Three-Class Association Schemes
Based On A Construction By Mathon

Sven Reichard

TU Dresden

Villanova, June 5, 2014
An $d$-class association scheme is a finite set $\Omega$ together with binary relations $R_i$, $i = 0..d$.

- $\bigcup_i R_i = \Omega^2$
- $R_0 = id_\Omega$
- $R_i^{-1} = R_j$ for some $j$
- If $(x, z) \in R_k$, then the number of $y$ with
  - $(x, y) \in R_i$ and
  - $(y, z) \in R_j$

depends only on $i, j, k$. These numbers $p_{ij}^k$ are called intersection numbers.
We can represent each relation $R_i$ by its adjacency matrix $A_i$. We get the equivalent definition:

- $\sum_i A_i = J$ (all-one matrix)
- $A_0 = I$ (identity matrix)
- $A_i^T = A_j$
- $A_i A_j = \sum p_{ij}^k A_k$

So the space spanned by these matrices is an algebra.
Permutation groups are one way to construct association schemes:

Let \((G, \Omega)\) be a finite transitive permutation group. Consider the action of \(G\) on \(\Omega^2\). Then the orbits of this action form an association scheme.

We call this scheme \(V(G, \Omega)\).

Any scheme that arises in this way is called Schurian.
The existence of Schurian schemes can be explained using Group Theory.

For a non-Schurian scheme we need some “combinatorial coincidence”.

A common approach: Start with a Schurian scheme; merge relations to obtain a new scheme.

There are algorithms to enumerate mergings in concrete schemes: COCO (Faradžev-Klin); newer implementations in GAP (Pech-R)
Nevo and Thurston posed questions about a particular action of $PSL(2, q)$.
Together with Klin we found a few interesting (non-Schurian) mergings.
It turns out they can be described on a theoretical level.
Here, we want to give the construction of a new infinite family of non-Schurian schemes. We need the following ingredients:

1. Quasi-projective points
2. Symplectic forms
3. Cyclic difference sets
Let $F = F_q$ be a finite field of order $q$.
Let $F^*$ be its multiplicative group.
Let $V = F^2$ be the two-dimensional vectors space over $F$.
Then
\[(V \setminus \{0\})/F^* = \{F^*x : 0 \neq x \in V\}\]
is the projective line over $F$; its elements are projective points.
Now we consider a subgroup $K \leq F^*$. We call the elements of

$$\Omega = (V \setminus \{0\})/K$$

quasi-projective points.

Their number is $\frac{q^2 - 1}{k}$, where $k = |K|$.

We will also consider $F/K$ (as a ring) and $F^*/K$ (as a cyclic group).
Example

Let $q = 29$, and let $K$ be the subgroup of order $4 = \frac{29-1}{7}$ in the multiplicative group of $F$. We get $\frac{29^2 - 1}{4} = 210$ quasi-projective points.
Symplectic forms

- We keep the notation $V = F^2$.
- A symplectic form $\langle \cdot , \cdot \rangle$ is an alternating (non-degenerate) bilinear form.
- By choosing a convenient basis we can express such a form as a determinant:

$$\langle \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} , \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \rangle = \begin{vmatrix} u_1 & v_1 \\ u_2 & v_2 \end{vmatrix}$$

- This shows that here the symplectic group is equal to the special linear group.
- Moreover, $\langle u , v \rangle = 0$ if and only if $u , v$ are linearly dependent.
We can apply the symplectic form to quasi-projective points.

The form is bilinear, so for \( x \in F \) we have

\[
\langle xu, v \rangle = x \langle u, v \rangle
\]

Thus we can regard \( \langle \cdot, \cdot \rangle \) as function from \( \Omega^2 \) to \( F/K \).

In the case of projective points we only get two values, 0 and \( K = F^* \).
Cyclic difference sets

- Let $C$ be a cyclic group of order $v$.
- Let $D$ be a subset of $C$ of size $k$.
- $D$ is a difference set if there is a number $\lambda$ such that for any non-zero element $c \in C$,

  $$x - y = c$$

  has exactly $\lambda$ solutions with $x, y \in D$.
- $(v, k, \lambda)$ are the parameters of $D$.
- Equivalent: $2 - (v, k, \lambda)$ design
Small example

- Let $C = C_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- Let $D = \{1, 2, 4\}$.
- This is a cyclic $(7, 3, 1)$-difference set:
  
  \[
  \begin{align*}
  1 &= 2 - 1 \\
  2 &= 4 - 2 \\
  3 &= 4 - 1 \\
  4 &= 1 - 4 \\
  5 &= 2 - 4 \\
  6 &= 1 - 2 
  \end{align*}
  \]
Let $p = 4k + 3$ be a prime.
Let $C = \mathbb{Z}_p$.
Let $D$ be the set of non-zero squares in $C$.
This is a cyclic $(4k + 3, 2k + 1, k)$-difference set.
The small example is cyclotomic for $k = 1$. 
Let \( q \) be a prime power, \( n \geq 3 \) an integer.

Consider the \( n-1 \)-dimensional projective space over the field with \( q \) elements.

It admits a Singer cycle \( C \): A cyclic group acting regularly on points.

A projective hyperplane is a \( \left( \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1} \right) \) difference set in \( C \).

The small example is a Singer difference set for \( q = 2, n = 3 \).
Construction 1

Let $F, K, \Omega, \langle \cdot, \cdot \rangle$ be as before. Let $x \in F/K$ be non-zero, e.g., $x = K$. Define the following binary relations on $\Omega$:

- $R_0$ is the identity;
- $R_1$: $\langle u, v \rangle = 0$;
- $R_2$: $\langle u, v \rangle = x$;
- $R_3$: Everything else.

This defines an association scheme. In fact, $R_2$ defines a distance-regular graph. $R_1$ is an equivalence relation.

It was first described by R. Mathon, in slightly different terms.
Theorem

Construction 1 gives a three-class association scheme with valencies

- 1,
- \( r - 1 \),
- \( q \),
- \( (r - 1)q \).

Here, \( q = |F| \), and \( r = |F^*/K| \).
Example

Choosing, as before, $q = 29$ and $k = 4$, we get $r = 7$, the number of points is 210, and the valencies are 1, 6, 29, 174.
Now let $D$ be a difference set in the cyclic group $F^*/K$. We define new binary relations on $\Omega$:

- $R_0$ is the identity;
- $R_1$: $\langle u, v \rangle = 0$;
- $R_2$: $\langle u, v \rangle \in D$;
- $R_3$: Everything else, i.e., $0 \neq \langle u, v \rangle \notin D$.

This defines an association scheme.
Construction 2 is a generalization of Construction 1, since a singleton in $F^*/K$ is a difference set. In fact we can generalize Theorem 1:

**Theorem**

*Construction 2 gives a three-class association scheme with valencies*

- 1,
- $r - 1$,
- $dq$,
- $(r - d)q$.

*Here, $d = |D|$.*
Actually, we can compute all the structure constants:

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>∑</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>r - 1</td>
<td>0</td>
<td>0</td>
<td>r - 1</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>r - 2</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>d - 1</td>
<td>r - d</td>
<td>r - d - 1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>dq</td>
<td>0</td>
<td>dq</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>λq</td>
<td>(d - λ)q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>d - 1</td>
<td>d^2 m</td>
<td>dm(r - d)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>d</td>
<td>d^2 m</td>
<td>dm(r - d)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>(r - d)q</td>
<td>(r - d)q</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>(d - λ)q</td>
<td>(r - 2d + λ)q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>r - d</td>
<td>d(q - 1 - dm)</td>
<td>(r - d)(q - 1 - dm)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1</td>
<td>r - d - 1</td>
<td>d(q - 1 - dm)</td>
<td>(r - d)(q - 1 - dm)</td>
<td></td>
</tr>
</tbody>
</table>

∑ | 1   | r - 1 | dq  | (r - d)q | r(q + 1) |
Example

Choosing \( q = 29 \) and \( k = 4 \), we get \( r = 7 \), the number of points is 210.
If we take a difference set \( D \) with 3 elements in \( F^*/K \), we get a scheme with the valencies are 1, 6, 87, 116.
Theorem

*Constructions 1 and 2 yield infinite families of association schemes.*

Proof.

- There are infinitely many orders for which cyclic difference sets exist.
- Each difference set gives infinitely many schemes as for fixed $r$, $rk + 1$ is prime for infinitely many $k$ (Dirichlet’s Theorem).
Toward non-Schurity

Conjecture

The association schemes constructed above are non-Schurian.

Ideas:

- 4-vertex condition (Hestenes-Higman)
- Consider one basis relation $R_2$.
- Count complete graphs $K_4$ containing a given edge.
- We can distinguish various orbit of $PSL$.
- Hence the automorphism group is intransitive on $R_2$. 
Counting $K_4$:

- Fix two points $x,y$ (linearly independent).
- Consider common neighbors $w,z$ of $x$ and $y$.
- $\langle w,z \rangle$ can be computed from $\langle x,y \rangle$, $\langle x,w \rangle$, $\langle x,z \rangle$, $\langle y,w \rangle$, $\langle y,z \rangle$.
- Count how often $\langle w,z \rangle \in D$; this depends on $\langle x,y \rangle$.
- Thus we can recover the symplectic group from our scheme.
More to the point: We need to count the number of solutions of the equation

\[ \langle w, z \rangle = \frac{\langle y, z \rangle \langle x, w \rangle - \langle y, w \rangle \langle x, z \rangle}{\langle x, y \rangle} \]

where \( \langle x, y \rangle \) is given, and all values of \( \langle \cdot, \cdot \rangle \) are in \( D \). It is sufficient to find \( \langle x_1, y_1 \rangle \) and \( \langle x_2, y_2 \rangle \) with different numbers of solutions.
Finish the counting business

Muzychuk suggested the following. In a nutshell:

- Start with a scheme which admits a cyclic group acting on its relations.
- Find a difference set $D$ in that group.
- Merge according to $D$.

Does this work more generally?
Eran Nevo (BGU) first asked questions regarding this particular group action.

Misha Klin (BGU) found the first examples, and suggesting considering cyclic difference sets.