Algebraic Relation of Three MinRank Algebraic Modelings

Who? Hao Guo[1] Jintai Ding[2,3]

From? [1]Tsinghua University

[2]Ding Lab
Yanqi Lake Beijing Institute of Mathematical Sciences and Applications

[3]Yau Mathematical Sciences Center
Tsinghua University

When? 4th PQC Standardization Conference

Algebraic Relation of Three MinRank Algebraic Modelings

Who? Hao Guo[1] Jintai Ding[2,3]

From? [1]Tsinghua University

[2]Ding Lab
Yanqi Lake Beijing Institute of Mathematical Sciences and Applications

[3]Yau Mathematical Sciences Center
Tsinghua University

When? 4th PQC Standardization Conference

Algebraic Relation of Three MinRank Algebraic Modelings

Who? Hao Guo[1] Jintai Ding[2,3]

From? [1]Tsinghua University

[2]Ding Lab
Yanqi Lake Beijing Institute of Mathematical Sciences and Applications

[3]Yau Mathematical Sciences Center
Tsinghua University

When? 4th PQC Standardization Conference

Algebraic Relation of Three MinRank Algebraic Modelings

Who? Hao Guo[1] Jintai Ding[2,3]

From? [1]Tsinghua University

[2]Ding Lab
Yanqi Lake Beijing Institute of Mathematical Sciences and Applications

[3]Yau Mathematical Sciences Center
Tsinghua University

When? 4th PQC Standardization Conference

Outline

Motivation

About MinRank Problem
Previous Work

Our Results/Contribution

Main Results
Cauchy–Binet Formula
Basic Ideas for Proofs

Definition

- Given a field K, matrices $M_1, \ldots, M_l \in K^{m \times n}$ over K, target rank r.
- Asks for a nonzero linear combination $M = \sum_{k=1}^{l} x_k M_k$ which has rank no more than r. Solves for $(x_1, \ldots, x_l)$.

Example Over $GF(2)$, given target rank $r = 2$, we have

$$1 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + 1 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

whose rank is 2. So $(1, 1)$ is a solution. (unique solution in this case)

Definition

- Given a field K, matrices $M_1, \ldots, M_l \in K^{m \times n}$ over K, target rank r.
- Asks for a nonzero linear combination $M = \sum_{k=1}^{l} x_k M_k$ which has rank no more than r. Solves for $(x_1, \ldots, x_l)$.

Example

Over $GF(2)$, given target rank $r = 2$, we have

$$1 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + 1 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

whose rank is 2. So $(1, 1)$ is a solution. (unique solution in this case)

Definition

- Given a field K, matrices $M_1, \ldots, M_l \in K^{m \times n}$ over K, target rank r.
- Asks for a nonzero linear combination $M = \sum_{k=1}^{l} x_k M_k$ which has rank no more than r. Solves for $(x_1, \ldots, x_l)$.

Example

Over $GF(2)$, given target rank $r = 2$, we have

$$1 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} + 1 \cdot \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

whose rank is 2. So $(1, 1)$ is a solution. (unique solution in this case)

History

- First introduced in Kipnis and Shamir's attack on HFE scheme
- Invoked attacks on Rainbow and ROLLO
- Buss proved NP-completeness for the case of finite field and singular matrix
- General complexity remains unknown, believed to be computationally hard

History

- First introduced in Kipnis and Shamir's attack on HFE scheme
- Invoked attacks on Rainbow and ROLLO
- Buss proved NP-completeness for the case of finite field and singular matrix
- General complexity remains unknown, believed to be computationally hard

History

- First introduced in Kipnis and Shamir's attack on HFE scheme
- Invoked attacks on Rainbow and ROLLO
- Buss proved NP-completeness for the case of finite field and singular matrix
- General complexity remains unknown, believed to be computationally hard

History

- First introduced in Kipnis and Shamir's attack on HFE scheme
- Invoked attacks on Rainbow and ROLLO
- Buss proved NP-completeness for the case of finite field and singular matrix
- General complexity remains unknown, believed to be computationally hard

Algebraic Modelings

- Minors modeling
- Kipnis–Shamir modeling
- Support minors modeling (new!)

Algebraic Modelings

- Minors modeling
- Kipnis–Shamir modeling
- Support minors modeling (new!)

Algebraic Modelings

- Minors modeling
- Kipnis–Shamir modeling
- Support minors modeling (new!)

Minors Modeling

- All $(r+1)$-minors of $M = \sum_{k=1}^{l} x_k M_k$ should be zero
- Totally $\binom{m}{r+1}\binom{n}{r+1}$ equations of degree $(r+1)$ with l unknowns

Example $M = \begin{bmatrix} x_1+x_2 & 0 & 0 \\ x_2 & x_1+x_2 & 0 \\ x_2 & x_2 & x_1+x_2 \end{bmatrix}$ over $GF(2)$, $r = 2$. We get

$$(x_1 + x_2)^3 = 0$$

Minors Modeling

- All $(r+1)$-minors of $M = \sum_{k=1}^{l} x_k M_k$ should be zero
- Totally $\binom{m}{r+1}\binom{n}{r+1}$ equations of degree $(r+1)$ with l unknowns

Example $M = \begin{bmatrix} x_1+x_2 & 0 & 0 \\ x_2 & x_1+x_2 & 0 \\ x_2 & x_2 & x_1+x_2 \end{bmatrix}$ over $GF(2)$, $r = 2$. We get

$$(x_1 + x_2)^3 = 0$$

Minors Modeling

- All $(r+1)$-minors of $M = \sum_{k=1}^{l} x_k M_k$ should be zero
- Totally $\binom{m}{r+1}\binom{n}{r+1}$ equations of degree $(r+1)$ with l unknowns

Example $M = \begin{bmatrix} x_1+x_2 & 0 & 0 \\ x_2 & x_1+x_2 & 0 \\ x_2 & x_2 & x_1+x_2 \end{bmatrix}$ over $GF(2)$, $r = 2$. We get

$$(x_1 + x_2)^3 = 0$$

Kipnis–Shamir Modeling

- Should exist a full rank n-by-$(n-r)$ matrix Y such that $MY = 0$
- Choose last $(n-r)$ rows of Y to form the identity matrix
- Totally $m(n-r)$ equations of degree 2 with $\left(l + r(n-r)\right)$ unknowns

Example

$M = \begin{bmatrix} x_1+x_2 & 0 & 0 \\ x_2 & x_1+x_2 & 0 \\ x_2 & x_2 & x_1+x_2 \end{bmatrix}$ over $GF(2)$, $r = 2$. We get $Y = \begin{bmatrix} -y_{1,1} \\ -y_{2,1} \\ 1 \end{bmatrix}$,

$$\begin{cases} -y_{1,1}(x_1 + x_2) = 0 \\ -y_{1,1}x_2 - y_{2,1}(x_1 + x_2) = 0 \\ -y_{1,1}x_2 - y_{2,1}x_2 + (x_1 + x_2) = 0 \end{cases}$$

Kipnis–Shamir Modeling

- Should exist a full rank n-by-$(n-r)$ matrix Y such that $MY = 0$
- Choose last $(n-r)$ rows of Y to form the identity matrix
- Totally $m(n-r)$ equations of degree 2 with $\left(l + r(n-r)\right)$ unknowns

Example

$M = \begin{bmatrix} x_1+x_2 & 0 & 0 \\ x_2 & x_1+x_2 & 0 \\ x_2 & x_2 & x_1+x_2 \end{bmatrix}$ over $GF(2)$, $r = 2$. We get $Y = \begin{bmatrix} -y_{1,1} \\ -y_{2,1} \\ 1 \end{bmatrix}$,

$$\begin{cases} -y_{1,1}(x_1 + x_2) = 0 \\ -y_{1,1}x_2 - y_{2,1}(x_1 + x_2) = 0 \\ -y_{1,1}x_2 - y_{2,1}x_2 + (x_1 + x_2) = 0 \end{cases}$$

Kipnis–Shamir Modeling

- Should exist a full rank n-by-$(n-r)$ matrix Y such that $MY = 0$
- Choose last $(n-r)$ rows of Y to form the identity matrix
- Totally $m(n-r)$ equations of degree 2 with $\left(l + r(n-r)\right)$ unknowns

Example $M = \begin{bmatrix} x_1+x_2 & 0 & 0 \\ x_2 & x_1+x_2 & 0 \\ x_2 & x_2 & x_1+x_2 \end{bmatrix}$ over $GF(2)$, $r = 2$. We get $Y = \begin{bmatrix} -y_{1,1} \\ -y_{2,1} \\ 1 \end{bmatrix}$,

$$\begin{cases} -y_{1,1}(x_1 + x_2) = 0 \\ -y_{1,1}x_2 - y_{2,1}(x_1 + x_2) = 0 \\ -y_{1,1}x_2 - y_{2,1}x_2 + (x_1 + x_2) = 0 \end{cases}$$

Kipnis–Shamir Modeling

- Should exist a full rank n-by-$(n-r)$ matrix Y such that $MY = 0$
- Choose last $(n-r)$ rows of Y to form the identity matrix
- Totally $m(n-r)$ equations of degree 2 with $\big(l + r(n-r)\big)$ unknowns

Example $M = \begin{bmatrix} x_1+x_2 & 0 & 0 \\ x_2 & x_1+x_2 & 0 \\ x_2 & x_2 & x_1+x_2 \end{bmatrix}$ over $GF(2)$, $r = 2$. We get $Y = \begin{bmatrix} -y_{1,1} \\ -y_{2,1} \\ 1 \end{bmatrix}$,

$$\begin{cases} -y_{1,1}(x_1 + x_2) = 0 \\ -y_{1,1}x_2 - y_{2,1}(x_1 + x_2) = 0 \\ -y_{1,1}x_2 - y_{2,1}x_2 + (x_1 + x_2) = 0 \end{cases}$$

Support Minors Modeling

- A rank r matrix M can be decomposed as $M = SC$ for a full rank r-by-n matrix C
- Augmenting C by each row of M gives a $(r+1)$-by-n matrix of rank r
- Cauculate all $(r+1)$-minors of each augmented matrix
- Use maximal minors of C as variables c_T
- Totally $m\binom{n}{r+1}$ equations of degree 2 with $l + \binom{n}{r}$ unknowns

Example $M = \begin{bmatrix} x_1+x_2 & 0 & 0 \\ x_2 & x_1+x_2 & 0 \\ x_2 & x_2 & x_1+x_2 \end{bmatrix}$ over $GF(2)$, $r = 2$. We get $C \in GF(2)^{2\times 3}$,

$$\begin{cases} (x_1+x_2)c_{\{2,3\}} = 0 \\ x_2 c_{\{2,3\}} - (x_1+x_2)c_{\{1,3\}} = 0 \\ x_2 c_{\{2,3\}} - x_2 c_{\{1,3\}} + (x_1+x_2)c_{\{1,2\}} = 0 \end{cases}$$

Support Minors Modeling

- A rank r matrix M can be decomposed as $M = SC$ for a full rank r-by-n matrix C
- Augmenting C by each row of M gives a $(r+1)$-by-n matrix of rank r
- Cauculate all $(r+1)$-minors of each augmented matrix
- Use maximal minors of C as variables c_T
- Totally $m\binom{n}{r+1}$ equations of degree 2 with $l + \binom{n}{r}$ unknowns

Example $M = \begin{bmatrix} x_1+x_2 & 0 & 0 \\ x_2 & x_1+x_2 & 0 \\ x_2 & x_2 & x_1+x_2 \end{bmatrix}$ over $GF(2)$, $r = 2$. We get $C \in GF(2)^{2\times 3}$,

$$\begin{cases} (x_1+x_2)c_{\{2,3\}} = 0 \\ x_2 c_{\{2,3\}} - (x_1+x_2)c_{\{1,3\}} = 0 \\ x_2 c_{\{2,3\}} - x_2 c_{\{1,3\}} + (x_1+x_2)c_{\{1,2\}} = 0 \end{cases}$$

Support Minors Modeling

- A rank r matrix M can be decomposed as $M = SC$ for a full rank r-by-n matrix C
- Augmenting C by each row of M gives a $(r+1)$-by-n matrix of rank r
- Cauculate all $(r+1)$-minors of each augmented matrix
- Use maximal minors of C as variables c_T
- Totally $m\binom{n}{r+1}$ equations of degree 2 with $l + \binom{n}{r}$ unknowns

Example $M = \begin{bmatrix} x_1+x_2 & 0 & 0 \\ x_2 & x_1+x_2 & 0 \\ x_2 & x_2 & x_1+x_2 \end{bmatrix}$ over $GF(2)$, $r = 2$. We get $C \in GF(2)^{2\times 3}$,

$$\begin{cases} (x_1+x_2)c_{\{2,3\}} = 0 \\ x_2 c_{\{2,3\}} - (x_1+x_2)c_{\{1,3\}} = 0 \\ x_2 c_{\{2,3\}} - x_2 c_{\{1,3\}} + (x_1+x_2)c_{\{1,2\}} = 0 \end{cases}$$

Support Minors Modeling

- A rank r matrix M can be decomposed as $M = SC$ for a full rank r-by-n matrix C
- Augmenting C by each row of M gives a $(r+1)$-by-n matrix of rank r
- Cauculate all $(r+1)$-minors of each augmented matrix
- Use maximal minors of C as variables c_T
- Totally $m\binom{n}{r+1}$ equations of degree 2 with $l + \binom{n}{r}$ unknowns

Example $M = \begin{bmatrix} x_1+x_2 & 0 & 0 \\ x_2 & x_1+x_2 & 0 \\ x_2 & x_2 & x_1+x_2 \end{bmatrix}$ over $GF(2)$, $r = 2$. We get $C \in GF(2)^{2\times 3}$,

$$\begin{cases} (x_1+x_2)c_{\{2,3\}} = 0 \\ x_2 c_{\{2,3\}} - (x_1+x_2)c_{\{1,3\}} = 0 \\ x_2 c_{\{2,3\}} - x_2 c_{\{1,3\}} + (x_1+x_2)c_{\{1,2\}} = 0 \end{cases}$$

Support Minors Modeling

- A rank r matrix M can be decomposed as $M = SC$ for a full rank r-by-n matrix C
- Augmenting C by each row of M gives a $(r+1)$-by-n matrix of rank r
- Cauculate all $(r+1)$-minors of each augmented matrix
- Use maximal minors of C as variables c_T
- Totally $m\binom{n}{r+1}$ equations of degree 2 with $I + \binom{n}{r}$ unknowns

Example $M = \begin{bmatrix} x_1+x_2 & 0 & 0 \\ x_2 & x_1+x_2 & 0 \\ x_2 & x_2 & x_1+x_2 \end{bmatrix}$ over $GF(2)$, $r = 2$. We get $C \in GF(2)^{2\times 3}$,

$$\begin{cases} (x_1+x_2)c_{\{2,3\}} = 0 \\ x_2 c_{\{2,3\}} - (x_1+x_2)c_{\{1,3\}} = 0 \\ x_2 c_{\{2,3\}} - x_2 c_{\{1,3\}} + (x_1+x_2)c_{\{1,2\}} = 0 \end{cases}$$

Support Minors Modeling

- A rank r matrix M can be decomposed as $M = SC$ for a full rank r-by-n matrix C
- Augmenting C by each row of M gives a $(r+1)$-by-n matrix of rank r
- Cauculate all $(r+1)$-minors of each augmented matrix
- Use maximal minors of C as variables c_T
- Totally $m\binom{n}{r+1}$ equations of degree 2 with $l + \binom{n}{r}$ unknowns

Example $M = \begin{bmatrix} x_1+x_2 & 0 & 0 \\ x_2 & x_1+x_2 & 0 \\ x_2 & x_2 & x_1+x_2 \end{bmatrix}$ over $GF(2)$, $r = 2$. We get $C \in GF(2)^{2\times 3}$,

$$\begin{cases} (x_1+x_2)c_{\{2,3\}} = 0 \\ x_2 c_{\{2,3\}} - (x_1+x_2)c_{\{1,3\}} = 0 \\ x_2 c_{\{2,3\}} - x_2 c_{\{1,3\}} + (x_1+x_2)c_{\{1,2\}} = 0 \end{cases}$$

Previous Work

- Bardet et al. showed that support minors modeling is more powerful than Kipnis–Shamir modeling.
  $\Longrightarrow$ Want to know whether support minors modeling makes more use of rank conditions or it just chooses the equations more cleverly.
- Faugére et al. used Nullstellensatz to give relation between minors modeling and Kipnis–Shamir modeling.
  $\Longrightarrow$ Not applicable for finite field!

Previous Work

- Bardet et al. showed that support minors modeling is more powerful than Kipnis–Shamir modeling.
  $\Longrightarrow$ Want to know whether support minors modeling makes more use of rank conditions or it just chooses the equations more cleverly.
- Faugére et al. used Nullstellensatz to give relation between minors modeling and Kipnis–Shamir modeling.
  $\Longrightarrow$ Not applicable for finite field!

Our Result

- We show the equivalence of Kipnis–Shamir modeling and support minors modeling, using determinant-like variable substitution and Cauchy–Binet formula.
- We also use Cauchy–Binet formula to give a constructive proof of relation between minors modeling and Kipnis–Shamir modeling, which is applicable to any field.

Similar work has also been done by Bardet and Bertin.

Our Result

- We show the equivalence of Kipnis–Shamir modeling and support minors modeling, using determinant-like variable substitution and Cauchy–Binet formula.
- We also use Cauchy–Binet formula to give a constructive proof of relation between minors modeling and Kipnis–Shamir modeling, which is applicable to any field.

  Similar work has also been done by Bardet and Bertin.

Cauchy–Binet Formula

We recover a conclusion from linear algebra:

Lemma *Let A be an m-by-n matrix and B an n-by-m matrix, where $m \leq n$. Then*

$$z^{n-m} \det(zI_m + AB) = \det(zI_n + BA)$$

where z is the indeterminate.

Consider the coefficient of z^{n-m} on both sides, we get

Theorem (Cauchy–Binet formula)

$$\det(AB) = \sum_{S \in \binom{[n]}{m}} \det((BA)_{S,S}) = \sum_{S \in \binom{[n]}{m}} \det((B)_{S,[m]}) \det((A)_{[m],S})$$

Cauchy–Binet Formula

We recover a conclusion from linear algebra:

Lemma *Let A be an m-by-n matrix and B an n-by-m matrix, where $m \leq n$. Then*

$$z^{n-m} \det(zI_m + AB) = \det(zI_n + BA)$$

where z is the indeterminate.

Consider the coefficient of z^{n-m} on both sides, we get

Theorem (Cauchy–Binet formula)

$$\det(AB) = \sum_{S \in \binom{[n]}{m}} \det((BA)_{S,S}) = \sum_{S \in \binom{[n]}{m}} \det((B)_{S,[m]}) \det((A)_{[m],S})$$

Cauchy–Binet Formula

A simple corollary of previous formula is

Corollary *Let A be an m-by-l matrix and B an l-by-n matrix, $k \leq \min(m, n)$, $\mathcal{I} \subset [m]$, $\mathcal{J} \subset [n]$, $|\mathcal{I}| = |\mathcal{J}| = k$, then*

$$\det((AB)_{\mathcal{I},\mathcal{J}}) = \sum_{S \in \binom{[l]}{k}} \det((A)_{\mathcal{I},S}) \det((B)_{S,\mathcal{J}})$$

Equivalence of KS modeling and SM modeling

We consider the substitution

$$C \mapsto C' = \begin{bmatrix} 1 & \cdots & 0 & y_{1,1} & \cdots & y_{1,n-r} \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & y_{r,1} & \cdots & y_{r,n-r} \end{bmatrix}$$

which induces substitution of c_T's to determinant-like polynomials in $y_{i,j}$'s.

Under this substitution, it suffices to show that

1. All the polynomials of Kipnis–Shamir modeling falls in some maximal minor of some augmented matrix, when replacing C by C'.
2. All the maximal minors of augmented matrices, when replacing C by C', falls in the ideal of polynomials of Kipnis–Shamir modeling.

Equivalence of KS modeling and SM modeling

We consider the substitution

$$C \mapsto C' = \begin{bmatrix} 1 & \cdots & 0 & y_{1,1} & \cdots & y_{1,n-r} \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & y_{r,1} & \cdots & y_{r,n-r} \end{bmatrix}$$

which induces substitution of c_T's to determinant-like polynomials in $y_{i,j}$'s.

Under this substitution, it suffices to show that

1. All the polynomials of Kipnis–Shamir modeling falls in some maximal minor of some augmented matrix, when replacing C by C'.
2. All the maximal minors of augmented matrices, when replacing C by C', falls in the ideal of polynomials of Kipnis–Shamir modeling.

Proof of Equivalence, First Part

The first part is easy: All the polynomials of Kipnis–Shamir modeling has the form

$$f_{i,j} := a_{i,r+j} - \sum_{k=1}^{r} a_{i,k} y_{k,j}$$

where $a_{i,j}$ represents the (i,j)-th element of M.
Calculating the maximal minor of $\begin{bmatrix} v_i \\ C' \end{bmatrix}$ with columns $([r] \cup \{r+j\}) \setminus \{i\}$ gives $(-1)^{r-i} f_{i,j}$, where v_i represents the i-th row of M.

Proof of Equivalence, Second Part

The second part uses Cauchy–Binet formula: we have

$$
\begin{aligned}
1 \cdot \det & \begin{bmatrix} a_{i,1} & \cdots & a_{i,r} & a_{i,r+1} & \cdots & a_{i,n} \\ 1 & \cdots & 0 & y_{1,1} & \cdots & y_{1,n-r} \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 1 & y_{r,1} & \cdots & y_{r,n-r} \end{bmatrix}_{[r+1],\mathcal{J}} \\
= \det & \left(\begin{bmatrix} 1 & -a_{i,1} & \cdots & -a_{i,r} \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} a_{i,1} & \cdots & a_{i,r} & a_{i,r+1} & \cdots & a_{i,n} \\ 1 & \cdots & 0 & y_{1,1} & \cdots & y_{1,n-r} \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 1 & y_{r,1} & \cdots & y_{r,n-r} \end{bmatrix} \right)_{[r+1],\mathcal{J}} \\
= \det & \begin{bmatrix} 0 & \cdots & 0 & f_{i,1} & \cdots & f_{i,n-r} \\ 1 & \cdots & 0 & y_{1,1} & \cdots & y_{1,n-r} \\ \vdots & \ddots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 1 & y_{r,1} & \cdots & y_{r,n-r} \end{bmatrix}_{[r+1],\mathcal{J}}
\end{aligned}
$$

So each maximal minor of $\begin{bmatrix} r_i \\ C' \end{bmatrix}$ falls in the ideal of $f_{i,j}$'s.

Example

For given example $M_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $M_2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$, SM modeling gives

$$\begin{cases} (x_1 + x_2)c_{\{2,3\}} = 0 \\ x_2 c_{\{2,3\}} - (x_1 + x_2)c_{\{1,3\}} = 0 \\ x_2 c_{\{2,3\}} - x_2 c_{\{1,3\}} + (x_1 + x_2)c_{\{1,2\}} = 0 \end{cases}$$

By plugging in $c_{\{1,2\}} \mapsto 1$, $c_{\{1,3\}} \mapsto y_{21}$, $c_{\{2,3\}} \mapsto -y_{11}$ we get

$$\begin{cases} -y_{11}(x_1 + x_2) = 0 \\ -y_{11}x_2 - y_{21}(x_1 + x_2) = 0 \\ (x_1 + x_2) - y_{11}x_2 - y_{21}x_2 = 0 \end{cases}$$

which are the equations from KS modeling.

Proof of Relation

Consider the matrix

$$M' = \begin{bmatrix} a_{1,1} & \cdots & a_{1,r} & f_{1,1} & \cdots & f_{1,n-r} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{m,1} & \cdots & a_{m,r} & f_{m,1} & \cdots & f_{m,n-r} \end{bmatrix}$$

Proof of Relation

M and M' are related by the matrix equation $M = M'R$, where

$$R = \begin{bmatrix} 1 & \cdots & 0 & y_{1,1} & \cdots & y_{1,n-r} \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & y_{r,1} & \cdots & y_{r,n-r} \\ 0 & \cdots & 0 & 1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 1 \end{bmatrix}$$

By Cauchy–Binet formula we have $|M|_{\mathcal{I},\mathcal{J}} = \sum_{S \in \binom{[n]}{m}} |M'|_{\mathcal{I},S} |R|_{S,\mathcal{J}}$.

From pigeonhole principle we know that $M'_{\mathcal{I},S}$ contains a column with entries $f_{i,j}$, so its determinant is in the ideal of $f_{i,j}$'s.

Therefore $|M|_{\mathcal{I},\mathcal{J}}$ also belongs to this ideal.

Example

For given example $M_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $M_2 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$, KS modeling gives

$$\begin{cases} f_{1,1} = -y_{1,1}(x_1 + x_2) = 0 \\ f_{2,1} = -y_{1,1}x_2 - y_{2,1}(x_1 + x_2) = 0 \\ f_{3,1} = (x_1 + x_2) - y_{1,1}x_2 - y_{2,1}x_2 = 0 \end{cases}$$

From matrix identity

$$\begin{bmatrix} x_1 + x_2 & 0 & 0 \\ x_2 & x_1 + x_2 & 0 \\ x_2 & x_2 & x_1 + x_2 \end{bmatrix} = \begin{bmatrix} x_1 + x_2 & 0 & f_{1,1} \\ x_2 & x_1 + x_2 & f_{2,1} \\ x_2 & x_2 & f_{3,1} \end{bmatrix} \begin{bmatrix} 1 & 0 & y_{1,1} \\ 0 & 1 & y_{2,1} \\ 0 & 0 & 1 \end{bmatrix}$$

by taking the determinant we get

$$(x_1 + x_2)^3 = -x_1x_2f_{1,1} - x_2(x_1 + x_2)f_{2,1} + (x_1 + x_2)^2 f_{3,1}$$

Summary

- The MinRank problem remains ad-hoc, with novel modelings appearing.
- We give algebraic relation of some modelings for solving the MinRank problem.

- Outlook
  - Learn more about implementation efficiency difference of these modelings.

Summary

- The MinRank problem remains ad-hoc, with novel modelings appearing.
- We give algebraic relation of some modelings for solving the MinRank problem.

- Outlook
  - Learn more about implementation efficiency difference of these modelings.

Summary

- The MinRank problem remains ad-hoc, with novel modelings appearing.
- We give algebraic relation of some modelings for solving the MinRank problem.

- Outlook
  - Learn more about implementation efficiency difference of these modelings.

Summary

- The MinRank problem remains ad-hoc, with novel modelings appearing.
- We give algebraic relation of some modelings for solving the MinRank problem.

- Outlook
  - Learn more about implementation efficiency difference of these modelings.