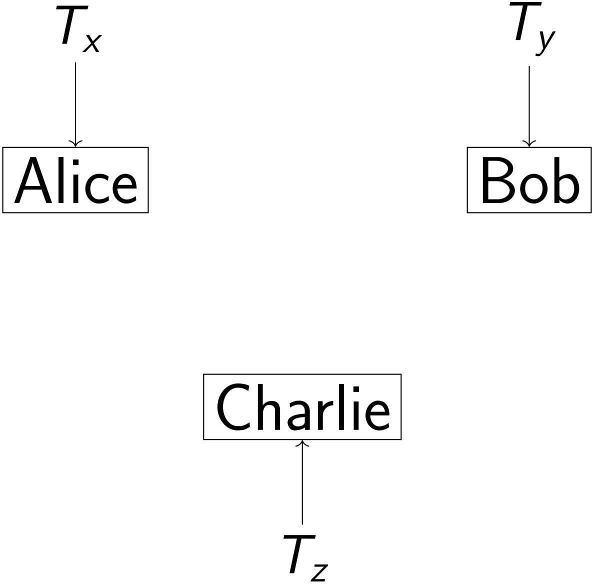
T_x, T_y, T_z comprise a 3-AP that is trivial $\Leftrightarrow \Delta = 0$.

$\Delta = N - (x + y + z)$, so $\Delta = 0 \Leftrightarrow \textsc{Exactly}N(x, y, z) = 1$.

Chandra/Furst/Lipton protocol for EXACTLYN



Chandra/Furst/Lipton protocol for ExactlyN



We have reduced NOF EXACTLYN to NIH EQUALITY where the inputs are promised to comprise a k-AP!

k-AP-free colorings

Color $[N]$ such that no color has a nontrivial k-AP.

$$\begin{tikzcd} \boxed{\begin{array}{c}\text{NIH } \textsc{Equality} \\ \text{with } k\text{-AP promise}\end{array}} \arrow[r] & \boxed{\begin{array}{c}k\text{-AP-free} \\ \text{coloring of } [N]\end{array}} \end{tikzcd}$$

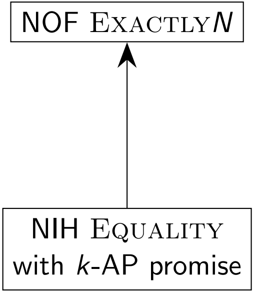
Color $w \in [N]$ with transcript of $\textsc{Equality}$ protocol on (w, w, w).

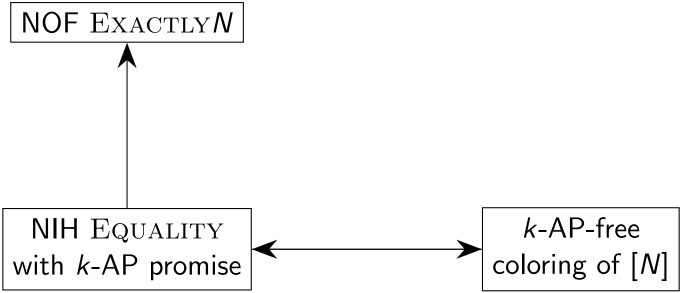
k-AP-free colorings

Color $[N]$ such that no color has a nontrivial k-AP.

$$\begin{tikzcd} \boxed{\begin{array}{c}\text{NIH }\textsc{Equality}\\ \text{with } k\text{-AP promise}\end{array}} & \boxed{\begin{array}{c}k\text{-AP-free}\\ \text{coloring of } [N]\end{array}} \arrow[l] \end{tikzcd}$$

Alice announces the color of her input.
Bob and Charlie announce if they agree.

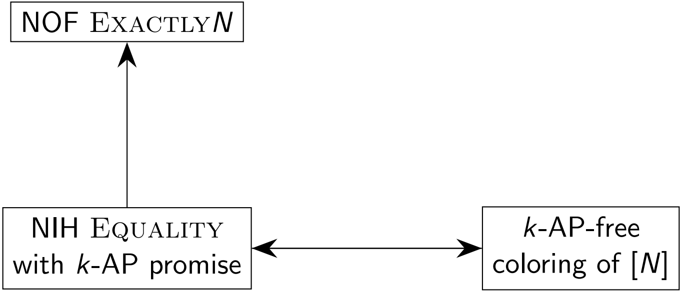

NOF ExactlyN
NIH Equality
with k-AP promise


NOF EXACTLYN
NIH EQUALITY with k-AP promise
k-AP-free coloring of $[N]$

k-AP-free colorings

Theorem (Behrend): $[N]$ has a 3-AP-free coloring with $2^{O(\sqrt{\log N})}$ colors

So $\textsc{Exactly}N$ for 3 players can be solved using $O(\sqrt{\log N})$ bits of communication!


NOF EXACTLYN
NIH EQUALITY with k-AP promise
k-AP-free coloring of $[N]$

Behrend's construction

Salem/Spencer: map $[N]$ to vectors in $[n]^d$ by base-n representation

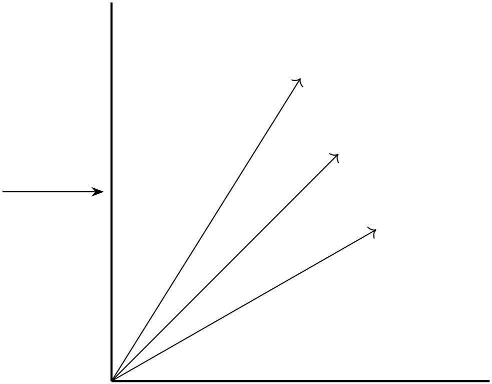
Example: $x = 184$, $N = 300$

$$
\begin{array}{ll}
n = 10 & \mathrm{vec}(x) = (1, 8, 4) \\
n = 16 & \mathrm{vec}(x) = (0, 11, 8)
\end{array}
$$

Behrend's construction

Behrend's idea: look at the *lengths* of the Salem/Spencer vectors

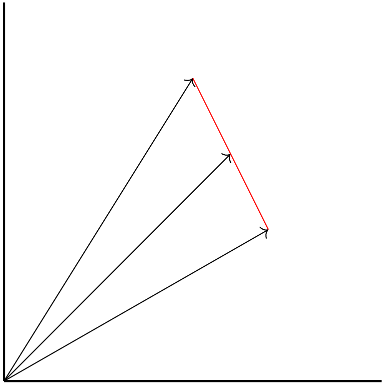
$\{a, a+b, a+2b\}$



Behrend's construction

Behrend's idea: look at the *lengths* of the Salem/Spencer vectors

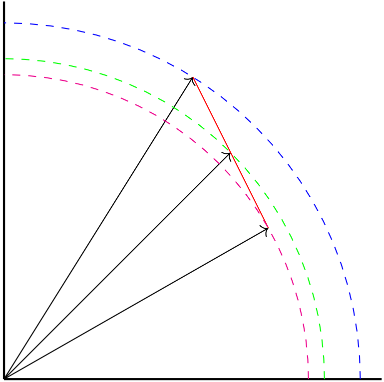
$\{a, a+b, a+2b\} \longrightarrow$



Behrend's construction

Behrend's idea: look at the *lengths* of the Salem/Spencer vectors

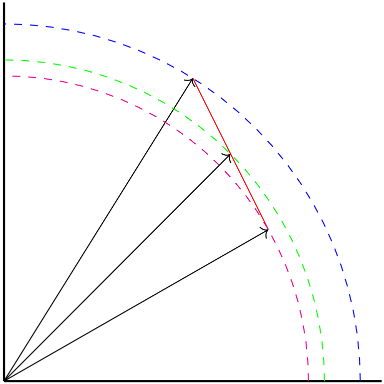
$\{a, a+b, a+2b\} \longrightarrow$



Behrend's construction

Behrend's idea: look at the *lengths* of the Salem/Spencer vectors

$\{a, a+b, a+2b\} \longrightarrow$



If 3 vectors have the same length, they can't be a 3-AP!
Color $x \in [N]$ by the (squared) length of $\mathrm{vec}(x)$.

Behrend's construction

Problem: x, y, z are a 3-AP $\not\Rightarrow \mathrm{vec}(x), \mathrm{vec}(y), \mathrm{vec}(z)$ are a 3-AP

Behrend's construction

Problem: x, y, z are a 3-AP $\not\Rightarrow$ $\text{vec}(x), \text{vec}(y), \text{vec}(z)$ are a 3-AP

Solution: Restrict to vectors with ℓ_∞-norm $\leq n/3$

Behrend's construction

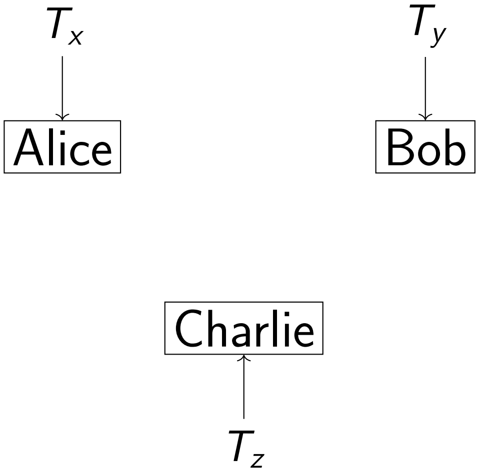
Problem: x, y, z are a 3-AP $\not\Rightarrow \text{vec}(x), \text{vec}(y), \text{vec}(z)$ are a 3-AP

Solution: Restrict to vectors with ℓ_∞-norm $\leq n/3$

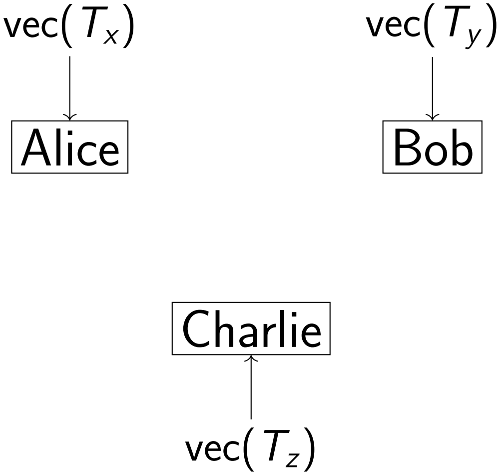
Use a pigeonhole argument to find a large 3-AP-free *set*

From a large set, we can get a small coloring (by translation)
Behrend: set of size $N/2^{O(\sqrt{\log N})} \Rightarrow$ coloring of size $2^{O(\sqrt{\log N})}$

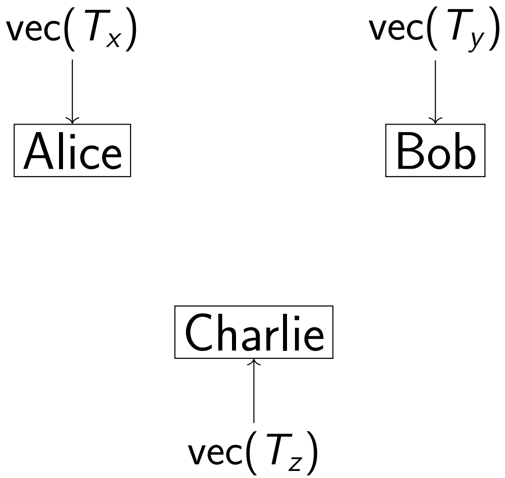
Chandra/Furst/Lipton protocol for Exactly$N$



Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$



Chandra/Furst/Lipton protocol for $\textsc{Exactly}N$



What if the vectors have large ℓ_∞ norm?

Linial/Pitassi/Shraibman protocol

Explicitly reason about the possibility of carries!

Alice announces her best guess for the **carry vector** of $x + y + z$

If the parties agree on the carry vector, they can use this to ensure that the vectors for T_x, T_y, T_z are a 3-AP (details omitted).

Linial/Pitassi/Shraibman protocol

How much communication?

- Send carry vector: $O(d)$ bits
- Send (squared) vector length: $O(\log n)$ bits
- Bob and Charlie confirm: $O(1)$ bits

Balanced at $d = O(\sqrt{\log N})$, $n = 2^{O(\sqrt{\log N})}$ (matches Behrend)

Q: Why do we care about explicit protocols?

Q: Why do we care about explicit protocols?

A: Another connection to combinatorics: corners!

Corners

A corner in $[N] \times [N]$ is a set of the form

$$\{(x, y), (x + \xi, y), (x, y + \xi)\}$$

for $\xi \neq 0$.

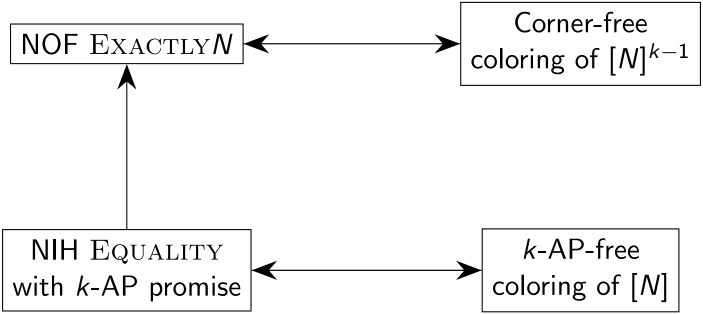
Corner-free colorings from $\textsc{Exactly}N$ protocols

Color (y, z) by the message that Alice sends.

Let $x^\star = N - y - z - \xi$
Bob can't distinguish between $(x^\star, y, z)$ and $(x^\star, y + \xi, z)$
Charlie can't distinguish between $(x^\star, y, z)$ and $(x^\star, y, z + \xi)$
So if $\{(y, z), (y + \xi, z), (y, z + \xi)\}$ are colored the same, the protocol claims $x^\star + y + z = N$, which is only true when $\xi = 0$.

$\textsc{Exactly}N$ protocols from corner-free colorings

Compare the colors of $(N - y - z, y), (x, N - x - z)$, and (x, y).
This is $\{(x + \xi, y), (x, y + \xi), (x, y)\}$ with $\xi = \Delta$.


NOF EXACTLYN
Corner-free coloring of $[N]^{k-1}$
NIH EQUALITY with k-AP promise
k-AP-free coloring of $[N]$

Better corner-free colorings

Linial/Shraibman show that we don't need to communicate the whole carry vector!

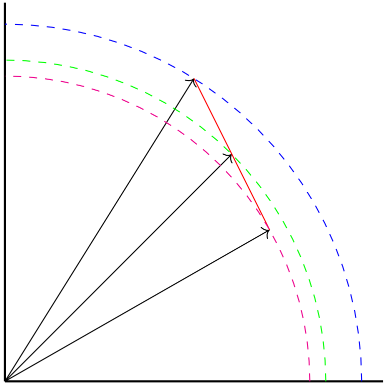
This gives the best improvement on corner-free colorings since Behrend.

Green gives a further improvement.

What about when $k > 3$?

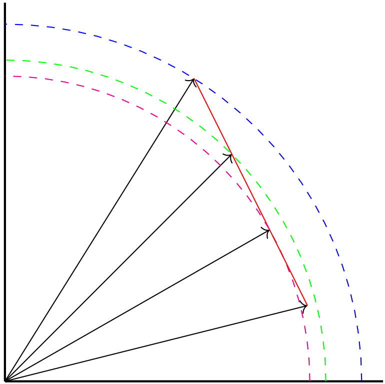
$k > 3$

Behrend still works...



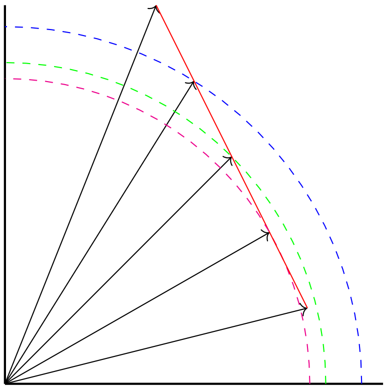
$k > 3$

Behrend still works...



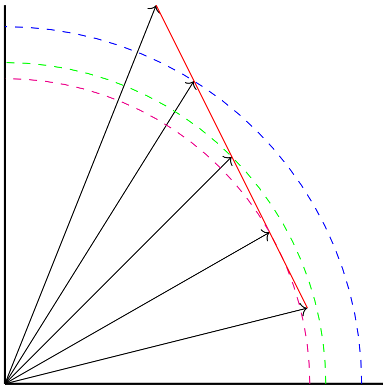
$k > 3$

Behrend still works...



$k > 3$

Behrend still works...



...but we can do better.

Rankin gives a better construction of k-AP-free colorings!

Higher-degree progressions

A degree-m k-term polynomial progression (k-$\mathrm{P}_m\mathrm{P}$) is a set of the form

$$\{p(0), p(1), \ldots, p(k-1)\}$$

where p is a polynomial of degree at most m.

Lifting to higher-degree progressions

Theorem (Rankin, Łaba/Lacey): If $x_1, \ldots, x_k$ are a k-P$_m$P with:

- $k > 2m$
- $\mathrm{vec}(x_1), \ldots, \mathrm{vec}(x_k)$ have low ℓ_∞-norm (less than n/c_m)
- $\{x_1, \ldots, x_k\}$ is not a singleton

then $\|\mathrm{vec}(x_1)\|_2^2, \ldots, \|\mathrm{vec}(x_k)\|_2^2$ is a non-trivial k-P$_{2m}$P

Behrend's construction as lifting

x_1, x_2, x_3 are a 3-AP (3-P$_1$P) with:

- $k > 2m$
- $\mathrm{vec}(x_1), \mathrm{vec}(x_2), \mathrm{vec}(x_3)$ have low ℓ_∞-norm

so if $\|\mathrm{vec}(x_1)\|_2^2 = \|\mathrm{vec}(x_2)\|_2^2 = \|\mathrm{vec}(x_3)\|_2^2$ it must be that $\{x_1, x_2, x_3\}$ is a singleton.

Behrend's construction as lifting

x_1, x_2, x_3 are a 3-AP (3-P$_1$P) with:

- $3 > 2$
- $\text{vec}(x_1), \text{vec}(x_2), \text{vec}(x_3)$ have low ℓ_∞-norm

so if $\|\text{vec}(x_1)\|_2^2 = \|\text{vec}(x_2)\|_2^2 = \|\text{vec}(x_3)\|_2^2$ it must be that $\{x_1, x_2, x_3\}$ is a singleton.

Rankin's construction

Repeated apply lifting! Let $k = 2^r + 1$

k-$\mathrm{P}_1\mathrm{P} \to k$-$\mathrm{P}_2\mathrm{P} \to k$-$\mathrm{P}_4\mathrm{P} \to \ldots \to k$-$\mathrm{P}_{2^{r-1}}\mathrm{P} \to k$-$\mathrm{P}_{2^r}\mathrm{P}$

If the the k-$\mathrm{P}_{2^r}\mathrm{P}$ is a singleton, the original k-$\mathrm{P}_1\mathrm{P}$ was also!

Each time the range of values shrinks from n^d to $n^2 d$ for some n, d

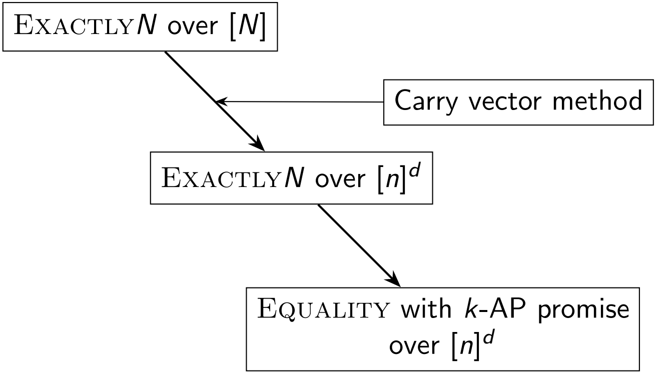
Theorem (Rankin): [N] has a k-AP-free coloring with $2^{O(\log N^{1/\log(k-1)})}$ colors

Previous explicit protocols can't use Rankin's construction.

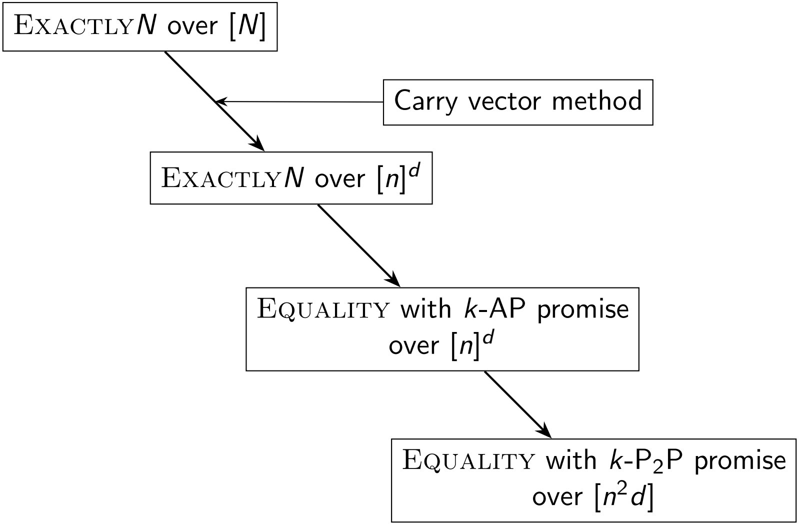
Rankin's construction with carry vectors

$$\begin{tikzcd}
\boxed{\textsc{Exactly}N \text{ over } [N]} \arrow[dr] & & \\
& \boxed{\textsc{Exactly}N \text{ over } [n]^d} \arrow[dr] & \\
& & \boxed{\begin{array}{c}\textsc{Equality} \text{ with } k\text{-AP promise} \\ \text{over } [n]^d\end{array}}
\end{tikzcd}$$

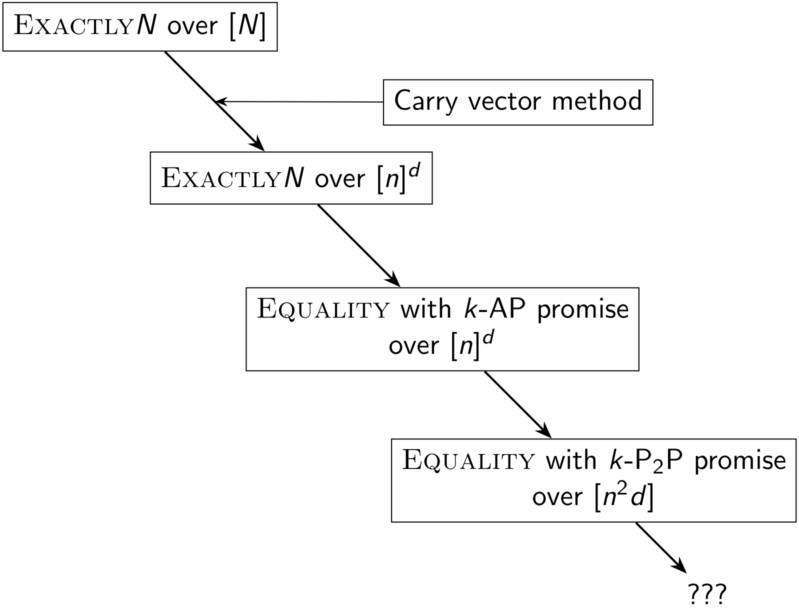
Rankin's construction with carry vectors



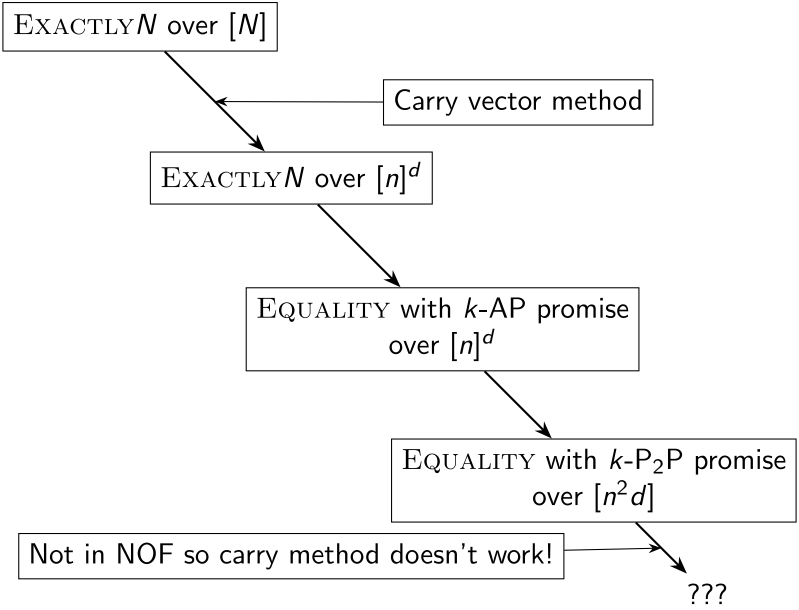
Rankin's construction with carry vectors



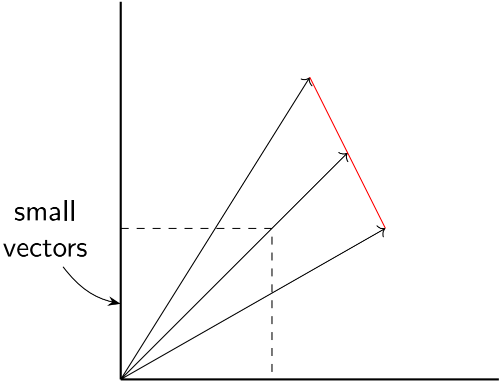
Rankin's construction with carry vectors



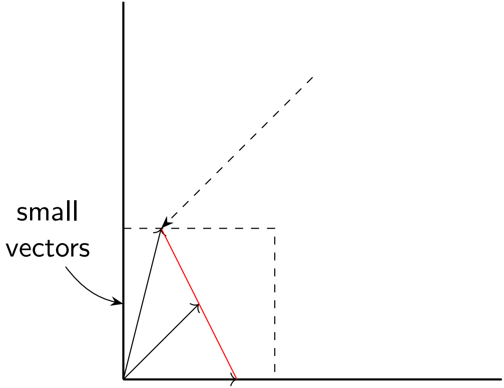
Rankin's construction with carry vectors



In order to ensure that the vectors have small ℓ_∞ norm...



In order to ensure that the vectors have small ℓ_∞ norm...



Alice announces how much she needs to *shift* her vector to make it small. We shift all of the vectors by this much!

Our protocol

Rankin's construction with *shifts* between rounds.

- Other players need different shifts: the vectors are not equal, and so we're done!
- Otherwise, we can proceed: the vectors are now short!

Communication cost:

- $O(\log k)$ rounds of shifts: $d \cdot c_k$ communication each
- Length at final step (complicated expression)

This ends up being balanced by choosing

$$d \approx O\left((\log N)^{1/(\log(k-1))}\right)$$

every round, which matches Rankin

Ongoing work and future directions

- Can Linial/Shraibman corner result generalize with shifts?
- Can Green's improvement of Linial/Shraibman be generalized?
- Use these techniques with other NOF functions.

Thanks!

Extra slides

Graph functions

Given $x_1, \ldots, x_{k-1}$ there is *at most one* value $g(x_1, \ldots, x_{k-1})$ for x_k such that $F(x_1, \ldots, x_k) = 1$.

Easy with randomness: $g(x_1, \ldots, x_{k-1}) = x_k$?

Theorem (Beame, David, Pitassi, and Woelfel): There are graph functions that are hard to compute deterministically.

Linial/Pitassi/Shraibman protocol

Alice announces her best guess for the **carry vector** of $x + y + z$
$N_i + (C_i - 1)n < y_i + z_i + C_{i-1} \leq N_i + (C_i)n$

Example: $N = 300$, $n = 10$, $\text{vec}(N) = (3, 0, 0)$

$\text{vec}(y) = (1, 8, 4)$ $\text{vec}(z) = (0, 0, 7)$

$4 + 7 + 0 \leq 0 + 20$
$8 + 0 + 2 \leq 0 + 10$
$1 + 0 + 1 \leq 3 + 0$
$C(y, z) = (0, 1, 2)$

Linial/Pitassi/Shraibman protocol

Alice announces $C(y, z)$
Bob and Charlie announce whether $C(y, z) = C(x, z) = C(x, y)$

(As observed previously) if $x + y + z = N$, the guessed carry vectors are all the same.
Abort otherwise.

Linial/Pitassi/Shraibman protocol

Alice announces $C(y, z)$
Bob and Charlie announce whether $C(y, z) = C(x, z) = C(x, y)$

(As observed previously) if $x + y + z = N$, the guessed carry vectors are all the same.
Abort otherwise.

$\text{vec}(x) = (1, 0, 9)$ $\quad$ $\text{vec}(y) = (1, 8, 4)$ $\quad$ $\text{vec}(z) = (0, 0, 7)$

$4 + 7 + 0 \leq 0 + 20$	$9 + 7 + 0 \leq 0 + 20$	$9 + 4 + 0 \leq 0 + 20$
$8 + 0 + 2 \leq 0 + 10$	$0 + 0 + 2 \leq 0 + 10$	$8 + 0 + 2 \leq 0 + 10$
$1 + 0 + 1 \leq 3 + 0$	$1 + 0 + 1 \leq 3 + 0$	$1 + 1 + 1 \leq 3 + 0$
$C(y, z) = (0, 1, 2)$	$C(x, z) = (0, 1, 2)$	$C(x, y) = (0, 1, 2)$

Linial/Pitassi/Shraibman protocol

Alice announces $C(y, z)$
Bob and Charlie announce whether $C(y, z) = C(x, z) = C(x, y)$

(As observed previously) if $x + y + z = N$, the guessed carry vectors are all the same.
Abort otherwise.

$\text{vec}(x) = (1, 0, 6)$ $\quad$ $\text{vec}(y) = (1, 8, 4)$ $\quad$ $\text{vec}(z) = (0, 0, 7)$

$4 + 7 + 0 \leq 0 + 20$	$6 + 7 + 0 \leq 0 + 20$	$6 + 4 + 0 \leq 0 + 10$
$8 + 0 + 2 \leq 0 + 10$	$0 + 0 + 2 \leq 0 + 10$	$8 + 0 + 1 \leq 0 + 10$
$1 + 0 + 1 \leq 3 + 0$	$1 + 0 + 1 \leq 3 + 0$	$1 + 1 + 1 \leq 3 + 0$
$C(y, z) = (0, 1, 2)$	$C(x, z) = (0, 1, 2)$	$C(x, y) = (0, 1, 1)$

Linial/Pitassi/Shraibman protocol

Alice announces $C(y, z)$
Bob and Charlie announce whether $C(y, z) = C(x, z) = C(x, y)$

(As observed previously) if $x + y + z = N$, the guessed carry vectors are all the same.
Abort otherwise.

$\text{vec}(x) = (1, 0, 8)$ $\text{vec}(y) = (1, 8, 4)$ $\text{vec}(z) = (0, 0, 7)$

$4 + 7 + 0 \leq 0 + 20$	$8 + 7 + 0 \leq 0 + 20$	$8 + 4 + 0 \leq 0 + 20$
$8 + 0 + 2 \leq 0 + 10$	$0 + 0 + 2 \leq 0 + 10$	$8 + 0 + 2 \leq 0 + 10$
$1 + 0 + 1 \leq 3 + 0$	$1 + 0 + 1 \leq 3 + 0$	$1 + 1 + 1 \leq 3 + 0$
$C(y, z) = (0, 1, 2)$	$C(x, z) = (0, 1, 2)$	$C(x, y) = (0, 1, 2)$