Application of Ramsey Theory to Multiparty Comm Complexity

Exposition by William Gasarch

April 15, 2022

Credit where Credit is Due

The results in this talk are due to
Chandra, Furst, Lipton.

Multi-Party Protocols

Proc of the 15th ACM Syp on Theory of Comp (STOC)

1983

The Problem

Alice is A, Bob is B, Carol is C.

The Problem

Alice is A, Bob is B, Carol is C.

1. A, B, and C have a string of length n on their foreheads.

The Problem

Alice is A, Bob is B, Carol is C.

1. A, B, and C have a string of length n on their foreheads.
2. A's forehead has a, B's has b, C's has c.

The Problem

Alice is A, Bob is B, Carol is C.

1. A, B, and C have a string of length n on their foreheads.
2. A's forehead has a, B's has b, C's has c.
3. They want to know if $a + b + c = 2^{n+1} - 1$.

The Problem

Alice is A, Bob is B, Carol is C.

1. A, B, and C have a string of length n on their foreheads.
2. A's forehead has a, B's has b, C's has c.
3. They want to know if $a + b + c = 2^{n+1} - 1$.
4. **Solution** A says b, B then computes $a + b + c$ and then says YES if $a + b + c = 2^{n+1} - 1$, NO if not.

The Problem

Alice is A, Bob is B, Carol is C.

1. A, B, and C have a string of length n on their foreheads.
2. A's forehead has a, B's has b, C's has c.
3. They want to know if $a + b + c = 2^{n+1} - 1$.
4. **Solution** A says b, B then computes $a + b + c$ and then says YES if $a + b + c = 2^{n+1} - 1$, NO if not.
5. **Solution** uses $n + 1$ bits of comm. Can do better?

Vote

Vote

1. Any protocol requires $n+1$ bits, hence the one given that takes $n+1$ is the best you can do. The proof uses Theorems that could be in this course.

Vote

1. Any protocol requires $n+1$ bits, hence the one given that takes $n+1$ is the best you can do. The proof uses Theorems that could be in this course.
2. There is a protocol that takes αn bits for some $\alpha < 1$ but any protocol requires $\Omega(n)$ bits. Either the proof of the upper bound or the proof of the lower bound or both use Theorems that could be in this course.

Vote

1. Any protocol requires $n+1$ bits, hence the one given that takes $n+1$ is the best you can do. The proof uses Theorems that could be in this course.
2. There is a protocol that takes αn bits for some $\alpha < 1$ but any protocol requires $\Omega(n)$ bits. Either the proof of the upper bound or the proof of the lower bound or both use Theorems that could be in this course.
3. There is a protocol that takes $\ll n$ bits. The proof uses Theorems that could be in this course.

Vote

1. Any protocol requires $n+1$ bits, hence the one given that takes $n+1$ is the best you can do. The proof uses Theorems that could be in this course.
2. There is a protocol that takes αn bits for some $\alpha < 1$ but any protocol requires $\Omega(n)$ bits. Either the proof of the upper bound or the proof of the lower bound or both use Theorems that could be in this course.
3. There is a protocol that takes $\ll n$ bits. The proof uses Theorems that could be in this course.

STUDENTS WORK IN GROUPS

Protocol in $\frac{n}{2} + O(1)$ bits

1. A:$a_0 \cdots a_{n-1}$, B:$b_0 \cdots b_{n-1}$, C:$c_0 \cdots c_{n-1}$.
2. A says: $b_{n-1} \oplus c_0, b_{n-2} \oplus c_1, \cdots, b_{n/2} \oplus c_{n/2-1}$.
3. Bob knows c_i's so he now knows $b_{n/2}, \ldots, b_{n-1}$.
4. Carol knows b_i's so she now knows $c_0, \ldots, c_{n/2-1}$.
5. 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
   $a_{n/2-1} \cdots a_0 + b_{n/2-1} \cdots b_0 + c_{n/2-1} \cdots c_0$.
   View this as an $(n/2)$-bit string s and a carry bit z.
6. $s = 1^{n/2}$: Carol says (MAYBE,z). Otherwise: Carol says NO.
7. Bob knows $a_{n/2}, \ldots, a_{n-1}$, $b_{n/2}, \ldots, b_{n-1}$, $c_{n/2}, \ldots, c_{n-1}$ and z so he can compute $a + b + c$. If $= M$ then say YES, if not then say NO.

Vote Again

Vote

Vote Again

Vote

- There is a protocol that uses $\ll n$ bits AND I use Ramsey Theory to prove it.

Vote Again

Vote

- There is a protocol that uses $\ll n$ bits AND I use Ramsey Theory to prove it.
- There exists a $0 < \beta < \frac{1}{2}$ such that **any** protocol requires $\geq \beta n$ bits AND I use Ramsey Theory to prove it.

Vote Again

Vote

- There is a protocol that uses $\ll n$ bits AND I use Ramsey Theory to prove it.
- There exists a $0 < \beta < \frac{1}{2}$ such that **any** protocol requires $\geq \beta n$ bits AND I use Ramsey Theory to prove it.

I will show a $\sqrt{n} \ll n$ protocol, which will use 3-free sets so will indeed use Ramsey Theory.

We Look At the L-Theorem Backwards

Notation M will be $2^{n+1}-1$ which is 1^{n+1} in binary.
***L*-Theorem** For all c there exists M such that for all c-colorings of $[M] \times [M]$ there exists a mono L or $\urcorner$.

We Look At the L-Theorem Backwards

Notation M will be $2^{n+1}-1$ which is 1^{n+1} in binary.
***L*-Theorem** For all c there exists M such that for all c-colorings of $[M]\times[M]$ there exists a mono L or $\urcorner$.

Fix M.
Q $(\exists c)$: $[M]\times[M]$ can be c-colored w/o mono L or $\urcorner$?

We Look At the L-Theorem Backwards

Notation M will be $2^{n+1}-1$ which is 1^{n+1} in binary.
***L*-Theorem** For all c there exists M such that for all c-colorings of $[M]\times[M]$ there exists a mono L or $\urcorner$.

Fix M.
Q $(\exists c)$: $[M]\times[M]$ can be c-colored w/o mono L or $\urcorner$?

Yes $c=M^2$, color every point differently.

We Look At the L-Theorem Backwards

Notation M will be $2^{n+1}-1$ which is 1^{n+1} in binary.
***L*-Theorem** For all c there exists M such that for all c-colorings of $[M] \times [M]$ there exists a mono L or $\urcorner$.

Fix M.
Q $(\exists c)$: $[M] \times [M]$ can be c-colored w/o mono L or $\urcorner$?

Yes $c = M^2$, color every point differently.

Q $(\exists c \ll M^2)$: $[M] \times [M]$ can be c-colored w/o mono L or $\urcorner$?

We Look At the L-Theorem Backwards

Notation M will be $2^{n+1}-1$ which is 1^{n+1} in binary.

***L*-Theorem** For all c there exists M such that for all c-colorings of $[M]\times[M]$ there exists a mono L or $\urcorner$.

Fix M.

Q $(\exists c)$: $[M]\times[M]$ can be c-colored w/o mono L or $\urcorner$?

Yes $c=M^2$, color every point differently.

Q $(\exists c \ll M^2)$: $[M]\times[M]$ can be c-colored w/o mono L or $\urcorner$?

Yes, $c=M$, color every row differently.

We Look At the L-Theorem Backwards

Notation M will be $2^{n+1}-1$ which is 1^{n+1} in binary.
***L*-Theorem** For all c there exists M such that for all c-colorings of $[M]\times[M]$ there exists a mono L or $\urcorner$.

Fix M.

Q $(\exists c)$: $[M]\times[M]$ can be c-colored w/o mono L or $\urcorner$?

Yes $c=M^2$, color every point differently.

Q $(\exists c \ll M^2)$: $[M]\times[M]$ can be c-colored w/o mono L or $\urcorner$?

Yes, $c=M$, color every row differently.

Q $(\exists c)$: ALL c-colorings of $[M]\times[M]$ there is a mono L or $\urcorner$?

We Look At the L-Theorem Backwards

Notation M will be $2^{n+1} - 1$ which is 1^{n+1} in binary.
***L*-Theorem** For all c there exists M such that for all c-colorings of $[M] \times [M]$ there exists a mono L or $\urcorner$.

Fix M.

Q $(\exists c)$: $[M] \times [M]$ can be c-colored w/o mono L or $\urcorner$?

Yes $c = M^2$, color every point differently.

Q $(\exists c \ll M^2)$: $[M] \times [M]$ can be c-colored w/o mono L or $\urcorner$?

Yes, $c = M$, color every row differently.

Q $(\exists c)$: ALL c-colorings of $[M] \times [M]$ there is a mono L or $\urcorner$?

Yes $c = 1$. Stupid but true.

We Look At the *L*-Theorem Backwards

Notation M will be $2^{n+1}-1$ which is 1^{n+1} in binary.
***L*-Theorem** For all c there exists M such that for all c-colorings of $[M]\times[M]$ there exists a mono L or $\urcorner$.

Fix M.

Q $(\exists c)$: $[M]\times[M]$ can be c-colored w/o mono L or $\urcorner$?

Yes $c=M^2$, color every point differently.

Q $(\exists c \ll M^2)$: $[M]\times[M]$ can be c-colored w/o mono L or $\urcorner$?

Yes, $c=M$, color every row differently.

Q $(\exists c)$: ALL c-colorings of $[M]\times[M]$ there is a mono L or $\urcorner$?

Yes $c=1$. Stupid but true.

We actually need a stronger condition:
Definition $\Gamma(M)$ is the least c such that there is a c-coloring of $[M]\times[M]$ w/o mono L or $\urcorner$.

We Look At the L-Theorem Backwards

Notation M will be $2^{n+1}-1$ which is 1^{n+1} in binary.
***L*-Theorem** For all c there exists M such that for all c-colorings of $[M]\times[M]$ there exists a mono L or $\urcorner$.

Fix M.
Q $(\exists c)$: $[M]\times[M]$ can be c-colored w/o mono L or $\urcorner$?

Yes $c=M^2$, color every point differently.

Q $(\exists c \ll M^2)$: $[M]\times[M]$ can be c-colored w/o mono L or $\urcorner$?

Yes, $c=M$, color every row differently.

Q $(\exists c)$: ALL c-colorings of $[M]\times[M]$ there is a mono L or $\urcorner$?

Yes $c=1$. Stupid but true.

We actually need a stronger condition:
Definition $\Gamma(M)$ is the least c such that there is a c-coloring of $[M]\times[M]$ w/o mono L or $\urcorner$.

We give a $3\lg(\Gamma(M))+O(1)$ bit protocol and then bound $\Gamma(M)$.

Protocol

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

1. Pre-step: A, B, and C agree on a $\Gamma(M)$-coloring χ of $[M] \times [M]$ that has no mono L or $\urcorner$.
2. A: b, c, B: a, c, C:a, b. $a, b, c \in \{0,1\}^n$ numbers in binary.
3. If A sees $b + c > M$, says NO and protocol stops. B,C, sim.
4. A finds a', s.t. $a' + b + c = M$ and says $\chi(a', b)$.
5. B finds b' s.t. $a + b' + c = M$ and says $\chi(a, b')$.
6. C says Y if both colors agree with $\chi(a, b)$, no otherwise.
7. If they all broadcast the same color A says Y, else A says NO.

Protocol

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

1. Pre-step: A, B, and C agree on a $\Gamma(M)$-coloring χ of $[M] \times [M]$ that has no mono L or $\urcorner$.
2. A: b, c, B: a, c, C:a, b. $a, b, c \in \{0,1\}^n$ numbers in binary.
3. If A sees $b + c > M$, says NO and protocol stops. B,C, sim.
4. A finds a', s.t. $a' + b + c = M$ and says $\chi(a', b)$.
5. B finds b' s.t. $a + b' + c = M$ and says $\chi(a, b')$.
6. C says Y if both colors agree with $\chi(a, b)$, no otherwise.
7. If they all broadcast the same color A says Y, else A says NO.

Number of bits: $2\lg(\Gamma(M)) + O(1)$. We show this is $\leq O(\sqrt{n})$.

Protocol

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

1. Pre-step: A, B, and C agree on a $\Gamma(M)$-coloring χ of $[M] \times [M]$ that has no mono L or $\urcorner$.
2. A: b, c, B: a, c, C:a, b. $a, b, c \in \{0, 1\}^n$ numbers in binary.
3. If A sees $b + c > M$, says NO and protocol stops. B,C, sim.
4. A finds a', s.t. $a' + b + c = M$ and says $\chi(a', b)$.
5. B finds b' s.t. $a + b' + c = M$ and says $\chi(a, b')$.
6. C says Y if both colors agree with $\chi(a, b)$, no otherwise.
7. If they all broadcast the same color A says Y, else A says NO.

Number of bits: $2\lg(\Gamma(M)) + O(1)$. We show this is $\le O(\sqrt{n})$.
But first we show that it works.

Why Does This Work?

Assume $a+b+c = M - \lambda$ where $\lambda \in \mathbb{Z}$.

Why Does This Work?

Assume $a + b + c = M - \lambda$ where $\lambda \in \mathbb{Z}$.

$a' = M - b - c = M - (a + b + c) + (a + b + c) - b - c = M - (M - \lambda) + a = a + \lambda$

Why Does This Work?

Assume $a + b + c = M - \lambda$ where $\lambda \in \mathbb{Z}$.

$a' = M - b - c = M - (a + b + c) + (a + b + c) - b - c = M - (M - \lambda) + a = a + \lambda$

$b' = b + \lambda$ (similar reasoning)

Why Does This Work?

Assume $a + b + c = M - \lambda$ where $\lambda \in \mathbb{Z}$.

$a' = M - b - c = M - (a + b + c) + (a + b + c) - b - c = M - (M - \lambda) + a = a + \lambda$

$b' = b + \lambda$ (similar reasoning)

$(a', b) = (a + \lambda, b)$

Why Does This Work?

Assume $a + b + c = M - \lambda$ where $\lambda \in \mathbb{Z}$.

$a' = M - b - c = M - (a + b + c) + (a + b + c) - b - c = M - (M - \lambda) + a = a + \lambda$

$b' = b + \lambda$ (similar reasoning)

$(a', b) = (a + \lambda, b)$

$(a, b') = (a, b + \lambda)$

Why Does This Work?

Assume $a+b+c = M-\lambda$ where $\lambda \in \mathbb{Z}$.

$a' = M-b-c = M-(a+b+c)+(a+b+c)-b-c = M-(M-\lambda)+a = a+\lambda$

$b' = b+\lambda$ (similar reasoning)

$(a', b) = (a+\lambda, b)$

$(a, b') = (a, b+\lambda)$

If protocol says YES then $\chi(a+\lambda, b) = \chi(a, b+\lambda) = \chi(a, b)$.
Since χ has no mono L or $\urcorner$, $\lambda = 0$ so $a+b+c = M$.

Why Does This Work?

Assume $a + b + c = M - \lambda$ where $\lambda \in \mathbb{Z}$.

$a' = M - b - c = M - (a + b + c) + (a + b + c) - b - c =$
$M - (M - \lambda) + a = a + \lambda$

$b' = b + \lambda$ (similar reasoning)

$(a', b) = (a + \lambda, b)$

$(a, b') = (a, b + \lambda)$

If protocol says YES then $\chi(a + \lambda, b) = \chi(a, b + \lambda) = \chi(a, b)$.
Since χ has no mono L or $\urcorner$, $\lambda = 0$ so $a + b + c = M$.

If protocol says NO then either
$\chi(a + \lambda, b) \neq \chi(a, b + \lambda)$: so $\lambda \neq 0$.
$\chi(a + \lambda, b) \neq \chi(a, b)$: so $\lambda \neq 0$.
$\chi(a, b + \lambda) \neq \chi(a, b)$: so $\lambda \neq 0$.

Why Does This Work?

Assume $a + b + c = M - \lambda$ where $\lambda \in \mathbb{Z}$.

$a' = M - b - c = M - (a + b + c) + (a + b + c) - b - c = M - (M - \lambda) + a = a + \lambda$

$b' = b + \lambda$ (similar reasoning)

$(a', b) = (a + \lambda, b)$

$(a, b') = (a, b + \lambda)$

If protocol says YES then $\chi(a + \lambda, b) = \chi(a, b + \lambda) = \chi(a, b)$.
Since χ has no mono L or $\urcorner$, $\lambda = 0$ so $a + b + c = M$.

If protocol says NO then either
$\chi(a + \lambda, b) \neq \chi(a, b + \lambda)$: so $\lambda \neq 0$.
$\chi(a + \lambda, b) \neq \chi(a, b)$: so $\lambda \neq 0$.
$\chi(a, b + \lambda) \neq \chi(a, b)$: so $\lambda \neq 0$.

In all cases $\lambda \neq 0$ so $a + b + c \neq M$.

Relating $\Gamma(M)$ with VDW

We need to bound $\lg(\Gamma(M))$.

Relating $\Gamma(M)$ with VDW

We need to bound $\lg(\Gamma(M))$.

Lemma Let Z be such that $3M < W(3, Z)$. Then $\Gamma(M) \leq Z$.

Relating $\Gamma(M)$ with VDW

We need to bound $\lg(\Gamma(M))$.

Lemma Let Z be such that $3M < W(3, Z)$. Then $\Gamma(M) \leq Z$.
Proof

Relating $\Gamma(M)$ with VDW

We need to bound $\lg(\Gamma(M))$.

Lemma Let Z be such that $3M < W(3, Z)$. Then $\Gamma(M) \le Z$.
Proof
Let COL be an Z-coloring of $\{1, \ldots, 3M\}$ with no mono 3-AP's.

Relating $\Gamma(M)$ with VDW

We need to bound $\lg(\Gamma(M))$.

Lemma Let Z be such that $3M < W(3, Z)$. Then $\Gamma(M) \le Z$.
Proof
Let COL be an Z-coloring of $\{1, \ldots, 3M\}$ with no mono 3-AP's.
Define $\mathrm{COL}'\colon [M] \times [M] \to [Z]$

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

Relating $\Gamma(M)$ with VDW

We need to bound $\lg(\Gamma(M))$.

Lemma Let Z be such that $3M < W(3, Z)$. Then $\Gamma(M) \le Z$.

Proof

Let COL be an Z-coloring of $\{1, \ldots, 3M\}$ with no mono 3-AP's.
Define $\mathrm{COL}'\colon [M] \times [M] \to [Z]$

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

Claim COL' has no mono L's or $\urcorner$.

Relating $\Gamma(M)$ with VDW

We need to bound $\lg(\Gamma(M))$.

Lemma Let Z be such that $3M < W(3, Z)$. Then $\Gamma(M) \le Z$.

Proof

Let COL be an Z-coloring of $\{1, \ldots, 3M\}$ with no mono 3-AP's.
Define $\mathrm{COL}'\colon [M] \times [M] \to [Z]$

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

Claim COL' has no mono L's or $\urcorner$.
If COL' has a mono L or $\urcorner$ then there exists $x, y \in [M], \lambda \in \mathbb{Z}$:

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

Relating $\Gamma(M)$ with VDW

We need to bound $\lg(\Gamma(M))$.

Lemma Let Z be such that $3M < W(3, Z)$. Then $\Gamma(M) \le Z$.

Proof

Let COL be an Z-coloring of $\{1, \ldots, 3M\}$ with no mono 3-AP's.

Define $\mathrm{COL}'\colon [M] \times [M] \to [Z]$

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

Claim COL' has no mono L's or $\urcorner$.

If COL' has a mono L or $\urcorner$ then there exists $x, y \in [M], \lambda \in \mathbb{Z}$:

$$COL'(x, y) = COL'(x + \lambda, y) = COL'(x, y + \lambda) \text{ hence}$$

Relating $\Gamma(M)$ with VDW

We need to bound $\lg(\Gamma(M))$.

Lemma Let Z be such that $3M < W(3, Z)$. Then $\Gamma(M) \le Z$.

Proof

Let COL be an Z-coloring of $\{1, \ldots, 3M\}$ with no mono 3-AP's.
Define $\mathrm{COL}'\colon [M] \times [M] \to [Z]$

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

Claim COL' has no mono L's or $\urcorner$.
If COL' has a mono L or $\urcorner$ then there exists $x, y \in [M], \lambda \in \mathbb{Z}$:

$$COL'(x, y) = COL'(x + \lambda, y) = COL'(x, y + \lambda) \text{ hence}$$

$COL(x+2y) = COL(x+2y+\lambda) = COL(x+2y+2\lambda)$: a mono 3-AP

(If $\lambda < 0$ then $x + 2y + 2\lambda, x + 2y + \lambda, x + 2y$ is the 3-AP.

Recall Last Slide From 3freetalk

In talk on $W(3, c)$ we proved:

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

Recall Last Slide From 3freetalk

In talk on $W(3,c)$ we proved:

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

In talk on $W(3,c)$ we sketched:

Thm There exists a 3-free subset of $[V]$ of size $\ge V^{1-\frac{1}{\sqrt{\lg V}}}$

Recall Last Slide From 3freetalk

In talk on $W(3,c)$ we proved:

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

In talk on $W(3,c)$ we sketched:

Thm There exists a 3-free subset of $[V]$ of size $\ge V^{1-\frac{1}{\sqrt{\lg V}}}$

We combine these two to get:

Thm Let $V \in \mathbb{N}$. Then there is a $V^{\frac{1}{\sqrt{\lg V}}}\ln(V)$-coloring of $[V]$ with no mono 3-APs. Hence

$$W(3, V^{\frac{1}{\sqrt{\lg V}}}\ln(V)) \ge V.$$

Just Plug in $V = 3M$

Thm Let $V \in \mathbb{N}$. Then there is a $V^{\frac{1}{\sqrt{\lg V}}} \ln(V)$-coloring of $[V]$ with no mono 3-APs. Hence

$$W(3, V^{\frac{1}{\sqrt{\lg V}}} \ln(V)) \geq V.$$

$$\text{Hence } W(3, (3M)^{\frac{1}{\sqrt{\lg 3M}}} \ln(3M)) \geq 3M.$$

$$\text{Hence } \Gamma(M) \leq (3M)^{\frac{1}{\sqrt{\lg 3M}}} \ln(3M))$$

$$\text{Hence } \lg(\Gamma(M)) \leq \frac{1}{\sqrt{\lg 3M}} \lg(3M) + \lg(\ln(3M)) = O(\sqrt{\log(M)})$$

$$M = 2^{n+1} - 1 \sim 2^n \text{ so } \lg(\Gamma(M)) \leq O(\sqrt{n})$$

Upper and Lower Bound on Protocol

- We showed our protocol uses $\le 3\lg(\Gamma(M)) \le O(\sqrt{n})$.
- Known: lower bound of $\Omega(\lg(\Gamma(M))$.
- Original paper had lower bound of $\Omega(1)$ which is all they needed for their goal which was non-linear lower bounds on branching programs.
- Gasarch showed lower bound of $\Omega(\log\log n)$.
- k-player version of this game has also been studied.