IMPERIAL

Association Schemes From Matrix Rings Over Finite Fields

Andrew Mendelsohn, Christian Porter
27/06/2025

Introduction

- The study of association schemes dates back to the work of Bose and Mesner [**BoseMesner59**], who introduced this object to further the study of designs in statistics.

Introduction

- The study of association schemes dates back to the work of Bose and Mesner [**BoseMesner59**], who introduced this object to further the study of designs in statistics.
- The notion was expanded by Higman [**Higman1970**], who introduced a generalisation known as coherent configurations, which relate to permutation groups.

Introduction

- The study of association schemes dates back to the work of Bose and Mesner [**BoseMesner59**], who introduced this object to further the study of designs in statistics.
- The notion was expanded by Higman [**Higman1970**], who introduced a generalisation known as coherent configurations, which relate to permutation groups.
- Delsarte [**Delsarte1973**] later connected association schemes to coding theory via the Hamming scheme, which takes as an underlying set vectors over a finite field and uses the rank of vectors to induce an association scheme structure on the set.
- The applications to coding theory have been greatly explored, such as by Sloane [**SLOANE1975**].

Introduction

- The study of association schemes dates back to the work of Bose and Mesner [**BoseMesner59**], who introduced this object to further the study of designs in statistics.
- The notion was expanded by Higman [**Higman1970**], who introduced a generalisation known as coherent configurations, which relate to permutation groups.
- Delsarte [**Delsarte1973**] later connected association schemes to coding theory via the Hamming scheme, which takes as an underlying set vectors over a finite field and uses the rank of vectors to induce an association scheme structure on the set.
- The applications to coding theory have been greatly explored, such as by Sloane [**SLOANE1975**].
- Similarly, it is known that one may consider matrices over finite fields and use the rank to induce a coherent configuration on the set of pairs of matrices: if the difference of two matrices has rank 0, place the pair into relation R_0; else place the pair into R_1. This is in fact an association scheme.

Introduction

- The study of association schemes dates back to the work of Bose and Mesner [**BoseMesner59**], who introduced this object to further the study of designs in statistics.
- The notion was expanded by Higman [**Higman1970**], who introduced a generalisation known as coherent configurations, which relate to permutation groups.
- Delsarte [**Delsarte1973**] later connected association schemes to coding theory via the Hamming scheme, which takes as an underlying set vectors over a finite field and uses the rank of vectors to induce an association scheme structure on the set.
- The applications to coding theory have been greatly explored, such as by Sloane [**SLOANE1975**].
- Similarly, it is known that one may consider matrices over finite fields and use the rank to induce a coherent configuration on the set of pairs of matrices: if the difference of two matrices has rank 0, place the pair into relation R_0; else place the pair into R_1. This is in fact an association scheme.
- We extend this notion using the determinant.

Overview

Coherent Configurations

A coherent configuration $\mathcal{C}$ is a set X with a set of binary operations $\mathcal{R}$ on X (i.e. relations on X^2) such that:

1. $\mathcal{R}$ is a partition of $X \times X$, that is, any ordered pair of points is in a unique relation R_i, $i \in I$.
2. There is a subset $H \subset I$ such that $\{R_h : h \in H\}$ partitions the diagonal $\{(x, x) : x \in X\}$.
3. For each R_i, its converse $\{(y, x) : (x, y) \in R_i\}$ is also one of the relations in $\mathcal{R}$, say $R_{i'}$.
4. For $i, j, k \in I$ and $(x, y) \in \mathcal{R}_k$, the number of $z \in X$ such that $(x, z) \in R_i$ and $(z, y) \in R_j$ is a constant ρ_{ij}^k, called the intersection number, that does not depend on the choice of x, y.

Association Schemes

Let $\mathcal{C}$ be a coherent configuration on X.

1. The sets F such that $\{(\alpha, \alpha) : \alpha \in F\}$ belong to $\mathcal{C}$ are called the fibres of P. We say that $\mathcal{C}$ is **homogeneous** if there is only one fibre.
2. The symmetrisation $\mathcal{C}^{sym}$ of $\mathcal{C}$ is the partition of X^2 whose parts are all unions of the parts of $\mathcal{C}$ and their converses. If $\mathcal{C}^{sym}$ is a coherent configuration, we say that $\mathcal{C}$ is **stratifiable**.
3. $\mathcal{C}$ is called **commutative** if its basis matrices commute with one another. In this case we have $\rho_{ij}^k = \rho_{ji}^k$.
4. $\mathcal{C}$ is called **symmetric** if all the relations are symmetric, that is, if each relation coincides with its converse, that is $R_{i'} = R_i$.

Association Schemes

Let $\mathcal{C}$ be a coherent configuration on X.

1. The sets F such that $\{(\alpha, \alpha) : \alpha \in F\}$ belong to $\mathcal{C}$ are called the fibres of P. We say that $\mathcal{C}$ is **homogeneous** if there is only one fibre.
2. The symmetrisation $\mathcal{C}^{sym}$ of $\mathcal{C}$ is the partition of X^2 whose parts are all unions of the parts of $\mathcal{C}$ and their converses. If $\mathcal{C}^{sym}$ is a coherent configuration, we say that $\mathcal{C}$ is **stratifiable**.
3. $\mathcal{C}$ is called **commutative** if its basis matrices commute with one another. In this case we have $\rho_{ij}^k = \rho_{ji}^k$.
4. $\mathcal{C}$ is called **symmetric** if all the relations are symmetric, that is, if each relation coincides with its converse, that is $R_{i'} = R_i$.

These properties are related as follows:

A symmetric coherent configuration is commutative; a commutative coherent configuration is stratifiable; and a stratifiable coherent configuration is homogeneous.

Association Schemes

Let $\mathcal{C}$ be a coherent configuration on X.

1. The sets F such that $\{(\alpha, \alpha) : \alpha \in F\}$ belong to $\mathcal{C}$ are called the fibres of P. We say that $\mathcal{C}$ is **homogeneous** if there is only one fibre.
2. The symmetrisation $\mathcal{C}^{sym}$ of $\mathcal{C}$ is the partition of X^2 whose parts are all unions of the parts of $\mathcal{C}$ and their converses. If $\mathcal{C}^{sym}$ is a coherent configuration, we say that $\mathcal{C}$ is **stratifiable**.
3. $\mathcal{C}$ is called **commutative** if its basis matrices commute with one another. In this case we have $\rho_{ij}^k = \rho_{ji}^k$.
4. $\mathcal{C}$ is called **symmetric** if all the relations are symmetric, that is, if each relation coincides with its converse, that is $R_{i'} = R_i$.

These properties are related as follows:

A symmetric coherent configuration is commutative; a commutative coherent configuration is stratifiable; and a stratifiable coherent configuration is homogeneous.

A symmetric coherent configuration is also known as an **association scheme**.

Motivating Example: Hamming Scheme

Let $X = \mathbb{F}_q^n$ and $\delta_H(x, y)$ denote the Hamming weight of $x - y$. For $i = 0, ..., n$, set

$$R_i = \{(x, y) \in X^2 : \delta_H(x, y) = i\}$$

Then $H_q^n = (X, \{R_i\}_i)$ is an association scheme.

Motivating Example: Hamming Scheme

Let $X = \mathbb{F}_q^n$ and $\delta_H(x, y)$ denote the Hamming weight of $x - y$. For $i = 0, ..., n$, set

$$R_i = \{(x, y) \in X^2 : \delta_H(x, y) = i\}$$

Then $H_q^n = (X, \{R_i\}_i)$ is an association scheme.

A **code** in an association scheme is a subset of X with relations inherited from the R_i.

Motivating Example: Hamming Scheme

Let $X = \mathbb{F}_q^n$ and $\delta_H(x, y)$ denote the Hamming weight of $x - y$. For $i = 0, ..., n$, set

$$R_i = \{(x, y) \in X^2 : \delta_H(x, y) = i\}$$

Then $H_q^n = (X, \{R_i\}_i)$ is an association scheme.

A **code** in an association scheme is a subset of X with relations inherited from the R_i.

"Block codes of length n over a q-ary alphabet" = "codes in the Hamming scheme H_q^n".

Motivating Example: Hamming Scheme

Let $X = \mathbb{F}_q^n$ and $\delta_H(x, y)$ denote the Hamming weight of $x - y$. For $i = 0, ..., n$, set

$$R_i = \{(x, y) \in X^2 : \delta_H(x, y) = i\}$$

Then $H_q^n = (X, \{R_i\}_i)$ is an association scheme.

A **code** in an association scheme is a subset of X with relations inherited from the R_i.

"Block codes of length n over a q-ary alphabet" = "codes in the Hamming scheme H_q^n".

Closed form solution for ρ_{ij}^k:

$$\rho_{i,j}^k = \sum_{\delta=0}^{\lfloor i+j-k/2 \rfloor} (q-2)^{i+j-k-2\delta} \binom{k}{j-\delta} \binom{j-\delta}{k-i+\delta} \binom{n-k}{(i+j-w)/2}$$

Motivating Example: Hamming Scheme

Let $X = \mathbb{F}_q^n$ and $\delta_H(x, y)$ denote the Hamming weight of $x - y$. For $i = 0, ..., n$, set

$$R_i = \{(x, y) \in X^2 : \delta_H(x, y) = i\}$$

Then $H_q^n = (X, \{R_i\}_i)$ is an association scheme.

A **code** in an association scheme is a subset of X with relations inherited from the R_i.

"Block codes of length n over a q-ary alphabet" = "codes in the Hamming scheme H_q^n".

Closed form solution for ρ_{ij}^k:

$$\rho_{i,j}^k = \sum_{\delta=0}^{\lfloor i+j-k/2 \rfloor} (q-2)^{i+j-k-2\delta} \binom{k}{j-\delta} \binom{j-\delta}{k-i+\delta} \binom{n-k}{(i+j-w)/2}$$

Codes in association schemes are useful because of the 'linear programming bound', which helps one to construct codes with desired minimum distance.

Linear Programming Bound

If $(X, \mathcal{R})$ is an association scheme and $Y \subset X$, the distribution vector of Y is the vector with i^{th} entry

$$a_i = \frac{|(Y \times Y) \cap R_i|}{|Y|}$$

Linear Programming Bound

If $(X, \mathcal{R})$ is an association scheme and $Y \subset X$, the distribution vector of Y is the vector with i^{th} entry

$$a_i = \frac{|(Y \times Y) \cap R_i|}{|Y|}$$

[**Roman92**] Let $\mathcal{A}$ be an association scheme with dual eigenmatrix Q, diameter d, and distribution vector $\mathbf{a} = (a_0, a_1, \ldots, a_d)$. Then any code C with minimum distance r in $\mathcal{A}$ satisfies

$$|C| \leq \max\left(\sum_{i=0}^{d} a_i\right)$$

where the maximum is taken over all $\{a_0, \ldots, a_d\}$ where the a_i satisfy
1. $a_0 = 1$, 2. $a_i = 0$ for $1 \leq i \leq r$, 3. $a_i \geq 0 \quad \forall \quad i$, and 4. $aQ \geq \mathbf{0}$

P- and Q-Polynomiality

Assume $\mathcal{A} = \{X, \mathcal{R}\}$ is an association scheme. For each i, $0 \leq i \leq d$, define the matrix A_i by

$$(A_i)_{u,v} = \begin{cases} 1 & (u,v) \in R_i \\ 0 & (u,v) \notin R_i \end{cases}$$

P- and Q-Polynomiality

Assume $\mathcal{A} = \{X, \mathcal{R}\}$ is an association scheme. For each i, $0 \leq i \leq d$, define the matrix A_i by

$$(A_i)_{u,v} = \begin{cases} 1 & (u,v) \in R_i \\ 0 & (u,v) \notin R_i \end{cases}$$

The A_i satisfy: 1. $A_0 = I$, 2. $\sum_{i=0}^{d} A_i = J$, 3. $A_j A_i = \sum_{h=0}^{d} p_{i,j}^h A_h$ 4. Linearly independence.

P- and Q-Polynomiality

Assume $\mathcal{A} = \{X, \mathcal{R}\}$ is an association scheme. For each i, $0 \leq i \leq d$, define the matrix A_i by

$$(A_i)_{u,v} = \begin{cases} 1 & (u,v) \in R_i \\ 0 & (u,v) \notin R_i \end{cases}$$

The A_i satisfy: 1. $A_0 = I$, 2. $\sum_{i=0}^{d} A_i = J$, 3. $A_j A_i = \sum_{h=0}^{d} p_{i,j}^h A_h$ 4. Linearly independence. The product of matrices in the span of the A_i is again in the span of the A_i, so $\{A_0, A_1, \ldots, A_d\}$ forms a basis for a commutative algebra $\mathcal{M}_{\mathcal{A}} \subseteq \mathrm{M}_{|X|}(\mathbb{C})$, the Bose-Mesner Algebra.

P- and Q-Polynomiality

Assume $\mathcal{A} = \{X, \mathcal{R}\}$ is an association scheme. For each i, $0 \leq i \leq d$, define the matrix A_i by

$$(A_i)_{u,v} = \begin{cases} 1 & (u,v) \in R_i \\ 0 & (u,v) \notin R_i \end{cases}$$

The A_i satisfy: 1. $A_0 = I$, 2. $\sum_{i=0}^{d} A_i = J$, 3. $A_j A_i = \sum_{h=0}^{d} p_{i,j}^h A_h$ 4. Linearly independence. The product of matrices in the span of the A_i is again in the span of the A_i, so $\{A_0, A_1, \ldots, A_d\}$ forms a basis for a commutative algebra $\mathcal{M}_{\mathcal{A}} \subseteq \mathrm{M}_{|X|}(\mathbb{C})$, the Bose-Mesner Algebra.
$\mathcal{M}_{\mathcal{A}}$ has a 2nd basis: a set of mutually-orthogonal primitive idempotents. Since the A_i are real and symmetric, they satisfy $A_i = \overline{A_i^t}$, so by spectral theory there exist symmetric $E_0, E_1, \ldots, E_d \in \mathcal{M}_{\mathcal{A}}$:
1. $E_i E_j = \begin{cases} 0 & i \neq j \\ E_i & i = j \end{cases}$, 2. $A = \sum_{i=0}^{d} \lambda_i E_i$, 3. $\sum_{i=0}^{d} E_i = I$, 4. $AE_i = \lambda_i E_i$,
and the λ_i are the $d+1$ distinct eigenvalues of A.

P- and Q-Polynomiality

Assume $\mathcal{A} = \{X, \mathcal{R}\}$ is an association scheme. For each i, $0 \leq i \leq d$, define the matrix A_i by

$$(A_i)_{u,v} = \begin{cases} 1 & (u,v) \in R_i \\ 0 & (u,v) \notin R_i \end{cases}$$

The A_i satisfy: 1. $A_0 = I$, 2. $\sum_{i=0}^{d} A_i = J$, 3. $A_j A_i = \sum_{h=0}^{d} p_{i,j}^h A_h$ 4. Linearity independence. The product of matrices in the span of the A_i is again in the span of the A_i, so $\{A_0, A_1, \ldots, A_d\}$ forms a basis for a commutative algebra $\mathcal{M}_\mathcal{A} \subseteq \mathrm{M}_{|X|}(\mathbb{C})$, the Bose-Mesner Algebra.
$\mathcal{M}_\mathcal{A}$ has a 2nd basis: a set of mutually-orthogonal primitive idempotents. Since the A_i are real and symmetric, they satisfy $A_i = \overline{A_i^t}$, so by spectral theory there exist symmetric $E_0, E_1, \ldots, E_d \in \mathcal{M}_\mathcal{A}$:
1. $E_i E_j = \begin{cases} 0 & i \neq j \\ E_i & i = j \end{cases}$, 2. $A = \sum_{i=0}^{d} \lambda_i E_i$, 3. $\sum_{i=0}^{d} E_i = I$, 4. $AE_i = \lambda_i E_i$,
and the λ_i are the $d+1$ distinct eigenvalues of A.The first and second eigenmatrices P and Q:

$$(A_0, A_1, \ldots, A_d) = (E_0, E_1, \ldots, E_d)\, P, \quad (E_0, E_1, \ldots, E_d) = |X|^{-1} (A_0, A_1, \ldots, A_d)\, Q$$

From these definitions, and the relations between the A_i and E_i, we have $PQ = |X|I$.

P- and Q-Polynomiality

Assume $\mathcal{A} = \{X, \mathcal{R}\}$ is an association scheme. For each i, $0 \leq i \leq d$, define the matrix A_i by

$$(A_i)_{u,v} = \begin{cases} 1 & (u,v) \in R_i \\ 0 & (u,v) \notin R_i \end{cases}$$

The A_i satisfy: 1. $A_0 = I$, 2. $\sum_{i=0}^{d} A_i = J$, 3. $A_j A_i = \sum_{h=0}^{d} p_{i,j}^h A_h$ 4. Linearly independence. The product of matrices in the span of the A_i is again in the span of the A_i, so $\{A_0, A_1, \ldots, A_d\}$ forms a basis for a commutative algebra $\mathcal{M}_\mathcal{A} \subseteq \mathrm{M}_{|X|}(\mathbb{C})$, the Bose-Mesner Algebra.
$\mathcal{M}_\mathcal{A}$ has a 2nd basis: a set of mutually-orthogonal primitive idempotents. Since the A_i are real and symmetric, they satisfy $A_i = \overline{A_i^t}$, so by spectral theory there exist symmetric $E_0, E_1, \ldots, E_d \in \mathcal{M}_\mathcal{A}$:
1. $E_i E_j = \begin{cases} 0 & i \neq j \\ E_i & i = j \end{cases}$, 2. $A = \sum_{i=0}^{d} \lambda_i E_i$, 3. $\sum_{i=0}^{d} E_i = I$, 4. $AE_i = \lambda_i E_i$,
and the λ_i are the $d+1$ distinct eigenvalues of A.The first and second eigenmatrices P and Q:

$$(A_0, A_1, \ldots, A_d) = (E_0, E_1, \ldots, E_d)\, P, \quad (E_0, E_1, \ldots, E_d) = |X|^{-1} (A_0, A_1, \ldots, A_d)\, Q$$

From these definitions, and the relations between the A_i and E_i, we have $PQ = |X|I$.
We say $\mathcal{A}$ is P-polynomial (Q-polynomial) if in $A_i = \sum_{k=0}^{n} p_i(k) E_k$ $(|X| E_k = \sum_{i=0}^{n} q_k(i) A_i)$ the $p_k(i)$ ($q_k(i)$) are real polynomials evaluated at real numbers.

Further Properties of Association Schemes

1. Let X be a finite Abelian group and (X, R) an association scheme. If (X, R) is $(X, +)$-invariant, i.e.

$$\text{if } (x, y) \in R_i, \text{ then } (x + z, y + z) \in R_i$$

for all $z \in X, i \in I$, then (X, R) is a **translation scheme** with respect to the group $(X, +)$.

Further Properties of Association Schemes

1. Let X be a finite Abelian group and (X, R) an association scheme. If (X, R) is $(X, +)$-invariant, i.e.

$$\text{if } (x, y) \in R_i, \text{ then } (x + z, y + z) \in R_i$$

   for all $z \in X, i \in I$, then (X, R) is a **translation scheme** with respect to the group $(X, +)$.
2. An association scheme $(X, \mathcal{R}')$ is a **fusion** of $(X, \mathcal{R})$ if every $R' \in \mathcal{S}$ is a union of R_i. An association scheme $(X, \mathcal{R})$ is **amorphic** if every fusion of $(X, \mathcal{R})$ is an association scheme.

Further Properties of Association Schemes

1. Let X be a finite Abelian group and (X, R) an association scheme. If (X, R) is $(X, +)$-invariant, i.e.

$$\text{if } (x, y) \in R_i, \text{ then } (x + z, y + z) \in R_i$$

   for all $z \in X, i \in I$, then (X, R) is a **translation scheme** with respect to the group $(X, +)$.
2. An association scheme $(X, \mathcal{R}')$ is a **fusion** of $(X, \mathcal{R})$ if every $R' \in \mathcal{S}$ is a union of R_i. An association scheme $(X, \mathcal{R})$ is **amorphic** if every fusion of $(X, \mathcal{R})$ is an association scheme.
3. An association scheme with fibre R_0 is P-**polynomial** if for all integers i, j, k $(0 \leq i, j, k \leq |I|)$, $p_{ij}^k = 0$ whenever one of i, j, k is greater than the sum of the other two.

Further Properties of Association Schemes

1. Let X be a finite Abelian group and (X, R) an association scheme. If (X, R) is $(X, +)$-invariant, i.e.

$$\text{if } (x, y) \in R_i, \text{ then } (x + z, y + z) \in R_i$$

   for all $z \in X, i \in I$, then (X, R) is a **translation scheme** with respect to the group $(X, +)$.
2. An association scheme $(X, \mathcal{R}')$ is a **fusion** of $(X, \mathcal{R})$ if every $R' \in \mathcal{S}$ is a union of R_i. An association scheme $(X, \mathcal{R})$ is **amorphic** if every fusion of $(X, \mathcal{R})$ is an association scheme.
3. An association scheme with fibre R_0 is P-**polynomial** if for all integers i, j, k $(0 \leq i, j, k \leq |I|)$, $p_{ij}^k = 0$ whenever one of i, j, k is greater than the sum of the other two.
4. A homogeneous coherent configuration is **thin** if all basis matrices have row and column sums equal to 1.

Further Properties of Association Schemes

1. Let X be a finite Abelian group and (X, R) an association scheme. If (X, R) is $(X, +)$-invariant, i.e.

$$\text{if } (x, y) \in R_i, \text{ then } (x + z, y + z) \in R_i$$

   for all $z \in X, i \in I$, then (X, R) is a **translation scheme** with respect to the group $(X, +)$.
2. An association scheme $(X, \mathcal{R}')$ is a **fusion** of $(X, \mathcal{R})$ if every $R' \in \mathcal{S}$ is a union of R_i. An association scheme $(X, \mathcal{R})$ is **amorphic** if every fusion of $(X, \mathcal{R})$ is an association scheme.
3. An association scheme with fibre R_0 is P-**polynomial** if for all integers i, j, k $(0 \leq i, j, k \leq |I|)$, $p_{ij}^k = 0$ whenever one of i, j, k is greater than the sum of the other two.
4. A homogeneous coherent configuration is **thin** if all basis matrices have row and column sums equal to 1.
5. If G is any permutation group on X, then the partition of X^2 into orbits of G is a coherent configuration, denoted by $K(G)$. A coherent configuration of the form $K(G)$ is called **Schurian**.

Further Properties of Association Schemes

1. Let X be a finite Abelian group and (X, R) an association scheme. If (X, R) is $(X, +)$-invariant, i.e.

$$\text{if } (x, y) \in R_i, \text{ then } (x + z, y + z) \in R_i$$

   for all $z \in X, i \in I$, then (X, R) is a **translation scheme** with respect to the group $(X, +)$.
2. An association scheme $(X, \mathcal{R}')$ is a **fusion** of $(X, \mathcal{R})$ if every $R' \in \mathcal{S}$ is a union of R_i. An association scheme $(X, \mathcal{R})$ is **amorphic** if every fusion of $(X, \mathcal{R})$ is an association scheme.
3. An association scheme with fibre R_0 is P-**polynomial** if for all integers i, j, k $(0 \leq i, j, k \leq |I|)$, $p_{ij}^k = 0$ whenever one of i, j, k is greater than the sum of the other two.
4. A homogeneous coherent configuration is **thin** if all basis matrices have row and column sums equal to 1.
5. If G is any permutation group on X, then the partition of X^2 into orbits of G is a coherent configuration, denoted by $K(G)$. A coherent configuration of the form $K(G)$ is called **Schurian**.

A thin homogeneous coherent configuration is Schurian.

Our Work: A Construction Via the Determinant

Theorem

Let $M_2(\mathbb{F}_q)$ denote the set of two-by-two matrices over a finite field. Define $q+1$ relations R_i on $M_2(\mathbb{F}_q) \times M_2(\mathbb{F}_q)$ as follows:

- If $i \in \{0, 1, ..., q-1\}$, then set

$$R_i = \{(A, B) : A \neq B, \text{ and } \det(A - B) = i\},$$

  and

- if $i = q$ then set $R_q = \{(A, B) : A = B\}$.

Then $(M_2(\mathbb{F}_q), \mathcal{R} = \{R_0, R_1, ..., R_q\})$ is a coherent configuration.

Our Work: A Construction Via the Determinant

Theorem

Let $M_2(\mathbb{F}_q)$ denote the set of two-by-two matrices over a finite field. Define $q+1$ relations R_i on $M_2(\mathbb{F}_q) \times M_2(\mathbb{F}_q)$ as follows:

- If $i \in \{0, 1, ..., q-1\}$, then set

$$R_i = \{(A, B) : A \neq B, \text{ and } \det(A - B) = i\},$$

  and

- if $i = q$ then set $R_q = \{(A, B) : A = B\}$.

Then $(M_2(\mathbb{F}_q), \mathcal{R} = \{R_0, R_1, ..., R_q\})$ is a coherent configuration.

We denote this coherent configuration by $\mathcal{C}(2, q)$.

Our Work: A Construction Via the Determinant

Theorem

Let $M_2(\mathbb{F}_q)$ denote the set of two-by-two matrices over a finite field. Define $q+1$ relations R_i on $M_2(\mathbb{F}_q) \times M_2(\mathbb{F}_q)$ as follows:

- If $i \in \{0, 1, ..., q-1\}$, then set

$$R_i = \{(A, B) : A \neq B, \text{ and } \det(A - B) = i\},$$

  and
- if $i = q$ then set $R_q = \{(A, B) : A = B\}$.

Then $(M_2(\mathbb{F}_q), \mathcal{R} = \{R_0, R_1, ..., R_q\})$ is a coherent configuration.

We denote this coherent configuration by $\mathcal{C}(2, q)$.

The first three properties of a coherent configuration can be seen to hold directly:
1 ($\mathcal{R}$ is a partition of X) holds as the difference of any two matrices has unique determinant,
2 (the diagonal is partitioned) since R_q is the required partition of the diagonal, and
3 (converse relations are relations) since flipping the order of elements of a pair is equivalent to multiplying the determinant by $(-1)^2$.
Finally, 4 holds by the following proof (sketch).

Proof of Property 4

The $\rho_{i,j}^k$ are constants independent of choice of $(x, y) \in R_k$, and:

- 1. $\rho_{i,j}^q = 0$ if $q \neq i \neq j \neq q$.
  2. $\rho_{i,j}^q = (q^2 - 1)q$ if $i = j \neq 0, q$.
  3. $\rho_{i,j}^q = (q^2 + q - 1)q - 1$ if $i = j = 0$.
- 1. $\rho_{i,j}^0 = q^2$ if $q \neq i \neq j \neq q$.
  2. $\rho_{i,j}^0 = q(q - 1)$ if $i = j \neq 0, q$.
  3. $\rho_{i,j}^0 = q(2q - 1)$ if $i = j = 0$.
- 1. $\rho_{i,q}^k = \begin{cases} 1 & \text{if } k = i, \text{ for any } i. \\ 0 & \text{else} \end{cases}$ (and similarly for $\rho_{q,j}^k$).
- For all $k \notin \{0, q\}$, we have $\rho_{i,j}^k = q(q + \epsilon_{i,j,k} - 1)$ where $x^2 - k^{-1}(i + k - j)x + k^{-1}i = 0$ has $\epsilon_{i,j,k}$ solutions mod q (not counting multiplicity) for all $i, j \neq q$.

Proof of Property 4

The $\rho_{i,j}^k$ are constants independent of choice of $(x, y) \in R_k$, and:

- 1. $\rho_{i,j}^q = 0$ if $q \neq i \neq j \neq q$.
  2. $\rho_{i,j}^q = (q^2 - 1)q$ if $i = j \neq 0, q$.
  3. $\rho_{i,j}^q = (q^2 + q - 1)q - 1$ if $i = j = 0$.
- 1. $\rho_{i,j}^0 = q^2$ if $q \neq i \neq j \neq q$.
  2. $\rho_{i,j}^0 = q(q - 1)$ if $i = j \neq 0, q$.
  3. $\rho_{i,j}^0 = q(2q - 1)$ if $i = j = 0$.
- 1. $\rho_{i,q}^k = \begin{cases} 1 & \text{if } k = i, \text{ for any } i. \\ 0 & \text{else} \end{cases}$ (and similarly for $\rho_{q,j}^k$).
- For all $k \notin \{0, q\}$, we have $\rho_{i,j}^k = q(q + \epsilon_{i,j,k} - 1)$ where $x^2 - k^{-1}(i + k - j)x + k^{-1}i = 0$ has $\epsilon_{i,j,k}$ solutions mod q (not counting multiplicity) for all $i, j \neq q$.

Proof.

$\rho_{i,q}^k$: This is the quantity

$$|\{z \in M_n(\mathbb{F}_q) : \det(x - z) = i \text{ and } z = y\}|$$

for some $(x, y) \in R_k$. Since (x, y) is fixed, $i = \det(x - z) = \det(x - y)$ which is not fulfilled if $(x, y) \notin R_i$, and which yields a set of size one if $(x, y) \in R_i$, comprising the singleton set $\{y\}$.

Proof of Property 4

Set $\rho_{i,j}(a,b) = |\{z \in M_2(\mathbb{F}_q) : \det(a-z) = i, \det(z-b) = j\}|$, for $(a,b) \in R_k$ and

$$\rho_{i,j}(c) = |\{z \in M_2(\mathbb{F}_q) : \det(z) = i, \det(z-c) = j\}|.$$

Then $\rho_{i,j}(a,b) = \rho_{i,j}(c)$ for any $(a,b) \in R_k$ with $c = a - b$. Let $z_{ij}, c_i \in \mathbb{F}_q$ and write

$$z = \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix}, c = \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix}$$

Proof of Property 4

Set $\rho_{i,j}(a,b) = |\{z \in M_2(\mathbb{F}_q) : \det(a-z) = i, \det(z-b) = j\}|$, for $(a,b) \in R_k$ and

$$\rho_{i,j}(c) = |\{z \in M_2(\mathbb{F}_q) : \det(z) = i, \det(z-c) = j\}|.$$

Then $\rho_{i,j}(a,b) = \rho_{i,j}(c)$ for any $(a,b) \in R_k$ with $c = a - b$. Let $z_{ij}, c_i \in \mathbb{F}_q$ and write

$$z = \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix}, c = \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix}$$

$\rho^q_{i,j}$: this corresponds to the case of $c = 0$.
If $i \neq j$, then $\rho^q_{ij} = 0$.

Proof of Property 4

Set $\rho_{i,j}(a,b) = |\{z \in M_2(\mathbb{F}_q) : \det(a-z) = i, \det(z-b) = j\}|$, for $(a,b) \in R_k$ and

$$\rho_{i,j}(c) = |\{z \in M_2(\mathbb{F}_q) : \det(z) = i, \det(z-c) = j\}|.$$

Then $\rho_{i,j}(a,b) = \rho_{i,j}(c)$ for any $(a,b) \in R_k$ with $c = a - b$. Let $z_{ij}, c_i \in \mathbb{F}_q$ and write

$$z = \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix}, c = \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix}$$

$\rho^q_{i,j}$: this corresponds to the case of $c = 0$.
If $i \neq j$, then $\rho^q_{ij} = 0$.
Let $i = j \neq 0$. Note that z_{11}, z_{21} may be freely chosen satisfying $(z_{11}, z_{21}) \neq (0,0)$. Then $z_{11}z_{22} - z_{12}z_{21} = i$, so there are q choices for z_{22}, and the variable z_{21} is entirely dependent on z_{22}.
Therefore $\rho^q_{ii} = (q^2 - 1)q$ when $i \neq 0$.

Proof of Property 4

Set $\rho_{i,j}(a,b) = |\{z \in M_2(\mathbb{F}_q) : \det(a-z) = i, \det(z-b) = j\}|$, for $(a,b) \in R_k$ and

$$\rho_{i,j}(c) = |\{z \in M_2(\mathbb{F}_q) : \det(z) = i, \det(z-c) = j\}|.$$

Then $\rho_{i,j}(a,b) = \rho_{i,j}(c)$ for any $(a,b) \in R_k$ with $c = a - b$. Let $z_{ij}, c_i \in \mathbb{F}_q$ and write

$$z = \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix}, c = \begin{bmatrix} c_1 & c_2 \\ c_3 & c_4 \end{bmatrix}$$

$\rho^q_{i,j}$: this corresponds to the case of $c = 0$.
If $i \neq j$, then $\rho^q_{ij} = 0$.
Let $i = j \neq 0$. Note that z_{11}, z_{21} may be freely chosen satisfying $(z_{11}, z_{21}) \neq (0,0)$. Then $z_{11}z_{22} - z_{12}z_{21} = i$, so there are q choices for z_{22}, and the variable z_{21} is entirely dependent on z_{22}.
Therefore $\rho^q_{ii} = (q^2-1)q$ when $i \neq 0$.
When $i = 0$, since there are q^4 total matrices in $M_2(\mathbb{F}_q)$, we have $\rho^k_{00} = q^4 - (q-1)(q^2-1)q$.

Proof of Property 4

$\rho^0_{i,j}$: this corresponds to $c \neq 0$ with $\det(c) = 0$.
Since $c \neq 0$, assume $c_1 \neq 0$ wlog. Since $\det(c) = 0$ there exists $\alpha \in \mathbb{F}_q$ such that $c_3 = \alpha c_1, c_4 = \alpha c_2$.

Proof of Property 4

$\rho^0_{i,j}$: this corresponds to $c \neq 0$ with $\det(c) = 0$.
Since $c \neq 0$, assume $c_1 \neq 0$ wlog. Since $\det(c) = 0$ there exists $\alpha \in \mathbb{F}_q$ such that $c_3 = \alpha c_1, c_4 = \alpha c_2$.
If $i = j = 0$, then that for any matrix $M \in M_2(\mathbb{F}_q)$ with $\det(M) = 1$, we have $\rho_{i,j}(c) = \rho_{i,j}(Mc)$.
Consider the choice for matrix M and its action on c,

$$M = \begin{bmatrix} 1-\alpha & 1 \\ -\alpha & 1 \end{bmatrix}, \quad Mc = \begin{bmatrix} c_1 & c_2 \\ 0 & 0 \end{bmatrix}$$

So we can assume that $\alpha = 0$ wlog. Then the conditions $\det(z) = \det(z - c) = 0$ imply that

$$z_{11}z_{22} = z_{12}z_{21}, \tag{1}$$
$$(z_{11} - c_1)z_{22} - (z_{12} - c_2)z_{21} = 0 \tag{2}$$

Proof of Property 4

$\rho^0_{i,j}$: this corresponds to $c \neq 0$ with $\det(c) = 0$.
Since $c \neq 0$, assume $c_1 \neq 0$ wlog. Since $\det(c) = 0$ there exists $\alpha \in \mathbb{F}_q$ such that $c_3 = \alpha c_1, c_4 = \alpha c_2$.
If $i = j = 0$, then that for any matrix $M \in M_2(\mathbb{F}_q)$ with $\det(M) = 1$, we have $\rho_{i,j}(c) = \rho_{i,j}(Mc)$.
Consider the choice for matrix M and its action on c,

$$M = \begin{bmatrix} 1-\alpha & 1 \\ -\alpha & 1 \end{bmatrix}, \quad Mc = \begin{bmatrix} c_1 & c_2 \\ 0 & 0 \end{bmatrix}$$

So we can assume that $\alpha = 0$ wlog. Then the conditions $\det(z) = \det(z - c) = 0$ imply that

$$z_{11}z_{22} = z_{12}z_{21}, \tag{1}$$
$$(z_{11} - c_1)z_{22} - (z_{12} - c_2)z_{21} = 0 \tag{2}$$

Equation (2) and substituting back into (1) implies that

$$-c_1 z_{22} + c_2 z_{21} = 0 \iff z_{22} = c_1^{-1} c_2 z_{21} \iff c_1 c_2^{-1} z_{11} z_{21} = z_{12} z_{21}$$

Proof of Property 4

$\rho^0_{i,j}$: this corresponds to $c \neq 0$ with $\det(c) = 0$.
Since $c \neq 0$, assume $c_1 \neq 0$ wlog. Since $\det(c) = 0$ there exists $\alpha \in \mathbb{F}_q$ such that $c_3 = \alpha c_1, c_4 = \alpha c_2$.
If $i = j = 0$, then that for any matrix $M \in M_2(\mathbb{F}_q)$ with $\det(M) = 1$, we have $\rho_{i,j}(c) = \rho_{i,j}(Mc)$.
Consider the choice for matrix M and its action on c,

$$M = \begin{bmatrix} 1-\alpha & 1 \\ -\alpha & 1 \end{bmatrix}, \quad Mc = \begin{bmatrix} c_1 & c_2 \\ 0 & 0 \end{bmatrix}$$

So we can assume that $\alpha = 0$ wlog. Then the conditions $\det(z) = \det(z - c) = 0$ imply that

$$z_{11}z_{22} = z_{12}z_{21}, \tag{1}$$
$$(z_{11} - c_1)z_{22} - (z_{12} - c_2)z_{21} = 0 \tag{2}$$

Equation (2) and substituting back into (1) implies that

$$-c_1 z_{22} + c_2 z_{21} = 0 \iff z_{22} = c_1^{-1} c_2 z_{21} \iff c_1 c_2^{-1} z_{11} z_{21} = z_{12} z_{21}$$

Therefore, z can take the following forms:

$$\begin{bmatrix} z_{11} & z_{12} \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} z_{11} & c_1^{-1}c_2 z_{11} \\ z_{21} & c_1^{-1}c_2 z_{21} \end{bmatrix}, z_{21} \neq 0.$$

Proof of Property 4

$\rho^0_{i,j}$: this corresponds to $c \neq 0$ with $\det(c) = 0$.
Since $c \neq 0$, assume $c_1 \neq 0$ wlog. Since $\det(c) = 0$ there exists $\alpha \in \mathbb{F}_q$ such that $c_3 = \alpha c_1, c_4 = \alpha c_2$.
If $i = j = 0$, then that for any matrix $M \in M_2(\mathbb{F}_q)$ with $\det(M) = 1$, we have $\rho_{i,j}(c) = \rho_{i,j}(Mc)$.
Consider the choice for matrix M and its action on c,

$$M = \begin{bmatrix} 1-\alpha & 1 \\ -\alpha & 1 \end{bmatrix}, \quad Mc = \begin{bmatrix} c_1 & c_2 \\ 0 & 0 \end{bmatrix}$$

So we can assume that $\alpha = 0$ wlog. Then the conditions $\det(z) = \det(z - c) = 0$ imply that

$$z_{11}z_{22} = z_{12}z_{21}, \tag{1}$$
$$(z_{11} - c_1)z_{22} - (z_{12} - c_2)z_{21} = 0 \tag{2}$$

Equation (2) and substituting back into (1) implies that

$$-c_1 z_{22} + c_2 z_{21} = 0 \iff z_{22} = c_1^{-1} c_2 z_{21} \iff c_1 c_2^{-1} z_{11} z_{21} = z_{12} z_{21}$$

Therefore, z can take the following forms:

$$\begin{bmatrix} z_{11} & z_{12} \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} z_{11} & c_1^{-1}c_2 z_{11} \\ z_{21} & c_1^{-1}c_2 z_{21} \end{bmatrix}, z_{21} \neq 0.$$

In total, there are $q^2 + q(q-1) = q(2q-1)$ matrices for z, regardless of choice of c.

Proof of Property 4

Next, if $i = j \neq 0$, then

$$z_{11}z_{22} = i + z_{12}z_{21}, \tag{3}$$

$$-c_1 z_{22} - \alpha c_2 z_{11} + c_2 z_{21} + \alpha c_1 z_{12} = 0. \tag{4}$$

Proof of Property 4

Next, if $i = j \neq 0$, then

$$z_{11}z_{22} = i + z_{12}z_{21}, \tag{3}$$
$$-c_1 z_{22} - \alpha c_2 z_{11} + c_2 z_{21} + \alpha c_1 z_{12} = 0. \tag{4}$$

Now (4) gives

$$c_2(z_{21} - \alpha z_{11}) = c_1(z_{22} - \alpha z_{12}) \iff z_{22} = \alpha z_{12} + c_1^{-1}c_2(z_{21} - \alpha z_{11}),$$

which substituting into (3) implies that

$$z_{11}(\alpha z_{12} + c_1^{-1}c_2(z_{21} - \alpha z_{11})) = z_{12}z_{21} \iff (\alpha z_{11} - z_{21})(c_1^{-1}c_2 z_{11} - z_{12}) = -i.$$

Proof of Property 4

Next, if $i = j \neq 0$, then

$$z_{11}z_{22} = i + z_{12}z_{21}, \tag{3}$$
$$-c_1 z_{22} - \alpha c_2 z_{11} + c_2 z_{21} + \alpha c_1 z_{12} = 0. \tag{4}$$

Now (4) gives

$$c_2(z_{21} - \alpha z_{11}) = c_1(z_{22} - \alpha z_{12}) \iff z_{22} = \alpha z_{12} + c_1^{-1}c_2(z_{21} - \alpha z_{11}),$$

which substituting into (3) implies that

$$z_{11}(\alpha z_{12} + c_1^{-1}c_2(z_{21} - \alpha z_{11})) = z_{12}z_{21} \iff (\alpha z_{11} - z_{21})(c_1^{-1}c_2 z_{11} - z_{12}) = -i.$$

Since i is nonzero, $\alpha z_{11} - z_{21}, c_1^{-1}c_2 z_{11} - z_{12} \neq 0$. Therefore, z must be of the following form:

$$\begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix}, \quad \text{where} \quad \begin{aligned} z_{22} &= \alpha z_{12} + c_1^{-1}c_2(z_{21} - \alpha z_{11}), \\ z_{21} &= \alpha z_{11} + i(c_1^{-1}c_2 z_{11} - z_{12})^{-1}, \end{aligned}$$

subject to $c_1^{-1}c_2 z_{11} - z_{12} \neq 0$.

Proof of Property 4

Next, if $i = j \neq 0$, then

$$z_{11}z_{22} = i + z_{12}z_{21}, \tag{3}$$
$$-c_1 z_{22} - \alpha c_2 z_{11} + c_2 z_{21} + \alpha c_1 z_{12} = 0. \tag{4}$$

Now (4) gives

$$c_2(z_{21} - \alpha z_{11}) = c_1(z_{22} - \alpha z_{12}) \iff z_{22} = \alpha z_{12} + c_1^{-1}c_2(z_{21} - \alpha z_{11}),$$

which substituting into (3) implies that

$$z_{11}(\alpha z_{12} + c_1^{-1}c_2(z_{21} - \alpha z_{11})) = z_{12}z_{21} \iff (\alpha z_{11} - z_{21})(c_1^{-1}c_2 z_{11} - z_{12}) = -i.$$

Since i is nonzero, $\alpha z_{11} - z_{21}, c_1^{-1}c_2 z_{11} - z_{12} \neq 0$. Therefore, z must be of the following form:

$$\begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix}, \quad \text{where} \quad \begin{aligned} z_{22} &= \alpha z_{12} + c_1^{-1}c_2(z_{21} - \alpha z_{11}), \\ z_{21} &= \alpha z_{11} + i(c_1^{-1}c_2 z_{11} - z_{12})^{-1}, \end{aligned}$$

subject to $c_1^{-1}c_2 z_{11} - z_{12} \neq 0$. There are $q(q-1)$ such matrices, regardless of the choice of c (q choices for z_{11}, and $q-1$ for z_{12} for each z_{11}).

Proof of Property 4

If $i \neq j$, consider the matrix M with $\det(M) = 1$ and its action on c,

$$M = \begin{bmatrix} 1-\alpha & 1 \\ -\alpha & 1 \end{bmatrix}, \quad Mc = \begin{bmatrix} c_1 & c_2 \\ 0 & 0 \end{bmatrix}.$$

Therefore, we can assume that c has the above form wlog. Then

$$z_{11}z_{22} = i + z_{12}z_{21}, \tag{5}$$

$$-c_1 z_{22} + c_2 z_{21} = j - i \tag{6}$$

Proof of Property 4

If $i \neq j$, consider the matrix M with $\det(M) = 1$ and its action on c,

$$M = \begin{bmatrix} 1-\alpha & 1 \\ -\alpha & 1 \end{bmatrix}, \quad Mc = \begin{bmatrix} c_1 & c_2 \\ 0 & 0 \end{bmatrix}.$$

Therefore, we can assume that c has the above form wlog. Then

$$z_{11}z_{22} = i + z_{12}z_{21}, \tag{5}$$

$$-c_1 z_{22} + c_2 z_{21} = j - i \tag{6}$$

Now (6) and substituting into (5) gives

$$z_{22} = c_1^{-1}(c_2 z_{21} - (j-i)) \iff z_{11}(c_1^{-1}(c_2 z_{21} - (j-i))) = i + z_{12}z_{21}$$

We then have the cases $\begin{cases} z_{11} = -c_1(j-i)^{-1}i, & \text{if } z_{21} = 0 \\ z_{12} = z_{21}^{-1}(z_{11}(c_1^{-1}(c_2 z_{21} - (j-i))) - i), & \text{otherwise} \end{cases}$

Proof of Property 4

If $i \neq j$, consider the matrix M with $\det(M) = 1$ and its action on c,

$$M = \begin{bmatrix} 1-\alpha & 1 \\ -\alpha & 1 \end{bmatrix}, \quad Mc = \begin{bmatrix} c_1 & c_2 \\ 0 & 0 \end{bmatrix}.$$

Therefore, we can assume that c has the above form wlog. Then

$$z_{11}z_{22} = i + z_{12}z_{21}, \tag{5}$$

$$-c_1 z_{22} + c_2 z_{21} = j - i \tag{6}$$

Now (6) and substituting into (5) gives

$$z_{22} = c_1^{-1}(c_2 z_{21} - (j-i)) \iff z_{11}(c_1^{-1}(c_2 z_{21} - (j-i))) = i + z_{12}z_{21}$$

We then have the cases $\begin{cases} z_{11} = -c_1(j-i)^{-1}i, & \text{if } z_{21} = 0 \\ z_{12} = z_{21}^{-1}(z_{11}(c_1^{-1}(c_2 z_{21} - (j-i))) - i), & \text{otherwise} \end{cases}$

Therefore, z must take one of the following forms:

$$\begin{bmatrix} -c_1(j-i)^{-1}i & z_{12} \\ 0 & -c_1^{-1}(j-i) \end{bmatrix}, \quad \begin{bmatrix} z_{11} & z_{21}^{-1}(z_{11}(c_1^{-1}(c_2 z_{21} - (j-i))) - i) \\ z_{21} & c_1^{-1}(c_2 z_{21} - (j-i)) \end{bmatrix}, z_{21} \neq 0.$$

Proof of Property 4

If $i \neq j$, consider the matrix M with $\det(M) = 1$ and its action on c,

$$M = \begin{bmatrix} 1-\alpha & 1 \\ -\alpha & 1 \end{bmatrix}, \quad Mc = \begin{bmatrix} c_1 & c_2 \\ 0 & 0 \end{bmatrix}.$$

Therefore, we can assume that c has the above form wlog. Then

$$z_{11}z_{22} = i + z_{12}z_{21}, \tag{5}$$
$$-c_1 z_{22} + c_2 z_{21} = j - i \tag{6}$$

Now (6) and substituting into (5) gives

$$z_{22} = c_1^{-1}(c_2 z_{21} - (j-i)) \iff z_{11}(c_1^{-1}(c_2 z_{21} - (j-i))) = i + z_{12}z_{21}$$

We then have the cases $\begin{cases} z_{11} = -c_1(j-i)^{-1}i, & \text{if } z_{21} = 0 \\ z_{12} = z_{21}^{-1}(z_{11}(c_1^{-1}(c_2 z_{21} - (j-i))) - i), & \text{otherwise} \end{cases}$

Therefore, z must take one of the following forms:

$$\begin{bmatrix} -c_1(j-i)^{-1}i & z_{12} \\ 0 & -c_1^{-1}(j-i) \end{bmatrix}, \quad \begin{bmatrix} z_{11} & z_{21}^{-1}(z_{11}(c_1^{-1}(c_2 z_{21} - (j-i))) - i) \\ z_{21} & c_1^{-1}(c_2 z_{21} - (j-i)) \end{bmatrix}, z_{21} \neq 0.$$

So there are $q + q(q-1) = q^2$ matrices that z can take regardless of choice of c.

Proof of Property 4

The final case is $\det(c) \neq 0$. Again, since $c \neq 0$, we can assume wlog that $c_1 \neq 0$. Consider the matrix M with $\det(M) = 1$ and its action on c, where $k = \det(c)$:

$$M = \begin{bmatrix} 1 & 0 \\ -c_1^{-1}c_3 & 1 \end{bmatrix}, \quad Mc = \begin{bmatrix} c_1 & c_2 \\ 0 & c_1^{-1}k, \end{bmatrix}$$

We assume now that c takes has form wlog. The conditions $\det(z) = i, \det(z - c) = j$ imply

$$z_{11}z_{22} = i + z_{12}z_{21}, \tag{7}$$

$$(z_{11} - c_1)(z_{22} - c_1^{-1}k) - z_{21}(z_{12} - c_2) = j. \tag{8}$$

Proof of Property 4

The final case is $\det(c) \neq 0$. Again, since $c \neq 0$, we can assume wlog that $c_1 \neq 0$. Consider the matrix M with $\det(M) = 1$ and its action on c, where $k = \det(c)$:

$$M = \begin{bmatrix} 1 & 0 \\ -c_1^{-1}c_3 & 1 \end{bmatrix}, \quad Mc = \begin{bmatrix} c_1 & c_2 \\ 0 & c_1^{-1}k, \end{bmatrix}$$

We assume now that c takes has form wlog. The conditions $\det(z) = i, \det(z - c) = j$ imply

$$z_{11}z_{22} = i + z_{12}z_{21}, \tag{7}$$

$$(z_{11} - c_1)(z_{22} - c_1^{-1}k) - z_{21}(z_{12} - c_2) = j. \tag{8}$$

The equation (8) implies that

$$-c_1z_{22} - c_1^{-1}kz_{11} + c_2z_{21} + i + k = j \iff z_{22} = c_1^{-1}(i + k - j - c_1^{-1}kz_{11} + c_2z_{21}).$$

Substituting back into (7):

$$c_1^{-1}z_{11}(i + k - j - c_1^{-1}kz_{11} + c_2z_{21}) = i + z_{12}z_{21}.$$

Proof of Property 4

The final case is $\det(c) \neq 0$. Again, since $c \neq 0$, we can assume wlog that $c_1 \neq 0$. Consider the matrix M with $\det(M) = 1$ and its action on c, where $k = \det(c)$:

$$M = \begin{bmatrix} 1 & 0 \\ -c_1^{-1}c_3 & 1 \end{bmatrix}, \quad Mc = \begin{bmatrix} c_1 & c_2 \\ 0 & c_1^{-1}k, \end{bmatrix}$$

We assume now that c takes has form wlog. The conditions $\det(z) = i, \det(z - c) = j$ imply

$$z_{11}z_{22} = i + z_{12}z_{21}, \tag{7}$$

$$(z_{11} - c_1)(z_{22} - c_1^{-1}k) - z_{21}(z_{12} - c_2) = j. \tag{8}$$

The equation (8) implies that

$$-c_1 z_{22} - c_1^{-1}kz_{11} + c_2 z_{21} + i + k = j \iff z_{22} = c_1^{-1}(i + k - j - c_1^{-1}kz_{11} + c_2 z_{21}).$$

Substituting back into (7):

$$c_1^{-1}z_{11}(i + k - j - c_1^{-1}kz_{11} + c_2 z_{21}) = i + z_{12}z_{21}.$$

If $z_{21} = 0$, then

$$c_1^{-1}z_{11}(i + k - j - c_1^{-1}kz_{11}) = i \iff c_1^{-2}z_{11}^2 - k^{-1}z_{11}(i + k - j) + i = 0, \tag{9}$$

and there are $\epsilon_{i,j,k}$ solutions for z_{11} modulo q to the above polynomial.

Proof of Property 4

If $z_{21} = 0$, then

$$c_1^{-1} z_{11}(i + k - j - c_1^{-1} k z_{11}) = i \iff c_1^{-2} z_{11}^2 - k^{-1} z_{11}(i + k - j) + i = 0, \tag{10}$$

and there are $\epsilon_{i,j,k}$ solutions for z_{11} modulo q to the above polynomial.

Proof of Property 4

If $z_{21} = 0$, then

$$c_1^{-1} z_{11}(i + k - j - c_1^{-1} k z_{11}) = i \iff c_1^{-2} z_{11}^2 - k^{-1} z_{11}(i + k - j) + i = 0, \tag{10}$$

and there are $\epsilon_{i,j,k}$ solutions for z_{11} modulo q to the above polynomial.

If $z_{21} \neq 0$, then $z_{12} = z_{21}^{-1}(c_1^{-1} z_{11}(i + k - j - c_1^{-1} k z_{11} + c_2 z_{21}) - i)$. So z must take one of the forms:

$$\begin{bmatrix} z_{11} & z_{12} \\ 0 & z_{22} \end{bmatrix}, \quad \text{or} \quad \begin{bmatrix} z'_{11} & z'_{12} \\ z_{21} & z_{22} \end{bmatrix}, z_{21} \neq 0,$$

where z_{11} is any of the $\epsilon_{i,j,k}$ solutions to the polynomial (10), and

$$\begin{aligned} z_{22} &= c_1^{-1}(i + k - j - c_1^{-1} k z_{11} + c_2 z_{21}), \\ z'_{12} &= z_{21}^{-1}(c_1^{-1} z'_{11}(i + k - j - c_1^{-1} k z'_{11} + c_2 z_{21}) - i). \end{aligned}$$

Proof of Property 4

If $z_{21} = 0$, then

$$c_1^{-1} z_{11}(i + k - j - c_1^{-1} k z_{11}) = i \iff c_1^{-2} z_{11}^2 - k^{-1} z_{11}(i + k - j) + i = 0, \tag{10}$$

and there are $\epsilon_{i,j,k}$ solutions for z_{11} modulo q to the above polynomial.

If $z_{21} \neq 0$, then $z_{12} = z_{21}^{-1}(c_1^{-1} z_{11}(i + k - j - c_1^{-1} k z_{11} + c_2 z_{21}) - i)$. So z must take one of the forms:

$$\begin{bmatrix} z_{11} & z_{12} \\ 0 & z_{22} \end{bmatrix}, \quad \text{or} \quad \begin{bmatrix} z'_{11} & z'_{12} \\ z_{21} & z_{22} \end{bmatrix}, z_{21} \neq 0,$$

where z_{11} is any of the $\epsilon_{i,j,k}$ solutions to the polynomial (10), and

$$\begin{aligned} z_{22} &= c_1^{-1}(i + k - j - c_1^{-1} k z_{11} + c_2 z_{21}), \\ z'_{12} &= z_{21}^{-1}(c_1^{-1} z'_{11}(i + k - j - c_1^{-1} k z'_{11} + c_2 z_{21}) - i). \end{aligned}$$

There are $\epsilon_{i,j,k} q + q(q-1) = q(q + \epsilon_{i,j,k} - 1)$ matrices that z can be regardless of choice of c ($\epsilon_{i,j,k}$ choices for z_{11}, q for z_{12} in the first matrix type, q for z'_{11}, and $q - 1$ for z_{21} in the second type). □

Properties: the Size of Relations

The relations R_i of $\mathcal{C}(2, q)$ satisfy

$$|R_i| = \begin{cases} q^4, & i = q \\ q^5(q^2 - 1), & i = 1, ..., q - 1 \\ q^4(q^3 + q^2 - q - 1), & i = 0 \end{cases}$$

Properties: the Size of Relations

The relations R_i of $\mathcal{C}(2,q)$ satisfy

$$|R_i| = \begin{cases} q^4, & i = q \\ q^5(q^2-1), & i = 1, \ldots, q-1 \\ q^4(q^3+q^2-q-1), & i = 0 \end{cases}$$

Proof.
R_q has size $|R_q| = |M_2(\mathbb{F}_q)| = q^4$.

Properties: the Size of Relations

The relations R_i of $\mathcal{C}(2,q)$ satisfy

$$|R_i| = \begin{cases} q^4, & i = q \\ q^5(q^2-1), & i = 1,\ldots,q-1 \\ q^4(q^3+q^2-q-1), & i = 0 \end{cases}$$

Proof.

R_q has size $|R_q| = |M_2(\mathbb{F}_q)| = q^4$.
Recall for $i = 1,\ldots,q-1$ each R_i consists of pairs (x,y) such that $\det(x-y) = i$. For each $i \in \mathbb{F}_q^\times$ there are $(q+1)(q^2-q)$ matrices of determinant i, and so for each fixed x there are $(q+1)(q^2-q)$ possible y such that $\det(x-y) = i$; since there are q^4 choices for x, we arrive at
$q^4 \cdot (q+1)(q^2-q) = q^5(q^2-1)$.

Properties: the Size of Relations

The relations R_i of $\mathcal{C}(2,q)$ satisfy

$$|R_i| = \begin{cases} q^4, & i = q \\ q^5(q^2-1), & i = 1,\ldots,q-1 \\ q^4(q^3+q^2-q-1), & i = 0 \end{cases}$$

Proof.

R_q has size $|R_q| = |M_2(\mathbb{F}_q)| = q^4$.
Recall for $i = 1,\ldots,q-1$ each R_i consists of pairs (x,y) such that $\det(x-y) = i$. For each $i \in \mathbb{F}_q^\times$ there are $(q+1)(q^2-q)$ matrices of determinant i, and so for each fixed x there are $(q+1)(q^2-q)$ possible y such that $\det(x-y) = i$; since there are q^4 choices for x, we arrive at $q^4 \cdot (q+1)(q^2-q) = q^5(q^2-1)$.
The size of R_0 is then

$$|R_0| = |M_2(\mathbb{F}_q)|^2 - (q-1)|R_1| - |R_q|,$$

since the relations partition $M_2(\mathbb{F}_q)^2$, which yields the recorded value. □

Properties: Relations among Intersection Numbers

For any $\lambda \in \mathbb{F}_q^\times$ and $i, j, k \neq q$ the intersection numbers of $\mathcal{C}(2, q)$ satisfy

$$\rho_{ij}^k = \rho_{\lambda^2 i \lambda^2 j}^{\lambda^{-2} k}$$

$$\rho_{\lambda^2 i \lambda^2 j}^{\lambda^{-2} k} = |\{z \in M_n(\mathbb{F}_q) : \det(x - z) = \lambda^2 i \text{ and } \det(z - y) = \lambda^2 j, \text{ some } (x, y) \in R_{\lambda^{-2} k}\}|$$
$$= |\{\lambda^{-1} z \in M_n(\mathbb{F}_q) : \det(x - \lambda^{-1} z) = \lambda^2 i \text{ and } \det(\lambda^{-1} z - y) = \lambda^2 j, \text{ some } x, y : \det(x - y) = \lambda^{-2} k\}|$$
$$= |\{\lambda^{-1} z \in M_n(\mathbb{F}_q) : \det(\lambda x - z) = i \text{ and } \det(z - \lambda y) = j, \text{ some } x, y : \lambda^2 \det(x - y) = k\}| = \rho_{ij}^k$$

Properties: Relations among Intersection Numbers

For any $\lambda \in \mathbb{F}_q^\times$ and $i, j, k \neq q$ the intersection numbers of $\mathcal{C}(2, q)$ satisfy

$$\rho_{ij}^k = \rho_{\lambda^2 i \lambda^2 j}^{\lambda^{-2} k}$$

$$\rho_{\lambda^2 i \lambda^2 j}^{\lambda^{-2} k} = |\{z \in M_n(\mathbb{F}_q) : \det(x - z) = \lambda^2 i \text{ and } \det(z - y) = \lambda^2 j, \text{ some } (x, y) \in R_{\lambda^{-2} k}\}|$$
$$= |\{\lambda^{-1} z \in M_n(\mathbb{F}_q) : \det(x - \lambda^{-1} z) = \lambda^2 i \text{ and } \det(\lambda^{-1} z - y) = \lambda^2 j, \text{ some } x, y : \det(x - y) = \lambda^{-2} k\}|$$
$$= |\{\lambda^{-1} z \in M_n(\mathbb{F}_q) : \det(\lambda x - z) = i \text{ and } \det(z - \lambda y) = j, \text{ some } x, y : \lambda^2 \det(x - y) = k\}| = \rho_{ij}^k$$

For any $\lambda \in \mathbb{F}_q^\times$ and $k \neq q$ the intersection numbers of $\mathcal{C}(2, q)$ satisfy

$$\rho_{ij}^k = \rho_{\lambda i \lambda j}^{\lambda k}$$

Let $M \in M_2(\mathbb{F}_q)$ satisfy $\det(M) = \lambda$. Then

$$\rho_{\lambda i \lambda j}^{\lambda k} = |\{z \in M_n(q) : \det(x - z) = \lambda i \text{ and } \det(z - y) = \lambda j \text{ for some } (x, y) \in R_{\lambda k}\}|$$
$$= |\{Mz \in M_n(q) : \det(x - Mz) = \lambda i \text{ and } \det(Mz - y) = \lambda j \text{ for some } (x, y) \in R_{\lambda k}\}|$$
$$= |\{Mz \in M_n(q) : \det(M^{-1} x - z) = i \text{ and } \det(z - M^{-1} y) = j \text{ for some } (M^{-1} x, M^{-1} y) \in R_k\}| = \rho_{ij}^k$$

Properties: Algebraic Properties

$\mathcal{C}(2, q)$ is a symmetric coherent configuration.

Proof.

A coherent configuration is symmetric if all relations are symmetric. Clearly R_q is symmetric. Let $i \in \{0, 1, ..., q-1\}$. Then $R_i = \{(A, B) : A \neq B \text{ and } \det(A - B) = i\}$, and the R_i are symmetric since

$$\det(A - B) = \det(-(B - A) = (-1)^2 \det(B - A) = \det(B - A) \quad \square$$

That is, $\mathcal{C}(2, q)$ is an association scheme.

Properties: Algebraic Properties

$\mathcal{C}(2,q)$ is a symmetric coherent configuration.

Proof.

A coherent configuration is symmetric if all relations are symmetric. Clearly R_q is symmetric. Let $i \in \{0,1,...,q-1\}$. Then $R_i = \{(A,B) : A \neq B \text{ and } \det(A-B) = i\}$, and the R_i are symmetric since

$$\det(A-B) = \det(-(B-A) = (-1)^2 \det(B-A) = \det(B-A) \quad \square$$

That is, $\mathcal{C}(2,q)$ is an association scheme.
So $\mathcal{C}(2,q)$ is a homogeneous, stratifiable, commutative translation scheme:

$$\det(x+z-(y+z)) = \det(x-y)$$

Properties: Algebraic Properties

$\mathcal{C}(2,q)$ is a symmetric coherent configuration.

Proof.

A coherent configuration is symmetric if all relations are symmetric. Clearly R_q is symmetric. Let $i \in \{0,1,...,q-1\}$. Then $R_i = \{(A,B) : A \neq B \text{ and } \det(A-B) = i\}$, and the R_i are symmetric since

$$\det(A-B) = \det(-(B-A) = (-1)^2 \det(B-A) = \det(B-A) \quad \square$$

That is, $\mathcal{C}(2,q)$ is an association scheme.
So $\mathcal{C}(2,q)$ is a homogeneous, stratifiable, commutative translation scheme:

$$\det(x+z-(y+z)) = \det(x-y)$$

$\mathcal{C}(2,q)$ is not P-polynomial for $q \geq 3$.

Proof.

Relabel the indices such that the fibre of $\mathcal{C}(2,q)$ is R_0, so that we may use the definition given above. Then observe that $\rho^q_{\frac{q-1}{2},\frac{q-1}{2}} \neq 0$ by our Theorem, and that $\frac{q-1}{2} + \frac{q-1}{2} < q$. $\square$

Properties: Thinness

$\mathcal{C}(2, q)$ is not thin.

Proof.

Consider relation R_0 and the matrices $x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $y_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, and $y_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Then

$$\det(x - y_1) = \det(x - y_2) = 0$$

so the xth row of $A(R_0)$ contains ones in both the y_1th and y_2th positions. □

Properties: Thinness

$\mathcal{C}(2, q)$ is not thin.

Proof.

Consider relation R_0 and the matrices $x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $y_1 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, and $y_2 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Then

$$\det(x - y_1) = \det(x - y_2) = 0$$

so the xth row of $A(R_0)$ contains ones in both the y_1th and y_2th positions. □

It is therefore unclear if $\mathcal{C}(2, q)$ is Schurian.

Note furthermore that $\mathcal{C}(2, q)$ gets 'further' away from being thin as q increases, since non-zero scalar multiples of y_1 and y_2 (to name just two matrices) also yield ones in the (x, y_i) locations in $A(R_0)$, $i = 1, 2$.

Properties of $\mathcal{C}(2,3)$

When $q=3$ we have a three-class association scheme. In this case the following result holds:

[**XiaTanLiangKoolen**] Let $\mathfrak{X}=\left(X,\{R_i\}_{i=0}^{3}\right)$ be a three-class scheme. Then exactly one of the following holds:

1. $\mathfrak{X}$ is polynomial; 2. $\mathfrak{X}$ is amorphic; 3. $\mathfrak{X}$ is degenerate.

We can prove: $\mathcal{C}(2,3)$ is amorphic (tedious proof by exhaustion).

Properties of $\mathcal{C}(2,3)$

When $q = 3$ we have a three-class association scheme. In this case the following result holds:

[**XiaTanLiangKoolen**] Let $\mathfrak{X} = \left(X, \{R_i\}_{i=0}^{3}\right)$ be a three-class scheme. Then exactly one of the following holds:

1. $\mathfrak{X}$ is polynomial; 2. $\mathfrak{X}$ is amorphic; 3. $\mathfrak{X}$ is degenerate.

We can prove: $\mathcal{C}(2,3)$ is amorphic (tedious proof by exhaustion).

Using

Theorem

[**XiaTanLiangKoolen**] Let $\mathfrak{X}$ be a Q-polynomial association scheme. Then $\mathfrak{X}$ is polynomial.

We thus conclude

Theorem

$\mathcal{C}(2,3)$ is not Q-polynomial.

Proof.

By [**XiaTanLiangKoolen**], a Q-polynomial association scheme is polynomial, so an association scheme which is not polynomial is not Q-polynomial. We know $\mathcal{C}(2,3)$ is amorphic, and hence by [**XiaTanLiangKoolen**] is not polynomial. □

Open Questions

- Disproof of Property 4 for $\mathcal{C}(n, q)$, $n > 2$?
- Tweak $\mathcal{C}(n, q)$, $n > 2$, to get a scheme?
- $\mathcal{C}(2, q)$ Q-polynomial for $q > 3$? Use translation scheme properties?

IMPERIAL

Thank you. Questions?