Complete Mappings for Semigroups

Michael Kinyon

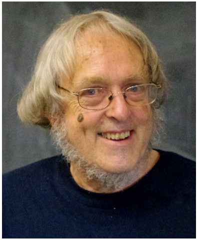
AGTA, University of Naples Federico II, 24 June 2025

Whom to blame

This is joint work with. . .

João Araújo
(Nova U. Lisboa)

Wolfram Bentz
(U. Aberta)



Peter Cameron
(St. Andrews U.)

Motivation: Orthogonal latin squares

A *latin square* is an $n \times n$ array filled with n different symbols, each occurring exactly once in each row and exactly once in each column.

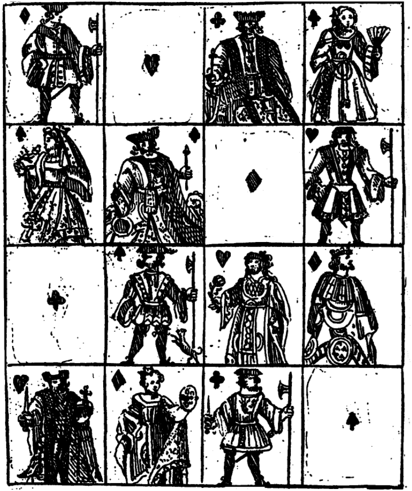
Two Latin squares of the same size are *orthogonal* if, when they are superimposed, the ordered paired entries are all distinct.

J	A	K	Q
Q	K	A	J
A	J	Q	K
K	Q	J	A

$\diamondsuit$	$\heartsuit$	$\spadesuit$	$\clubsuit$
$\spadesuit$	$\clubsuit$	$\diamondsuit$	$\heartsuit$
$\clubsuit$	$\spadesuit$	$\heartsuit$	$\diamondsuit$
$\heartsuit$	$\diamondsuit$	$\clubsuit$	$\spadesuit$

J $\diamondsuit$	A $\heartsuit$	K $\spadesuit$	Q $\clubsuit$
Q $\spadesuit$	K $\clubsuit$	A $\diamondsuit$	J $\heartsuit$
A $\clubsuit$	J $\spadesuit$	Q $\heartsuit$	K $\diamondsuit$
K $\heartsuit$	Q $\diamondsuit$	J $\clubsuit$	A $\spadesuit$

Euler’s work in 1776 is usually cited as the beginning of the study of orthogonal latin squares (“Graeco-Roman squares”). But there was a predecessor. Here is a picture from the 1725 four-volume edition of Jacques Ozanam’s (1640–1718) *Récréations mathématiques et physiques*. . .



Transversals

A *transversal* of a latin square of size n is a set of n entries such that no two entries share the same row, column, or symbol.

In the card example, the suit square determines 4 transversals of the letter square (and vice versa).

J	A	K	Q
Q	K	A	J
A	J	Q	K
K	Q	J	A

J $\diamondsuit$	A $\heartsuit$	K $\spadesuit$	Q $\clubsuit$
Q $\spadesuit$	K $\clubsuit$	A $\diamondsuit$	J $\heartsuit$
A $\clubsuit$	J $\spadesuit$	Q $\heartsuit$	K $\diamondsuit$
K $\heartsuit$	Q $\diamondsuit$	J $\clubsuit$	A $\spadesuit$

A latin square of size n has an orthogonal mate if and only if it has n disjoint tranversals which partition the cells of the square.

Groups

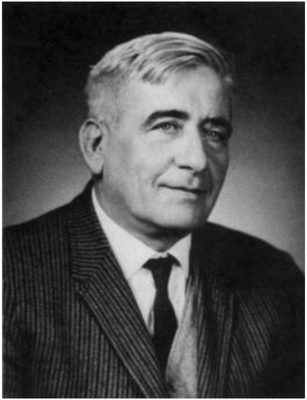
After Arthur Cayley (1821–1895) observed that the operation table (which we now call a Cayley table) of a group is a latin square, it was natural to use group tables, especially for abelian groups, to construct orthogonal latin squares.

It's not clear who was the first to do this. There were some constructions in the late 1930s by:

- Raj Chandra Bose (1901–1987),
- Ronald A. Fisher (1890–1962) and Frank Yates (1902–1994) in their book *Statistical Tables*, and
- W.L. Stevens (??–??), a protégé of Fisher

Complete mappings

Complete mappings for groups were introduced by Henry B. Mann (1905–2000) in 1942. The definition works for any magma.



H.B. Mann

A *complete mapping* of a magma M is a bijection $\alpha : M \to M$ such that the mapping $\theta : M \to M$ defined by $x^\theta = x \cdot x^\alpha$ is also a bijection. The bijection θ is called an *orthomorphism* (a term introduced in 1961).

In (quasi)groups, complete mappings and orthomorphisms determine each other, so it is a matter of taste which one to emphasize.

Complete mappings and transversals

Observation: *A mapping $\alpha : Q \to Q$ is a complete mapping if and only if there exists a transversal determined by assigning to each row i, the entry in column i^α.*

In the card example, let's label the rows and columns:

$\cdot$	A	K	Q	J
A	J $\diamondsuit$	A	K	Q
K	Q	K	A $\diamondsuit$	J
Q	A	J	Q	K $\diamondsuit$
J	K	Q $\diamondsuit$	J	A

The complete mapping α for the $\diamondsuit$ transversal is:

$$A^\alpha = A, \qquad K^\alpha = Q, \qquad Q^\alpha = J, \qquad J^\alpha = K$$

and the orthomorphism θ is:

$$A^\theta = J, \qquad K^\theta = A, \qquad Q^\theta = K, \qquad J^\theta = Q$$

One complete mapping is enough for groups

Mann's key observation was that for groups, having just *one* complete mapping α is equivalent to having an orthogonal mate. List the group elements $e = g_1, g_2, \ldots, g_n$. Here is α's transversal:

$$(g_1, g_1^\alpha), \;\; (g_2, g_2^\alpha), \;\; \ldots \; (g_n, g_n^\alpha)$$

Then we obtain $n - 1$ more disjoint transversals as follows:

$$(g_1, g_1^\alpha g_2), \;\; (g_2, g_2^\alpha g_2), \;\; \ldots \; (g_n, g_n^\alpha g_2)$$

$$\vdots$$

$$(g_1, g_1^\alpha g_n), \;\; (g_2, g_2^\alpha g_n), \;\; \ldots \; (g_n, g_n^\alpha g_n)$$

This depends heavily on associativity! It doesn't work for quasigroups; having one transversal doesn't guarantee there are any others.

Hall and Paige

In 1955, Marshall Hall Jr (1910–1990) and Lowell J. Paige (1919–2010) took the next step of asking precisely which finite groups have complete mappings.

Marshall Hall Jr.

Lowell J. Paige

The Hall-Paige Conjecture

Hall and Paige observed that the cyclic groups C_{2^n} do not have complete mappings. (Try it yourself for small n.) They conjectured that this is essentially the only obstruction.

Conjecture. *A finite group G has a complete mapping if and only if the Sylow 2-subgroups of G are either trivial or noncyclic.*

Among other things, Hall and Paige (1955) proved;

- The condition is necessary;
- A_n has a complete mapping for all n;
- Every finite solvable group satisfies the Conjecture.

From Conjecture to Theorem

In 2009, Stewart Wilcox proved that a minimal counterexample to the Hall-Paige conjecture must be a nonabelian simple group.

The alternating groups have complete mappings, so that left the simple groups of Lie type and the sporadic simple groups as possible counterexamples.

Wilcox proved that no finite simple group of Lie type, with the possible exception of the Tits group, could be a minimal counterexample.

The Mathieu groups were already known to have complete mappings (Dalla Volta and Gavioli, 1993).

From Conjecture to Theorem II

Still in 2009, Tony Evans took care of the Tits group and all but one of the remaining sporadic groups: the Janko group J_4.

During the same time period, John Bray showed that J_4 has a complete mapping. However, he didn't publish the result right away.

Bray finally published his proof in 2020 as part of a larger paper with Qi Cai, Peter Cameron, Pablo Spiga, and Hua Zhang, who needed the Hall-Paige Conjecture to be a theorem in order to prove some results in permutation group theory.

What now?

So much for groups. The study of complete mappings for quasigroups, or equivalently, of transversals for latin squares, continues. One of the main motivating problems is **Ryser's Conjecture**: *Every latin square of odd order has a transversal.*

We decided to try a different direction. The notions of complete mapping, orthomorphism, transversal and so on make sense in any magma.

So as the talk title says, what about complete mappings for finite semigroups? Can we characterize, at least conjecturally, which finite semigroups have complete mappings?

Refresher

Given a semigroup (or just a magma) S, a *complete mapping* of S is a bijection $\alpha : S \to S$ such that the mapping $\theta : S \to S; x \mapsto x \cdot x^{\alpha}$ (called an *orthomorphism*) is also a bijection.

The correspondence between complete mappings and transversals is the same as before. Here is the Brandt semigroup of order 5. It has exactly two transversals.

$\cdot$	0	1	2	3	4
0	$0^{*,\dagger}$	0	0	0	0
1	0	1^{*}	0	$3^{\dagger}$	0
2	0	0	$2^{\dagger}$	0	4^{*}
3	0	0	3^{*}	0	$1^{\dagger}$
4	0	$4^{\dagger}$	0	2^{*}	0

Zeros

As is common in semigroup theory, special attention must be paid to semigroups with a zero (absorbing element). Fortunately, complete mappings and orthomorphisms behave exactly as one would hope.

Proposition. *Let S be a semigroup with zero* 0*, and let* $\alpha : S \to S$ *be a complete mapping with orthomorphism* $\theta : S \to S; x \mapsto x \cdot x^{\alpha}$*. Then* $0^{\alpha} = 0^{\theta} = 0$*.*

Monoids

What if you hate semigroups but love monoids?

Well, first, you can always change what you hate into something you love by adjoining an identity element. Second...

Proposition. *If a finite monoid has a complete mapping and orthomorphism, then it has a complete mapping and orthomorphism fixing the identity element.*

Regularity

A semigroup S is (von Neumann) *regular* if for each $x \in S$, there exists $x' \in S$ such that

$$xx'x = x \qquad \text{and} \qquad x'xx' = x'.$$

Such an x' is called an *inverse* of x. Inverses need not be unique.

Theorem. *Let S be a finite semigroup with a complete mapping $\alpha : S \to S$ and orthomorphism $\theta : S \to S; x \mapsto x \cdot x^{\alpha}$. Then:*

- *S is regular, and*
- *there exists an inverse mapping $x \mapsto x'$ satisfying $x' \cdot x^{\theta} = x^{\alpha}$ for all $x \in S$.*

Unlike in the (quasi)group case, orthomorphisms do not determine complete mappings, despite what the previous result might suggest.

Example. Let S be a finite left zero semigroup with $|S| > 1$, that is, S satisfies $xy = x$ for all $x, y \in S$.

Every permutation α of S is a complete mapping with the identity mapping as orthomorphism:

$$x^\theta = x \cdot x^\alpha = x$$

In addition, $x \mapsto x^\alpha =: x'$ is an inverse mapping, and $x' \cdot x^\theta = x^\alpha$.

Inverse semigroups

A semigroup S is an *inverse semigroup* if every $x \in S$ has a *unique* inverse $x^{-1} \in S$ such that $xx^{-1}x = x$, $x^{-1}xx^{-1} = x^{-1}$.

Example: The *symmetric inverse monoid* $\mathcal{I}_X$ on a set X is the set of all partial bijections on the set X under composition of partial mappings.

In finite inverse semigroups, orthomorphisms determine complete mappings.

Proposition. *Let S be a finite inverse semigroup, let $\theta : S \to S$ be a permutation, and define $\alpha : S \to S; x \mapsto x^{-1} \cdot x^{\theta}$. The following are equivalent:*

- *α is a permutation;*
- *α is a complete mapping with orthomorphism θ.*

Ideals

A subset I of a semigroup S is a

- *left ideal* if $xI \subseteq I$ for all $x \in S$;
- *right ideal* if $Ix \subseteq I$ for all $x \in S$;
- *ideal* if it is both a left and a right ideal.

Theorem. *Let $\alpha : S \to S$ be a complete mapping of a finite semigroup S with orthomorphism θ. Then:*

- *If $I \subseteq S$ is a right ideal, then $I^\theta = I$.*
- *If $I \subseteq S$ is an ideal, then $I^\alpha = I$.*

Rees quotients

Corresponding to any ideal I of a semigroup S is a *Rees quotient*:

$$S/I \equiv (S - I) \cup \{I\}$$

where I is a zero. (This is isomorphic to modding out a congruence corresponding to I, but this description is easier to work with.)

Proposition. *A semigroup S with ideal I has a complete mapping if and only if both I and S/I have complete mappings.*

This reduces the study of complete mappings to two cases: semigroups with zero and *simple* semigroups (no proper ideals). We will make a further reduction momentarily.

Principal ideals

For an element a of a semigroup S, define:

- $S^1a = \{a\} \cup Sa$, *principal left ideal*;
- $aS^1 = \{a\} \cup aS$, *principal right ideal*;
- $S^1aS^1 = SaS \cup Sa \cup aS \cup \{a\}$, *principal ideal*

Proposition. *Let $\alpha : S \to S$ be a complete mapping of a finite semigroup S with orthomorphism θ. For each $a \in S$,*

- $(aS^1)^\theta = a^\theta S^1$
- $(S^1aS)^\alpha = S^1a^\alpha S^1$.

Green's preorders and equivalences

Green's preorders:

$$a \preceq_{\mathcal{L}} b \iff S^1 a \subseteq S^1 b$$
$$a \preceq_{\mathcal{R}} b \iff aS^1 \subseteq bS^1$$
$$a \preceq_{\mathcal{J}} b \iff S^1 aS^1 \subseteq S^1 bS^1$$

Green's equivalences:

$$a \,\mathcal{L}\, b \iff a \preceq_{\mathcal{L}} b \text{ and } b \preceq_{\mathcal{L}} a$$
$$a \,\mathcal{R}\, b \iff a \preceq_{\mathcal{R}} b \text{ and } b \preceq_{\mathcal{R}} a$$
$$a \,\mathcal{J}\, b \iff a \preceq_{\mathcal{J}} b \text{ and } b \preceq_{\mathcal{J}} a$$

Theorem. *Let $\alpha : S \to S$ be a complete mapping of a finite semigroup S with orthomorphism θ.*

- *θ preserves $\preceq_{\mathcal{R}}$, hence $\mathcal{R}$*
- *α preserves $\preceq_{\mathcal{J}}$, hence $\mathcal{J}$*

Complete mappings of partial semigroups

Since a complete mapping of a finite semigroup S preserves $\mathcal{J}$-classes, it is tempting to say that a complete mapping of S exists if and only if each $\mathcal{J}$-class has a "complete mapping".

However, $\mathcal{J}$-classes are not necessarily subsemigroups. Instead, each $\mathcal{J}$-class J is a *partial* semigroup: For $x, y \in J$, define $x * y = xy$ if $xy \in J$; otherwise $x * y$ is undefined.

We'll say that a bijection $\alpha : J \to J$ is a complete mapping if the mapping $\theta : J \to J; x \mapsto x * x^\alpha$ is defined for all $x \in J$ and is a bijection.

Proposition. *A finite semigroup S has a complete mapping if and only if each $\mathcal{J}$-class, viewed as a partial semigroup, has a complete mapping.*

Adjoining a zero

Given a partial semigroup $(J, *)$, we can construct a semigroup $(J^0, \star)$ by adjoining a zero: $J^0 := J \cup \{0\}$ where

$$x \star y = \begin{cases} x * y & \text{if } x * y \text{ is defined} \\ 0 & \text{if } x * y \text{ is not defined or if } x = 0 \text{ or if } y = 0 \end{cases}$$

Lemma. *If $(J, *)$ is a partial semigroup, then J has a complete mapping as a partial semigroup if and only if J^0 has a complete mapping.*

[0]-simple semigroups

David Rees (1918–2013)

It follows that to characterize which finite semigroups have complete mappings, it is enough to do so for [0]-*simple* semigroups, that is, semigroups that are either:

- *simple*, consisting of one $\mathcal{J}$-class, or
- 0-*simple*, consisting of a zero 0 and one $\mathcal{J}$-class above it.

Fortunately, there is a nice representation of finite [0]-simple semigroups. . . .

Rees' Theorem for simple semigroups

Let's start with the easier simple case (no zero).

Given a group G and nonempty sets I, Λ,

- a *Rees matrix* is a map $P : \Lambda \times I \to G$
- P is *normalized* if its first row and first column consist of 1's, the identity element of G.
- This data determines a *Rees matrix semigroup*

  $$\mathcal{M}[G; I, \Lambda; P] = I \times G \times \Lambda$$

  with multiplication

  $$(a, g, \alpha)(b, h, \beta) := (a, g\, P_{\beta,a}\, h, \beta)\,.$$

Theorem (Rees). *A finite semigroup S is simple if and only if it is isomorphic to a Rees matrix semigroup $\mathcal{M}[G; I, \Lambda; P]$ for some group G, nonempty sets I, Λ and normalized Rees matrix $P : \Lambda \times I \to G$.*

Complete mappings for finite simple semigroups

We can give a complete (pun intended) characterization of the existence of complete mappings for finite simple semigroups.

Theorem. *A Rees matrix semigroup* $\mathcal{M}[G; I, \Lambda; P]$ *with normalized* P *has a complete mapping if and only if one of the following holds:*

- *G has a complete mapping (that is, G has trivial or noncyclic Sylow 2-subgroups);*
- $|I| \cdot |\Lambda|$ *is even;*
- *P has at least one entry of even order.*

Rees 0-matrix semigroups

The idea is similar, but with the following modifications:

- $\mathcal{M}^0[G; I, \Lambda; P] = (I \times G \times \Lambda) \cup \{0\}$
- the *Rees* 0*-matrix* $P : \Lambda \times I \to G \cup \{0\}$ has no row or column consisting entirely of zeros.
- $$(a, g, \alpha)(b, h, \beta) = \begin{cases} (a, g\, P_{\beta,a}\, h, \beta) & \text{if } P_{\beta,a} \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

Theorem (Rees). *A finite semigroup S is* 0*-simple if and only if it is isomorphic to a Rees* 0*-matrix semigroup $\mathcal{M}^0[G; I, \Lambda; P]$ for some group G, nonempty sets I, Λ and normalized* 0*-Rees matrix $P : \Lambda \times I \to G \cup \{0\}$.*

For Rees 0-matrix semigroups, there are two cases to consider: when the group G has a complete mapping and when it does not.

We don't have the full answer in either case. We have a conjecture in the former case and various sufficient conditions in the latter.

The *pattern* of a Rees 0-matrix $P : \Lambda \times I \to G^0$ is the matrix Q obtained by replacing every nonzero entry of P with 1, the identity element of G.

Conjecture

Let Q be a $\Lambda \times I$ zero-one matrix. The following are equivalent:

(a) *For any group G with a complete mapping, and any 0-Rees matrix $P : \Lambda \times I \to G \cup \{0\}$ with pattern Q, $\mathcal{M}^0[G; I, \Lambda; P]$ has a complete mapping.*

(b) *$\mathcal{M}^0(1, I, \Lambda, Q)$ has a complete mapping, where 1 denotes the trivial group.*

(c) *For any s rows of Q, there are at least $s|I|/|\Lambda|$ columns which contain nonzero entries in some of the chosen rows.*

(d) *For any r columns of Q, there are at least $r|\Lambda|/|I|$ rows which contain nonzero entries in some of the chosen columns.*

We know: (a) $\iff$ (b), (c) $\iff$ (d), (b) $\implies$ (d).

We know all four statements are equivalent if $|I| = |\Lambda|$ and in several other cases.

Final remarks

For the case where the group G does not have a complete mapping, we do not have a conjectural characterization. It seems that we need to resolve the case where G has a complete mapping first. We have some sufficient conditions which are based on the conditions (c),(d) of the conjecture.

We were able to characterize precisely which finite *inverse* semigroups have complete mappings. As an application, the following makes a nice conclusion.

Theorem. *Let $\mathcal{I}_n$ be the symmetric inverse monoid on n symbols. Then $\mathcal{I}_n$ has a complete mapping if and only if $n \equiv 0, 1 \pmod 4$.*

If you want to learn more, the preprint will be up on the arXiv as soon as my coauthors are finished with it. In the meantime…

Grazie per l'attenzione