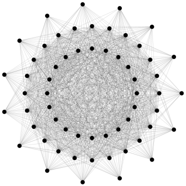
Graphs defined on groups

Peter J. Cameron
University of St Andrews
QMUL (emeritus)



Lecture 8: Other worlds
9 June 2021

Magmas

Many of our graphs can be defined on structures much more general than groups. We can't expect such a rich theory, but maybe there is something to be said.

Magmas

Many of our graphs can be defined on structures much more general than groups. We can't expect such a rich theory, but maybe there is something to be said.

I will start with a magma, a set with a binary operation (without further restriction). (These objects are sometimes called groupoids, but this term is also used in category theory for a category with all morphisms invertible, so I will avoid it here.)

Magmas

Many of our graphs can be defined on structures much more general than groups. We can't expect such a rich theory, but maybe there is something to be said.

I will start with a magma, a set with a binary operation (without further restriction). (These objects are sometimes called groupoids, but this term is also used in category theory for a category with all morphisms invertible, so I will avoid it here.)

Sometimes I will write the operation as $x \circ y$, and sometimes I will just concatenate, as is usually done for multiplication in a group.

Magmas

Many of our graphs can be defined on structures much more general than groups. We can't expect such a rich theory, but maybe there is something to be said.

I will start with a magma, a set with a binary operation (without further restriction). (These objects are sometimes called groupoids, but this term is also used in category theory for a category with all morphisms invertible, so I will avoid it here.)

Sometimes I will write the operation as $x \circ y$, and sometimes I will just concatenate, as is usually done for multiplication in a group.

The definition of the commuting graph of an arbitrary magma is straightforward. We cannot expect to define, say, the deep commuting graph. But what about the power graph?

Power-associative magmas

There are several ways to define powers in a magma. For example, we could set

- $x^1 = x$;

Power-associative magmas

There are several ways to define powers in a magma. For example, we could set

- $x^1 = x$;
- $x^{n+1} = (x^n) \circ x$ for $n \geq 1$.

Power-associative magmas

There are several ways to define powers in a magma. For example, we could set

- $x^1 = x$;
- $x^{n+1} = (x^n) \circ x$ for $n \geq 1$.

But different definitions (for example, $x^{n+1} = x \circ (x^n)$) could give different results. We define a magma to be power-associative if the value of x^n is independent of the definition. This can be expressed by the equations

$$(x^m) \circ (x^n) = x^{m+n} \text{ for } n \in \mathbb{N}.$$

Power-associative magmas

There are several ways to define powers in a magma. For example, we could set

- $x^1 = x$;
- $x^{n+1} = (x^n) \circ x$ for $n \geq 1$.

But different definitions (for example, $x^{n+1} = x \circ (x^n)$) could give different results. We define a magma to be power-associative if the value of x^n is independent of the definition. This can be expressed by the equations

$$(x^m) \circ (x^n) = x^{m+n} \text{ for } n \in \mathbb{N}.$$

Now in any magma we could define the directed power graph by the rule that $a \to b$ if $b = a^n$ for some $n \in \mathbb{N}$, and the power graph by the rule that $x \sim y$ if either $x \to y$ or $y \to x$. But this is not likely to make much sense unless the magma is power-associative.

Theorem

In a power-associative magma M,

Theorem

In a power-associative magma M,

- *the directed power graph is a partial preorder;*

Theorem

In a power-associative magma M,

- *the directed power graph is a partial preorder;*
- *the power graph is the comparability graph of a partial order;*

Theorem

In a power-associative magma M,

- *the directed power graph is a partial preorder;*
- *the power graph is the comparability graph of a partial order;*
- *the power graph is perfect.*

Theorem

In a power-associative magma M,

- *the directed power graph is a partial preorder;*
- *the power graph is the comparability graph of a partial order;*
- *the power graph is perfect.*

The proof is immediate.

Theorem

In a power-associative magma M,

- *the directed power graph is a partial preorder;*
- *the power graph is the comparability graph of a partial order;*
- *the power graph is perfect.*

The proof is immediate.
Now one of our early theorems about groups asserted that if two groups have isomorphic power graphs, then they have isomorphic directed power graphs.

Question

What assumptions on a magma are required for this theorem to hold?

Quasigroups and loops

The Cayley table of a magma M of order n is the $n \times n$ array with rows and columns indexed by M, having (x, y) entry $x \circ y$. (Note that some people reserve the term "Cayley table" for groups, and would call this an "operation table".)

Quasigroups and loops

The Cayley table of a magma M of order n is the $n \times n$ array with rows and columns indexed by M, having (x, y) entry $x \circ y$. (Note that some people reserve the term "Cayley table" for groups, and would call this an "operation table".)

A magma is a quasigroup if it satisfies the left and right division laws; that is, for any a and b, each of the equations $x \circ a = b$ and $a \circ y = b$ has a unique solution. A quasigroup is a loop if it has an identity element.

Quasigroups and loops

The Cayley table of a magma M of order n is the $n \times n$ array with rows and columns indexed by M, having (x, y) entry $x \circ y$. (Note that some people reserve the term "Cayley table" for groups, and would call this an "operation table".)

A magma is a quasigroup if it satisfies the left and right division laws; that is, for any a and b, each of the equations $x \circ a = b$ and $a \circ y = b$ has a unique solution. A quasigroup is a loop if it has an identity element.

In terms of the Cayley table, a quasigroup is a magma for which each element occurs once in each row and once in each column of the Cayley table (in other words, the Cayley table is a Latin square). If the quasigroup is a loop, and we order it so that the identity is the first element, then the first row agrees with the row of column labels, and the first column agrees with the column of row labels.

Moufang loops

A group is a loop which satisfies the associative law.

Moufang loops

A group is a loop which satisfies the associative law.
There are two important classes of loops which satisfy a relaxation of the associative law, and so are more general than groups: Moufang loops and Bol loops. I will treat Moufang loops here.

Moufang loops

A group is a loop which satisfies the associative law.
There are two important classes of loops which satisfy a relaxation of the associative law, and so are more general than groups: Moufang loops and Bol loops. I will treat Moufang loops here.
A Moufang loop is a loop satisfying the identity

$$z(x(zy)) = ((zx)z)y$$

(or any one of three equivalent identities).

Moufang loops

A group is a loop which satisfies the associative law.
There are two important classes of loops which satisfy a relaxation of the associative law, and so are more general than groups: Moufang loops and Bol loops. I will treat Moufang loops here.
A Moufang loop is a loop satisfying the identity

$$z(x(zy)) = ((zx)z)y$$

(or any one of three equivalent identities).

Theorem
In a Moufang loop M,

Moufang loops

A group is a loop which satisfies the associative law.
There are two important classes of loops which satisfy a relaxation of the associative law, and so are more general than groups: Moufang loops and Bol loops. I will treat Moufang loops here.
A Moufang loop is a loop satisfying the identity

$$z(x(zy)) = ((zx)z)y$$

(or any one of three equivalent identities).

Theorem

In a Moufang loop M,

- *if $x(yz) = (xy)z$, then the subloop generated by x, y, z satisfies the associative law;*

Moufang loops

A group is a loop which satisfies the associative law.
There are two important classes of loops which satisfy a relaxation of the associative law, and so are more general than groups: Moufang loops and Bol loops. I will treat Moufang loops here.
A Moufang loop is a loop satisfying the identity

$$z(x(zy)) = ((zx)z)y$$

(or any one of three equivalent identities).

Theorem

In a Moufang loop M,

- *if $x(yz) = (xy)z$, then the subloop generated by x, y, z satisfies the associative law;*
- $x(xy) = (xx)y$*,* $y(xx) = (yx)x$*, and* $(xy)x = x(yx)$*;*

Moufang loops

A group is a loop which satisfies the associative law.
There are two important classes of loops which satisfy a relaxation of the associative law, and so are more general than groups: Moufang loops and Bol loops. I will treat Moufang loops here.
A Moufang loop is a loop satisfying the identity

$$z(x(zy)) = ((zx)z)y$$

(or any one of three equivalent identities).

Theorem

In a Moufang loop M,

- *if $x(yz) = (xy)z$, then the subloop generated by x, y, z satisfies the associative law;*
- *$x(xy) = (xx)y$, $y(xx) = (yx)x$, and $(xy)x = x(yx)$;*
- *any 2-generated subloop is associative.*

Arguably, Moufang loops are so close to groups that they may be expected to have some of the properties of groups.

Arguably, Moufang loops are so close to groups that they may be expected to have some of the properties of groups.
After proving that the power graph of a group determines the directed power graph up to isomorphism, I conjectured that the same holds for Moufang loops.

Arguably, Moufang loops are so close to groups that they may be expected to have some of the properties of groups.
After proving that the power graph of a group determines the directed power graph up to isomorphism, I conjectured that the same holds for Moufang loops.
This has very recently been proved by Nick Britten:

Arguably, Moufang loops are so close to groups that they may be expected to have some of the properties of groups.
After proving that the power graph of a group determines the directed power graph up to isomorphism, I conjectured that the same holds for Moufang loops.
This has very recently been proved by Nick Britten:

Theorem

If M and N are Mougang loops whose power graphs are isomorphic, then their directed power graphs are isomorphic.

Arguably, Moufang loops are so close to groups that they may be expected to have some of the properties of groups.
After proving that the power graph of a group determines the directed power graph up to isomorphism, I conjectured that the same holds for Moufang loops.
This has very recently been proved by Nick Britten:

Theorem

If M and N are Mougang loops whose power graphs are isomorphic, then their directed power graphs are isomorphic.

Here is a sketch of the proof. It follows the corresponding proof for groups. If only the identity is a dominating vertex, the same argument works.

In the group case, if the power graph has other dominating vertices, the group must be cyclic or generalised quaternion. A generalised quaternion group can be characterised as a group in which every commutative subgroup is cyclic.

In the group case, if the power graph has other dominating vertices, the group must be cyclic or generalised quaternion. A generalised quaternion group can be characterised as a group in which every commutative subgroup is cyclic.

A generalised octonion loop is a non-associative Moufang loop in which every commutative and associative subloop is cyclic.

A construction due to Chein produces Moufang loops.

In the group case, if the power graph has other dominating vertices, the group must be cyclic or generalised quaternion. A generalised quaternion group can be characterised as a group in which every commutative subgroup is cyclic.

A generalised octonion loop is a non-associative Moufang loop in which every commutative and associative subloop is cyclic.

A construction due to Chein produces Moufang loops.

Theorem

The following are equivalent for a Moufang loop M:

In the group case, if the power graph has other dominating vertices, the group must be cyclic or generalised quaternion. A generalised quaternion group can be characterised as a group in which every commutative subgroup is cyclic.

A generalised octonion loop is a non-associative Moufang loop in which every commutative and associative subloop is cyclic. A construction due to Chein produces Moufang loops.

Theorem

The following are equivalent for a Moufang loop M:

- *M is a generalized octonion loop;*

In the group case, if the power graph has other dominating vertices, the group must be cyclic or generalised quaternion. A generalised quaternion group can be characterised as a group in which every commutative subgroup is cyclic.
A generalised octonion loop is a non-associative Moufang loop in which every commutative and associative subloop is cyclic.
A construction due to Chein produces Moufang loops.

Theorem

The following are equivalent for a Moufang loop M:

- *M is a generalized octonion loop;*
- *M is a specific subloop of the unit octonions;*

In the group case, if the power graph has other dominating vertices, the group must be cyclic or generalised quaternion. A generalised quaternion group can be characterised as a group in which every commutative subgroup is cyclic.
A generalised octonion loop is a non-associative Moufang loop in which every commutative and associative subloop is cyclic.
A construction due to Chein produces Moufang loops.

Theorem

The following are equivalent for a Moufang loop M:

- *M is a generalized octonion loop;*
- *M is a specific subloop of the unit octonions;*
- *M is a finite Moufang loop of 2-power exponent with a unique element of order 2;*

In the group case, if the power graph has other dominating vertices, the group must be cyclic or generalised quaternion. A generalised quaternion group can be characterised as a group in which every commutative subgroup is cyclic.

A generalised octonion loop is a non-associative Moufang loop in which every commutative and associative subloop is cyclic.

A construction due to Chein produces Moufang loops.

Theorem

The following are equivalent for a Moufang loop M:

- *M is a generalized octonion loop;*
- *M is a specific subloop of the unit octonions;*
- *M is a finite Moufang loop of 2-power exponent with a unique element of order 2;*
- *M is produced by Chein's construction.*

Now let M be a Moufang loop whose power graph has a dominating vertex.

Now let M be a Moufang loop whose power graph has a dominating vertex.

The proof shows that, if the order of M is not a 2-power, then it must be a cyclic group; if it is a 2-power, then M is cyclic, generalised quaternion, or generalised octonion, depending on whether the largest complete subgraph has size $|M|$, $|M|/2$ or $|M|/4$.

Now let M be a Moufang loop whose power graph has a dominating vertex.
The proof shows that, if the order of M is not a 2-power, then it must be a cyclic group; if it is a 2-power, then M is cyclic, generalised quaternion, or generalised octonion, depending on whether the largest complete subgraph has size $|M|$, $|M|/2$ or $|M|/4$.

Question

Can anything similar be done for other classes of loops?

There is a body of research on special loops, especially Moufang and Bol loops, which I cannot describe here.

There is a body of research on special loops, especially Moufang and Bol loops, which I cannot describe here.
As far as I am aware, the enhanced power graph of a power-associative loop has not been studied, although the definition presents no problems.

There is a body of research on special loops, especially Moufang and Bol loops, which I cannot describe here.
As far as I am aware, the enhanced power graph of a power-associative loop has not been studied, although the definition presents no problems.
It is probably true that the deep commuting graph makes little sense outside the context of groups.

Semigroups and monoids

The other type of magmas of wide interest is semigroups. A semigroup is a magma satisfying the associative law $x(yz) = (xy)z$. A semigroup with an identity element is a monoid.

Semigroups and monoids

The other type of magmas of wide interest is semigroups. A semigroup is a magma satisfying the associative law $x(yz) = (xy)z$. A semigroup with an identity element is a monoid.

There are various classes of semigroups which resemble groups to a greater or lesser degree. Perhaps the class which is closest to groups, and so most likely to give an interesting theory, consists of inverse semigroups.

Semigroups and monoids

The other type of magmas of wide interest is semigroups. A semigroup is a magma satisfying the associative law $x(yz) = (xy)z$. A semigroup with an identity element is a monoid.

There are various classes of semigroups which resemble groups to a greater or lesser degree. Perhaps the class which is closest to groups, and so most likely to give an interesting theory, consists of inverse semigroups.

An inverse semigroup is a semigroup in which, for each element x, there is a unique generalised inverse y satisfying $xyx = x$ and $yxy = y$. The element y is denoted by x^*.

Random walks

We saw in the first lecture that the random walk on the commuting graph of a group (with a loop at every vertex) has limiting distribution which is uniform on conjugacy classes.

Random walks

We saw in the first lecture that the random walk on the commuting graph of a group (with a loop at every vertex) has limiting distribution which is uniform on conjugacy classes.

Question

Are there any classes of magmas beyond groups for which the limiting distribution of the random walk on the commuting graph can be described in terms of the structure of the magma?

Random walks

We saw in the first lecture that the random walk on the commuting graph of a group (with a loop at every vertex) has limiting distribution which is uniform on conjugacy classes.

Question

Are there any classes of magmas beyond groups for which the limiting distribution of the random walk on the commuting graph can be described in terms of the structure of the magma?

Our proof for groups involved the action of the group on itself by conjugation. This can be extended to inverse semigroups, where conjugation by a is the map $x \mapsto a^*xa$, where a^* is the quasi-inverse of a.

Random walks

We saw in the first lecture that the random walk on the commuting graph of a group (with a loop at every vertex) has limiting distribution which is uniform on conjugacy classes.

Question

Are there any classes of magmas beyond groups for which the limiting distribution of the random walk on the commuting graph can be described in terms of the structure of the magma?

Our proof for groups involved the action of the group on itself by conjugation. This can be extended to inverse semigroups, where conjugation by a is the map $x \mapsto a^*xa$, where a^* is the quasi-inverse of a.
So inverse semigroups might be candidates for the above question ...

Rings

Once we move on to structures with two binary operations, there are more opportunities for defining graphs to reflect the structure.

Rings

Once we move on to structures with two binary operations, there are more opportunities for defining graphs to reflect the structure.

Recall that a ring has two operations, addition and multiplication, written in the usual way: the ring forms an abelian group with the operation $+$ (the identity and inverse of x are denoted 0 and $-x$), while multiplication is associative and distributive over addition. Important classes of rings are commutative rings and rings with identity (these refer to the multiplication).

Rings

Once we move on to structures with two binary operations, there are more opportunities for defining graphs to reflect the structure.

Recall that a ring has two operations, addition and multiplication, written in the usual way: the ring forms an abelian group with the operation $+$ (the identity and inverse of x are denoted 0 and $-x$), while multiplication is associative and distributive over addition. Important classes of rings are commutative rings and rings with identity (these refer to the multiplication).

In what follows, "ring" will mean "commutative ring with identity".

Rings

Once we move on to structures with two binary operations, there are more opportunities for defining graphs to reflect the structure.

Recall that a ring has two operations, addition and multiplication, written in the usual way: the ring forms an abelian group with the operation $+$ (the identity and inverse of x are denoted 0 and $-x$), while multiplication is associative and distributive over addition. Important classes of rings are commutative rings and rings with identity (these refer to the multiplication).

In what follows, “ring” will mean “commutative ring with identity”.

I will talk about the zero-divisor graph, though other graphs such as the unit graph have been considered.

Finite rings

An ideal in a ring R is the kernel of a ring homomorphism. Thus it is a non-empty subset I closed under addition, with the property that for any $a \in I$ and $r \in R$, we have $ar \in I$.

Finite rings

An ideal in a ring R is the kernel of a ring homomorphism. Thus it is a non-empty subset I closed under addition, with the property that for any $a \in I$ and $r \in R$, we have $ar \in I$.
A ring is local if it has a unique maximal ideal, and semi-local if it has only finitely many. Clearly a finite ring is semi-local.

Finite rings

An ideal in a ring R is the kernel of a ring homomorphism. Thus it is a non-empty subset I closed under addition, with the property that for any $a \in I$ and $r \in R$, we have $ar \in I$.
A ring is local if it has a unique maximal ideal, and semi-local if it has only finitely many. Clearly a finite ring is semi-local.

Theorem

A finite ring is isomorphic to a direct sum of local rings.

Finite rings

An ideal in a ring R is the kernel of a ring homomorphism. Thus it is a non-empty subset I closed under addition, with the property that for any $a \in I$ and $r \in R$, we have $ar \in I$.
A ring is local if it has a unique maximal ideal, and semi-local if it has only finitely many. Clearly a finite ring is semi-local.

Theorem

A finite ring is isomorphic to a direct sum of local rings.

This uses some standard results from ring theory. The radical I of a finite ring R is nilpotent, and hence R is complete in the I-adic topology.

The zero-divisor graph

An element a of a ring R is a zero-divisor if $a \neq 0$ and there exists $b \in R$ with $b \neq 0$ such that $ab = 0$.

The zero-divisor graph

An element a of a ring R is a zero-divisor if $a \neq 0$ and there exists $b \in R$ with $b \neq 0$ such that $ab = 0$.
The zero-divisor graph of R has vertex set the set of zero-divisors in R, with a and b joined if $ab = 0$.

The zero-divisor graph

An element a of a ring R is a zero-divisor if $a \neq 0$ and there exists $b \in R$ with $b \neq 0$ such that $ab = 0$.
The zero-divisor graph of R has vertex set the set of zero-divisors in R, with a and b joined if $ab = 0$.
For example, in the ring $\mathbb{Z}/(6)$ of integers mod 6, the zero-divisors are $2, 3, 4$, and the zero-divisor graph is a 3-vertex path.

The zero-divisor graph

An element a of a ring R is a zero-divisor if $a \neq 0$ and there exists $b \in R$ with $b \neq 0$ such that $ab = 0$.
The zero-divisor graph of R has vertex set the set of zero-divisors in R, with a and b joined if $ab = 0$.
For example, in the ring $\mathbb{Z}/(6)$ of integers mod 6, the zero-divisors are $2, 3, 4$, and the zero-divisor graph is a 3-vertex path.
This graph was introduced by Anderson and Livingston in 1999.

Universality

Theorem

Every finite graph is an induced subgraph of the zero-divisor graph of a finite ring.

Universality

Theorem

Every finite graph is an induced subgraph of the zero-divisor graph of a finite ring.

Proof.

We use Boolean rings: the elements are all subsets of a set X, with symmetric difference for addition and intersection for multiplication. Now $ab = 0$ if and only if a and b are disjoint. So if we represent the given graph as an intersection graph, it is naturally embedded in the zero-divisor graph of a Boolean ring. $\square$

Universality

Theorem

Every finite graph is an induced subgraph of the zero-divisor graph of a finite ring.

Proof.

We use Boolean rings: the elements are all subsets of a set X, with symmetric difference for addition and intersection for multiplication. Now $ab = 0$ if and only if a and b are disjoint. So if we represent the given graph as an intersection graph, it is naturally embedded in the zero-divisor graph of a Boolean ring. $\square$

I am grateful to G. Arun Kumar for this proof.

Local rings

In a finite ring, every non-zero element is either a zero-divisor or invertible. (If multiplication by a is not injective, then a is a zero-divisor; if it is surjective, then a is a unit.) So in a local ring, the zero-divisors are the non-zero elements of the maximal ideal.

Local rings

In a finite ring, every non-zero element is either a zero-divisor or invertible. (If multiplication by a is not injective, then a is a zero-divisor; if it is surjective, then a is a unit.) So in a local ring, the zero-divisors are the non-zero elements of the maximal ideal.

Question

Are the zero-divisor graphs of local rings universal (in the previous sense)?

Local rings

In a finite ring, every non-zero element is either a zero-divisor or invertible. (If multiplication by a is not injective, then a is a zero-divisor; if it is surjective, then a is a unit.) So in a local ring, the zero-divisors are the non-zero elements of the maximal ideal.

Question

Are the zero-divisor graphs of local rings universal (in the previous sense)?

The answer is negative in one special case.

An ideal of a ring is principal if it is generated by a single element.

An ideal of a ring is principal if it is generated by a single element.

Theorem

If R is a finite local ring whose maximal ideal is principal, then the zero-divisor graph of R is a threshold graph.

An ideal of a ring is principal if it is generated by a single element.

Theorem

If R is a finite local ring whose maximal ideal is principal, then the zero-divisor graph of R is a threshold graph.

Proof.

Let m generate the maximal ideal. Then every element of R has the form um^i, where u is a unit. There is a minimum i such that $m^i = 0$, say $i = k$; then um^i is joined to vm^j if and only if $i + j \geq k$. So the zero-divisor graph is a threshold graph. $\square$

An ideal of a ring is principal if it is generated by a single element.

Theorem

If R is a finite local ring whose maximal ideal is principal, then the zero-divisor graph of R is a threshold graph.

Proof.

Let m generate the maximal ideal. Then every element of R has the form um^i, where u is a unit. There is a minimum i such that $m^i = 0$, say $i = k$; then um^i is joined to vm^j if and only if $i + j \geq k$. So the zero-divisor graph is a threshold graph. □

However, not all finite local rings have their maximal ideals principal, and the zero-divisor graph is not always a threshold graph. (I am grateful to T. Kavaskar for an example.) The question above remains unanswered.

… for lasting to the end of the course.

… for lasting to the end of the course.

I hope you have enough information now to begin tackling some of the open questions I have mentioned.

… for lasting to the end of the course.

I hope you have enough information now to begin tackling some of the open questions I have mentioned.
Take a look at my paper on this topic in the *International Journal of Group Theory*, which you can download from

`https://ijgt.ui.ac.ir/article_25608.html`

This paper also contains an extensive bibliography.

… for lasting to the end of the course.

I hope you have enough information now to begin tackling some of the open questions I have mentioned.
Take a look at my paper on this topic in the *International Journal of Group Theory*, which you can download from

`https://ijgt.ui.ac.ir/article_25608.html`

This paper also contains an extensive bibliography.

Please tell me about anything you manage to find!