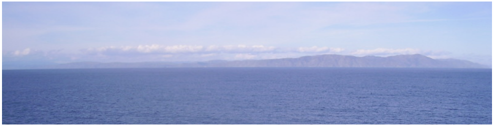
Beyond matroids?
Permutation group bases and Boolean representable complexes

Peter J. Cameron
University of St Andrews



Conference in honour of Geoff Whittle
University of Wellington
December 2015

Happy birthday, Geoff!

Beyond matroids?

There are a number of situations where specially nice cases are matroids, but the general case is more unruly.

Beyond matroids?

There are a number of situations where specially nice cases are matroids, but the general case is more unruly.
For example, minimal generating sets for elementary abelian p-groups are the bases of a matroid, but minimal generating sets for general groups (even abelian groups) do not.

Beyond matroids?

There are a number of situations where specially nice cases are matroids, but the general case is more unruly.
For example, minimal generating sets for elementary abelian p-groups are the bases of a matroid, but minimal generating sets for general groups (even abelian groups) do not.
Thus, the symmetric group S_n can be generated by two elements, but it also has a minimal (with respect to inclusion) generating set of size $n - 1$; and indeed, a theorem of Julius Whiston shows that this is best possible.

Beyond matroids?

There are a number of situations where specially nice cases are matroids, but the general case is more unruly.

For example, minimal generating sets for elementary abelian p-groups are the bases of a matroid, but minimal generating sets for general groups (even abelian groups) do not.

Thus, the symmetric group S_n can be generated by two elements, but it also has a minimal (with respect to inclusion) generating set of size $n-1$; and indeed, a theorem of Julius Whiston shows that this is best possible.

But Philippe Cara and I showed that minimal generating sets of size $n-1$ for S_n are derived from labelled trees on n vertices in a simple way; these objects are not so badly behaved ...

Set families

I will start with a rather general situation involving families of sets.

Set families

I will start with a rather general situation involving families of sets.

This arose from work on the groups which arise as automorphism groups of independence algebras, but Dima Fon-Der-Flaass realised that it could be done much more generally. Note that bases here are ordered.

Set families

I will start with a rather general situation involving families of sets.

This arose from work on the groups which arise as automorphism groups of independence algebras, but Dima Fon-Der-Flaass realised that it could be done much more generally. Note that bases here are ordered.

Let $\mathcal{F} = (F_e : e \in E)$ be a family of subsets of a set X. We use intersection to define a matroid-like structure on E. Thus, we say that an irredundant base is a sequence $(e_1, \ldots, e_k)$ with the properties:

- $\displaystyle\bigcap_{j=1}^{k} F_{e_j} = \bigcap_{e \in E} F_e$;
- for $j = 1, \ldots, k$, F_{e_j} does not contain $\displaystyle\bigcap_{l=1}^{j-1} F_{e_l}$.

Set families

I will start with a rather general situation involving families of sets.

This arose from work on the groups which arise as automorphism groups of independence algebras, but Dima Fon-Der-Flaass realised that it could be done much more generally. Note that bases here are ordered.

Let $\mathcal{F} = (F_e : e \in E)$ be a family of subsets of a set X. We use intersection to define a matroid-like structure on E. Thus, we say that an irredundant base is a sequence $(e_1, \ldots, e_k)$ with the properties:

- $\displaystyle\bigcap_{j=1}^{k} F_{e_j} = \bigcap_{e \in E} F_e$;
- for $j = 1, \ldots, k$, F_{e_j} does not contain $\displaystyle\bigcap_{l=1}^{j-1} F_{e_l}$.

The first condition defines the notion of spanning, the second the notion of independent.

IBIS families

Theorem

For a family $(F_e : e \in E)$ *of sets, the following conditions are equivalent:*

IBIS families

Theorem

For a family $(F_e : e \in E)$ of sets, the following conditions are equivalent:

- *all irredundant bases have the same size;*

IBIS families

Theorem

For a family $(F_e : e \in E)$ *of sets, the following conditions are equivalent:*

- *all irredundant bases have the same size;*
- *the irredundant bases are inariant under re-ordering;*

IBIS families

Theorem

For a family $(F_e : e \in E)$ of sets, the following conditions are equivalent:

- *all irredundant bases have the same size;*
- *the irredundant bases are inariant under re-ordering;*
- *the irredundant bases are the bases of a matroid on E.*

IBIS families

Theorem

For a family $(F_e : e \in E)$ *of sets, the following conditions are equivalent:*

- *all irredundant bases have the same size;*
- *the irredundant bases are inariant under re-ordering;*
- *the irredundant bases are the bases of a matroid on E.*

A family of sets satisfying these three conditions is called an IBIS family (for **I**rredundant **B**ases of **I**nvariant **S**ize).

IBIS families

Theorem

For a family $(F_e : e \in E)$ of sets, the following conditions are equivalent:

- *all irredundant bases have the same size;*
- *the irredundant bases are inariant under re-ordering;*
- *the irredundant bases are the bases of a matroid on E.*

A family of sets satisfying these three conditions is called an IBIS family (for **I**rredundant **B**ases of **I**nvariant **S**ize).

In reverse

A family $\mathcal{S}$ of flats in a matroid is separating if, for every independent set I and every $e \in I$, there is a flat $S \in \mathcal{S}$ such that $I \setminus \{e\} \subseteq S$, $e \notin S$. Note that a set of flats is separating if and only if it contains all hyperplanes.

In reverse

A family $\mathcal{S}$ of flats in a matroid is separating if, for every independent set I and every $e \in I$, there is a flat $S \in \mathcal{S}$ such that $I \setminus \{e\} \subseteq S$, $e \notin S$. Note that a set of flats is separating if and only if it contains all hyperplanes.

Now every IBIS family of sets is obtained by the following construction:

In reverse

A family $\mathcal{S}$ of flats in a matroid is separating if, for every independent set I and every $e \in I$, there is a flat $S \in \mathcal{S}$ such that $I \setminus \{e\} \subseteq S$, $e \notin S$. Note that a set of flats is separating if and only if it contains all hyperplanes.
Now every IBIS family of sets is obtained by the following construction:

- Choose any matroid M;

In reverse

A family $\mathcal{S}$ of flats in a matroid is separating if, for every independent set I and every $e \in I$, there is a flat $S \in \mathcal{S}$ such that $I \setminus \{e\} \subseteq S$, $e \notin S$. Note that a set of flats is separating if and only if it contains all hyperplanes.
Now every IBIS family of sets is obtained by the following construction:

- Choose any matroid M;
- Choose any separating family of flats (each flat can be repeated arbitrarily many times);

In reverse

A family $\mathcal{S}$ of flats in a matroid is separating if, for every independent set I and every $e \in I$, there is a flat $S \in \mathcal{S}$ such that $I \setminus \{e\} \subseteq S$, $e \notin S$. Note that a set of flats is separating if and only if it contains all hyperplanes.
Now every IBIS family of sets is obtained by the following construction:

- Choose any matroid M;
- Choose any separating family of flats (each flat can be repeated arbitrarily many times);
- Take the dual.

In reverse

A family $\mathcal{S}$ of flats in a matroid is separating if, for every independent set I and every $e \in I$, there is a flat $S \in \mathcal{S}$ such that $I \setminus \{e\} \subseteq S$, $e \notin S$. Note that a set of flats is separating if and only if it contains all hyperplanes.
Now every IBIS family of sets is obtained by the following construction:

- Choose any matroid M;
- Choose any separating family of flats (each flat can be repeated arbitrarily many times);
- Take the dual.

In particular, every matroid can be represented by an IBIS family of sets.

Bases for permutation groups

Let G be a permutation group on a set E.

Bases for permutation groups

Let G be a permutation group on a set E.
A base for E is a sequence of points of E whose pointwise stabiliser is trivial.

Bases for permutation groups

Let G be a permutation group on a set E.

A base for E is a sequence of points of E whose pointwise stabiliser is trivial.

A base is irredundant if no point is fixed by the pointwise stabiliser of its predecessors.

Bases for permutation groups

Let G be a permutation group on a set E.
A base for E is a sequence of points of E whose pointwise stabiliser is trivial.
A base is irredundant if no point is fixed by the pointwise stabiliser of its predecessors.
Bases are used in computational group theory: every element of G is uniquely determined by its effect on a base, so a small base gives an efficient representation of group elements.

IBIS groups

Theorem

Let G be a permutation group on E. Then the following are equivalent:

IBIS groups

Theorem

Let G be a permutation group on E. Then the following are equivalent:

- *all irredundant bases for G have the same size;*

IBIS groups

Theorem

Let G be a permutation group on E. Then the following are equivalent:

- *all irredundant bases for G have the same size;*
- *the irredundant bases for G are preserved by re-ordering;*

IBIS groups

Theorem

Let G be a permutation group on E. Then the following are equivalent:

- *all irredundant bases for G have the same size;*
- *the irredundant bases for G are preserved by re-ordering;*
- *the irredundant bases for G are the bases of a matroid.*

IBIS groups

Theorem

Let G be a permutation group on E. Then the following are equivalent:

- *all irredundant bases for G have the same size;*
- *the irredundant bases for G are preserved by re-ordering;*
- *the irredundant bases for G are the bases of a matroid.*

A permutation group satisfying these conditions is called an IBIS group.

The theorem is proved by applying the result about IBIS families to the family of point stabilisers in the group.

IBIS groups

Theorem

Let G be a permutation group on E. Then the following are equivalent:

- *all irredundant bases for G have the same size;*
- *the irredundant bases for G are preserved by re-ordering;*
- *the irredundant bases for G are the bases of a matroid.*

A permutation group satisfying these conditions is called an IBIS group.
The theorem is proved by applying the result about IBIS families to the family of point stabilisers in the group.
The IBIS groups form a generalisation of the automorphism groups of independence algebras.

Open questions

- Which matroids arise from IBIS families of subgroups of a group? (If the family of subgroups is closed under conjugation, then the group can be represented as an IBIS permutation group; not all matroids can occur here.)

Open questions

- Which matroids arise from IBIS families of subgroups of a group? (If the family of subgroups is closed under conjugation, then the group can be represented as an IBIS permutation group; not all matroids can occur here.)
- What about IBIS families of substructures of other kinds of structure (subrings of a ring, sub-Latin squares of a Latin square, etc.)?

Open questions

- Which matroids arise from IBIS families of subgroups of a group? (If the family of subgroups is closed under conjugation, then the group can be represented as an IBIS permutation group; not all matroids can occur here.)
- What about IBIS families of substructures of other kinds of structure (subrings of a ring, sub-Latin squares of a Latin square, etc.)?
- Which set families, or permutation groups, have the weaker property that all minimal bases have the same size? The minimal bases need not be the bases of a matroid in this case; is there a theory of the structures that arise in this way?

Beyond matroids?

I have wondered for some time whether there is a concept more general than a matroid which can encompass, for example, permutation group bases (even if the group is not an IBIS group).

Beyond matroids?

I have wondered for some time whether there is a concept more general than a matroid which can encompass, for example, permutation group bases (even if the group is not an IBIS group).
Recently, Rhodes and Silva have published a book entitled *Boolean Representations of Simplicial Complexes and Matroids*, which leads me to wonder if this is the right place to look.

Beyond matroids?

I have wondered for some time whether there is a concept more general than a matroid which can encompass, for example, permutation group bases (even if the group is not an IBIS group).

Recently, Rhodes and Silva have published a book entitled *Boolean Representations of Simplicial Complexes and Matroids*, which leads me to wonder if this is the right place to look.

The notion of Boolean representable simplicial complexes developed in the book includes all matroids, but not all simplicial complexes; and it is the authors' claim that these objects have a rich structure theory. They invite readers

> to consider the new class of boolean representable simplicial complexes as a brave new world to explore (we believe many of the theorems in matroid theory will extend to boolean representable simplicial complexes).

I haven't learned enough about Boolean representable complexes yet to say for sure that such things as permutation group bases are Boolean representable.

I haven’t learned enough about Boolean representable complexes yet to say for sure that such things as permutation group bases are Boolean representable.
Indeed, there are some difficulties.

I haven't learned enough about Boolean representable complexes yet to say for sure that such things as permutation group bases are Boolean representable.

Indeed, there are some difficulties.

The definitions I gave for both families of sets and permutation group bases had the property that bases were ordered, and re-ordering irredundant bases might destroy the irredundance.

There are some indications that this problem can be got round directly.

I haven't learned enough about Boolean representable complexes yet to say for sure that such things as permutation group bases are Boolean representable.

Indeed, there are some difficulties.

The definitions I gave for both families of sets and permutation group bases had the property that bases were ordered, and re-ordering irredundant bases might destroy the irredundance. There are some indications that this problem can be got round directly.

Another approach might be to choose only, for example, minimal bases for permutation groups, those for which no proper subset is a basis. The analogue of independent sets would then be sets of points such that the pointwise stabiliser of a subset fixes no additional point in the set. I won't pursue this here.

I haven't learned enough about Boolean representable complexes yet to say for sure that such things as permutation group bases are Boolean representable.

Indeed, there are some difficulties.

The definitions I gave for both families of sets and permutation group bases had the property that bases were ordered, and re-ordering irredundant bases might destroy the irredundance. There are some indications that this problem can be got round directly.

Another approach might be to choose only, for example, minimal bases for permutation groups, those for which no proper subset is a basis. The analogue of independent sets would then be sets of points such that the pointwise stabiliser of a subset fixes no additional point in the set. I won't pursue this here.

I will spend the rest of the time on a very brief introduction to Boolean representable complexes. But don't take this as gospel; go and read the book instead!

The boolean and superboolean semirings

A commutative semiring is a structure with addition, multiplication, and elements 0 and 1 such that

- addition and multiplication are commutative and associative and have 0 and 1 respectively as identities;

The boolean and superboolean semirings

A commutative semiring is a structure with addition, multiplication, and elements 0 and 1 such that

- addition and multiplication are commutative and associative and have 0 and 1 respectively as identities;
- multiplication distributes over addition;

The boolean and superboolean semirings

A commutative semiring is a structure with addition, multiplication, and elements 0 and 1 such that

- addition and multiplication are commutative and associative and have 0 and 1 respectively as identities;
- multiplication distributes over addition;
- $a \cdot 0 = 0$ for all a.

The boolean and superboolean semirings

A commutative semiring is a structure with addition, multiplication, and elements 0 and 1 such that

- addition and multiplication are commutative and associative and have 0 and 1 respectively as identities;
- multiplication distributes over addition;
- $a \cdot 0 = 0$ for all a.

The standard example is the semiring of natural numbers $\mathbb{N}$. We form an $(m+1)$-element semiring $\mathbb{N}_m$ by identifying all elements $\geq m$ (this equivalence relation is a congruence on $\mathbb{N}$).

The boolean and superboolean semirings

A commutative semiring is a structure with addition, multiplication, and elements 0 and 1 such that

- addition and multiplication are commutative and associative and have 0 and 1 respectively as identities;
- multiplication distributes over addition;
- $a \cdot 0 = 0$ for all a.

The standard example is the semiring of natural numbers $\mathbb{N}$. We form an $(m+1)$-element semiring $\mathbb{N}_m$ by identifying all elements $\geq m$ (this equivalence relation is a congruence on $\mathbb{N}$). Now the boolean semiring $\mathbb{B}$ is $\mathbb{N}_1$, and the superboolean semiring $\mathbb{SB}$ is $\mathbb{N}_2$.

The boolean and superboolean semirings

A commutative semiring is a structure with addition, multiplication, and elements 0 and 1 such that

- addition and multiplication are commutative and associative and have 0 and 1 respectively as identities;
- multiplication distributes over addition;
- $a \cdot 0 = 0$ for all a.

The standard example is the semiring of natural numbers $\mathbb{N}$.
We form an $(m+1)$-element semiring $\mathbb{N}_m$ by identifying all elements $\geq m$ (this equivalence relation is a congruence on $\mathbb{N}$).
Now the boolean semiring $\mathbb{B}$ is $\mathbb{N}_1$, and the superboolean semiring $\mathbb{SB}$ is $\mathbb{N}_2$.
Note that $\mathbb{B}$ is not a subsemiring of $\mathbb{SB}$; it is a quotient of it.

The addition and multiplication tables of $\mathbb{B}$ are

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

Note that it can be identified with the usual Boolean algebra on $\{0, 1\}$, with $+$ as join and $\cdot$ as meet.

The addition and multiplication tables of $\mathbb{B}$ are

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

Note that it can be identified with the usual Boolean algebra on $\{0,1\}$, with $+$ as join and $\cdot$ as meet.
The tables for $\mathbb{SB}$ are

$+$	0	1	2
0	0	1	2
1	1	2	2
2	2	2	2

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	2

Representability

The set $\mathcal{G} = \{0, 2\} \subset \mathbb{SB}$ is called the ghost ideal.

Representability

The set $\mathcal{G} = \{0, 2\} \subset \mathbb{SB}$ is called the ghost ideal.
A set of n-vectors $v_1, \ldots, v_m \in \mathbb{SB}^n$ is independent if, for all $\lambda_1, \ldots, \lambda_m \in \{0, 1\}$,

$$\lambda_1 v_1 + \cdots + \lambda_m v_m \in \mathcal{G}^n \Rightarrow \lambda_1 = \ldots = \lambda_m = 0.$$

Representability

The set $\mathcal{G} = \{0, 2\} \subset \mathbb{SB}$ is called the ghost ideal.
A set of n-vectors $v_1, \ldots, v_m \in \mathbb{SB}^n$ is independent if, for all $\lambda_1, \ldots, \lambda_m \in \{0, 1\}$,

$$\lambda_1 v_1 + \cdots + \lambda_m v_m \in \mathcal{G}^n \Rightarrow \lambda_1 = \ldots = \lambda_m = 0.$$

Now it can be shown quite easily that a square matrix has independent columns (or rows) if and only if it can be put into lower unitriangular form by row and column permutations, and this holds if and only if its permanent is 1.

Representability

The set $\mathcal{G} = \{0, 2\} \subset \mathbb{SB}$ is called the ghost ideal.
A set of n-vectors $v_1, \ldots, v_m \in \mathbb{SB}^n$ is independent if, for all $\lambda_1, \ldots, \lambda_m \in \{0, 1\}$,

$$\lambda_1 v_1 + \cdots + \lambda_m v_m \in \mathcal{G}^n \Rightarrow \lambda_1 = \ldots = \lambda_m = 0.$$

Now it can be shown quite easily that a square matrix has independent columns (or rows) if and only if it can be put into lower unitriangular form by row and column permutations, and this holds if and only if its permanent is 1.
A superboolean representation of a simplicial complex is a matrix whose independent sets of columns are the simplices. A boolean representation is one given by a matrix with entries 0 and 1 only. Note that even in the boolean case, independence is defined over $\mathbb{SB}$.

A small example

Let G be the cyclic group of order 6 generated by

$$(1,4)(2,5,6)(3,7,8,9,10,11).$$

The irredundant bases are, up to parallel elements, $(1,2)$ and (3). So the "independent sets" are the empty set, the singletons, and $\{1,2\}$.

Define a matrix with rows and columns indexed by $1,2,3$, with (i,j) entry 1 if $G_i = G_j$, 2 if $G_i < G_j$ or *vice versa*, and 0 if G_i and G_j are incomparable. The matrix is

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 2 & 2 & 1 \end{pmatrix}.$$

A small example

Let G be the cyclic group of order 6 generated by

$$(1,4)(2,5,6)(3,7,8,9,10,11).$$

The irredundant bases are, up to parallel elements, $(1,2)$ and (3). So the "independent sets" are the empty set, the singletons, and $\{1,2\}$.
Define a matrix with rows and columns indexed by $1,2,3$, with (i,j) entry 1 if $G_i = G_j$, 2 if $G_i < G_j$ or *vice versa*, and 0 if G_i and G_j are incomparable. The matrix is

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 2 & 2 & 1 \end{pmatrix}.$$

The independent sets of rows (as defined earlier) are precisely the ones we want! So at least some non-IBIS groups arise.

A small example

Let G be the cyclic group of order 6 generated by

$$(1,4)(2,5,6)(3,7,8,9,10,11).$$

The irredundant bases are, up to parallel elements, $(1,2)$ and (3). So the "independent sets" are the empty set, the singletons, and $\{1,2\}$.

Define a matrix with rows and columns indexed by $1,2,3$, with (i,j) entry 1 if $G_i = G_j$, 2 if $G_i < G_j$ or *vice versa*, and 0 if G_i and G_j are incomparable. The matrix is

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & 1 & 2 \\ 2 & 2 & 1 \end{pmatrix}.$$

The independent sets of rows (as defined earlier) are precisely the ones we want! So at least some non-IBIS groups arise.

Warning: This is a superboolean, not a boolean representation. Also, this simple construction doesn't work for all permutation group bases!

Which complexes are representable?

Theorem

- *Every simplicial complex is superboolean representable.*

Which complexes are representable?

Theorem

- *Every simplicial complex is superboolean representable.*
- *Not every simplicial complex is boolean representable.*

Which complexes are representable?

Theorem

- *Every simplicial complex is superboolean representable.*
- *Not every simplicial complex is boolean representable.*
- *Every matroid is boolean representable.*

Which complexes are representable?

Theorem

- *Every simplicial complex is superboolean representable.*
- *Not every simplicial complex is boolean representable.*
- *Every matroid is boolean representable.*

So the general question is:

> *How much of matroid theory can be done for boolean representable simplicial complexes? More generally, how can matroid theory guide the development of this new theory?*

Which complexes are representable?

Theorem

- *Every simplicial complex is superboolean representable.*
- *Not every simplicial complex is boolean representable.*
- *Every matroid is boolean representable.*

So the general question is:

> *How much of matroid theory can be done for boolean representable simplicial complexes? More generally, how can matroid theory guide the development of this new theory?*

And with that I had better stop, and repeat …

Which complexes are representable?

Theorem

- *Every simplicial complex is superboolean representable.*
- *Not every simplicial complex is boolean representable.*
- *Every matroid is boolean representable.*

So the general question is:

> *How much of matroid theory can be done for boolean representable simplicial complexes? More generally, how can matroid theory guide the development of this new theory?*

And with that I had better stop, and repeat …

Happy birthday Geoff!