# Bases for structures and permutation groups

Peter J. Cameron

Babai60
Columbus, OH, USA
March 2010

# Fixed-point-free permutations

Input: A set $S$ of permutations of $\{1, \ldots, n\}$.

Problem: Does $G = \langle S \rangle$ contain a fixed-point-free element?

# Fixed-point-free permutations

Input: A set $S$ of permutations of $\{1, \ldots, n\}$.

Problem: Does $G = \langle S \rangle$ contain a fixed-point-free element?

This problem is NP-complete in general.

# Fixed-point-free permutations

Input: A set $S$ of permutations of $\{1, \ldots, n\}$.

Problem: Does $G = \langle S \rangle$ contain a fixed-point-free element?

This problem is NP-complete in general.
However, if we are promised that $G$ is transitive, then it has a constant-time algorithm

# Fixed-point-free permutations

Input: A set $S$ of permutations of $\{1, \ldots, n\}$.

Problem: Does $G = \langle S \rangle$ contain a fixed-point-free element?

This problem is NP-complete in general.
However, if we are promised that $G$ is transitive, then it has a constant-time algorithm (Jordan 1873)

# Fixed-point-free permutations

Input: A set $S$ of permutations of $\{1, \ldots, n\}$.

Problem: Does $G = \langle S \rangle$ contain a fixed-point-free element?

This problem is NP-complete in general.
However, if we are promised that $G$ is transitive, then it has a constant-time algorithm (Jordan 1873)

# Fixed-point-free permutations, 2

Now let's change the problem to

Input: A set $S$ of permutations of $\{1, \ldots, n\}$, generating a transitive group.

Problem: Find a fixed-point-free element in $G$.

# Fixed-point-free permutations, 2

Now let's change the problem to

> Input: A set $S$ of permutations of $\{1, \ldots, n\}$, generating a transitive group.
>
> Problem: Find a fixed-point-free element in $G$.

This is in RP

# Fixed-point-free permutations, 2

Now let's change the problem to

Input: A set $S$ of permutations of $\{1, \ldots, n\}$, generating a transitive group.

Problem: Find a fixed-point-free element in $G$.

This is in RP (Cameron and Cohen 1993)

# Fixed-point-free permutations, 2

Now let's change the problem to

> Input: A set $S$ of permutations of $\{1, \ldots, n\}$, generating a transitive group.
>
> Problem: Find a fixed-point-free element in $G$.

This is in RP (Cameron and Cohen 1993)
In fact it is in P, but the proof uses the Classification of Finite Simple Groups.

# Fixed-point-free permutations, 2

Now let's change the problem to

> Input: A set $S$ of permutations of $\{1, \ldots, n\}$, generating a transitive group.
>
> Problem: Find a fixed-point-free element in $G$.

This is in RP (Cameron and Cohen 1993)
In fact it is in P, but the proof uses the Classification of Finite Simple Groups.
Is this really necessary?

# Bases

A base for a structure $S$ should be a list $B$ of elements of $S$ with the property that every element of $S$ is uniquely specified by its relationship to the elements in $B$.

# Bases

A base for a structure $S$ should be a list $B$ of elements of $S$ with the property that every element of $S$ is uniquely specified by its relationship to the elements in $B$.
For example, a basis in a vector space has the property that different vectors have different expressions as linear combinations of basis vectors.

# Bases for permutation groups

If $G$ is a permutation group on a set $\Omega$, a base for $G$ is a list $B$ of elements of $\Omega$ whose pointwise stabiliser in $G$ is the identity.

# Bases for permutation groups

If $G$ is a permutation group on a set $\Omega$, a base for $G$ is a list $B$ of elements of $\Omega$ whose pointwise stabiliser in $G$ is the identity.

Our philosophy is:

> *A list of points of the structure $S$ which is a base for the automorphism group of $S$ should be in some sense a base for $S$.*

# Bases for permutation groups

If $G$ is a permutation group on a set $\Omega$, a base for $G$ is a list $B$ of elements of $\Omega$ whose pointwise stabiliser in $G$ is the identity.

Our philosophy is:

> *A list of points of the structure $S$ which is a base for the automorphism group of $S$ should be in some sense a base for $S$.*

That is: *If we cannot move $x$ to $y$ by an automorphism fixing $B$ pointwise, this is because the structures of $(S, [B, x])$ and $(S, [B, y])$ are different.*

# Bases for permutation groups

If $G$ is a permutation group on a set $\Omega$, a base for $G$ is a list $B$ of elements of $\Omega$ whose pointwise stabiliser in $G$ is the identity. Our philosophy is:

> *A list of points of the structure $S$ which is a base for the automorphism group of $S$ should be in some sense a base for $S$.*

That is: *If we cannot move $x$ to $y$ by an automorphism fixing $B$ pointwise, this is because the structures of $(S, [B, x])$ and $(S, [B, y])$ are different.*
We'd like to have an efficient method to recognise this difference. This would have practical implications for graph isomorphism, as well as its theoretical interest.

# Bases, determining sets, metric dimension, . . .

The notion of a base, and various combinatorial variants on it, have been rediscovered many times in different parts of combinatorics, especially graph theory: base size has been called fixing number, determining number, rigidity index, etc.

# Bases, determining sets, metric dimension, . . .

The notion of a base, and various combinatorial variants on it, have been rediscovered many times in different parts of combinatorics, especially graph theory: base size has been called fixing number, determining number, rigidity index, etc. Robert Bailey and I have written a survey paper attempting to describe all these and related concepts and results:

# Bases, determining sets, metric dimension, ...

The notion of a base, and various combinatorial variants on it, have been rediscovered many times in different parts of combinatorics, especially graph theory: base size has been called fixing number, determining number, rigidity index, etc. Robert Bailey and I have written a survey paper attempting to describe all these and related concepts and results:

- Robert F. Bailey and Peter J. Cameron, Base size, metric dimension and other invariants of groups and graphs, preprint (available from

`http://www.math.uregina.ca/~bailey/papers/basesize_metdim.pdf`

# Bases, determining sets, metric dimension, ...

The notion of a base, and various combinatorial variants on it, have been rediscovered many times in different parts of combinatorics, especially graph theory: base size has been called fixing number, determining number, rigidity index, etc. Robert Bailey and I have written a survey paper attempting to describe all these and related concepts and results:

- Robert F. Bailey and Peter J. Cameron, Base size, metric dimension and other invariants of groups and graphs, preprint (available from

http://www.math.uregina.ca/~bailey/papers/basesize_metdim.pdf

A set $S$ of vertices is a determining set for a graph if different points outside $S$ have different neighbour sets in $S$. The determining number is the size of the smallest such set.

# Base size for permutation groups

If the permutation group $G$ on $\Omega$ (where $|\Omega| = n$) has a base of size $b$, then $|G| \leq n^b$. Moreover, if $B$ is a base of minimum size, then $|G| \geq 2^b$.

# Base size for permutation groups

If the permutation group $G$ on $\Omega$ (where $|\Omega| = n$) has a base of size $b$, then $|G| \leq n^b$. Moreover, if $B$ is a base of minimum size, then $|G| \geq 2^b$.
In other words, $\log_n(G) \leq b(G) \leq \log_2(G)$, where $b(G)$ is the minimum base size of $G$.

# Base size for permutation groups

If the permutation group $G$ on $\Omega$ (where $|\Omega| = n$) has a base of size $b$, then $|G| \leq n^b$. Moreover, if $B$ is a base of minimum size, then $|G| \geq 2^b$.
In other words, $\log_n(G) \leq b(G) \leq \log_2(G)$, where $b(G)$ is the minimum base size of $G$.
Thus base size is closely connected with order of permutation groups, a very important concern of nineteenth-century group theory.

# Base size for permutation groups

If the permutation group $G$ on $\Omega$ (where $|\Omega| = n$) has a base of size $b$, then $|G| \leq n^b$. Moreover, if $B$ is a base of minimum size, then $|G| \geq 2^b$.
In other words, $\log_n(G) \leq b(G) \leq \log_2(G)$, where $b(G)$ is the minimum base size of $G$.
Thus base size is closely connected with order of permutation groups, a very important concern of nineteenth-century group theory.
Clearly any determining set for a graph is a base for its automorphism group; so the minimal base size does not exceed the determining number.

# Babai's Theorem

One of the most dramatic developments in the theory of permutation group bases came when Laci Babai applied techniques of probabilistic combinatorics to the problem in 1980.

# Babai's Theorem

One of the most dramatic developments in the theory of permutation group bases came when Laci Babai applied techniques of probabilistic combinatorics to the problem in 1980.
The central result can be summarised like this.

# Babai's Theorem

One of the most dramatic developments in the theory of permutation group bases came when Laci Babai applied techniques of probabilistic combinatorics to the problem in 1980.
The central result can be summarised like this.

**Theorem**
*Let $G$ be a primitive but not 2-transitive permutation group of degree $n$. Then, for any pair $x, y$ of distinct points, there are at least $(\sqrt{n}-1)/2$ points $z$ for which $(x,z)$ and $(y,z)$ lie in different $G$-orbits.*

# Babai's Theorem

One of the most dramatic developments in the theory of permutation group bases came when Laci Babai applied techniques of probabilistic combinatorics to the problem in 1980.
The central result can be summarised like this.

### Theorem

*Let $G$ be a primitive but not 2-transitive permutation group of degree $n$. Then, for any pair $x, y$ of distinct points, there are at least $(\sqrt{n} - 1)/2$ points $z$ for which $(x, z)$ and $(y, z)$ lie in different $G$-orbits.*

This is proved by a detailed analysis of the coherent configuration associated with $G$. (I say more about coherent configurations later.)

# Babai's Theorem, 2

Now consider the hypergraph whose vertices are the pairs of points of $\Omega$, and whose edges are indexed by points of $\Omega$; the edge labelled $z$ consists of the pairs "distinguished" by $z$. A theorem of Lovász shows that there are $b = 4\sqrt{n}\log n$ edges which cover all vertices – these edges can be chosen at random and cover with non-zero probability.

# Babai's Theorem, 2

Now consider the hypergraph whose vertices are the pairs of points of $\Omega$, and whose edges are indexed by points of $\Omega$; the edge labelled $z$ consists of the pairs "distinguished" by $z$. A theorem of Lovász shows that there are $b = 4\sqrt{n}\log n$ edges which cover all vertices – these edges can be chosen at random and cover with non-zero probability.
The corresponding $b$ points of $\Omega$ form a base; so $|G| \leq n^b$.

# Babai's Theorem, 2

Now consider the hypergraph whose vertices are the pairs of points of $\Omega$, and whose edges are indexed by points of $\Omega$; the edge labelled $z$ consists of the pairs "distinguished" by $z$. A theorem of Lovász shows that there are $b = 4\sqrt{n}\log n$ edges which cover all vertices – these edges can be chosen at random and cover with non-zero probability.
The corresponding $b$ points of $\Omega$ form a base; so $|G| \leq n^b$.

The bound is best possible up to a factor of $c \log n$ in the exponent.

# The $\log n$ factor

In situations like this we expect a $\log n$ factor. The simplest possible example is the following:

### Theorem

*Suppose that a k-uniform hypergraph on n points has a vertex-transitive automorphism group. Then there is a set of at most $(n/k)\log n$ edges that cover the vertex set.*

# The $\log n$ factor

In situations like this we expect a $\log n$ factor. The simplest possible example is the following:

## Theorem

*Suppose that a k-uniform hypergraph on n points has a vertex-transitive automorphism group. Then there is a set of at most* $(n/k)\log n$ *edges that cover the vertex set.*

Choose $m$ images of a fixed edge under random automorphisms. The probability of a given vertex being uncovered is $(1 - k/n)^m$, and so the expected number of uncovered vertices is $n(1 - k/n)^m$. If this is less than 1, then there is a choice with no uncovered vertices.

# The $\log n$ factor

In situations like this we expect a $\log n$ factor. The simplest possible example is the following:

### Theorem

*Suppose that a k-uniform hypergraph on n points has a vertex-transitive automorphism group. Then there is a set of at most* $(n/k)\log n$ *edges that cover the vertex set.*

Choose $m$ images of a fixed edge under random automorphisms. The probability of a given vertex being uncovered is $(1 - k/n)^m$, and so the expected number of uncovered vertices is $n(1 - k/n)^m$. If this is less than 1, then there is a choice with no uncovered vertices.
Can we get rid of it by more intricate combinatorics?

# Symmetry and logic, 1

One of the most remarkable theorems about symmetry for finite and countably infinite structures was proved by Engeler, Ryll-Nardzewski and Svenonius in 1959. Structures here are allowed to have relations (graphs, orders, hypergraphs) and functions (groups, rings). All structures are (at most) countable.

# Symmetry and logic, 1

One of the most remarkable theorems about symmetry for finite and countably infinite structures was proved by Engeler, Ryll-Nardzewski and Svenonius in 1959. Structures here are allowed to have relations (graphs, orders, hypergraphs) and functions (groups, rings). All structures are (at most) countable.

A structure $M$ is countably categorical if any (at most) countable structure $N$ satisfying the same first-order sentences as $M$ is isomorphic to $M$.

# Symmetry and logic, 1

One of the most remarkable theorems about symmetry for finite and countably infinite structures was proved by Engeler, Ryll-Nardzewski and Svenonius in 1959. Structures here are allowed to have relations (graphs, orders, hypergraphs) and functions (groups, rings). All structures are (at most) countable.
A structure $M$ is countably categorical if any (at most) countable structure $N$ satisfying the same first-order sentences as $M$ is isomorphic to $M$.
In other words, such a structure can be specified up to isomorphism by first-order axioms and the requirement of countability.

# Symmetry and logic, 1

One of the most remarkable theorems about symmetry for finite and countably infinite structures was proved by Engeler, Ryll-Nardzewski and Svenonius in 1959. Structures here are allowed to have relations (graphs, orders, hypergraphs) and functions (groups, rings). All structures are (at most) countable.

A structure $M$ is countably categorical if any (at most) countable structure $N$ satisfying the same first-order sentences as $M$ is isomorphic to $M$.

In other words, such a structure can be specified up to isomorphism by first-order axioms and the requirement of countability.

Cantor's theorem shows that $(\mathbb{Q}, <)$ is countably categorical (it is the unique countable dense total order without endpoints).

# Symmetry and logic, 2

A permutation group $G$ on $\Omega$ is oligomorphic if it has only finitely many orbits on $\Omega^n$ for all $n$.

# Symmetry and logic, 2

A permutation group $G$ on $\Omega$ is oligomorphic if it has only finitely many orbits on $\Omega^n$ for all $n$.
Such a group is "large", in a sense: we are excluding things like Frobenius groups.

# Symmetry and logic, 2

A permutation group $G$ on $\Omega$ is oligomorphic if it has only finitely many orbits on $\Omega^n$ for all $n$.
Such a group is "large", in a sense: we are excluding things like Frobenius groups.
The group of order-preserving permutations of $\mathbb{Q}$ is oligomorphic: two $n$-tuples of distinct elements lie in the same orbit if and only if they are themselves order-isomorphic – we can extend the order-isomorphism to a piecewise-linear map on $\mathbb{Q}$ – so there are $n!$ orbits on $n$-tuples of distinct elements.

# Symmetry and logic, 3

### Theorem

*A structure $M$ (at most countable) is countably categorical if and only if its automorphism group is oligomorphic.*

# Symmetry and logic, 3

### Theorem

*A structure $M$ (at most countable) is countably categorical if and only if its automorphism group is oligomorphic.*

In other words, for countable structures, a high degree of symmetry is equivalent to axiomatisability!

# Symmetry and logic, 3

### Theorem

*A structure $M$ (at most countable) is countably categorical if and only if its automorphism group is oligomorphic.*

In other words, for countable structures, a high degree of symmetry is equivalent to axiomatisability!

More is true. If $M$ is countably categorical, then two $n$-tuples lie in the same orbit of $\mathrm{Aut}(M)$ if and only if they satisfy the same first-order formulae (that is, they have the same first-order type).

# Symmetry and logic, 4

This wonderful theorem about the countably infinite tells us nothing about the finite.

# Symmetry and logic, 4

This wonderful theorem about the countably infinite tells us nothing about the finite.

- Every finite permutation group is oligomorphic.

# Symmetry and logic, 4

This wonderful theorem about the countably infinite tells us nothing about the finite.

- Every finite permutation group is oligomorphic.
- Every finite first-order structure is categorical.

# Symmetry and logic, 4

This wonderful theorem about the countably infinite tells us nothing about the finite.

- Every finite permutation group is oligomorphic.
- Every finite first-order structure is categorical.

Indeed, if the automorphism group of the $n$-element structure $M$ has a base of size $k$, then every point of $M$ is uniquely identified by a formula having the elements of the base as parameters.

# Symmetry and logic, 4

This wonderful theorem about the countably infinite tells us nothing about the finite.

- Every finite permutation group is oligomorphic.
- Every finite first-order structure is categorical.

Indeed, if the automorphism group of the $n$-element structure $M$ has a base of size $k$, then every point of $M$ is uniquely identified by a formula having the elements of the base as parameters.
So our philosophical principle holds for first-order structure.

# Symmetry and regularity, 1

Is there a simpler type of formula which detects symmetry of a graph, for example? For example, can we bound the number of variables?

# Symmetry and regularity, 1

Is there a simpler type of formula which detects symmetry of a graph, for example? For example, can we bound the number of variables?

A graph is said to be $t$-strongly regular if, for any set $S$ of vertices with $|S| \leq t$, the number of common neighbours of $S$ depends only on the isomorphism type of the induced subgraph on $S$.

# Symmetry and regularity, 1

Is there a simpler type of formula which detects symmetry of a graph, for example? For example, can we bound the number of variables?

A graph is said to be $t$-strongly regular if, for any set $S$ of vertices with $|S| \leq t$, the number of common neighbours of $S$ depends only on the isomorphism type of the induced subgraph on $S$.

- Every graph is 0-strongly regular.

# Symmetry and regularity, 1

Is there a simpler type of formula which detects symmetry of a graph, for example? For example, can we bound the number of variables?

A graph is said to be $t$-strongly regular if, for any set $S$ of vertices with $|S| \leq t$, the number of common neighbours of $S$ depends only on the isomorphism type of the induced subgraph on $S$.

- Every graph is 0-strongly regular.
- A graph is 1-strongly regular if and only if it is regular.

# Symmetry and regularity, 1

Is there a simpler type of formula which detects symmetry of a graph, for example? For example, can we bound the number of variables?

A graph is said to be $t$-strongly regular if, for any set $S$ of vertices with $|S| \leq t$, the number of common neighbours of $S$ depends only on the isomorphism type of the induced subgraph on $S$.

- Every graph is 0-strongly regular.
- A graph is 1-strongly regular if and only if it is regular.
- A graph is 2-strongly regular if and only if it is strongly regular in the usual sense.

# Symmetry and regularity, 1

Is there a simpler type of formula which detects symmetry of a graph, for example? For example, can we bound the number of variables?

A graph is said to be $t$-strongly regular if, for any set $S$ of vertices with $|S| \leq t$, the number of common neighbours of $S$ depends only on the isomorphism type of the induced subgraph on $S$.

- Every graph is 0-strongly regular.
- A graph is 1-strongly regular if and only if it is regular.
- A graph is 2-strongly regular if and only if it is strongly regular in the usual sense.

In these cases, almost all such structures have no non-trivial automorphisms.

# Digression

It is not easy to make sense of the statement "almost all strongly regular graphs have trivial automorphism group". Here are two relevant pieces of information.

# Digression

It is not easy to make sense of the statement "almost all strongly regular graphs have trivial automorphism group". Here are two relevant pieces of information.

- A theorem of Neumaier shows that strongly regular graphs with least eigenvalue $-m$ (an integer) are complete multipartite with parts of size $m$, or line graphs of linear spaces or transversal designs with block size $m$, or one of a finite list $\mathcal{L}(m)$ of exceptions. Laci Babai showed that almost all Steiner triple systems (linear spaces with block size 3) have trivial automorphism group; the same is true for Latin squares (equivalent to transversal designs with block size 3).

# Digression

It is not easy to make sense of the statement "almost all strongly regular graphs have trivial automorphism group". Here are two relevant pieces of information.

- A theorem of Neumaier shows that strongly regular graphs with least eigenvalue $-m$ (an integer) are complete multipartite with parts of size $m$, or line graphs of linear spaces or transversal designs with block size $m$, or one of a finite list $\mathcal{L}(m)$ of exceptions. Laci Babai showed that almost all Steiner triple systems (linear spaces with block size 3) have trivial automorphism group; the same is true for Latin squares (equivalent to transversal designs with block size 3).
- There are known to be 32548 strongly regular graphs with parameters $(36, 15, 6, 6)$; all but 11 of them belong to the list $\mathcal{L}(3)$. Most have trivial automorphism group (but I don't have the exact number).

# Symmetry and regularity, 2

A graph is $t$-homogeneous if any isomorphism between sets of at most $t$ vertices can be extended to an automorphism of the graph. Clearly $t$-homogeneity implies $t$-strong regularity.

# Symmetry and regularity, 2

A graph is *$t$-homogeneous* if any isomorphism between sets of at most $t$ vertices can be extended to an automorphism of the graph. Clearly $t$-homogeneity implies $t$-strong regularity.

Theorem

*A 5-strongly regular graph is $t$-homogeneous for all $t$.*

# Symmetry and regularity, 2

A graph is *t-homogeneous* if any isomorphism between sets of at most $t$ vertices can be extended to an automorphism of the graph. Clearly $t$-homogeneity implies $t$-strong regularity.

**Theorem**

*A 5-strongly regular graph is $t$-homogeneous for all $t$.*

The proof involves determining by combinatorial methods the 5-strongly regular graphs and showing that the class coincides with the class of homogeneous graphs determined by Sheehan and Gardiner.

# Symmetry and regularity, 2

A graph is *$t$-homogeneous* if any isomorphism between sets of at most $t$ vertices can be extended to an automorphism of the graph. Clearly $t$-homogeneity implies $t$-strong regularity.

Theorem

*A 5-strongly regular graph is $t$-homogeneous for all $t$.*

The proof involves determining by combinatorial methods the 5-strongly regular graphs and showing that the class coincides with the class of homogeneous graphs determined by Sheehan and Gardiner.

This and some related results suggest that perhaps there is an absolute bound on the number of variables required in formulae "labelling" the vertices of a graph in terms of a base for its automorphism group.

# A test case: Paley graphs

Let $q$ be a prime power congruent to 1 mod 4. (Then $-1$ is a square in the field $\mathbb{F}_q$.) The Paley graph $P_q$ has as vertex set the field $\mathbb{F}_q$, with an edge from $x$ to $y$ if and only if $y - x$ is a non-zero square in $\mathbb{F}_q$. (The remark shows that this is a symmetric relation.)

# A test case: Paley graphs

Let $q$ be a prime power congruent to 1 mod 4. (Then $-1$ is a square in the field $\mathbb{F}_q$.) The Paley graph $P_q$ has as vertex set the field $\mathbb{F}_q$, with an edge from $x$ to $y$ if and only if $y - x$ is a non-zero square in $\mathbb{F}_q$. (The remark shows that this is a symmetric relation.)

The automorphism group of $P_q$ is the group

$$\{x \mapsto ax^\sigma + b : a, b \in \mathbb{F}_q, a \neq 0, a \text{ square}, \sigma \in \mathrm{Aut}(\mathbb{F}_q)\}.$$

# A test case: Paley graphs

Let $q$ be a prime power congruent to 1 mod 4. (Then $-1$ is a square in the field $\mathbb{F}_q$.) The Paley graph $P_q$ has as vertex set the field $\mathbb{F}_q$, with an edge from $x$ to $y$ if and only if $y - x$ is a non-zero square in $\mathbb{F}_q$. (The remark shows that this is a symmetric relation.)

The automorphism group of $P_q$ is the group

$$\{x \mapsto ax^\sigma + b : a, b \in \mathbb{F}_q, a \neq 0, a \text{ square}, \sigma \in \mathrm{Aut}(\mathbb{F}_q)\}.$$

Hence

- If $q$ is prime, then any two points form a base;

# A test case: Paley graphs

Let $q$ be a prime power congruent to 1 mod 4. (Then $-1$ is a square in the field $\mathbb{F}_q$.) The Paley graph $P_q$ has as vertex set the field $\mathbb{F}_q$, with an edge from $x$ to $y$ if and only if $y - x$ is a non-zero square in $\mathbb{F}_q$. (The remark shows that this is a symmetric relation.)

The automorphism group of $P_q$ is the group

$$\{x \mapsto ax^\sigma + b : a, b \in \mathbb{F}_q, a \neq 0, a \text{ square}, \sigma \in \mathrm{Aut}(\mathbb{F}_q)\}.$$

Hence

- If $q$ is prime, then any two points form a base;
- Otherwise, some well-chosen triples form bases, but if we choose badly we might need as many as $\sqrt{q} + 1$ points in a base.

# Digression

Dima Fon-Der-Flaass and I investigated, among other things, which groups have the property that every set of size $k$ is a minimal base. We showed:

# Digression

Dima Fon-Der-Flaass and I investigated, among other things, which groups have the property that every set of size $k$ is a minimal base. We showed:

### Theorem

*Let $G$ be a permutation group with the property that any set of $k$ points is a minimal base. Then $G$ is $(k-1)$-transitive. In particular, if $k \geq 5$, then $G$ is sharply $k$-transitive (and so is $S_k$, $S_{k+1}$, $A_{k+2}$, or $M_{12}$ for $k = 5$).*

# Digression

Dima Fon-Der-Flaass and I investigated, among other things, which groups have the property that every set of size $k$ is a minimal base. We showed:

### Theorem

*Let $G$ be a permutation group with the property that any set of $k$ points is a minimal base. Then $G$ is $(k-1)$-transitive. In particular, if $k \geq 5$, then $G$ is sharply $k$-transitive (and so is $S_k$, $S_{k+1}$, $A_{k+2}$, or $M_{12}$ for $k = 5$).*

For $k = 2, 3$ we have Frobenius and Zassenhaus groups respectively.

# Paley graphs

It turns out that the determining number for Paley graphs is about $\log q$.

# Paley graphs

It turns out that the determining number for Paley graphs is about $\log q$.
A different approach was proposed by Evdokimov and Ponomarenko, using the notion of coherent configuration (which of course also occurs in Babai's classic proof). This notion was developed by Donald Higman in the west and Boris Weisfeiler in the Soviet Union from the notion of association scheme in statistics.

# Coherent configurations

A coherent configuration on $\Omega$ is a partition $C$ of $\Omega \times \Omega$ satisfying the following conditions:

# Coherent configurations

A coherent configuration on $\Omega$ is a partition $C$ of $\Omega \times \Omega$ satisfying the following conditions:

- the diagonal is a union of parts of $C$;

# Coherent configurations

A coherent configuration on $\Omega$ is a partition $C$ of $\Omega \times \Omega$ satisfying the following conditions:

- the diagonal is a union of parts of $C$;
- the converse of a part of $C$ is a part of $C$;

# Coherent configurations

A coherent configuration on $\Omega$ is a partition $C$ of $\Omega \times \Omega$ satisfying the following conditions:

- the diagonal is a union of parts of $C$;
- the converse of a part of $C$ is a part of $C$;
- if $(x, y) \in C_k$, then the number of $z \in \Omega$ such that $(x, z) \in C_i$ and $(z, y) \in C_j$ depends only on $i, j, k$ and not on $x, y$.

# Coherent configurations, 2

The set of partitions of $\Omega \times \Omega$ forms a lattice (with "smaller"=finer), called the partition lattice.

# Coherent configurations, 2

The set of partitions of $\Omega \times \Omega$ forms a lattice (with "smaller"=finer), called the partition lattice.
The set of coherent configurations is a meet-semilattice of the partition lattice.

# Coherent configurations, 2

The set of partitions of $\Omega \times \Omega$ forms a lattice (with "smaller"=finer), called the partition lattice.

The set of coherent configurations is a meet-semilattice of the partition lattice.

Hence, given any family $F$ of subsets of $\Omega \times \Omega$, there is a unique finest coherent configuration containing them, which we call the coherent configuration generated by $F$.

# Coherent configurations, 2

The set of partitions of $\Omega \times \Omega$ forms a lattice (with "smaller"=finer), called the partition lattice.
The set of coherent configurations is a meet-semilattice of the partition lattice.
Hence, given any family $F$ of subsets of $\Omega \times \Omega$, there is a unique finest coherent configuration containing them, which we call the coherent configuration generated by $F$.
In particular, the partition into singletons forms the "trivial" coherent configuration, which we denote by $E$.

# EP-dimension

The EP-dimension of a coherent configuration $C$ is the smallest number $k$ for which there exist $k$ points $a_1, \ldots, a_k \in \Omega$ such that the coherent configuration generated by $C$ and $(a_1, a_1), \ldots, (a_k, a_k)$ is the trivial configuration $E$.

# EP-dimension

The EP-dimension of a coherent configuration $C$ is the smallest number $k$ for which there exist $k$ points $a_1, \ldots, a_k \in \Omega$ such that the coherent configuration generated by $C$ and $(a_1, a_1), \ldots, (a_k, a_k)$ is the trivial configuration $E$.
Clearly the EP-dimension of a coherent configuration is not smaller than the base size of its automorphism group, and is not greater than the determining number of the configuration (suitably defined); so it *might* be strong enough for good bounds on base size but simple enough that it can be computed fairly efficiently …

# Paley graphs

## Conjecture

*Let $q$ be a prime congruent to $1 \pmod 4$. Then the EP-dimension of the Paley graph $P_q$ is $2$.*

# Paley graphs

## Conjecture

*Let $q$ be a prime congruent to $1 \pmod 4$. Then the EP-dimension of the Paley graph $P_q$ is $2$.*

Here is how it works for $p = 13$. Without loss, choose the potential base $\{0, 1\}$. This "distinguishes" four sets of the remaining vertices. The vertices joined to 0 but not 1 are $3, 9, 12$, and the induced subgraph is a path $3 \sim 12 \sim 9$. So 12 is "distinguished". Now 12 and 0 distinguish 11, and we can work all the way around.

# The story continues

The EP-dimension of a coherent configuration is sandwiched between the base size of its automorphism group and the determining number. Both inequalities can be strict.

# The story continues

The EP-dimension of a coherent configuration is sandwiched between the base size of its automorphism group and the determining number. Both inequalities can be strict.

## Example

Very many, probably "almost all", strongly regular graphs have trivial automorphism group. Such graphs have base size 0, but the EP-dimension is strictly positive.

# The story continues

The EP-dimension of a coherent configuration is sandwiched between the base size of its automorphism group and the determining number. Both inequalities can be strict.

### Example

Very many, probably "almost all", strongly regular graphs have trivial automorphism group. Such graphs have base size 0, but the EP-dimension is strictly positive.

### Example

We certainly know that the EP-dimension of some small Paley graphs of prime degree is 2; but the determining number is about $\log q$.