Complete mappings of semigroups

Peter J. Cameron, University of St Andrews (joint with João Araújo, Wolfram Bentz and Michael Kinyon)



AMS Special Session Recent Trends in Semigroup Theory 14 May 2022

As you will see from the title slide, this talk has added one co-author.

As you will see from the title slide, this talk has added one co-author. Also, the conjecture in the abstract has become a theorem.

As you will see from the title slide, this talk has added one co-author.

Also, the conjecture in the abstract has become a theorem. The two events are not unconnected, as you will see. So welcome to the team, Wolfram!

As you will see from the title slide, this talk has added one co-author.

Also, the conjecture in the abstract has become a theorem. The two events are not unconnected, as you will see. So welcome to the team, Wolfram! Everything in this talk will be finite.

Complete mappings

Let (A, \circ) be a magma (a set with a binary operation).

Complete mappings

Let (A, \circ) be a magma (a set with a binary operation). A complete mapping on *A* is a bijection $\phi : A \to A$ with the property that the map $\psi : A \to A$ defined by

$$\psi(a)=a\circ\phi(a)$$

is also a bijection. The mapping ψ is called the orthomorphism associated with ϕ .

Complete mappings

Let (A, \circ) be a magma (a set with a binary operation). A complete mapping on *A* is a bijection $\phi : A \to A$ with the property that the map $\psi : A \to A$ defined by

 $\psi(a) = a \circ \phi(a)$

is also a bijection. The mapping ψ is called the orthomorphism associated with ϕ .

The very general question, which I am not going to address, is:

Question

Which magmas have complete mappings?

Groups

The general question, for the case of groups, was studied by Marshall Hall and Lowell Paige in the 1950s.

Groups

The general question, for the case of groups, was studied by Marshall Hall and Lowell Paige in the 1950s.

The cyclic group *G* of order 4 has no complete mapping. For suppose that it does. Then

$$\sum_{g \in G} g + \sum_{g \in G} \phi(g) = \sum_{g \in G} \psi(g).$$

Each of the three sums is the sum of all elements of *G*, and is equal to the unique involution *t* in *G*. But then t + t = t, which is false.

Groups

The general question, for the case of groups, was studied by Marshall Hall and Lowell Paige in the 1950s.

The cyclic group *G* of order 4 has no complete mapping. For suppose that it does. Then

$$\sum_{g \in G} g + \sum_{g \in G} \phi(g) = \sum_{g \in G} \psi(g).$$

Each of the three sums is the sum of all elements of *G*, and is equal to the unique involution *t* in *G*. But then t + t = t, which is false.

By similar reasoning, and using Burnside's transfer theorem, they proved

Theorem

Let G be a group of even order whose Sylow 2-subgroups are cyclic. Then G has no complete mapping.

Hall and Paige conjectured the converse:

Conjecture

If either |G| is odd or G has non-cyclic Sylow 2-subgroups, then G has a complete mapping.

They proved this for some special groups such as symmetric and alternating groups.

Hall and Paige conjectured the converse:

Conjecture

If either |G| is odd or G has non-cyclic Sylow 2-subgroups, then G has a complete mapping.

They proved this for some special groups such as symmetric and alternating groups.

In 2009, three things happened:

Hall and Paige conjectured the converse:

Conjecture

If either |G| is odd or G has non-cyclic Sylow 2-subgroups, then G has a complete mapping.

They proved this for some special groups such as symmetric and alternating groups.

In 2009, three things happened:

Stuart Wilcox reduced the conjecture to the case of finite simple groups *G*, and dealt with all groups of Lie type except the Tits group ²*F*₄(2)';

Hall and Paige conjectured the converse:

Conjecture

If either |G| is odd or G has non-cyclic Sylow 2-subgroups, then G has a complete mapping.

They proved this for some special groups such as symmetric and alternating groups.

In 2009, three things happened:

- Stuart Wilcox reduced the conjecture to the case of finite simple groups *G*, and dealt with all groups of Lie type except the Tits group ²*F*₄(2)';
- Tony Evans dealt with this group and 25 of the 26 sporadic simple groups;

Hall and Paige conjectured the converse:

Conjecture

If either |G| is odd or G has non-cyclic Sylow 2-subgroups, then G has a complete mapping.

They proved this for some special groups such as symmetric and alternating groups.

In 2009, three things happened:

- Stuart Wilcox reduced the conjecture to the case of finite simple groups *G*, and dealt with all groups of Lie type except the Tits group ²*F*₄(2)';
- Tony Evans dealt with this group and 25 of the 26 sporadic simple groups;
- John Bray handled the remaining sporadic group (the Janko group J₄).

Hall and Paige conjectured the converse:

Conjecture

If either |G| is odd or G has non-cyclic Sylow 2-subgroups, then G has a complete mapping.

They proved this for some special groups such as symmetric and alternating groups.

In 2009, three things happened:

- Stuart Wilcox reduced the conjecture to the case of finite simple groups *G*, and dealt with all groups of Lie type except the Tits group ²*F*₄(2)';
- Tony Evans dealt with this group and 25 of the 26 sporadic simple groups;
- John Bray handled the remaining sporadic group (the Janko group J₄).

So the conjecture was proved, though Bray's proof was not published until 2020.

I will take a small detour here to talk about synchronization, where this topic connects with semigroup theory in a different way.

I will take a small detour here to talk about synchronization, where this topic connects with semigroup theory in a different way.

We consider finite-state automata, very simple machines with a finite set Ω of internal states, which read symbols from an alphabet *A* and change their state to a function of the current state and the symbol read.

I will take a small detour here to talk about synchronization, where this topic connects with semigroup theory in a different way.

We consider finite-state automata, very simple machines with a finite set Ω of internal states, which read symbols from an alphabet *A* and change their state to a function of the current state and the symbol read.

An automaton can read a word in the alphabet and perform a sequence of state changes. It is said to be synchronizing if there is a word (called a reset word) with the property that reading this word brings the automaton to a known state, independent of its starting state.

I will take a small detour here to talk about synchronization, where this topic connects with semigroup theory in a different way.

We consider finite-state automata, very simple machines with a finite set Ω of internal states, which read symbols from an alphabet *A* and change their state to a function of the current state and the symbol read.

An automaton can read a word in the alphabet and perform a sequence of state changes. It is said to be synchronizing if there is a word (called a reset word) with the property that reading this word brings the automaton to a known state, independent of its starting state.

There is an example on the next slide.





It can be verified that **BRRRBRRB** is a reset word (and indeed that it is the shortest possible reset word for this automaton).



It can be verified that BRRRBRRB is a reset word (and indeed that it is the shortest possible reset word for this automaton).

Problem

Show that, if an n-state automaton is synchronizing, it has a reset word of length at most $(n-1)^2$.



It can be verified that **BRRRBRRB** is a reset word (and indeed that it is the shortest possible reset word for this automaton).

Problem

Show that, if an n-state automaton is synchronizing, it has a reset word of length at most $(n-1)^2$.

This is the Černý conjecture, posed in the 1960s and still open.

Automata to transformation semigroups

In a finite automaton with set of states Ω , each letter of the alphabet corresponds to a map from Ω to itself. Reading a word corresponds to the composition of the corresponding maps. Of course the empty word corresponds to the identity transformation.

Automata to transformation semigroups

In a finite automaton with set of states Ω , each letter of the alphabet corresponds to a map from Ω to itself. Reading a word corresponds to the composition of the corresponding maps. Of course the empty word corresponds to the identity transformation.

So an automaton gives rise to a transformation monoid on Ω with a distinguished set of generators (corresponding to the letters in the alphabet).

Automata to transformation semigroups

In a finite automaton with set of states Ω , each letter of the alphabet corresponds to a map from Ω to itself. Reading a word corresponds to the composition of the corresponding maps. Of course the empty word corresponds to the identity transformation.

So an automaton gives rise to a transformation monoid on Ω with a distinguished set of generators (corresponding to the letters in the alphabet).

The automaton is synchronizing if and only if the monoid contains an element of rank 1. So we call a transformation monoid synchronizing if it contains a rank 1 transformation.

A permutation group *G* on Ω cannot be synchronizing (according to the above definition) unless $|\Omega| = 1$. So we re-purpose the term as follows.

A permutation group *G* on Ω cannot be synchronizing (according to the above definition) unless $|\Omega| = 1$. So we re-purpose the term as follows.

The group *G* synchronizes the non-permutation *t* if the monoid $\langle G, t \rangle$ is synchronizing. We also say that the group *G* is synchronizing if it synchronizes every non-permutation on Ω .

A permutation group *G* on Ω cannot be synchronizing (according to the above definition) unless $|\Omega| = 1$. So we re-purpose the term as follows.

The group *G* synchronizes the non-permutation *t* if the monoid $\langle G, t \rangle$ is synchronizing. We also say that the group *G* is synchronizing if it synchronizes every non-permutation on Ω .

Question

Which permutation groups are synchronizing?

A permutation group *G* on Ω cannot be synchronizing (according to the above definition) unless $|\Omega| = 1$. So we re-purpose the term as follows.

The group *G* synchronizes the non-permutation *t* if the monoid $\langle G, t \rangle$ is synchronizing. We also say that the group *G* is synchronizing if it synchronizes every non-permutation on Ω .

Question

Which permutation groups are synchronizing?

I do not intend to give a course on permutation groups here, but in the next slide I will summarise our current knowledge. Synchronizing permutation groups must be primitive (i.e., preserve no non-trivial equivalence relation).

Synchronizing permutation groups must be primitive (i.e., preserve no non-trivial equivalence relation). The primitive groups are classified by the O'Nan–Scott Theorem, which divides them into four types: wreath product, affine, diagonal, or simple. Synchronizing permutation groups must be primitive (i.e., preserve no non-trivial equivalence relation).

The primitive groups are classified by the O'Nan–Scott Theorem, which divides them into four types: wreath product, affine, diagonal, or simple.

Wreath product groups are always non-synchronizing. Affine and almost simple groups may or may not be synchronizing, and we know exactly what happens for degree up to several hundred. Synchronizing permutation groups must be primitive (i.e., preserve no non-trivial equivalence relation).

The primitive groups are classified by the O'Nan–Scott Theorem, which divides them into four types: wreath product, affine, diagonal, or simple.

Wreath product groups are always non-synchronizing. Affine and almost simple groups may or may not be synchronizing, and we know exactly what happens for degree up to several hundred.

The truth of the Hall–Paige conjecture shows:

Theorem

Diagonal groups with more than two factors in the socle are non-synchronizing.
Synchronizing permutation groups must be primitive (i.e., preserve no non-trivial equivalence relation).

The primitive groups are classified by the O'Nan–Scott Theorem, which divides them into four types: wreath product, affine, diagonal, or simple.

Wreath product groups are always non-synchronizing. Affine and almost simple groups may or may not be synchronizing, and we know exactly what happens for degree up to several hundred.

The truth of the Hall–Paige conjecture shows:

Theorem

Diagonal groups with more than two factors in the socle are non-synchronizing.

For two-factor socles, the groups may or may not be synchronizing.

The proof of the Hall–Paige Conjecture used the Classification of Finite Simple Groups.

The proof of the Hall–Paige Conjecture used the Classification of Finite Simple Groups.

Last year, Sean Eberhard, Freddie Manners and Rudi Mrazović posted on the arXiv a paper in which they used analytic number theory to obtain an estimate for the number of complete mappings of a group (this includes an existence proof for sufficiently large groups).

The proof of the Hall–Paige Conjecture used the Classification of Finite Simple Groups.

Last year, Sean Eberhard, Freddie Manners and Rudi Mrazović posted on the arXiv a paper in which they used analytic number theory to obtain an estimate for the number of complete mappings of a group (this includes an existence proof for sufficiently large groups).

This year, Alp Müyesser and Alexey Pokrovskiy posted on the arXiv a proof of a generalization of the Hall–Paige conjecture for large groups (concerning the existence of complete mappings on large subsets of the group), using methods of probabilistic combinatorics.

The proof of the Hall–Paige Conjecture used the Classification of Finite Simple Groups.

Last year, Sean Eberhard, Freddie Manners and Rudi Mrazović posted on the arXiv a paper in which they used analytic number theory to obtain an estimate for the number of complete mappings of a group (this includes an existence proof for sufficiently large groups).

This year, Alp Müyesser and Alexey Pokrovskiy posted on the arXiv a proof of a generalization of the Hall–Paige conjecture for large groups (concerning the existence of complete mappings on large subsets of the group), using methods of probabilistic combinatorics.

But my goal is to speak about semigroups ...

Let *S* be a finite semigroup.

Let *S* be a finite semigroup.

Recall Green's relation \mathcal{J} , an equivalence relation on S defined by $a \mathcal{J} b$ if $S^1 a S^1 = S^1 b S^1$, where S^1 denotes S with an identity adjoined if necessary.

Let *S* be a finite semigroup.

Recall Green's relation \mathcal{J} , an equivalence relation on S defined by $a \mathcal{J} b$ if $S^1 a S^1 = S^1 b S^1$, where S^1 denotes S with an identity adjoined if necessary.

Now let J_a denote the \mathcal{J} -class of a, and add a new element 0 to J_a , with a multiplication defined on this set J_a^0 by

$$u \times v = \begin{cases} uv & \text{if } u, v, uv \in J_a, \\ 0 & \text{otherwise.} \end{cases}$$

Let *S* be a finite semigroup.

Recall Green's relation \mathcal{J} , an equivalence relation on S defined by $a \mathcal{J} b$ if $S^1 a S^1 = S^1 b S^1$, where S^1 denotes S with an identity adjoined if necessary.

Now let J_a denote the \mathcal{J} -class of a, and add a new element 0 to J_a , with a multiplication defined on this set J_a^0 by

$$u imes v = egin{cases} uv & ext{if } u, v, uv \in J_a, \ 0 & ext{otherwise.} \end{cases}$$

Theorem

S has a complete mapping if and only if J_a^0 has a complete mapping for all $a \in S$.

Let *G* be a group and 0 an element not in *G*. Let *I* and Λ be finite index sets, and let *P* be a *I* × Λ matrix with entries from $G \cup \{0\}$. The Rees 0-matrix semigroup with sandwich matrix *P* is the set

$$\mathcal{M}^0[G, I, \Lambda; P] = (I \times G \times \Lambda) \cup \{0\}$$

with 0 a zero element and multiplication of other elements given by

$$(i,g,\lambda)(j,h,\mu) = \begin{cases} (i,gp_{j,\lambda}h,\mu) & \text{if } p_{j,\lambda} \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Let *G* be a group and 0 an element not in *G*. Let *I* and Λ be finite index sets, and let *P* be a *I* × Λ matrix with entries from $G \cup \{0\}$. The Rees 0-matrix semigroup with sandwich matrix *P* is the set

$$\mathcal{M}^0[G, I, \Lambda; P] = (I \times G \times \Lambda) \cup \{0\}$$

with 0 a zero element and multiplication of other elements given by

$$(i,g,\lambda)(j,h,\mu) = \begin{cases} (i,gp_{j,\lambda}h,\mu) & \text{if } p_{j,\lambda} \neq 0, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem (Rees)

Let *S* be a semigroup and $a \in S$. Then either J_a^0 satisfies xy = 0 for all x, y, or J_a^0 is a Rees 0-matrix semigroup.

This reduces our problem to dealing with Rees 0-matrix semigroups.

Recently, one of the organisers of this special session told me that he felt I now qualified as a paid-up semigroup theorist.

Recently, one of the organisers of this special session told me that he felt I now qualified as a paid-up semigroup theorist. Until a little over two years ago, when I started the I am talking about here, I knew what a Rees 0-matrix semigroup is, but I did not know the theorem on the preceding slide.

Recently, one of the organisers of this special session told me that he felt I now qualified as a paid-up semigroup theorist. Until a little over two years ago, when I started the I am talking about here, I knew what a Rees 0-matrix semigroup is, but I did not know the theorem on the preceding slide.

This seems to me to be such an important theorem that I don't see how I could qualify as a semigroup theorist without knowing it.

Recently, one of the organisers of this special session told me that he felt I now qualified as a paid-up semigroup theorist. Until a little over two years ago, when I started the I am talking about here, I knew what a Rees 0-matrix semigroup is, but I did not know the theorem on the preceding slide.

This seems to me to be such an important theorem that I don't see how I could qualify as a semigroup theorist without knowing it.

I don't know how other semigroup theorists feel about this. I have always felt that Sylow's Theorem is the analogous test for someone to be a group theorist.

A Rees matrix semigroup $\mathcal{M}[I, G, \Lambda; P]$ is a Rees 0-matrix semigroup without the 0 – thus every element of *P* belongs to *G*.

A Rees matrix semigroup $\mathcal{M}[I, G, \Lambda; P]$ is a Rees 0-matrix semigroup without the 0 – thus every element of *P* belongs to *G*.

For these we have a definitive result. We say that P is normalized if every element in the first row or column is the identity of G; we may assume this without loss of generality.

A Rees matrix semigroup $\mathcal{M}[I, G, \Lambda; P]$ is a Rees 0-matrix semigroup without the 0 – thus every element of *P* belongs to *G*.

For these we have a definitive result. We say that P is normalized if every element in the first row or column is the identity of G; we may assume this without loss of generality.

Theorem

A Rees matrix semigroup $\mathcal{M}[I, G, \Lambda; P]$ is a Rees 0-matrix semigroup without the 0 – thus every element of *P* belongs to *G*.

For these we have a definitive result. We say that P is normalized if every element in the first row or column is the identity of G; we may assume this without loss of generality.

Theorem

Assume that P is normalized. Then $\mathcal{M}[I, G, \Lambda; P]$ has a complete mapping if and only if one of the following conditions holds:

► |G| is odd;

A Rees matrix semigroup $\mathcal{M}[I, G, \Lambda; P]$ is a Rees 0-matrix semigroup without the 0 – thus every element of *P* belongs to *G*.

For these we have a definitive result. We say that P is normalized if every element in the first row or column is the identity of G; we may assume this without loss of generality.

Theorem

- ► |G| is odd;
- ▶ *G* has non-cyclic Sylow 2-subgroups;

A Rees matrix semigroup $\mathcal{M}[I, G, \Lambda; P]$ is a Rees 0-matrix semigroup without the 0 – thus every element of *P* belongs to *G*.

For these we have a definitive result. We say that P is normalized if every element in the first row or column is the identity of G; we may assume this without loss of generality.

Theorem

- ► |G| is odd;
- ► *G* has non-cyclic Sylow 2-subgroups;
- $|I| \cdot |\Lambda|$ is even;

A Rees matrix semigroup $\mathcal{M}[I, G, \Lambda; P]$ is a Rees 0-matrix semigroup without the 0 – thus every element of *P* belongs to *G*.

For these we have a definitive result. We say that P is normalized if every element in the first row or column is the identity of G; we may assume this without loss of generality.

Theorem

- ► |G| is odd;
- ► *G* has non-cyclic Sylow 2-subgroups;
- $|I| \cdot |\Lambda|$ is even;
- *some element of P has even order.*

A Rees matrix semigroup $\mathcal{M}[I, G, \Lambda; P]$ is a Rees 0-matrix semigroup without the 0 – thus every element of *P* belongs to *G*.

For these we have a definitive result. We say that P is normalized if every element in the first row or column is the identity of G; we may assume this without loss of generality.

Theorem

Assume that P is normalized. Then $\mathcal{M}[I, G, \Lambda; P]$ has a complete mapping if and only if one of the following conditions holds:

- ► |G| is odd;
- ► *G* has non-cyclic Sylow 2-subgroups;
- $|I| \cdot |\Lambda|$ is even;
- *some element of P has even order.*

Note that the first two conditions are necessary and sufficient for *G* to have a complete mapping.

For the forward direction: general arguments about the connection between complete mappings of a semigroup and of its group of units give the result if one of the first two conditions hold.

For the forward direction: general arguments about the connection between complete mappings of a semigroup and of its group of units give the result if one of the first two conditions hold.

For the third we give a direct construction.

For the forward direction: general arguments about the connection between complete mappings of a semigroup and of its group of units give the result if one of the first two conditions hold.

For the third we give a direct construction.

For the fourth, we have to partition the sandwich matrix into pieces and handle them separately; in one case, the pieces are not rectangular, so we have to find a complete mapping in a "partial semigroup".

For the forward direction: general arguments about the connection between complete mappings of a semigroup and of its group of units give the result if one of the first two conditions hold.

For the third we give a direct construction.

For the fourth, we have to partition the sandwich matrix into pieces and handle them separately; in one case, the pieces are not rectangular, so we have to find a complete mapping in a "partial semigroup".

For the converse, we may suppose that G has no complete mapping, so that its Sylow 2-subgroups are cyclic; an easy reduction allows us to assume that G is a cyclic 2-group. Then arguments similar to the one I gave earlier for C_4 apply.

It remains to extend the result to Rees 0-matrix semigroups. We have partial results in the case where the group *G* has a complete mapping.

It remains to extend the result to Rees 0-matrix semigroups. We have partial results in the case where the group *G* has a complete mapping.

Here is what we think holds. The pattern of a sandwich matrix is the matrix obtained by replacing the non-zero elements by 1; it can be regarded as a sandwich matrix over the trivial group.

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

► For any group G which has a complete mapping, and any matrix P over $G \cup \{0\}$ with pattern Q, $\mathcal{M}^0[G, I, \Lambda; P]$ has a complete mapping.

- For any group G which has a complete mapping, and any matrix P over G ∪ {0} with pattern Q, M⁰[G, I, Λ; P] has a complete mapping.
- $\mathcal{M}^0[1, I, \Lambda; Q]$ has a complete mapping.

- ► For any group G which has a complete mapping, and any matrix P over $G \cup \{0\}$ with pattern Q, $\mathcal{M}^0[G, I, \Lambda; P]$ has a complete mapping.
- $\mathcal{M}^0[1, I, \Lambda; Q]$ has a complete mapping.
- ► For any r rows of Q, there are at least r|Λ|/|I| columns with non-zero entries in some of the chosen rows.

- ► For any group G which has a complete mapping, and any matrix P over $G \cup \{0\}$ with pattern Q, $\mathcal{M}^0[G, I, \Lambda; P]$ has a complete mapping.
- $\mathcal{M}^0[1, I, \Lambda; Q]$ has a complete mapping.
- ► For any r rows of Q, there are at least r|Λ|/|I| columns with non-zero entries in some of the chosen rows.
- ► For any s columns of Q, there are at least s|I| / |Λ| rows with non-zero emtries in some of the chosen columns.

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

- ► For any group G which has a complete mapping, and any matrix P over $G \cup \{0\}$ with pattern Q, $\mathcal{M}^0[G, I, \Lambda; P]$ has a complete mapping.
- $\mathcal{M}^0[1, I, \Lambda; Q]$ has a complete mapping.
- For any r rows of Q, there are at least r|Λ|/|I| columns with non-zero entries in some of the chosen rows.
- ► For any s columns of Q, there are at least s|I| / |Λ| rows with non-zero emtries in some of the chosen columns.

We have shown that

$$(a) \Leftrightarrow (b) \Rightarrow (c) \Leftrightarrow (d),$$

and that if $|I| = |\Lambda|$ then all four are equivalent.

Matchings

Those of you who know Philip Hall's Marriage Theorem will probably see that conditions (c) and (d) in the above are connected with this theorem.
Matchings

Those of you who know Philip Hall's Marriage Theorem will probably see that conditions (c) and (d) in the above are connected with this theorem.

In particular, if $|I| = |\Lambda|$ then Hall's Theorem asserts that there is a matching from the rows to the columns of the sandwich matrix so that all elements in the positions picked out are equal to 1. By rearranging the columns, we may assume that these 1s are on the diagonal, and then it is enough to prove the result in the case where *P* is the identity matrix, since adding more 1s cannot hurt us.

Matchings

Those of you who know Philip Hall's Marriage Theorem will probably see that conditions (c) and (d) in the above are connected with this theorem.

In particular, if $|I| = |\Lambda|$ then Hall's Theorem asserts that there is a matching from the rows to the columns of the sandwich matrix so that all elements in the positions picked out are equal to 1. By rearranging the columns, we may assume that these 1s are on the diagonal, and then it is enough to prove the result in the case where *P* is the identity matrix, since adding more 1s cannot hurt us.

So probably the thing we are missing to complete the proof is a combinatorial argument ...

We have some apparently unrelated general results. For example, a short and ingenious argument involving simple manipulations shows:

Theorem

A semigroup which has a complete mapping is regular.

But we have not been able to use this or related results to help answer our question for Rees 0-matrix semigroups, since these are regular ...



... for your attention.