HW 10 Review

Exposition by William Gasarch

May 12, 2020

Sz Thm implies VDW's Thm

Assume, Sz true, and VDW's false. Exists k, c such that
For all W there is a c-coloring COL_W of $[W]$ with no mono k-AP.
We use these colorings to create a coloring of $\mathbb{N}$.

Sz Thm implies VDW's Thm

Assume, Sz true, and VDW's false. Exists k, c such that
For all W there is a c-coloring COL_W of $[W]$ with no mono k-AP.
We use these colorings to create a coloring of $\mathbb{N}$.
The usual
$COL(1)$ is the color that appears infinitely often. Kill...
$COL(2)$ is the color that appears infinitely often. Kill...

$\vdots$

Sz Thm implies VDW's Thm

Assume, Sz true, and VDW's false. Exists k, c such that
For all W there is a c-coloring COL_W of $[W]$ with no mono k-AP.
We use these colorings to create a coloring of $\mathbb{N}$.
The usual
$COL(1)$ is the color that appears infinitely often. Kill...
$COL(2)$ is the color that appears infinitely often. Kill...
$\vdots$.
We want to show that some color has positive upper density.

Sz Thm implies VDW's Thm

Assume, Sz true, and VDW's false. Exists k, c such that
For all W there is a c-coloring COL_W of $[W]$ with no mono k-AP.
We use these colorings to create a coloring of $\mathbb{N}$.
The usual
$COL(1)$ is the color that appears infinitely often. Kill...
$COL(2)$ is the color that appears infinitely often. Kill...
$\vdots$
We want to show that some color has positive upper density.
Colors are $1, \ldots, k$.

Sz Thm implies VDW's Thm (cont)

$(\forall n)\left[D_{i,n} = \frac{|\{x : COL(x)=i\} \cap [n]|}{n}\right]$. Note $\sum_{i=1}^{k} D_{i,n} = 1$.

Sz Thm implies VDW's Thm (cont)

$(\forall n)\left[D_{i,n} = \frac{|\{x : COL(x)=i\}\cap[n]|}{n}\right]$. Note $\sum_{i=1}^{k} D_{i,n} = 1$.

Hence, for all n, there exists i, $D_{i,n} \geq \frac{1}{k}$.

Sz Thm implies VDW's Thm (cont)

$(\forall n)\left[D_{i,n} = \frac{|\{x : COL(x)=i\} \cap [n]|}{n}\right]$. Note $\sum_{i=1}^{k} D_{i,n} = 1$.

Hence, for all n, there exists i, $D_{i,n} \geq \frac{1}{k}$.

Let i be the least number that appears infinitely often.

Sz Thm implies VDW's Thm (cont)

$(\forall n)\left[D_{i,n} = \frac{|\{x : COL(x)=i\} \cap [n]|}{n}\right]$. Note $\sum_{i=1}^{k} D_{i,n} = 1$.

Hence, for all n, there exists i, $D_{i,n} \geq \frac{1}{k}$.

Let i be the least number that appears infinitely often.

For an infinite number of n, $D_{i,n} \geq \frac{1}{k}$.

Sz Thm implies VDW's Thm (cont)

$(\forall n)\left[D_{i,n} = \frac{|\{x : COL(x)=i\}\cap[n]|}{n}\right]$. Note $\sum_{i=1}^{k} D_{i,n} = 1$.

Hence, for all n, there exists i, $D_{i,n} \geq \frac{1}{k}$.

Let i be the least number that appears infinitely often.

For an infinite number of n, $D_{i,n} \geq \frac{1}{k}$.

Hence $\{x : COL(x) = i\}$ has upper positive density.

Sz Thm implies VDW's Thm (cont)

$(\forall n)\left[D_{i,n} = \frac{|\{x : COL(x)=i\} \cap [n]|}{n}\right]$. Note $\sum_{i=1}^{k} D_{i,n} = 1$.

Hence, for all n, there exists i, $D_{i,n} \geq \frac{1}{k}$.

Let i be the least number that appears infinitely often.

For an infinite number of n, $D_{i,n} \geq \frac{1}{k}$.

Hence $\{x : COL(x) = i\}$ has upper positive density.

By Sz Thm there are k-APs $\{x : COL(x) = i\}$.

Sz Thm implies VDW's Thm (cont)

$(\forall n)\left[D_{i,n} = \frac{|\{x:COL(x)=i\}\cap[n]|}{n}\right]$. Note $\sum_{i=1}^{k} D_{i,n} = 1$.

Hence, for all n, there exists i, $D_{i,n} \geq \frac{1}{k}$.

Let i be the least number that appears infinitely often.

For an infinite number of n, $D_{i,n} \geq \frac{1}{k}$.

Hence $\{x : COL(x) = i\}$ has upper positive density.

By Sz Thm there are k-APs $\{x : COL(x) = i\}$.

$a, a+d, \ldots, a+(k-1)d$ all be in $\{x : COL(x) = i\}$.

Sz Thm implies VDW's Thm (cont)

$(\forall n)\left[D_{i,n} = \frac{|\{x:COL(x)=i\}\cap[n]|}{n}\right]$. Note $\sum_{i=1}^{k} D_{i,n} = 1$.

Hence, for all n, there exists i, $D_{i,n} \geq \frac{1}{k}$.

Let i be the least number that appears infinitely often.

For an infinite number of n, $D_{i,n} \geq \frac{1}{k}$.

Hence $\{x : COL(x) = i\}$ has upper positive density.

By Sz Thm there are k-APs $\{x : COL(x) = i\}$.

$a, a + d, \ldots, a + (k - 1)d$ all be in $\{x : COL(x) = i\}$.

By the definition of COL there is an i (actually infinitely many) such that COL and COL_i agree on $a, a + d, \ldots, a + (k - 1)d$.

Sz Thm implies VDW's Thm (cont)

$(\forall n)\left[D_{i,n} = \frac{|\{x:COL(x)=i\}\cap[n]|}{n}\right]$. Note $\sum_{i=1}^{k} D_{i,n} = 1$.

Hence, for all n, there exists i, $D_{i,n} \geq \frac{1}{k}$.

Let i be the least number that appears infinitely often.

For an infinite number of n, $D_{i,n} \geq \frac{1}{k}$.

Hence $\{x : COL(x) = i\}$ has upper positive density.

By Sz Thm there are k-APs $\{x : COL(x) = i\}$.

$a, a+d, \ldots, a+(k-1)d$ all be in $\{x : COL(x) = i\}$.

By the definition of COL there is an i (actually infinitely many) such that COL and COL_i agree on $a, a+d, \ldots, a+(k-1)d$.

Hence that COL_i has a mono k-AP, which is a contradiction.

HW10, Problem 3

Exposition by William Gasarch

May 12, 2020

Disjoint k-AP's

TRUE or FALSE:
For all $COL : \mathbb{N} \rightarrow [c]$ there exists, for all k, a mono k-AP AND the 3-AP, the 4-AP, the 5-AP, etc are all disjoint.

Disjoint k-AP's

TRUE or FALSE:
For all $COL : \mathbb{N} \to [c]$ there exists, for all k, a mono k-AP AND the 3-AP, the 4-AP, the 5-AP, etc are all disjoint.

TRUE: Divide $\mathbb{N}$ into disjoint blocks of size $W(3,c)$, $W(4,c)$, $\ldots$.
In the $W(k,c)$-sized block will be a mono k-AP.
Key VDW is about coloring $[W]$ but works just as well coloring

$$\{x, x+1, \ldots, x+W(k,c)-1\}.$$

ω-AP's

TRUE or FALSE:
For all $COL : \mathbb{N} \rightarrow [c]$ there exists a mono ω-AP

ω-AP's

TRUE or FALSE:
For all $COL : \mathbb{N} \rightarrow [c]$ there exists a mono ω-AP

FALSE: Here is a 2-coloring of $\mathbb{N}$ with no ω-APs.
If $2^{2i} \le x \le 2^{2i+1} - 1$ then $COL(x) = R$.
If $2^{2i+1} \le x \le 2^{2i+2} - 1$ then $COL(x) = B$.

ω-AP's

TRUE or FALSE:
For all $COL : \mathbb{N} \rightarrow [c]$ there exists a mono ω-AP

FALSE: Here is a 2-coloring of $\mathbb{N}$ with no ω-APs.
If $2^{2i} \le x \le 2^{2i+1} - 1$ then $COL(x) = R$.
If $2^{2i+1} \le x \le 2^{2i+2} - 1$ then $COL(x) = B$.

Assume, BWOC $\exists a, d$: $a, a+d, \ldots$ all same color.
i: (1) $(\exists X)[2^i \le a + Xd \le 2^{i+1} - 1]$ and (2) $d < 2^i$.

ω-AP's

TRUE or FALSE:
For all $COL : \mathbb{N} \rightarrow [c]$ there exists a mono ω-AP

FALSE: Here is a 2-coloring of $\mathbb{N}$ with no ω-APs.
If $2^{2i} \le x \le 2^{2i+1} - 1$ then $COL(x) = R$.
If $2^{2i+1} \le x \le 2^{2i+2} - 1$ then $COL(x) = B$.

Assume, BWOC $\exists a, d$: $a, a+d, \ldots$ all same color.
i: (1) $(\exists X)[2^i \le a + Xd \le 2^{i+1} - 1]$ and (2) $d < 2^i$.

Hence $a + Xd$ and $a + (X+1)d$ are colored differently.
Contradiction.

HW10, Problem 4

Exposition by William Gasarch

May 12, 2020

Problem 4

Assume for all V, there is a 4-free set $A \subseteq [V]$ of size $Ve^{-(\log V)^f}$. A, B, C, D each have a string of length n on their foreheads The strings are a, b, c, d. Give a protocol for them to used such that

- At the end they all know if $a + b + c + d = 2^{n+1} - 1$.
- The number if bits communicated is $\ll n$.
- Assume that your reader is a student in this class who MISSED the lecture on multiparty Communication (but she saw all of the prior lectures).

Two Solutions

I present:

- The solution I had in mind from the **lit**erature.
- A **new** solution that Rob **Brady** showed me.

Both begin the same way with material on 4-free sets and 4-AP free colorings.

Recap

In the 3free slides we showed:
Thm Let $V \in \mathbb{N}$ and let $A \subseteq [V]$ be a 3-free set. Let $c = \frac{V \ln(V)}{|A|}$. Then there is a c-coloring of $[V]$ with no mono 3-APs. Hence $W(3, c) > V$.

Recap

In the 3free slides we showed:
Thm Let $V \in \mathbb{N}$ and let $A \subseteq [V]$ be a 3-free set. Let $c = \frac{V \ln(V)}{|A|}$. Then there is a c-coloring of $[V]$ with no mono 3-APs. Hence $W(3, c) > V$.

But the proof had **nothing** to do with 3-free sets. If $A \subseteq [V]$ is ANY set then there are c shifts of A that cover $[V]$. Hence we have the following:

Recap

In the 3free slides we showed:

Thm Let $V \in \mathbb{N}$ and let $A \subseteq [V]$ be a 3-free set. Let $c = \frac{V \ln(V)}{|A|}$. Then there is a c-coloring of $[V]$ with no mono 3-APs. Hence $W(3, c) > V$.

But the proof had **nothing** to do with 3-free sets. If $A \subseteq [V]$ is ANY set then there are c shifts of A that cover $[V]$. Hence we have the following:

Thm Let $V \in \mathbb{N}$ and let $A \subseteq [V]$ be a 4-free set. Let $c = \frac{V \ln(V)}{|A|}$. Then there is a c-coloring of $[V]$ with no mono 4-APs. Hence $W(4, c) > V$.

Definitions and Thms about Γ_{4AP}

$\Gamma_{4AP}(M)$ is the least c such that there is a c-coloring of $[M]$ with no mono 4-AP.

Definitions and Thms about Γ_{4AP}

$\Gamma_{4AP}(M)$ is the least c such that there is a c-coloring of $[M]$ with no mono 4-AP.

We rephrase the last theorem:

Definitions and Thms about Γ_{4AP}

$\Gamma_{4AP}(M)$ is the least c such that there is a c-coloring of $[M]$ with no mono 4-AP.

We rephrase the last theorem:

Thm If A is a 4-free set then $\Gamma_{4AP}(M) \le \frac{M \ln(M)}{|A|}$.

Definitions and Thms about Γ_{4AP}

$\Gamma_{4AP}(M)$ is the least c such that there is a c-coloring of $[M]$ with no mono 4-AP.

We rephrase the last theorem:

Thm If A is a 4-free set then $\Gamma_{4AP}(M) \le \frac{M \ln(M)}{|A|}$.

We are assuming there is a 4-free set of $[M]$ of size $\le Me^{-(\log M)^f}$ for some constant f.

Definitions and Thms about Γ_{4AP}

$\Gamma_{4AP}(M)$ is the least c such that there is a c-coloring of $[M]$ with no mono 4-AP.

We rephrase the last theorem:

Thm If A is a 4-free set then $\Gamma_{4AP}(M) \le \frac{M\ln(M)}{|A|}$.

We are assuming there is a 4-free set of $[M]$ of size $\le Me^{-(\log M)^f}$ for some constant f.

Hence

$$\Gamma_{4AP}(M) \le \frac{M\ln(M)}{Me^{-(\ln(M))^f}} = \frac{\ln(M)}{e^{-(\ln(M))^f}} = (\ln(M))e^{(\ln(M))^f}$$

Definitions of Γ_{sq} and Γ_{lit}

- A **lit** is 4 points in $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ of the form
  (x, y, z),
  $(x + \lambda, y, z)$,
  $(x, y + \lambda, z)$,
  $(x, y, z + \lambda)$ $(\lambda \in \mathbb{Z})$.
- $\Gamma_{sq}(M)$ is the least c such that there is a c-coloring of $[M] \times [M]$ with no mono square.
- $\Gamma_{lit}(M)$ is the least c such that there is a c-coloring of $[M] \times [M] \times [M]$ with no mono lit.

Off By One Notation

Usually $[M] = \{1, \ldots, M\}$.

Off By One Notation

Usually $[M] = \{1, \ldots, M\}$.

Since we will allow a forehead to have $0 \cdots 0$, in this talk $[M] = \{0, \ldots, M\}$.

Off By One Notation

Usually $[M] = \{1, \ldots, M\}$.

Since we will allow a forehead to have $0 \cdots 0$, in this talk $[M] = \{0, \ldots, M\}$.

We will still take $|[M]| = M$ since the $+1$ won't matter with the asymptotics.

Off By One Notation

Usually $[M] = \{1, \ldots, M\}$.

Since we will allow a forehead to have $0 \cdots 0$, in this talk $[M] = \{0, \ldots, M\}$.

We will still take $|[M]| = M$ since the $+1$ won't matter with the asymptotics.

In fact we will take $|[3M]| = M$ even though this is FALSE since it won't matter for the asymptotics.

Off By One Notation

Usually $[M] = \{1, \ldots, M\}$.

Since we will allow a forehead to have $0 \cdots 0$, in this talk $[M] = \{0, \ldots, M\}$.

We will still take $|[M]| = M$ since the $+1$ won't matter with the asymptotics.

In fact we will take $|[3M]| = M$ even though this is FALSE since it won't matter for the asymptotics.

Working out the real asymptotics is so boring that I WON"T say **might be on the HW or the FINAL**.

Thm about Γ_{sq} (For Brady Approach)

Thm $\Gamma_{sq}(M) \le \Gamma_{4AP}(3M) \le (\ln(3M))e^{(\ln(3M))^f}$
Pf
Let $c = \Gamma_{4AP}(3M)$.
Assume we have a 4-AP free coloring $COL\colon [3M] \to [c]$.

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

If
$COL'(x, y) = COL'(x+\lambda, y) = COL'(x, y+\lambda) = COL'(x+\lambda, y+\lambda)$
then
$COL(x + 2y) = COL(x + 2y + \lambda) = COL(x + 2y + 2\lambda) =$
$COL(x + 2y + 3\lambda)$, a mono 4-AP: $\lambda = 0$.

Thm about Γ_{lit} (For Lit Approach)

Thm $\Gamma_{lit}(M) \le \Gamma_{4AP}(6M) \le (\ln(6M))e^{(\ln(6M))^f}$

Pf

Let $c = \Gamma_{4AP}(6M)$.

Assume we have a 4-AP free coloring $COL\colon [6M] \to [c]$.

We use this to define a lit-free coloring

$COL'\colon [M] \times [M] \times [M] \to [c]$

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

If

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

then

$COL(x+2y+3z) = COL(x+2y+3z+\lambda) = COL(x+2y+3z+2\lambda) = COL(x+2y+3z+3\lambda)$, a mono 4-AP: $\lambda = 0$.

Brady's Protocol

Exposition by William Gasarch

May 12, 2020

Brady's Protocol

$M = 2^{n+1} - 1$ throughout.

1. Pre-step: A, B, C, D agree on a $\Gamma_{sq}(M)$-coloring χ of $[M] \times [M]$ that has no mono square.
2. A: b, c, d, B: a, c, d, C:a, b, d. $a, b, c, d \in \{0, 1\}^n$ binary.
3. If A sees $b + c + d > M$, says NO and protocol stops. B,C,D sim.
4. A finds a', s.t. $a' + b + c + d = M$ and says $\chi(a' + b, b + c)$.
5. B finds b' s.t. $a + b' + c + d = M$ and says $\chi(a + b', b' + c)$.
6. C finds c' s.t. $a + b + c' + d = M$ and says $\chi(a + b, b + c')$.
7. D says Y if all the χ's are $\chi(a + b, b + c)$, N otherwise

Brady's Protocol

$M = 2^{n+1} - 1$ throughout.

1. Pre-step: A, B, C, D agree on a $\Gamma_{sq}(M)$-coloring χ of $[M] \times [M]$ that has no mono square.
2. A: b, c, d, B: a, c, d, C:a, b, d. $a, b, c, d \in \{0, 1\}^n$ binary.
3. If A sees $b + c + d > M$, says NO and protocol stops. B,C,D sim.
4. A finds a', s.t. $a' + b + c + d = M$ and says $\chi(a' + b, b + c)$.
5. B finds b' s.t. $a + b' + c + d = M$ and says $\chi(a + b', b' + c)$.
6. C finds c' s.t. $a + b + c' + d = M$ and says $\chi(a + b, b + c')$.
7. D says Y if all the χ's are $\chi(a + b, b + c)$, N otherwise

Numb bits: $3 \lg(\Gamma(M)) + O(1)$. We show $\leq O(n^f)$.

Brady's Protocol

$M = 2^{n+1} - 1$ throughout.

1. Pre-step: A, B, C, D agree on a $\Gamma_{sq}(M)$-coloring χ of $[M] \times [M]$ that has no mono square.
2. A: b, c, d, B: a, c, d, C:a, b, d. $a, b, c, d \in \{0, 1\}^n$ binary.
3. If A sees $b + c + d > M$, says NO and protocol stops. B,C,D sim.
4. A finds a', s.t. $a' + b + c + d = M$ and says $\chi(a' + b, b + c)$.
5. B finds b' s.t. $a + b' + c + d = M$ and says $\chi(a + b', b' + c)$.
6. C finds c' s.t. $a + b + c' + d = M$ and says $\chi(a + b, b + c')$.
7. D says Y if all the χ's are $\chi(a + b, b + c)$, N otherwise

Numb bits: $3 \lg(\Gamma(M)) + O(1)$. We show $\leq O(n^f)$.
But first we show that it works.

Brady's Protocol Works

Assume $a + b + c + d = M - \lambda$ where $\in \mathbb{Z}$.
By Algebra one can show
$a' = a + \lambda$
$b' = b + \lambda$
$c' = c + \lambda$
Let $x = a + b$ and $y = b + c$.

Brady's Protocol Works

Assume $a+b+c+d = M - \lambda$ where $\in \mathbb{Z}$.
By Algebra one can show
$a' = a + \lambda$
$b' = b + \lambda$
$c' = c + \lambda$
Let $x = a + b$ and $y = b + c$.
$(a' + b, b + c) = (a + b + \lambda, b + c) = (x + \lambda, y)$.

Brady's Protocol Works

Assume $a + b + c + d = M - \lambda$ where $\in \mathbb{Z}$.
By Algebra one can show
$a' = a + \lambda$
$b' = b + \lambda$
$c' = c + \lambda$
Let $x = a + b$ and $y = b + c$.
$(a' + b, b + c) = (a + b + \lambda, b + c) = (x + \lambda, y)$.
$(a + b', b' + c) = (a + b + \lambda, b + c + \lambda) = (x + \lambda, y + \lambda)$.

Brady's Protocol Works

Assume $a + b + c + d = M - \lambda$ where $\in \mathbb{Z}$.
By Algebra one can show
$a' = a + \lambda$
$b' = b + \lambda$
$c' = c + \lambda$
Let $x = a + b$ and $y = b + c$.
$(a' + b, b + c) = (a + b + \lambda, b + c) = (x + \lambda, y)$.
$(a + b', b' + c) = (a + b + \lambda, b + c + \lambda) = (x + \lambda, y + \lambda)$.
$(a + b, b + c') = (a + b, b + c + \lambda) = (x, y + \lambda)$.

Brady's Protocol Works

Assume $a+b+c+d=M-\lambda$ where $\in \mathbb{Z}$.
By Algebra one can show
$a'=a+\lambda$
$b'=b+\lambda$
$c'=c+\lambda$
Let $x=a+b$ and $y=b+c$.
$(a'+b, b+c)=(a+b+\lambda, b+c)=(x+\lambda, y)$.
$(a+b', b'+c)=(a+b+\lambda, b+c+\lambda)=(x+\lambda, y+\lambda)$.
$(a+b, b+c')=(a+b, b+c+\lambda)=(x, y+\lambda)$.
$(a+b, b+c)=(a+b, b+c)=(x, y)$.
Note that these four form a square!

Brady's Protocol Works

Assume $a + b + c + d = M - \lambda$ where $\in \mathbb{Z}$.
By Algebra one can show
$a' = a + \lambda$
$b' = b + \lambda$
$c' = c + \lambda$
Let $x = a + b$ and $y = b + c$.
$(a' + b, b + c) = (a + b + \lambda, b + c) = (x + \lambda, y)$.
$(a + b', b' + c) = (a + b + \lambda, b + c + \lambda) = (x + \lambda, y + \lambda)$.
$(a + b, b + c') = (a + b, b + c + \lambda) = (x, y + \lambda)$.
$(a + b, b + c) = (a + b, b + c) = (x, y)$.
Note that these four form a square!

If protocol says YES then all the points of the square have the same color, so $\lambda = 0$ and $a + b + c + d = M$.

Brady's Protocol Works

Assume $a + b + c + d = M - \lambda$ where $\in \mathbb{Z}$.
By Algebra one can show
$a' = a + \lambda$
$b' = b + \lambda$
$c' = c + \lambda$
Let $x = a + b$ and $y = b + c$.
$(a' + b, b + c) = (a + b + \lambda, b + c) = (x + \lambda, y)$.
$(a + b', b' + c) = (a + b + \lambda, b + c + \lambda) = (x + \lambda, y + \lambda)$.
$(a + b, b + c') = (a + b, b + c + \lambda) = (x, y + \lambda)$.
$(a + b, b + c) = (a + b, b + c) = (x, y)$.
Note that these four form a square!

If protocol says YES then all the points of the square have the same color, so $\lambda = 0$ and $a + b + c + d = M$.

If $a + b + c + d = M$ then $\lambda = 0$ and all four points ARE the same point so protocol says YES.
So Protocol Works!

Brady's Protocol's Complexity

Brady's protocol takes $O(\lg(\Gamma_{sq}(M))$.

Brady's Protocol's Complexity

Brady's protocol takes $O(\lg(\Gamma_{sq}(M))$.

We know

$$\Gamma_{sq}(M) \le (\ln(3M))e^{(\ln(3M))^f}$$

So

Brady's Protocol's Complexity

Brady's protocol takes $O(\lg(\Gamma_{sq}(M))$.

We know

$$\Gamma_{sq}(M) \leq (\ln(3M))e^{(\ln(3M))^f}$$

So

$$\lg(\Gamma_{sq}(M)) \leq O(\log(\log(3M)) + (\log(3M))^f) = O((\log(3M)^f)$$

We could plug in $M = 2^{n+1} - 1$ but using $3M = 2^n$ is good enough since we don't care about order constants. We get:

$$O(n^f).$$

Protocol in the Literature

Exposition by William Gasarch

May 12, 2020

Protocol in the Literature

$M = 2^{n+1} - 1$ throughout.

1. Pre-step: A, B, C, D agree on a $\Gamma(M)$-coloring χ of $[M] \times [M] \times [M]$ that has no mono lit.
2. A: b, c, d, B: a, c, d, C:a, b, d. $a, b, c, d \in \{0, 1\}^n$ binary.
3. If A sees $b + c + d > M$, says NO and protocol stops. B,C,D sim.
4. A finds a', s.t. $a' + b + c + d = M$ and says $\chi(a', b, c)$.
5. B finds b' s.t. $a + b' + c + d = M$ and says $\chi(a, b', c)$.
6. C finds c' s.t. $a + b + c' + d = M$ and says $\chi(a, b, c')$.
7. D says Y if all the χ's are $\chi(a, b, c)$, N otherwise.

Protocol in the Literature

$M = 2^{n+1} - 1$ throughout.

1. Pre-step: A, B, C, D agree on a $\Gamma(M)$-coloring χ of $[M] \times [M] \times [M]$ that has no mono lit.
2. A: b, c, d, B: a, c, d, C:a, b, d. $a, b, c, d \in \{0, 1\}^n$ binary.
3. If A sees $b + c + d > M$, says NO and protocol stops. B,C,D sim.
4. A finds a', s.t. $a' + b + c + d = M$ and says $\chi(a', b, c)$.
5. B finds b' s.t. $a + b' + c + d = M$ and says $\chi(a, b', c)$.
6. C finds c' s.t. $a + b + c' + d = M$ and says $\chi(a, b, c')$.
7. D says Y if all the χ's are $\chi(a, b, c)$, N otherwise.

Numb bits: $3 \lg(\Gamma(M)) + O(1)$. We show this is $\leq O(n^f)$.

Protocol in the Literature

$M = 2^{n+1} - 1$ throughout.

1. Pre-step: A, B, C, D agree on a $\Gamma(M)$-coloring χ of $[M] \times [M] \times [M]$ that has no mono lit.
2. A: b, c, d, B: a, c, d, C:a, b, d. $a, b, c, d \in \{0, 1\}^n$ binary.
3. If A sees $b + c + d > M$, says NO and protocol stops. B,C,D sim.
4. A finds a', s.t. $a' + b + c + d = M$ and says $\chi(a', b, c)$.
5. B finds b' s.t. $a + b' + c + d = M$ and says $\chi(a, b', c)$.
6. C finds c' s.t. $a + b + c' + d = M$ and says $\chi(a, b, c')$.
7. D says Y if all the χ's are $\chi(a, b, c)$, N otherwise.

Numb bits: $3 \lg(\Gamma(M)) + O(1)$. We show this is $\leq O(n^f)$.
But first we show that it works.

Literature Protocol Works

Assume $a + b + c + d = M - \lambda$ where $\lambda \geq 0$.
By Algebra one can show
$a' = a + \lambda$
$b' = b + \lambda$
$c' = c + \lambda$

Literature Protocol Works

Assume $a + b + c + d = M - \lambda$ where $\lambda \geq 0$.
By Algebra one can show
$a' = a + \lambda$
$b' = b + \lambda$
$c' = c + \lambda$
$(a', b, c) = (a + \lambda, b + c)$

Literature Protocol Works

Assume $a + b + c + d = M - \lambda$ where $\lambda \geq 0$.
By Algebra one can show
$a' = a + \lambda$
$b' = b + \lambda$
$c' = c + \lambda$
$(a', b, c) = (a + \lambda, b + c)$
$(a, b', c) = (a, b + \lambda, c)$

Literature Protocol Works

Assume $a + b + c + d = M - \lambda$ where $\lambda \geq 0$.
By Algebra one can show
$a' = a + \lambda$
$b' = b + \lambda$
$c' = c + \lambda$
$(a', b, c) = (a + \lambda, b + c)$
$(a, b', c) = (a, b + \lambda, c)$
$(a, b, c') = (a, b, c + \lambda)$.

Literature Protocol Works

Assume $a + b + c + d = M - \lambda$ where $\lambda \geq 0$.
By Algebra one can show
$a' = a + \lambda$
$b' = b + \lambda$
$c' = c + \lambda$
$(a', b, c) = (a + \lambda, b + c)$
$(a, b', c) = (a, b + \lambda, c)$
$(a, b, c') = (a, b, c + \lambda)$.
$(a, b, c) = (a, b, c)$.
Note that these four form a lit!

Literature Protocol Works

Assume $a + b + c + d = M - \lambda$ where $\lambda \geq 0$.
By Algebra one can show
$a' = a + \lambda$
$b' = b + \lambda$
$c' = c + \lambda$
$(a', b, c) = (a + \lambda, b + c)$
$(a, b', c) = (a, b + \lambda, c)$
$(a, b, c') = (a, b, c + \lambda)$.
$(a, b, c) = (a, b, c)$.
Note that these four form a lit!

If protocol says YES then all the points of the lit have the same color, so $\lambda = 0$ and $a + b + c + d = M$.

Literature Protocol Works

Assume $a+b+c+d = M - \lambda$ where $\lambda \geq 0$.
By Algebra one can show
$a' = a + \lambda$
$b' = b + \lambda$
$c' = c + \lambda$
$(a', b, c) = (a + \lambda, b + c)$
$(a, b', c) = (a, b + \lambda, c)$
$(a, b, c') = (a, b, c + \lambda)$.
$(a, b, c) = (a, b, c)$.
Note that these four form a lit!

If protocol says YES then all the points of the lit have the same color, so $\lambda = 0$ and $a+b+c+d = M$.

If $a+b+c+d = M$ then $\lambda = 0$ and all four points ARE the same point so protocol says YES.
So Protocol Works!

Literature's Protocol's Complexity

Lit protocol takes $O(\lg(\Gamma_{lit}(M))$.

Literature's Protocol's Complexity

Lit protocol takes $O(\lg(\Gamma_{lit}(M))$.

We know

$$\Gamma_{lit}(M) \le (\ln(6M))e^{(\ln(6M))^f}$$

So

Literature's Protocol's Complexity

Lit protocol takes $O(\lg(\Gamma_{lit}(M))$.

We know

$$\Gamma_{lit}(M) \le (\ln(6M))e^{(\ln(6M))^f}$$

So

$$\lg(\Gamma_{sq}(M)) \le O(\log(\log(6M)) + (\log(6M))^f) \le O((\log(6M)^f)$$

We could plug in $M = 2^{n+1} - 1$ but using $6M = 2^n$ is good enough since we don't care about order constants. We get

$$O(n^f).$$