COMBINATORIAL SCHEMES IN ALGEBRAIC ALGORITHMS

Nitin Saxena
(with Manuel Arora, Gábor Ivanyos and Marek Karpinski)

1Indian Institute of Technology
Kanpur, India

MTAGT Conference 2014
Villanova, PA
COMBINATORIAL SCHEMES
Definitions
Conjecture

POLYNOMIAL FACTORING
The Problem
GRH Connection

OUR ALGORITHM
Tensor Powers
Schemes
The combinatorial objects in this talk are just partitions of $[n]^{(m)}$.

Where $[n]^{(m)}$ is $\{(i_1, \ldots, i_m) \mid \text{distinct } i_1, \ldots, i_m \in [n]\}$.

Let $\mathcal{P}$ be a partition of $[n]^{(m)}$. The elements of $\mathcal{P}$ are colors.

For eg. $\{\{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}\}$ is a partition of $[3]^{(2)}$ with two colors.

$\mathcal{P}$ is invariant if for every color $P \in \mathcal{P}$, $\forall \sigma \in \text{Symm}_m$, $P^\sigma \in \mathcal{P}$.
The combinatorial objects in this talk are just partitions of $[n]^{(m)}$.

Where $[n]^{(m)}$ is $\{(i_1, \ldots, i_m) | \text{distinct } i_1, \ldots, i_m \in [n]\}$.

Let $\mathcal{P}$ be a partition of $[n]^{(m)}$. The elements of $\mathcal{P}$ are colors.

For eg. $\{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}$ is a partition of $[3]^{(2)}$ with two colors.

$\mathcal{P}$ is invariant if for every color $P \in \mathcal{P}$, $\forall \sigma \in \text{Symm}_m$, $P^\sigma \in \mathcal{P}$.
The combinatorial objects in this talk are just partitions of $[n]^{(m)}$.

Where $[n]^{(m)}$ is $\{(i_1, \ldots, i_m) | \text{distinct } i_1, \ldots, i_m \in [n]\}$.

Let $\mathcal{P}$ be a partition of $[n]^{(m)}$. The elements of $\mathcal{P}$ are colors.

For eg. $\{\{(1,2), (2,3), (3,1)\}, \{(1,3), (2,1), (3,2)\}\}$ is a partition of $[3]^{(2)}$ with two colors.

$\mathcal{P}$ is invariant if for every color $P \in \mathcal{P}$, $\forall \sigma \in \text{Symm}_m$, $P^\sigma \in \mathcal{P}$. 

**Invariant Partition**

- The combinatorial objects in this talk are just partitions of $[n]^{(m)}$.
- Where $[n]^{(m)}$ is $\{(i_1, \ldots, i_m) |$ distinct $i_1, \ldots, i_m \in [n]\}$.
- Let $\mathcal{P}$ be a partition of $[n]^{(m)}$. The elements of $\mathcal{P}$ are colors.
- For eg. $\{\{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}\}$ is a partition of $[3]^{(2)}$ with two colors.
- $\mathcal{P}$ is invariant if for every color $P \in \mathcal{P}$, $\forall \sigma \in \text{Symm}_m$, $P^\sigma \in \mathcal{P}$. 

The combinatorial objects in this talk are just partitions of \([n]^{(m)}\).

Where \([n]^{(m)}\) is \(\{(i_1, \ldots, i_m) \mid \text{distinct } i_1, \ldots, i_m \in [n]\}\).

Let \(\mathcal{P}\) be a partition of \([n]^{(m)}\). The elements of \(\mathcal{P}\) are colors.

For eg. \(\{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}\) is a partition of \([3]^{(2)}\) with two colors.

\(\mathcal{P}\) is\(^\star\) invariant if for every color \(P \in \mathcal{P}, \forall \sigma \in \text{Symm}_m, P^\sigma \in \mathcal{P}\).
Combinatorial Schemes

Definitions

**Invariant + compatible + regular = $m$-SCHEME**

- Suppose we have an invariant partition $P_s$ of $[n]^{(s)}$, for $1 \leq s \leq m$.
- Define projection $\pi_i : [n]^{(s)} \to [n]^{(s-1)}$ to be the map that drops the $i$-th coordinate.
- We call $P_s$ compatible if $P \in P_s \Rightarrow \pi_i(P) \in P_{s-1}$.
- We call $P_s$ regular if $\forall P \in P_s$: the number of preimages of any tuple of $\pi_i(P)$ in $P$ is the same, i.e. $|P|/|\pi_i(P)|$. This can be thought of as a subdegree of color $P$.
- The collection $\{P_1, \ldots, P_m\}$ is an $m$-scheme (on $[n]$) if all the $m$ partitions are invariant, compatible and regular.
- For eg. $P_1 := \{[3]\}$ and $P_2 := \{\{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}\}$ comprise a 2-scheme on $[3]$. 
**Combinatorial Schemes**

**Definitions**

**Invariant + compatible + regular = \( m \)-Scheme**

- Suppose we have an invariant partition \( \mathcal{P}_s \) of \([n]^{(s)}\), for \( 1 \leq s \leq m \).
- Define projection \( \pi_i : [n]^{(s)} \rightarrow [n]^{(s-1)} \) to be the map that drops the \( i \)-th coordinate.
- We call \( \mathcal{P}_s \) compatible if \( P \in \mathcal{P}_s \Rightarrow \pi_i(P) \in \mathcal{P}_{s-1} \).
- We call \( \mathcal{P}_s \) regular if \( \forall P \in \mathcal{P}_s : \) the number of preimages of any tuple of \( \pi_i(P) \) in \( P \) is the same, i.e. \( |P|/|\pi_i(P)| \). This can be thought of as a subdegree of color \( P \).
- The collection \( \{\mathcal{P}_1, \ldots, \mathcal{P}_m\} \) is an \( m \)-scheme (on \([n]\)) if all the \( m \) partitions are invariant, compatible and regular.
- For eg. \( \mathcal{P}_1 := \{\{3\}\} \) and \( \mathcal{P}_2 := \{\{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}\} \) comprise a 2-scheme on \([3]\).
INARIANT + COMPATIBLE + REGULAR =  \textit{m-SHME}

• Suppose we have an invariant partition $\mathcal{P}_s$ of $[n]^{(s)}$, for $1 \leq s \leq m$.

• Define projection $\pi_i : [n]^{(s)} \to [n]^{(s-1)}$ to be the map that drops the $i$-th coordinate.

• We call $\mathcal{P}_s$ compatible if $P \in \mathcal{P}_s \Rightarrow \pi_i(P) \in \mathcal{P}_{s-1}$.

• We call $\mathcal{P}_s$ regular if $\forall P \in \mathcal{P}_s :$ the number of preimages of any tuple of $\pi_i(P)$ in $P$ is the same, i.e. $|P|/|\pi_i(P)|$. This can be thought of as a subdegree of color $P$.

• The collection $\{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$ is an $m$-scheme (on $[n]$) if all the $m$ partitions are invariant, compatible and regular.

• For eg. $\mathcal{P}_1 := \{[3]\}$ and $\mathcal{P}_2 := \{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}$ comprise a 2-scheme on $[3]$. 
Combinatorial Schemes

Definitions

**Invariant + compatible + regular = \( m \)-scheme**

- Suppose we have an invariant partition \( \mathcal{P}_s \) of \( [n]^{(s)} \), for \( 1 \leq s \leq m \).
- Define projection \( \pi_i : [n]^{(s)} \to [n]^{(s-1)} \) to be the map that drops the \( i \)-th coordinate.
- We call \( \mathcal{P}_s \) compatible if \( P \in \mathcal{P}_s \Rightarrow \pi_i(P) \in \mathcal{P}_{s-1} \).
- We call \( \mathcal{P}_s \) regular if \( \forall P \in \mathcal{P}_s : \) the number of preimages of any tuple of \( \pi_i(P) \) in \( P \) is the same, i.e. \( |P|/|\pi_i(P)| \). This can be thought of as a subdegree of color \( P \).
- The collection \( \{\mathcal{P}_1, \ldots, \mathcal{P}_m\} \) is an \( m \)-scheme (on \( [n] \)) if all the \( m \) partitions are invariant, compatible and regular.
- For eg. \( \mathcal{P}_1 := \{[3]\} \) and \( \mathcal{P}_2 := \{\{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}\} \) comprise a 2-scheme on \( [3] \).
Combinatorial Schemes

Definitions

**Invariant + compatible + regular = m-scheme**

- Suppose we have an invariant partition \( \mathcal{P}_s \) of \([n]^{(s)}\), for \(1 \leq s \leq m\).
- Define projection \( \pi_i : [n]^{(s)} \to [n]^{(s-1)} \) to be the map that drops the \(i\)-th coordinate.
- We call \( \mathcal{P}_s \) compatible if \( P \in \mathcal{P}_s \Rightarrow \pi_i(P) \in \mathcal{P}_{s-1} \).
- We call \( \mathcal{P}_s \) regular if \( \forall P \in \mathcal{P}_s : \) the number of preimages of any tuple of \( \pi_i(P) \) in \( P \) is the same, i.e. \(|P|/|\pi_i(P)|\). This can be thought of as a subdegree of color \( P \).
- The collection \( \{\mathcal{P}_1, \ldots, \mathcal{P}_m\} \) is an \( m \)-scheme (on \([n]\)) if all the \( m \) partitions are invariant, compatible and regular.
- For eg. \( \mathcal{P}_1 := \{[3]\} \) and \( \mathcal{P}_2 := \{\{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}\} \) comprise a 2-scheme on \([3]\).
Combinatorial Schemes

Definitions

**Invariant + Compatible + Regular = \textit{m-scheme}**

• Suppose we have an invariant partition $\mathcal{P}_s$ of $[n]^{(s)}$, for $1 \leq s \leq m$.

• Define projection $\pi_i : [n]^{(s)} \rightarrow [n]^{(s-1)}$ to be the map that drops the $i$-th coordinate.

• We call $\mathcal{P}_s$ compatible if $P \in \mathcal{P}_s \Rightarrow \pi_i(P) \in \mathcal{P}_{s-1}$.

• We call $\mathcal{P}_s$ regular if $\forall P \in \mathcal{P}_s$: the number of preimages of any tuple of $\pi_i(P)$ in $P$ is the same, i.e. $|P|/|\pi_i(P)|$. This can be thought of as a subdegree of color $P$.

• The collection $\{\mathcal{P}_1, \ldots, \mathcal{P}_m\}$ is an \textit{m-scheme} (on $[n]$) if all the $m$ partitions are invariant, compatible and regular.

• For eg. $\mathcal{P}_1 := \{[3]\}$ and $\mathcal{P}_2 := \{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}$ comprise a 2-scheme on $[3]$. 
Combinatorial Schemes
Definition

**Invariant + compatible + regular =** \textit{m-scheme}

• Suppose we have an invariant partition \( \mathcal{P}_s \) of \([n]^{(s)}\), for \(1 \leq s \leq m\).

• Define projection \( \pi_i : [n]^{(s)} \to [n]^{(s-1)} \) to be the map that drops the \( i \)-th coordinate.

• We call \( \mathcal{P}_s \) compatible if \( P \in \mathcal{P}_s \Rightarrow \pi_i(P) \in \mathcal{P}_{s-1} \).

• We call \( \mathcal{P}_s \) regular if \( \forall P \in \mathcal{P}_s : \) the number of preimages of any tuple of \( \pi_i(P) \) in \( P \) is the same, i.e. \(|P|/|\pi_i(P)|\). This can be thought of as a subdegree of color \( P \).

• The collection \( \{\mathcal{P}_1, \ldots, \mathcal{P}_m\} \) is an \textit{m-scheme} (on \([n]\)) if all the \( m \) partitions are invariant, compatible and regular.

• For eg. \( \mathcal{P}_1 := \{[3]\} \) and \( \mathcal{P}_2 := \{\{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}\} \) comprise a 2-scheme on \([3]\).
Examples of $m$-schemes are abundant in algebraic-combinatorics.

- A regular connected graph $(V, E)$ is a 2-scheme on $V$. Take $\mathcal{P}_1 = \{V\}$ and $\mathcal{P}_2 = \{E, \overline{E}\}$.

- A strongly regular connected graph $(V, E)$ is a 3-scheme on $V$. Define $\mathcal{P}_3$ with 8 colors each corresponding to the set of triples $(u, v, w) \in V^{(3)}$ with $(u, v)$, $(u, w)$ and $(v, w)$ being edges or non-edges.

- A permutation group $G \leq \text{Symm}_n$ gives an $m$-scheme on $[n]$. The colors of $\mathcal{P}_s$ are the various orbits of $G$ acting on $[n]^{(s)}$. 
• Examples of $m$-schemes are abundant in algebraic-combinatorics.

• A regular connected graph $(V, E)$ is a 2-scheme on $V$. Take $P_1 = \{V\}$ and $P_2 = \{E, \bar{E}\}$.

• A strongly regular connected graph $(V, E)$ is a 3-scheme on $V$. Define $P_3$ with 8 colors each corresponding to the set of triples $(u, v, w) \in V^{(3)}$ with $(u, v), (u, w)$ and $(v, w)$ being edges or non-edges.

• A permutation group $G \leq \text{Symm}_n$ gives an $m$-scheme on $[n]$. The colors of $P_s$ are the various orbits of $G$ acting on $[n]^{(s)}$. 
Examples of \( m \)-schemes are abundant in algebraic-combinatorics.

A *regular* connected graph \((V, E)\) is a 2-scheme on \(V\). Take \(\mathcal{P}_1 = \{V\}\) and \(\mathcal{P}_2 = \{E, \overline{E}\}\).

A *strongly regular* connected graph \((V, E)\) is a 3-scheme on \(V\). Define \(\mathcal{P}_3\) with 8 colors each corresponding to the set of triples \((u, v, w)\) \(\in V^{(3)}\) with \((u, v)\), \((u, w)\) and \((v, w)\) being edges or non-edges.

A *permutation group* \(G \leq \text{Symm}_n\) gives an \(m\)-scheme on \([n]\). The colors of \(\mathcal{P}_s\) are the various orbits of \(G\) acting on \([n]^{(s)}\).
Examples of $m$-schemes are abundant in algebraic-combinatorics.

A regular connected graph $(V, E)$ is a 2-scheme on $V$. Take $\mathcal{P}_1 = \{V\}$ and $\mathcal{P}_2 = \{E, \bar{E}\}$.

A strongly regular connected graph $(V, E)$ is a 3-scheme on $V$. Define $\mathcal{P}_3$ with 8 colors each corresponding to the set of triples $(u, v, w) \in V^{(3)}$ with $(u, v), (u, w)$, and $(v, w)$ being edges or non-edges.

A permutation group $G \leq \text{Symm}_n$ gives an $m$-scheme on $[n]$. The colors of $\mathcal{P}_s$ are the various orbits of $G$ acting on $[n]^{(s)}$. 
Examples of $m$-schemes are abundant in algebraic-combinatorics.

A regular connected graph $(V, E)$ is a 2-scheme on $V$. Take $P_1 = \{V\}$ and $P_2 = \{E, \bar{E}\}$.

A strongly regular connected graph $(V, E)$ is a 3-scheme on $V$. Define $P_3$ with 8 colors each corresponding to the set of triples $(u, v, w) \in V^{(3)}$ with $(u, v), (u, w)$ and $(v, w)$ being edges or non-edges.

A permutation group $G \leq \text{Symm}_n$ gives an $m$-scheme on $[n]$. The colors of $P_s$ are the various orbits of $G$ acting on $[n]^{(s)}$. 

Classic Examples
Classic Examples

- Examples of $m$-schemes are abundant in algebraic-combinatorics.

- A regular connected graph $(V, E)$ is a 2-scheme on $V$. Take $P_1 = \{V\}$ and $P_2 = \{E, \overline{E}\}$.

- A strongly regular connected graph $(V, E)$ is a 3-scheme on $V$. Define $P_3$ with 8 colors each corresponding to the set of triples $(u, v, w) \in V^{(3)}$ with $(u, v), (u, w)$ and $(v, w)$ being edges or non-edges.

- A permutation group $G \leq \text{Symm}_n$ gives an $m$-scheme on $[n]$. The colors of $P_s$ are the various orbits of $G$ acting on $[n]^{(s)}$. 
Classic Examples

- Examples of $m$-schemes are abundant in algebraic-combinatorics.

- A regular connected graph $(V, E)$ is a 2-scheme on $V$. Take $\mathcal{P}_1 = \{V\}$ and $\mathcal{P}_2 = \{E, \overline{E}\}$.

- A strongly regular connected graph $(V, E)$ is a 3-scheme on $V$. Define $\mathcal{P}_3$ with 8 colors each corresponding to the set of triples $(u, v, w) \in V^{(3)}$ with $(u, v)$, $(u, w)$ and $(v, w)$ being edges or non-edges.

- A permutation group $G \leq \text{Symm}_n$ gives an $m$-scheme on $[n]$. The colors of $\mathcal{P}_s$ are the various orbits of $G$ acting on $[n]^{(s)}$. 
We are interested in more special $m$-schemes:

- An $m$-scheme is homogeneous if $|\mathcal{P}_1| = 1$, i.e. $\mathcal{P}_1 = \{[n]\}$.
- An $m$-scheme is antisymmetric if $\forall P \in \mathcal{P}_s$ and $\sigma \neq id$: $P^\sigma \neq P$.
- For eg. $\mathcal{P}_1 := \{[3]\}$ and $\mathcal{P}_2 := \{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}$ comprise a homogeneous and antisymmetric 2-scheme on $[3]$. 
... + **Homogeneous** + **Antisymmetric**

- We are interested in more special $m$-schemes:
  - An $m$-scheme is **homogeneous** if $|P_1| = 1$, i.e. $P_1 = \{[n]\}$.
  - An $m$-scheme is **antisymmetric** if $\forall P \in P_s$ and $\sigma \neq id$: $P^\sigma \neq P$.
  - For eg. $P_1 := \{[3]\}$ and $P_2 := \{\{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}\}$ comprise a homogeneous and antisymmetric 2-scheme on $[3]$. 
... + **Homogeneous** + **Antisymmetric**

- We are interested in more special $m$-schemes:
- An $m$-scheme is **homogeneous** if $|P_1| = 1$, i.e. $P_1 = \{ [n] \}$.
- An $m$-scheme is **antisymmetric** if $\forall P \in P_s$ and $\sigma \neq id$: $P^\sigma \neq P$.
- For eg. $P_1 := \{ [3] \}$ and $P_2 := \{ \{ (1, 2), (2, 3), (3, 1) \}, \{ (1, 3), (2, 1), (3, 2) \} \}$ comprise a homogeneous and antisymmetric 2-scheme on $[3]$. 
We are interested in more special $m$-schemes:

- An $m$-scheme is **homogeneous** if $|P_1| = 1$, i.e. $P_1 = \{[n]\}$.
- An $m$-scheme is **antisymmetric** if $\forall P \in P_s$ and $\sigma \neq id$: $P^\sigma \neq P$.
- For eg. $P_1 := \{[3]\}$ and $P_2 := \{\{(1, 2), (2, 3), (3, 1)\}, \{(1, 3), (2, 1), (3, 2)\}\}$ comprise a homogeneous and antisymmetric 2-scheme on $[3]$. 
OUTLINE

COMBINATORIAL SCHEMES

Definitions
Conjecture

POLYNOMIAL FACTORING

The Problem
GRH Connection

OUR ALGORITHM

Tensor Powers
Schemes
We expect that the antisymmetry condition forces the subdegree to drop rapidly with $m$.

To formalize this, we call a color $P \in \mathcal{P}_s$, in a $m$-scheme, a matching if $|P|/|\pi_i(P)| = 1$ and $\pi_i(P) = \pi_j(P)$ for some $i \neq j$.

Schemes Conjecture: Every homogeneous, antisymmetric 4-scheme has a matching.

- We have proved this conjecture for the only such schemes we currently know: orbit schemes.
- ... using Seress (1996) result: Primitive solvable permutation groups have bases of size $\leq 3$.
- We do not know of a general proof even with the relaxation $|P|/|\pi_i(P)| = o(n)$.  

Schemes Conjecture
We expect that the antisymmetry condition forces the subdegree to drop *rapidly* with $m$.

To formalize this, we call a color $P \in \mathcal{P}_s$, in a $m$-scheme, a **matching** if $|P|/|\pi_i(P)| = 1$ and $\pi_i(P) = \pi_j(P)$ for some $i \neq j$.

**Schemes Conjecture:** Every homogeneous, antisymmetric 4-scheme has a matching.

- We have proved this conjecture for the only such schemes we currently know: orbit schemes.
- ... using Seress (1996) result: Primitive solvable permutation groups have bases of size $\leq 3$.
- We do not know of a general proof even with the relaxation $|P|/|\pi_i(P)| = o(n)$.
Combinatorial Schemes

Conjecture

Schemes Conjecture

- We expect that the antisymmetry condition forces the subdegree to drop rapidly with $m$.
- To formalize this, we call a color $P \in P_s$, in a $m$-scheme, a matching if $|P|/|\pi_i(P)| = 1$ and $\pi_i(P) = \pi_j(P)$ for some $i \neq j$.
- Schemes Conjecture: Every homogeneous, antisymmetric 4-scheme has a matching.
  - We have proved this conjecture for the only such schemes we currently know: orbit schemes.
  - ... using Seress (1996) result: Primitive solvable permutation groups have bases of size $\leq 3$.
  - We do not know of a general proof even with the relaxation $|P|/|\pi_i(P)| = o(n)$.  


Schemes Conjecture

• We expect that the antisymmetry condition forces the subdegree to drop rapidly with $m$.

• To formalize this, we call a color $P \in \mathcal{P}_s$, in a $m$-scheme, a matching if $|P|/|\pi_i(P)| = 1$ and $\pi_i(P) = \pi_j(P)$ for some $i \neq j$.

• Schemes Conjecture: Every homogeneous, antisymmetric 4-scheme has a matching.

  • We have proved this conjecture for the only such schemes we currently know: orbit schemes.
  • ... using Seress (1996) result: Primitive solvable permutation groups have bases of size $\leq 3$.
  • We do not know of a general proof even with the relaxation $|P|/|\pi_i(P)| = o(n)$. 
**Schemes Conjecture**

- We expect that the antisymmetry condition forces the subdegree to drop *rapidly* with $m$.
- To formalize this, we call a color $P \in \mathcal{P}_s$, in a $m$-scheme, a **matching** if $|P|/|\pi_i(P)| = 1$ and $\pi_i(P) = \pi_j(P)$ for some $i \neq j$.
- **Schemes Conjecture**: Every homogeneous, antisymmetric 4-scheme has a matching.
  - We have proved this conjecture for the only such schemes we currently know: *orbit schemes*.
  - ... using Seress (1996) result: Primitive solvable permutation groups have bases of size $\leq 3$.
  - We do not know of a general proof even with the relaxation $|P|/|\pi_i(P)| = o(n)$.
We expect that the antisymmetry condition forces the subdegree to drop rapidly with $m$.

To formalize this, we call a color $P \in \mathcal{P}_s$, in a $m$-scheme, a matching if $|P|/|\pi_i(P)| = 1$ and $\pi_i(P) = \pi_j(P)$ for some $i \neq j$.

**Schemes Conjecture:** Every homogeneous, antisymmetric 4-scheme has a matching.

- We have proved this conjecture for the only such schemes we currently know: orbit schemes.
- ... using Seress (1996) result: Primitive solvable permutation groups have bases of size $\leq 3$.
- We do not know of a general proof even with the relaxation $|P|/|\pi_i(P)| = o(n)$. 
Schemes Conjecture

- We expect that the antisymmetry condition forces the subdegree to drop rapidly with $m$.

- To formalize this, we call a color $P \in \mathcal{P}_s$, in a $m$-scheme, a matching if $|P|/|\pi_i(P)| = 1$ and $\pi_i(P) = \pi_j(P)$ for some $i \neq j$.

- **Schemes Conjecture:** Every homogeneous, antisymmetric 4-scheme has a matching.
  - We have proved this conjecture for the only such schemes we currently know: orbit schemes.
  - ... using Seress (1996) result: Primitive solvable permutation groups have bases of size $\leq 3$.
  - We do not know of a general proof even with the relaxation $|P|/|\pi_i(P)| = o(n)$. 
Towards the Conjecture

- It is easy to see that the subdegree of certain colors gets halved at each level due to antisymmetricity. But the conjecture asks for much more!
- We have the following partial results:
  1. Every homogeneous, antisymmetric $m$-scheme on $[n]$ has a matching if $n$ is prime and $(n - 1)$ has a large $m$-smooth factor.
  2. Every homogeneous, antisymmetric $m$-scheme on $[n]$ has a matching if $m = \lceil \frac{2}{3} \log_2 n \rceil$.
- Result (2) follows by a matrix calculation.
Towards the Conjecture

- It is easy to see that the subdegree of certain colors gets \textit{halved} at each level due to antisymmetricity. But the conjecture asks for much more!
- We have the following partial results:
  1. Every homogeneous, antisymmetric \( m \)-scheme on \([n]\) has a matching if \( n \) is prime and \((n-1)\) has a \textit{large} \( m \)-smooth factor.
  2. Every homogeneous, antisymmetric \( m \)-scheme on \([n]\) has a matching if \( m = \lceil \frac{2}{3} \log_2 n \rceil \).
- Result (2) follows by a matrix calculation.
Towards the Conjecture

- It is easy to see that the subdegree of certain colors gets *halved* at each level due to antisymmetricity. But the conjecture asks for much more!

- We have the following partial results:
  1. Every homogeneous, antisymmetric \( m \)-scheme on \([n]\) has a matching if \( n \) is prime and \((n - 1)\) has a *large* \( m \)-smooth factor.
  2. Every homogeneous, antisymmetric \( m \)-scheme on \([n]\) has a matching if \( m = \lceil \frac{2}{3} \log_2 n \rceil \).


- Result (2) follows by a matrix calculation.
Towards the Conjecture

- It is easy to see that the subdegree of certain colors gets *halved* at each level due to antisymmetricity. But the conjecture asks for much more!
- We have the following partial results:
  1. Every homogeneous, antisymmetric $m$-scheme on $[n]$ has a matching if $n$ is prime and $(n-1)$ has a *large* $m$-smooth factor.
  2. Every homogeneous, antisymmetric $m$-scheme on $[n]$ has a matching if $m = \lceil \frac{2}{3} \log_2 n \rceil$.
- Result (2) follows by a matrix calculation.
Towards the Conjecture

- It is easy to see that the subdegree of certain colors gets *halved* at each level due to antisymmetricity. But the conjecture asks for much more!
- We have the following partial results:
  1. Every homogeneous, antisymmetric $m$-scheme on $[n]$ has a matching if $n$ is prime and $(n - 1)$ has a large $m$-smooth factor.
  2. Every homogeneous, antisymmetric $m$-scheme on $[n]$ has a matching if $m = \lceil \frac{2}{3} \log_2 n \rceil$.
- Result (2) follows by a matrix calculation.
Towards the Conjecture

- It is easy to see that the subdegree of certain colors gets *halved* at each level due to antisymmetricity. But the conjecture asks for much more!
- We have the following partial results:
  1. Every homogeneous, antisymmetric $m$-scheme on $[n]$ has a matching if $n$ is prime and $(n - 1)$ has a *large* $m$-smooth factor.
  2. Every homogeneous, antisymmetric $m$-scheme on $[n]$ has a matching if $m = \lceil \frac{2}{3} \log_2 n \rceil$.
- Result (2) follows by a matrix calculation.
OUTLINE

COMBINATORIAL SCHEMES
Definitions
Conjecture

POLYNOMIAL FACTORING
The Problem
GRH Connection

OUR ALGORITHM
Tensor Powers
Schemes
Polynomial Factoring

The Problem

**Polynomial Factoring over Finite Fields**

- Given a polynomial $f(x) \in \mathbb{F}_q[x]$ we want a nontrivial factor.
- It is not only a fundamental problem but also has practical applications: coding theory, integer factoring algorithms, computer algebra, ...
- Berlekamp (1967) showed that the problem reduces in deterministic polynomial time to the problem of: *factoring a degree* $n$ *polynomial with* $n$ *distinct roots in a prime field* $\mathbb{F}_p$. 
Polynomial Factoring

The Problem

Polynomial Factoring over Finite Fields

• Given a polynomial \( f(x) \in \mathbb{F}_q[x] \) we want a nontrivial factor.

• It is not only a fundamental problem but also has practical applications: coding theory, integer factoring algorithms, computer algebra, ...

• Berlekamp (1967) showed that the problem reduces in deterministic polynomial time to the problem of: factoring a degree \( n \) polynomial with \( n \) distinct roots in a prime field \( \mathbb{F}_p \).
Given a polynomial \( f(x) \in \mathbb{F}_q[x] \) we want a nontrivial factor.

It is not only a fundamental problem but also has practical applications: coding theory, integer factoring algorithms, computer algebra, ...

Berlekamp (1967) showed that the problem reduces in deterministic polynomial time to the problem of: factoring a degree \( n \) polynomial with \( n \) distinct roots in a prime field \( \mathbb{F}_p \).
**Polynomial Factoring Methods**

- Let \( f(x) \) be the input polynomial of degree \( n \) with distinct \( n \) roots in \( \mathbb{F}_p \).


- It is an open question to derandomize them.
Let $f(x)$ be the input polynomial of degree $n$ with distinct $n$ roots in $\mathbb{F}_p$.


It is an open question to derandomize them.
Polynomial Factoring Methods

- Let $f(x)$ be the input polynomial of degree $n$ with distinct $n$ roots in $\mathbb{F}_p$.
- It is an open question to derandomize them.
Outline

Combinatorial Schemes
Definitions
Conjecture

Polynomial Factoring
The Problem
GRH Connection

Our Algorithm
Tensor Powers
Schemes
Riemann Hypothesis & Polynomial Factoring

• Generalized Riemann Hypothesis (GRH) has been useful in understanding the deterministic complexity of polynomial factoring, albeit only in special cases.

• There are results based on GRH and combinatorial tricks, a degree $n$ polynomial $f(x)$ can be nontrivially factored in deterministic:
  - $\text{poly}(\log p, n^r)$ time if $r|n$ (Rónyai 1987);
  - $\text{poly}(\log p, n^{\log n})$ time (Evdokimov 1994).

• We greatly generalize the combinatorial object associated with these polynomial factoring algorithms

• ...and homogeneous, antisymmetric $m$-schemes appear naturally in the analysis.
Riemann Hypothesis & Polynomial Factoring

- Generalized Riemann Hypothesis (GRH) has been useful in understanding the deterministic complexity of polynomial factoring, albeit only in special cases.

- There are results based on GRH and combinatorial tricks, a degree $n$ polynomial $f(x)$ can be nontrivially factored in deterministic:
  - $\text{poly}(\log p, n^r)$ time if $r \mid n$ (Rónyai 1987);
  - $\text{poly}(\log p, n^{\log n})$ time (Evdokimov 1994).

- We greatly generalize the combinatorial object associated with these polynomial factoring algorithms.

- ...and homogeneous, antisymmetric $m$-schemes appear naturally in the analysis.
Generalized Riemann Hypothesis (GRH) has been useful in understanding the deterministic complexity of polynomial factoring, albeit only in special cases.

There are results based on GRH and combinatorial tricks, a degree $n$ polynomial $f(x)$ can be nontrivially factored in deterministic:

- $\text{poly}(\log p, n^r)$ time if $r | n$ (Rónyai 1987);
- $\text{poly}(\log p, n^{\log n})$ time (Evdokimov 1994).

We greatly generalize the combinatorial object associated with these polynomial factoring algorithms...

...and homogeneous, antisymmetric $m$-schemes appear naturally in the analysis.
• Generalized Riemann Hypothesis (GRH) has been useful in understanding the deterministic complexity of polynomial factoring, albeit only in special cases.
• There are results based on GRH and combinatorial tricks, a degree $n$ polynomial $f(x)$ can be nontrivially factored in deterministic:
  - $\text{poly}(\log p, n^r)$ time if $r | n$ (Rónyai 1987);
  - $\text{poly}(\log p, n^{\log n})$ time (Evdokimov 1994).
• We greatly generalize the combinatorial object associated with these polynomial factoring algorithms
  • ...and homogeneous, antisymmetric $m$-schemes appear naturally in the analysis.
Riemann Hypothesis & Polynomial Factoring

- Generalized Riemann Hypothesis (GRH) has been useful in understanding the deterministic complexity of polynomial factoring, albeit only in special cases.
- There are results based on GRH and combinatorial tricks, a degree $n$ polynomial $f(x)$ can be nontrivially factored in deterministic:
  - $\text{poly}(\log p, n^r)$ time if $r|n$ (Rónyai 1987);
  - $\text{poly}(\log p, n^{\log n})$ time (Evdokimov 1994).
- We greatly generalize the combinatorial object associated with these polynomial factoring algorithms
- ...and homogeneous, antisymmetric $m$-schemes appear naturally in the analysis.
OUTLINE

COMBINATORIAL SCHEMES
Definitions
Conjecture

POLYNOMIAL FACTORING
The Problem
GRH Connection

OUR ALGORITHM
Tensor Powers
Schemes
Let the input be $f(x) \in \mathbb{F}_p[x]$ of degree $n$ having distinct roots $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_p$.

We have a natural associated algebra $\mathcal{A} := k[X]/(f(X))$. $\mathcal{A}$ is isomorphic to $k^n$, the direct sum of $n$ copies of the algebra $k$.

$\mathcal{A} \otimes s$, for $s \in [m]$, is the $s$-th tensor power of $\mathcal{A}$. $\mathcal{A} \otimes s$ is isomorphic to $k^{ns}$.

**Lemma:** These tensor powers can be computed (in basis form over $k$) in deterministic $\text{poly}(\log p, n^m)$ time.
Let the input be $f(x) \in \mathbb{F}_p[x]$ of degree $n$ having distinct roots $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_p$.

We have a natural associated algebra $\mathcal{A} := k[X]/(f(X))$. $\mathcal{A}$ is isomorphic to $k^n$, the direct sum of $n$ copies of the algebra $k$.

$\mathcal{A} \otimes^s$, for $s \in [m]$, is the $s$-th tensor power of $\mathcal{A}$. $\mathcal{A} \otimes^s$ is isomorphic to $k^{ns}$.

Lemma: These tensor powers can be computed (in basis form over $k$) in deterministic $\text{poly}(\log p, n^m)$ time.
Tensor Powers

- Let the input be $f(x) \in \mathbb{F}_p[x]$ of degree $n$ having distinct roots $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_p$.
- We have a natural associated algebra $\mathcal{A} := k[X]/(f(X))$. $\mathcal{A}$ is isomorphic to $k^n$, the direct sum of $n$ copies of the algebra $k$.
- $\mathcal{A} \otimes^s$, for $s \in [m]$, is the $s$-th tensor power of $\mathcal{A}$. $\mathcal{A} \otimes^s$ is isomorphic to $k^{ns}$.
- Lemma: These tensor powers can be computed (in basis form over $k$) in deterministic $\text{poly}(\log p, n^m)$ time.
Let the input be \( f(x) \in \mathbb{F}_p[x] \) of degree \( n \) having distinct roots \( \alpha_1, \ldots, \alpha_n \in \mathbb{F}_p \).

We have a natural associated algebra \( \mathcal{A} := k[X]/(f(X)) \). \( \mathcal{A} \) is isomorphic to \( k^n \), the direct sum of \( n \) copies of the algebra \( k \).

\( \mathcal{A} \otimes_s \), for \( s \in [m] \), is the \( s \)-th tensor power of \( \mathcal{A} \). \( \mathcal{A} \otimes_s \) is isomorphic to \( k^{ns} \).

**Lemma:** These tensor powers can be computed (in basis form over \( k \)) in deterministic \( \text{poly}(\log p, n^m) \) time.
Let the input be \( f(x) \in \mathbb{F}_p[x] \) of degree \( n \) having distinct roots \( \alpha_1, \ldots, \alpha_n \in \mathbb{F}_p \).

We have a natural associated algebra \( \mathcal{A} := k[X]/(f(X)) \). \( \mathcal{A} \) is isomorphic to \( k^n \), the direct sum of \( n \) copies of the algebra \( k \).

\( \mathcal{A} \otimes_s \), for \( s \in [m] \), is the \( s \)-th tensor power of \( \mathcal{A} \). \( \mathcal{A} \otimes_s \) is isomorphic to \( k^{ns} \).

**Lemma:** These tensor powers can be computed (in basis form over \( k \)) in deterministic \( \text{poly}(\log p, n^m) \) time.
Let the input be $f(x) \in \mathbb{F}_p[x]$ of degree $n$ having distinct roots $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_p$.

We have a natural associated algebra $\mathcal{A} := k[X]/(f(X))$. $\mathcal{A}$ is isomorphic to $k^n$, the direct sum of $n$ copies of the algebra $k$.

$\mathcal{A} \otimes^s$, for $s \in [m]$, is the $s$-th tensor power of $\mathcal{A}$. $\mathcal{A} \otimes^s$ is isomorphic to $k^{ns}$.

**Lemma:** These tensor powers can be computed (in basis form over $k$) in deterministic $\text{poly}(\log p, n^m)$ time.
Our Algorithm

Tensor Powers

**Initiation & Refinements**

• Intend to decompose the tensor powers $A^\otimes s$, for all $s \in [m]$, into ideals.

• $\text{Aut}_k(A^\otimes s)$ contains $\text{Symm}_s$. For $\sigma \in \text{Symm}_s$ the corresponding algebra automorphism action is:

$$(b_{i_1} \otimes \cdots \otimes b_{i_s})^\sigma = b_{i_1\sigma} \otimes \cdots \otimes b_{i_s\sigma}.$$ 

• These nontrivial automorphisms of $A^\otimes s$ (when $s > 1$) help decompose these algebras under GRH (Rónyai 1992).

• Thus, we can compute mutually orthogonal ideals $I_{s,i}$ of $A^\otimes s$ s.t. $A^\otimes s = I_{s,1} + \cdots + I_{s,t_s}$.

• Next try out quite natural refinements to either get a factor of $f(x)$ or a stable ideal decomposition.
Our Algorithm

Tensor Powers

**Initiation & Refinements**

- Intend to decompose the tensor powers $A^\otimes s$, for all $s \in [m]$, into ideals.

- $Aut_k(A^\otimes s)$ contains $\text{Symm}_s$. For $\sigma \in \text{Symm}_s$ the corresponding algebra automorphism action is:
  $$(b_{i_1} \otimes \cdots \otimes b_{i_s})^\sigma = b_{i_1\sigma} \otimes \cdots \otimes b_{i_s\sigma}.$$  

- These nontrivial automorphisms of $A^\otimes s$ (when $s > 1$) help decompose these algebras under GRH (Rónyai 1992).

- Thus, we can compute mutually orthogonal ideals $I_{s,i}$ of $A^\otimes s$ s.t. $A^\otimes s = I_{s,1} + \cdots + I_{s,t_s}$.

- Next try out quite natural refinements to either get a factor of $f(x)$ or a stable ideal decomposition.
Initiation & Refinements

- Intend to decompose the tensor powers $A^\otimes s$, for all $s \in [m]$, into ideals.
- $\text{Aut}_k(A^\otimes s)$ contains $\text{Symm}_s$. For $\sigma \in \text{Symm}_s$ the corresponding algebra automorphism action is:
  $$(b_{i_1} \otimes \cdots \otimes b_{i_s})^\sigma = b_{i_1\sigma} \otimes \cdots \otimes b_{i_s\sigma}.$$  
- These nontrivial automorphisms of $A^\otimes s$ (when $s > 1$) help decompose these algebras under GRH (Rónyai 1992).
- Thus, we can compute mutually orthogonal ideals $I_{s,i}$ of $A^\otimes s$ s.t. $A^\otimes s = I_{s,1} + \cdots + I_{s,t_s}$.
- Next try out quite natural refinements to either get a factor of $f(x)$ or a stable ideal decomposition.
Initiation & Refinements

- Intend to decompose the tensor powers $A^\otimes s$, for all $s \in [m]$, into ideals.

- $\text{Aut}_k(A^\otimes s)$ contains $\text{Symm}_s$. For $\sigma \in \text{Symm}_s$ the corresponding algebra automorphism action is:

  $$(b_{i_1} \otimes \cdots \otimes b_{i_s})^\sigma = b_{i_1\sigma} \otimes \cdots \otimes b_{i_s\sigma}.$$ 

- These nontrivial automorphisms of $A^\otimes s$ (when $s > 1$) help decompose these algebras under GRH (Rónyai 1992).

- Thus, we can compute mutually orthogonal ideals $I_{s,i}$ of $A^\otimes s$ s.t. $A^\otimes s = I_{s,1} + \cdots + I_{s,t_s}$.

- Next try out quite natural refinements to either get a factor of $f(x)$ or a stable ideal decomposition.
Our Algorithm

## Tensor Powers

**Initiation & Refinements**

- Intend to decompose the tensor powers $A^\otimes s$, for all $s \in [m]$, into ideals.
- $\text{Aut}_k(A^\otimes s)$ contains $\text{Symm}_s$. For $\sigma \in \text{Symm}_s$ the corresponding algebra automorphism action is:
  
  $$(b_{i_1} \otimes \cdots \otimes b_{i_s})^\sigma = b_{i_1\sigma} \otimes \cdots \otimes b_{i_s\sigma}.$$  

- These nontrivial automorphisms of $A^\otimes s$ (when $s > 1$) help decompose these algebras under GRH (Rónyai 1992).
- Thus, we can compute mutually orthogonal ideals $I_{s,i}$ of $A^\otimes s$ s.t. $A^\otimes s = I_{s,1} + \cdots + I_{s,t_s}$.
- Next try out quite natural refinements to either get a factor of $f(x)$ or a stable ideal decomposition.
Intention & Refinements

- Intend to decompose the tensor powers $A^\otimes s$, for all $s \in [m]$, into ideals.

- $\text{Aut}_k(A^\otimes s)$ contains $\text{Symm}_s$. For $\sigma \in \text{Symm}_s$ the corresponding algebra automorphism action is:
  $$(b_{i_1} \otimes \cdots \otimes b_{i_s})^\sigma = b_{i_1\sigma} \otimes \cdots \otimes b_{i_s\sigma}.$$ 

- These nontrivial automorphisms of $A^\otimes s$ (when $s > 1$) help decompose these algebras under GRH (Rónyai 1992).

- Thus, we can compute mutually orthogonal ideals $I_{s,i}$ of $A^\otimes s$ s.t. $A^\otimes s = I_{s,1} + \cdots + I_{s,t_s}$.

- Next try out quite natural refinements to either get a factor of $f(x)$ or a stable ideal decomposition.
OUTLINE

COMBINATORIAL SCHEMES
   Definitions
   Conjecture

POLYNOMIAL FACTORING
   The Problem
   GRH Connection

OUR ALGORITHM
   Tensor Powers
   Schemes
Let the **stable** tensor power decomposition into orthogonal nonzero ideals be: \( A^{\otimes s} = l_{s,1} + \cdots + l_{s,t_s} \), for all \( s \in [m] \).

Let \( V := \{ \alpha_1, \ldots, \alpha_n \} \) be the roots of \( f(x) \).

**Lemma:** The ideal \( l_{s,i} \) implicitly defines a subset of \( V^{(s)} \):
\[
\text{Supp}(l_{s,i}) := \{ \bar{v} \in V^{(s)} \mid \exists a \in l_{s,i}, a(\bar{v}) \neq 0 \}
\]

Thus, a decomposition of \( A^{\otimes s} \) induces a partition \( P_s \) of \( V^{(s)} \). Each ideal corresponds to a color!

The refinements are such that these \( P_s \) comprise a homogeneous, antisymmetric \( m \)-scheme with **no** matching.

Truly stuck 😞
The underlying Scheme

- Let the stable tensor power decomposition into orthogonal nonzero ideals be: \( A^{\otimes s} = l_{s,1} + \cdots + l_{s,t_s} \), for all \( s \in [m] \).
- Let \( V := \{\alpha_1, \ldots, \alpha_n\} \) be the roots of \( f(x) \).
- **Lemma:** The ideal \( l_{s,i} \) implicitly defines a subset of \( V^{(s)} \):
  \[
  \text{Supp}(l_{s,i}) := \{ \bar{v} \in V^{(s)} \mid \exists a \in l_{s,i}, a(\bar{v}) \neq 0 \}
  \]
- Thus, a decomposition of \( A^{\otimes s} \) induces a partition \( P_s \) of \( V^{(s)} \). Each ideal corresponds to a color!
- The refinements are such that these \( P_s \) comprise a homogeneous, antisymmetric \( m \)-scheme with no matching.

Truly stuck 😞
The underlying Scheme

- Let the stable tensor power decomposition into orthogonal nonzero ideals be: \( A^{\otimes s} = l_{s,1} + \cdots + l_{s,t_s} \), for all \( s \in [m] \).
- Let \( V := \{ \alpha_1, \ldots, \alpha_n \} \) be the roots of \( f(x) \).
- Lemma: The ideal \( l_{s,i} \) implicitly defines a subset of \( V^{(s)} \):
  \[
  \text{Supp}(l_{s,i}) := \{ \bar{v} \in V^{(s)} \mid \exists a \in l_{s,i}, a(\bar{v}) \neq 0 \}
  \]
- Thus, a decomposition of \( A^{\otimes s} \) induces a partition \( \mathcal{P}_s \) of \( V^{(s)} \). Each ideal corresponds to a color!
- The refinements are such that these \( \mathcal{P}_s \) comprise a homogeneous, antisymmetric \( m \)-scheme with no matching.

Truly stuck 😞
The underlying Scheme

- Let the stable tensor power decomposition into orthogonal nonzero ideals be: \( A^{\otimes s} = l_{s,1} + \cdots + l_{s,t_s} \), for all \( s \in [m] \).
- Let \( V := \{ \alpha_1, \ldots, \alpha_n \} \) be the roots of \( f(x) \).
- **Lemma:** The ideal \( l_{s,i} \) implicitly defines a subset of \( V^{(s)} \):
  \[
  \text{Supp}(l_{s,i}) := \{ \vec{v} \in V^{(s)} | \exists a \in l_{s,i}, a(\vec{v}) \neq 0 \}
  \]
- Thus, a decomposition of \( A^{\otimes s} \) induces a partition \( \mathcal{P}_s \) of \( V^{(s)} \). Each ideal corresponds to a color!
- The refinements are such that these \( \mathcal{P}_s \) comprise a homogeneous, antisymmetric \( m \)-scheme with no matching.

Truly stuck 😞
Our Algorithm

Schemes

The underlying Scheme

- Let the stable tensor power decomposition into orthogonal nonzero ideals be: \( A \otimes^s = l_{s,1} + \cdots + l_{s,t_s} \), for all \( s \in [m] \).
- Let \( V := \{ \alpha_1, \ldots, \alpha_n \} \) be the roots of \( f(x) \).
- **Lemma:** The ideal \( l_{s,i} \) implicitly defines a subset of \( V^{(s)} \):
  \[
  \text{Supp}(l_{s,i}) := \{ \bar{v} \in V^{(s)} \mid \exists a \in l_{s,i}, a(\bar{v}) \neq 0 \}
  \]
- Thus, a decomposition of \( A \otimes^s \) induces a partition \( P_s \) of \( V^{(s)} \). Each ideal corresponds to a color!
- The refinements are such that these \( P_s \) comprise a homogeneous, antisymmetric \( m \)-scheme with no matching.

Truly stuck 😞
Our Algorithm

Schemes

The underlying Scheme

• Let the stable tensor power decomposition into orthogonal nonzero ideals be: $A^\otimes s = l_{s,1} + \cdots + l_{s,t^s}$, for all $s \in [m]$.  
• Let $V := \{\alpha_1, \ldots, \alpha_n\}$ be the roots of $f(x)$.  
• Lemma: The ideal $l_{s,i}$ implicitly defines a subset of $V^{(s)}$: 
  \[ \text{Supp}(l_{s,i}) := \{\tilde{v} \in V^{(s)} \mid \exists a \in l_{s,i}, a(\tilde{v}) \neq 0\} \]
• Thus, a decomposition of $A^\otimes s$ induces a partition $\mathcal{P}_s$ of $V^{(s)}$. Each ideal corresponds to a color!  
• The refinements are such that these $\mathcal{P}_s$ comprise a homogeneous, antisymmetric $m$-scheme with no matching.

Truly stuck 😞
The underlying Scheme

- Let the stable tensor power decomposition into orthogonal nonzero ideals be: \( A \otimes^s = l_{s,1} + \cdots + l_{s,t_s} \), for all \( s \in [m] \).
- Let \( V := \{ \alpha_1, \ldots, \alpha_n \} \) be the roots of \( f(x) \).
- **Lemma:** The ideal \( l_{s,i} \) implicitly defines a subset of \( V^{(s)} \): \( \text{Supp}(l_{s,i}) := \{ \bar{v} \in V^{(s)} | \exists a \in l_{s,i}, a(\bar{v}) \neq 0 \} \)
- Thus, a decomposition of \( A \otimes^s \) induces a partition \( P_s \) of \( V^{(s)} \). Each ideal corresponds to a color!
- The refinements are such that these \( P_s \) comprise a homogeneous, antisymmetric \( m \)-scheme with no matching.

Truly stuck 😞
Invoking the Conjecture

- If each homogeneous, antisymmetric $m$-scheme has a matching then the above algorithm leads to factoring $f(x)$.

- Thus, the conjecture implies a deterministic polynomial time factoring under GRH. (Assuming $m$ small.)

- Applying the recent algebraic-combinatorics machinery we get a partial result:

  $poly(\log p, n^m)$ time factoring under GRH if $n$ is prime and $(n - 1)$ has a large $m$-smooth factor.
Invoking the Conjecture

- If each homogeneous, antisymmetric \( m \)-scheme has a matching then the above algorithm leads to factoring \( f(x) \).
- Thus, the conjecture implies a deterministic polynomial time factoring under GRH. (Assuming \( m \) small.)
- Applying the recent algebraic-combinatorics machinery we get a partial result:
  \[ \text{poly}(\log p, n^m) \text{ time factoring under GRH if } n \text{ is prime and } (n - 1) \text{ has a large } m \text{-smooth factor.} \]
Invoking the Conjecture

- If each homogeneous, antisymmetric $m$-scheme has a matching then the above algorithm leads to factoring $f(x)$.
- Thus, the conjecture implies a deterministic polynomial time factoring under GRH. (Assuming $m$ small.)
- Applying the recent algebraic-combinatorics machinery we get a partial result:

$\text{poly}(\log p, n^m)$ time factoring under GRH if $n$ is prime and $(n - 1)$ has a large $m$-smooth factor.
Invoking the Conjecture

- If each homogeneous, antisymmetric \( m \)-scheme has a matching then the above algorithm leads to factoring \( f(x) \).
- Thus, the conjecture implies a deterministic polynomial time factoring under GRH. (Assuming \( m \) small.)
- Applying the recent algebraic-combinatorics machinery we get a partial result:
  
  \[
  \text{poly}(\log p, n^m) \text{ time factoring under GRH if } n \text{ is prime and } (n - 1) \text{ has a large } m\text{-smooth factor.}
  \]
CONCLUSION

• We introduced a natural class of partitions of \([n]^m\) with an algebraic feel!
• We showed how it appears naturally in polynomial factoring algorithms.
• We proposed the schemes conjecture that holds true in all the currently known homogeneous, antisymmetric 4-schemes.
• Other examples of homogeneous, antisymmetric 4-schemes?
• Further development of representation theory for 4-schemes?

Thanks!
CONCLUSION

• We introduced a natural class of partitions of $[n]^m$ with an algebraic feel!
• We showed how it appears naturally in polynomial factoring algorithms.
• We proposed the schemes conjecture that holds true in all the currently known homogeneous, antisymmetric 4-schemes.
• Other examples of homogeneous, antisymmetric 4-schemes?
• Further development of representation theory for 4-schemes?

Thanks!
CONCLUSION

- We introduced a natural class of partitions of \([n]^m\) with an algebraic feel!
- We showed how it appears naturally in polynomial factoring algorithms.
- We proposed the schemes conjecture that holds true in all the currently known homogeneous, antisymmetric 4-schemes.
- Other examples of homogeneous, antisymmetric 4-schemes?
- Further development of representation theory for 4-schemes?

Thanks!
CONCLUSION

- We introduced a natural class of partitions of \([n]^m\) with an algebraic feel!
- We showed how it appears naturally in polynomial factoring algorithms.
- We proposed the schemes conjecture that holds true in all the currently known homogeneous, antisymmetric 4-schemes.
- Other examples of homogeneous, antisymmetric 4-schemes?
- Further development of representation theory for 4-schemes?

Thanks!
CONCLUSION

- We introduced a natural class of partitions of $[n]^m$ with an algebraic feel!
- We showed how it appears naturally in polynomial factoring algorithms.
- We proposed the schemes conjecture that holds true in all the currently known homogeneous, antisymmetric 4-schemes.
- **Other examples** of homogeneous, antisymmetric 4-schemes?
- Further development of representation theory for 4-schemes?

Thanks!
CONCLUSION

• We introduced a natural class of partitions of $[n]^m$ with an algebraic feel!
• We showed how it appears naturally in polynomial factoring algorithms.
• We proposed the schemes conjecture that holds true in all the currently known homogeneous, antisymmetric 4-schemes.
• Other examples of homogeneous, antisymmetric 4-schemes?
• Further development of representation theory for 4-schemes?

Thanks!