Critical groups and partitions of finite groups

Daniela Bubboloni
University of Florence (Italy)

Reinhold Baer Prize 2024

Napoli, 7-8 October 2024

A joint research with Nicolas Pinzauti

Power graphs

- G denotes a finite group

Definitions

Directed power graph $\vec{\mathcal{P}}(G)$

- Vertex set G
- for $x \neq y \in G$,

$$(x, y) \text{ arc if } y = x^m, \text{ for some } m \in \mathbb{N}$$

Power graph $\mathcal{P}(G)$:= The underlying undirected graph of $\vec{\mathcal{P}}(G)$

Power graphs := $\{\mathcal{P}(G) : \ G \text{ is a finite group}\}$

- Non-isomorphic groups may have the same power graph
- The directed power graph should encode more information than the power graph. Surprisingly, this is not the case.

Power graphs

- G denotes a finite group

Definitions

Directed power graph $\vec{\mathcal{P}}(G)$

- Vertex set G
- for $x \neq y \in G$,

$$(x, y) \text{ arc if } y = x^m, \text{ for some } m \in \mathbb{N}$$

Power graph $\mathcal{P}(G)$:= The underlying undirected graph of $\vec{\mathcal{P}}(G)$

Power graphs := $\{\mathcal{P}(G) : G \text{ is a finite group}\}$

- Non-isomorphic groups may have the same power graph
- The directed power graph should encode more information than the power graph. Surprisingly, this is not the case.

Power graphs

- G denotes a finite group

Definitions

Directed power graph $\vec{\mathcal{P}}(G)$

- Vertex set G
- for $x \neq y \in G$,

$$(x, y) \text{ arc if } y = x^m, \text{ for some } m \in \mathbb{N}$$

Power graph $\mathcal{P}(G)$:= The underlying undirected graph of $\vec{\mathcal{P}}(G)$

Power graphs := $\{\mathcal{P}(G) : G \text{ is a finite group}\}$

- Non-isomorphic groups may have the same power graph
- The directed power graph should encode more information than the power graph. Surprisingly, this is not the case.

Power graphs

- G denotes a finite group

Definitions

Directed power graph $\vec{\mathcal{P}}(G)$

- Vertex set G
- for $x \neq y \in G$,

$$(x, y) \text{ arc if } y = x^m, \text{ for some } m \in \mathbb{N}$$

Power graph $\mathcal{P}(G)$:= The underlying undirected graph of $\vec{\mathcal{P}}(G)$

Power graphs := $\{\mathcal{P}(G) : G \text{ is a finite group}\}$

- Non-isomorphic groups may have the same power graph
- The directed power graph should encode more information than the power graph. Surprisingly, this is not the case.

Power graphs

- G denotes a finite group

Definitions

Directed power graph $\vec{\mathcal{P}}(G)$

- Vertex set G
- for $x \neq y \in G$,

$$(x, y) \text{ arc if } y = x^m, \text{ for some } m \in \mathbb{N}$$

Power graph $\mathcal{P}(G)$:= The underlying undirected graph of $\vec{\mathcal{P}}(G)$

Power graphs := $\{\mathcal{P}(G) : \ G \text{ is a finite group}\}$

- Non-isomorphic groups may have the same power graph
- The directed power graph should encode more information than the power graph. Surprisingly, this is not the case.

Reconstructing directed power graphs

Theorem (Bubboloni, Pinzauti 2023)

Given a power graph Γ, by arithmetical and graph theoretical considerations, it is possible to do one of the following

1. Show that there exists a unique group G such that $\Gamma = \mathcal{P}(G)$ and exhibit such G
2. Exhibit a digraph $\vec{\Gamma} \cong \vec{\mathcal{P}}(G)$, which is the same for any choice of the group G such that $\Gamma = \mathcal{P}(G)$

- Based on a paper by Cameron (2010) and correcting a mistake there
- An answer to Question 2 in Cameron (2022) about the reconstruction of directed power graphs from power graphs
- The tools developed can be fruitfully applied to other kinds of research!

Reconstructing directed power graphs

Theorem (Bubboloni, Pinzauti 2023)

Given a power graph Γ, by arithmetical and graph theoretical considerations, it is possible to do one of the following

1. Show that there exists a unique group G such that $\Gamma = \mathcal{P}(G)$ and exhibit such G
2. Exhibit a digraph $\vec{\Gamma} \cong \vec{\mathcal{P}}(G)$, which is the same for any choice of the group G such that $\Gamma = \mathcal{P}(G)$

- Based on a paper by Cameron (2010) and correcting a mistake there
- An answer to Question 2 in Cameron (2022) about the reconstruction of directed power graphs from power graphs
- The tools developed can be fruitfully applied to other kinds of research!

Reconstructing directed power graphs

Theorem (Bubboloni, Pinzauti 2023)

Given a power graph Γ, by arithmetical and graph theoretical considerations, it is possible to do one of the following

1. Show that there exists a unique group G such that $\Gamma = \mathcal{P}(G)$ and exhibit such G
2. Exhibit a digraph $\vec{\Gamma} \cong \vec{\mathcal{P}}(G)$, which is the same for any choice of the group G such that $\Gamma = \mathcal{P}(G)$

- Based on a paper by Cameron (2010) and correcting a mistake there
- An answer to Question 2 in Cameron (2022) about the reconstruction of directed power graphs from power graphs
- The tools developed can be fruitfully applied to other kinds of research!

Reconstructing directed power graphs

Theorem (Bubboloni, Pinzauti 2023)

Given a power graph Γ, by arithmetical and graph theoretical considerations, it is possible to do one of the following

1. Show that there exists a unique group G such that $\Gamma = \mathcal{P}(G)$ and exhibit such G
2. Exhibit a digraph $\vec{\Gamma} \cong \vec{\mathcal{P}}(G)$, which is the same for any choice of the group G such that $\Gamma = \mathcal{P}(G)$

- Based on a paper by Cameron (2010) and correcting a mistake there
- An answer to Question 2 in Cameron (2022) about the reconstruction of directed power graphs from power graphs
- The tools developed can be fruitfully applied to other kinds of research!

Reconstructing directed power graphs

Theorem (Bubboloni, Pinzauti 2023)

Given a power graph Γ, by arithmetical and graph theoretical considerations, it is possible to do one of the following

1. Show that there exists a unique group G such that $\Gamma = \mathcal{P}(G)$ and exhibit such G
2. Exhibit a digraph $\vec{\Gamma} \cong \vec{\mathcal{P}}(G)$, which is the same for any choice of the group G such that $\Gamma = \mathcal{P}(G)$

- Based on a paper by Cameron (2010) and correcting a mistake there
- An answer to Question 2 in Cameron (2022) about the reconstruction of directed power graphs from power graphs
- The tools developed can be fruitfully applied to other kinds of research!

Reconstructing directed power graphs

Theorem (Bubboloni, Pinzauti 2023)

Given a power graph Γ, by arithmetical and graph theoretical considerations, it is possible to do one of the following

1. Show that there exists a unique group G such that $\Gamma = \mathcal{P}(G)$ and exhibit such G
2. Exhibit a digraph $\vec{\Gamma} \cong \vec{\mathcal{P}}(G)$, which is the same for any choice of the group G such that $\Gamma = \mathcal{P}(G)$

- Based on a paper by Cameron (2010) and correcting a mistake there
- An answer to Question 2 in Cameron (2022) about the reconstruction of directed power graphs from power graphs
- The tools developed can be fruitfully applied to other kinds of research!

Neighbours

Definition

$\Gamma = (V, E)$ graph, $x \in V$, $X \subseteq V$

- $N[x] := \{y \in V : \{x, y\} \in E\} \cup \{x\}$
- x is a star vertex if $N[x] = V$.

$$\mathcal{S} := \{x \in V : x \text{ is a star}\}$$

- the common closed neighbour

$$N[X] := \begin{cases} \bigcap_{x \in X} N[x] & \text{if } X \neq \varnothing \\ V & \text{if } X = \varnothing \end{cases}$$

- The neighbourhood closure $\hat{X} := N[N[X]]$

  This gives an original example of Moore closure for graphs

Neighbours

Definition

$\Gamma = (V, E)$ graph, $x \in V$, $X \subseteq V$

- $N[x] := \{y \in V : \{x, y\} \in E\} \cup \{x\}$
- x is a star vertex if $N[x] = V$.

$$\mathcal{S} := \{x \in V : x \text{ is a star}\}$$

- the common closed neighbour

$$N[X] := \begin{cases} \bigcap_{x \in X} N[x] & \text{if } X \neq \varnothing \\ V & \text{if } X = \varnothing \end{cases}$$

- The neighbourhood closure $\hat{X} := N[N[X]]$

  This gives an original example of Moore closure for graphs

Neighbours

Definition

$\Gamma = (V, E)$ graph, $x \in V$, $X \subseteq V$

- $N[x] := \{y \in V : \{x, y\} \in E\} \cup \{x\}$
- x is a star vertex if $N[x] = V$.

$$\mathcal{S} := \{x \in V : x \text{ is a star}\}$$

- the common closed neighbour

$$N[X] := \begin{cases} \bigcap_{x \in X} N[x] & \text{if } X \neq \varnothing \\ V & \text{if } X = \varnothing \end{cases}$$

- The neighbourhood closure $\hat{X} := N[N[X]]$

  This gives an original example of Moore closure for graphs

Neighbours

Definition

$\Gamma = (V, E)$ graph, $x \in V$, $X \subseteq V$

- $$N[x] := \{y \in V : \{x, y\} \in E\} \cup \{x\}$$
- x is a star vertex if $N[x] = V$.

$$\mathcal{S} := \{x \in V : x \text{ is a star}\}$$

- the common closed neighbour

$$N[X] := \begin{cases} \bigcap_{x \in X} N[x] & \text{if } X \neq \varnothing \\ V & \text{if } X = \varnothing \end{cases}$$

- The neighbourhood closure $\hat{X} := N[N[X]]$

  This gives an original example of Moore closure for graphs

Neighbours

Definition

$\Gamma = (V, E)$ graph, $x \in V$, $X \subseteq V$

- $N[x] := \{y \in V : \{x, y\} \in E\} \cup \{x\}$
- x is a star vertex if $N[x] = V$.

$$\mathcal{S} := \{x \in V : x \text{ is a star}\}$$

- the common closed neighbour

$$N[X] := \begin{cases} \bigcap_{x \in X} N[x] & \text{if } X \neq \varnothing \\ V & \text{if } X = \varnothing \end{cases}$$

- The neighbourhood closure $\hat{X} := N[N[X]]$

  This gives an original example of Moore closure for graphs

Equivalence relations on power graphs

Definition

$\Gamma = \mathcal{P}(G)$. For $x, y \in G$

- $x \mathrm{N} y$ if $N[x] = N[y]$
- $x \diamond y$ if $\langle x \rangle = \langle y \rangle$

define two equivalence relations in G.

N is called the closed twin relation.

- $[1]_{\mathrm{N}} = \mathcal{S}$ is the trivial N-class
- $\mathcal{S} \supsetneq \{1\} \iff G$ is cyclic or generalized quaternion
- $\diamond$ refines $\mathrm{N} \implies$ a N-class is union of $\diamond$-classes

Equivalence relations on power graphs

Definition

$\Gamma = \mathcal{P}(G)$. For $x, y \in G$

- $x \mathrm{N} y$ if $N[x] = N[y]$
- $x \diamond y$ if $\langle x \rangle = \langle y \rangle$

define two equivalence relations in G.

N is called the closed twin relation.

- $[1]_{\mathrm{N}} = \mathcal{S}$ is the trivial N-class
- $\mathcal{S} \supsetneq \{1\} \iff G$ is cyclic or generalized quaternion
- $\diamond$ refines $\mathrm{N} \implies$ a N-class is union of $\diamond$-classes

Equivalence relations on power graphs

Definition

$\Gamma = \mathcal{P}(G)$. For $x, y \in G$

- $x \mathrm{N} y$ if $N[x] = N[y]$
- $x \diamond y$ if $\langle x \rangle = \langle y \rangle$

define two equivalence relations in G.

N is called the closed twin relation.

- $[1]_{\mathrm{N}} = \mathcal{S}$ is the trivial N-class
- $\mathcal{S} \supsetneq \{1\} \iff G$ is cyclic or generalized quaternion
- $\diamond$ refines $\mathrm{N} \implies$ a N-class is union of $\diamond$-classes

Equivalence relations on power graphs

Definition

$\Gamma = \mathcal{P}(G)$. For $x, y \in G$

- $x \mathrm{N} y$ if $N[x] = N[y]$
- $x \diamond y$ if $\langle x \rangle = \langle y \rangle$

define two equivalence relations in G.

N is called the closed twin relation.

- $[1]_{\mathrm{N}} = \mathcal{S}$ is the trivial N-class
- $\mathcal{S} \supsetneq \{1\} \iff G$ is cyclic or generalized quaternion
- $\diamond$ refines $\mathrm{N} \implies$ a N-class is union of $\diamond$-classes

Equivalence relations on power graphs

Definition

$\Gamma = \mathcal{P}(G)$. For $x, y \in G$

- $x \mathrm{N} y$ if $N[x] = N[y]$
- $x \diamond y$ if $\langle x \rangle = \langle y \rangle$

define two equivalence relations in G.

N is called the closed twin relation.

- $[1]_{\mathrm{N}} = \mathcal{S}$ is the trivial N-class
- $\mathcal{S} \supsetneq \{1\} \iff G$ is cyclic or generalized quaternion
- $\diamond$ refines $\mathrm{N} \implies$ a N-class is union of $\diamond$-classes

Equivalence relations on power graphs

Definition

$\Gamma = \mathcal{P}(G)$. For $x, y \in G$

- $x \mathrm{N} y$ if $N[x] = N[y]$
- $x \diamond y$ if $\langle x \rangle = \langle y \rangle$

define two equivalence relations in G.

N is called the closed twin relation.

- $[1]_{\mathrm{N}} = \mathcal{S}$ is the trivial N-class
- $\mathcal{S} \supsetneq \{1\} \iff G$ is cyclic or generalized quaternion
- $\diamond$ refines $\mathrm{N} \implies$ a N-class is union of $\diamond$-classes

Equivalence relations on power graphs

Definition

$\Gamma = \mathcal{P}(G)$. For $x, y \in G$

- $x \mathrm{N} y$ if $N[x] = N[y]$
- $x \diamond y$ if $\langle x \rangle = \langle y \rangle$

define two equivalence relations in G.

N is called the closed twin relation.

- $[1]_{\mathrm{N}} = \mathcal{S}$ is the trivial N-class
- $\mathcal{S} \supsetneq \{1\} \iff G$ is cyclic or generalized quaternion
- $\diamond$ refines $\mathrm{N} \implies$ a N-class is union of $\diamond$-classes

Equivalence relations on power graphs

Definition

$\Gamma = \mathcal{P}(G)$. For $x, y \in G$

- $x \mathrm{N} y$ if $N[x] = N[y]$
- $x \diamond y$ if $\langle x \rangle = \langle y \rangle$

define two equivalence relations in G.

N is called the closed twin relation.

- $[1]_{\mathrm{N}} = \mathcal{S}$ is the trivial N-class
- $\mathcal{S} \supsetneq \{1\} \iff G$ is cyclic or generalized quaternion
- $\diamond$ refines $\mathrm{N} \implies$ a N-class is union of $\diamond$-classes

Plain and compound classes

Definition

An N-class $[x]_{\mathrm{N}}$ in a power graph is called

- plain if $[x]_{\mathrm{N}}$ consists of a single $\diamond$-class:

$$[x]_{\mathrm{N}} = [x]_{\diamond}$$

- compound if $[x]_{\mathrm{N}}$ is union of at least two $\diamond$-classes

- In an abelian group G every N-class different from S is plain (a rephrase of a result by Cameron and Gosh, 2011)
- S is plain $\iff S = \{1\}$

Plain and compound classes

Definition

An N-class $[x]_{\mathrm{N}}$ in a power graph is called

- plain if $[x]_{\mathrm{N}}$ consists of a single $\diamond$-class:

$$[x]_{\mathrm{N}} = [x]_{\diamond}$$

- compound if $[x]_{\mathrm{N}}$ is union of at least two $\diamond$-classes

- In an abelian group G every N-class different from $\mathcal{S}$ is plain (a rephrase of a result by Cameron and Gosh, 2011)
- $\mathcal{S}$ is plain $\iff \mathcal{S} = \{1\}$

Plain and compound classes

Definition

An N-class $[x]_{\mathrm{N}}$ in a power graph is called

- plain if $[x]_{\mathrm{N}}$ consists of a single $\diamond$-class:

$$[x]_{\mathrm{N}} = [x]_{\diamond}$$

- compound if $[x]_{\mathrm{N}}$ is union of at least two $\diamond$-classes

- In an abelian group G every N-class different from $\mathcal{S}$ is plain (a rephrase of a result by Cameron and Gosh, 2011)
- $\mathcal{S}$ is plain $\iff \mathcal{S} = \{1\}$

Plain and compound classes

Definition

An N-class $[x]_{\mathrm{N}}$ in a power graph is called

- plain if $[x]_{\mathrm{N}}$ consists of a single $\diamond$-class:

$$[x]_{\mathrm{N}} = [x]_{\diamond}$$

- compound if $[x]_{\mathrm{N}}$ is union of at least two $\diamond$-classes

- In an abelian group G every N-class different from $\mathcal{S}$ is plain (a rephrase of a result by Cameron and Gosh, 2011)
- $\mathcal{S}$ is plain $\Longleftrightarrow \mathcal{S} = \{1\}$

Proposition (Cameron, 2010)

Let $C \neq \mathcal{S}$ be a $\mathbb{N}$-class of G. The following facts are equivalent

(*i*) C is compound

(*ii*) If $y \in C$ has maximum order, then we have

- $o(y) = p^r$ for some prime p and some integer $r \geq 2$
- There exists $0 \leq s \leq r - 2$ such that

$$C = \left\{ z \in \langle y \rangle \mid p^{s+1} \leq o(z) \leq p^r \right\} .$$

(p, r, s) are called the parameters of C and y a root of C.

- If C is compound with parameters (p, r, s) and y is a root, then $\hat{C} = \langle y \rangle$. Thus

$$|C| = p^r - p^s \quad \text{and} \quad |\hat{C}| = p^r \tag{1}$$

- However we discovered that there exist plain classes C that satisfy condition (1). Cameron thought they did not exist.

Proposition (Cameron, 2010)

Let $C \neq \mathcal{S}$ be a $\mathtt{N}$-class of G. The following facts are equivalent

(*i*) C is compound

(*ii*) If $y \in C$ has maximum order, then we have

- $o(y) = p^r$ for some prime p and some integer $r \geq 2$
- There exists $0 \leq s \leq r-2$ such that

$$C = \left\{ z \in \langle y \rangle \mid p^{s+1} \leq o(z) \leq p^r \right\}.$$

(p, r, s) are called the parameters of C and y a root of C.

- If C is compound with parameters (p, r, s) and y is a root, then $\hat{C} = \langle y \rangle$. Thus

$$|C| = p^r - p^s \quad \text{and} \quad |\hat{C}| = p^r \tag{1}$$

- However we discovered that there exist plain classes C that satisfy condition (1). Cameron thought they did not exist.

Proposition (Cameron, 2010)

Let $C \neq \mathcal{S}$ be a $\mathbb{N}$-class of G. The following facts are equivalent

(*i*) C is compound

(*ii*) If $y \in C$ has maximum order, then we have

- $o(y) = p^r$ for some prime p and some integer $r \geq 2$
- There exists $0 \leq s \leq r-2$ such that

$$C = \{z \in \langle y \rangle \mid p^{s+1} \leq o(z) \leq p^r\}.$$

(p, r, s) are called the parameters of C and y a root of C.

- If C is compound with parameters (p, r, s) and y is a root, then $\hat{C} = \langle y \rangle$. Thus

$$|C| = p^r - p^s \quad \text{and} \quad |\hat{C}| = p^r \tag{1}$$

- However we discovered that there exist plain classes C that satisfy condition (1). Cameron thought they did not exist.

Proposition (Cameron, 2010)

Let $C \neq \mathcal{S}$ be a $\mathbb{N}$-class of G. The following facts are equivalent

(i) C is compound

(ii) If $y \in C$ has maximum order, then we have

- $o(y) = p^r$ for some prime p and some integer $r \geq 2$
- There exists $0 \leq s \leq r - 2$ such that

$$C = \left\{ z \in \langle y \rangle \mid p^{s+1} \leq o(z) \leq p^r \right\}.$$

(p, r, s) are called the parameters of C and y a root of C.

- If C is compound with parameters (p, r, s) and y is a root, then $\hat{C} = \langle y \rangle$. Thus

$$|C| = p^r - p^s \quad \text{and} \quad |\hat{C}| = p^r \tag{1}$$

- However we discovered that there exist plain classes C that satisfy condition (1). Cameron thought they did not exist.

Example

In D_{30}, $C := [y]_{\mathrm{N}}$, with $o(y) = 15$. Then

- C is plain because y is not a prime power
- $|C| = \phi(o(y)) = 8 = 3^2 - 3^0$
- $\hat{C} = C \dot\cup \{1\} \Rightarrow |\hat{C}| = 3^2$

- If a plain class C satisfies

$$|C| = p^r - p^s \quad \text{and} \quad |\hat{C}| = p^r,$$

we always have:

$$s = 0, \quad \hat{C} = C \dot\cup \{1\}.$$

Moreover, $C = [z]_\diamond$ for some $z \in G$ with $o(z) > 1$ not a prime power, and

$$|C| = \phi(o(z)) = p^r - 1$$

Example

In D_{30}, $C := [y]_{\mathrm{N}}$, with $o(y) = 15$. Then

- C is plain because y is not a prime power
- $|C| = \phi(o(y)) = 8 = 3^2 - 3^0$
- $\hat{C} = C \cup \{1\} \Rightarrow |\hat{C}| = 3^2$

- If a plain class C satisfies

$$|C| = p^r - p^s \quad \text{and} \quad |\hat{C}| = p^r,$$

we always have:

$$s = 0, \quad \hat{C} = C \cup \{1\}.$$

Moreover, $C = [z]_\diamond$ for some $z \in G$ with $o(z) > 1$ not a prime power, and

$$|C| = \phi(o(z)) = p^r - 1$$

Example

In D_{30}, $C := [y]_{\mathbb{N}}$, with $o(y) = 15$. Then

- C is plain because y is not a prime power
- $|C| = \phi(o(y)) = 8 = 3^2 - 3^0$
- $\hat{C} = C \mathbin{\dot\cup} \{1\} \Rightarrow |\hat{C}| = 3^2$

- If a plain class C satisfies

$$|C| = p^r - p^s \quad \text{and} \quad |\hat{C}| = p^r,$$

we always have:

$$s = 0, \quad \hat{C} = C \mathbin{\dot\cup} \{1\}.$$

Moreover, $C = [z]_\diamond$ for some $z \in G$ with $o(z) > 1$ not a prime power, and

$$|C| = \phi(o(z)) = p^r - 1$$

Example

In D_{30}, $C := [y]_{\mathbb{N}}$, with $o(y) = 15$. Then

- C is plain because y is not a prime power
- $|C| = \phi(o(y)) = 8 = 3^2 - 3^0$
- $\hat{C} = C \mathbin{\dot\cup} \{1\} \Rightarrow |\hat{C}| = 3^2$

- If a plain class C satisfies

$$|C| = p^r - p^s \quad \text{and} \quad |\hat{C}| = p^r,$$

we always have:

$$s = 0, \quad \hat{C} = C \mathbin{\dot\cup} \{1\}.$$

Moreover, $C = [z]_{\diamond}$ for some $z \in G$ with $o(z) > 1$ not a prime power, and

$$|C| = \phi(o(z)) = p^r - 1$$

Critical classes

Definition

In a power graph,

critical class:= a $\mathbb{N}$-class C such that

$$\hat{C} = C \cup \{1\}$$

and there exist a prime p and an integer $r \geq 2$ with

$$|\hat{C}| = p^r$$

- A critical class is an $\mathbb{N}$-class which cannot be recognized as plain or compound by arithmetical considerations on its size and on the size of its neighbourhood closure
- Critical classes are crucial for the reconstruction of the directed power graph from the power graph, and they make the work harder

Critical classes

Definition

In a power graph,

critical class:= a $\mathbb{N}$-class C such that

$$\hat{C} = C \cup \{1\}$$

and there exist a prime p and an integer $r \geq 2$ with

$$|\hat{C}| = p^r$$

- A critical class is an $\mathbb{N}$-class which cannot be recognized as plain or compound by arithmetical considerations on its size and on the size of its neighbourhood closure
- Critical classes are crucial for the reconstruction of the directed power graph from the power graph, and they make the work harder

Critical classes

Definition

In a power graph,

critical class:= a $\mathbb{N}$-class C such that

$$\hat{C} = C \,\dot\cup\, \{1\}$$

and there exist a prime p and an integer $r \geq 2$ with

$$|\hat{C}| = p^r$$

- A critical class is an $\mathbb{N}$-class which cannot be recognized as plain or compound by arithmetical considerations on its size and on the size of its neighbourhood closure
- Critical classes are crucial for the reconstruction of the directed power graph from the power graph, and they make the work harder

Examples

All four cases plain/compound combined with critical/not critical may appear

- In $\mathcal{P}(D_{30})$ the $\mathbb{N}$-class of an element of order 15 is plain critical. The other classes are plain not critical
- In $\mathcal{P}(S_4)$ the $\mathbb{N}$-class of a 4-cycle is compound critical
- In $\mathcal{P}(QD_{16})$ the $\mathbb{N}$-class of an element of order 8 is compound not critical. Recall

$$QD_{16} = \langle x, y | x^8 = y^2 = 1, x^y = x^3 \rangle$$

Examples

All four cases plain/compound combined with critical/not critical may appear

- In $\mathcal{P}(D_{30})$ the $\mathtt{N}$-class of an element of order 15 is plain critical. The other classes are plain not critical
- In $\mathcal{P}(S_4)$ the $\mathtt{N}$-class of a 4-cycle is compound critical
- In $\mathcal{P}(QD_{16})$ the $\mathtt{N}$-class of an element of order 8 is compound not critical. Recall

$$QD_{16} = \langle x, y | x^8 = y^2 = 1, x^y = x^3 \rangle$$

Examples

All four cases plain/compound combined with critical/not critical may appear

- In $\mathcal{P}(D_{30})$ the $\mathtt{N}$-class of an element of order 15 is plain critical. The other classes are plain not critical
- In $\mathcal{P}(S_4)$ the $\mathtt{N}$-class of a 4-cycle is compound critical
- In $\mathcal{P}(QD_{16})$ the $\mathtt{N}$-class of an element of order 8 is compound not critical. Recall

$$QD_{16} = \langle x, y | x^8 = y^2 = 1, x^y = x^3 \rangle$$

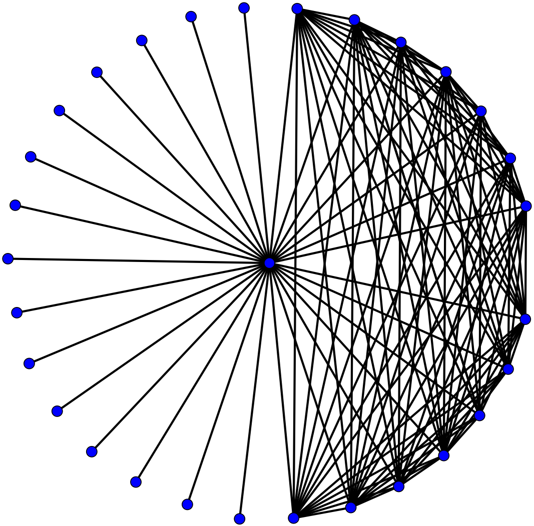
Examples

All four cases plain/compound combined with critical/not critical may appear

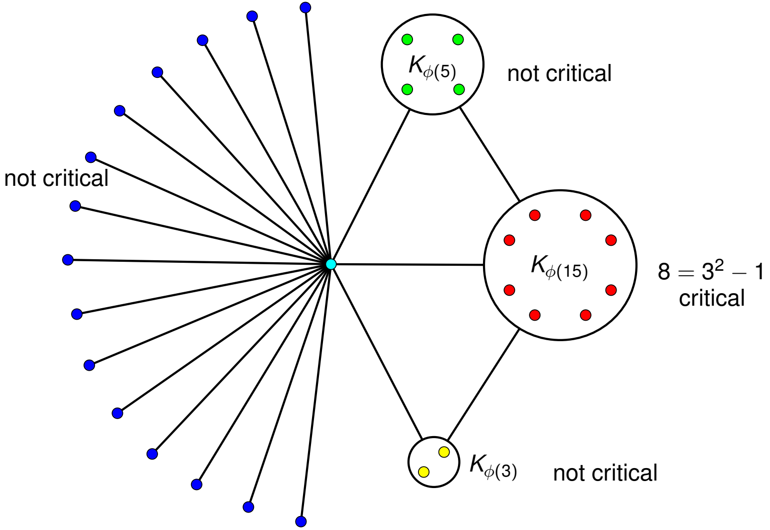
- In $\mathcal{P}(D_{30})$ the $\mathtt{N}$-class of an element of order 15 is plain critical. The other classes are plain not critical
- In $\mathcal{P}(S_4)$ the $\mathtt{N}$-class of a 4-cycle is compound critical
- In $\mathcal{P}(QD_{16})$ the $\mathtt{N}$-class of an element of order 8 is compound not critical. Recall

$$QD_{16} = \langle x, y | x^8 = y^2 = 1, x^y = x^3 \rangle$$

Example $\mathcal{P}(D_{30})$



Example $\mathcal{P}(D_{30})$: plain and critical plain classes



$\mathcal{P}(D_{30})$ with $\mathbb{N}$-classes highlighted

Critical elements

Question

What do critical classes tell about structure and properties of the group?

Definition

$x \in G$ is called

- critical if $[x]_{\mathrm{N}}$ is a critical class in $\mathcal{P}(G)$
- plain [compound] if $[x]_{\mathrm{N}}$ is a plain [compound] class in $\mathcal{P}(G)$

- The class $[1]_{\mathrm{N}} = \mathcal{S}$ is never critical $\Rightarrow$ 1 is never critical
- If there exists $x \in G$ critical, then $\mathcal{S} = \{1\}$ and $G \neq 1$
- $x \in G$ critical is compound iff $o(x) > 1$ is a prime power

Critical elements

Question

What do critical classes tell about structure and properties of the group?

Definition

$x \in G$ is called

- critical if $[x]_{\mathrm{N}}$ is a critical class in $\mathcal{P}(G)$
- plain [compound] if $[x]_{\mathrm{N}}$ is a plain [compound] class in $\mathcal{P}(G)$

- The class $[1]_{\mathrm{N}} = \mathcal{S}$ is never critical $\Rightarrow$ 1 is never critical
- If there exists $x \in G$ critical, then $\mathcal{S} = \{1\}$ and $G \neq 1$
- $x \in G$ critical is compound iff $o(x) > 1$ is a prime power

Critical elements

Question

What do critical classes tell about structure and properties of the group?

Definition

$x \in G$ is called

- critical if $[x]_{\mathrm{N}}$ is a critical class in $\mathcal{P}(G)$
- plain [compound] if $[x]_{\mathrm{N}}$ is a plain [compound] class in $\mathcal{P}(G)$

- The class $[1]_{\mathrm{N}} = \mathcal{S}$ is never critical $\Rightarrow$ 1 is never critical
- If there exists $x \in G$ critical, then $\mathcal{S} = \{1\}$ and $G \neq 1$
- $x \in G$ critical is compound iff $o(x) > 1$ is a prime power

Critical groups

Definition

$G \neq 1$ a group is called

1. critical if every $x \in G \setminus \{1\}$ is critical
2. plain [compound] if every $x \in G \setminus \{1\}$ is plain [compound]

- Critical groups represent an extreme situation.
  It is required that every non-trivial $\mathbb{N}$-class is critical
- We do not know immediately if critical groups exist
- If they exist, in principle, there are three possibilities:
  - every non-trivial class is compound
  - every non-trivial class is plain
  - there exist both plain and compound non-trivial classes

Critical groups

Definition

$G \neq 1$ a group is called

1. critical if every $x \in G \setminus \{1\}$ is critical
2. plain [compound] if every $x \in G \setminus \{1\}$ is plain [compound]

- Critical groups represent an extreme situation.
  It is required that every non-trivial $\mathbb{N}$-class is critical
- We do not know immediately if critical groups exist
- If they exist, in principle, there are three possibilities:
  - every non-trivial class is compound
  - every non-trivial class is plain
  - there exist both plain and compound non-trivial classes

Critical groups

Definition

$G \neq 1$ a group is called

1. critical if every $x \in G \setminus \{1\}$ is critical
2. plain [compound] if every $x \in G \setminus \{1\}$ is plain [compound]

- Critical groups represent an extreme situation.
  It is required that every non-trivial $\mathbb{N}$-class is critical
- We do not know immediately if critical groups exist
- If they exist, in principle, there are three possibilities:
  - every non-trivial class is compound
  - every non-trivial class is plain
  - there exist both plain and compound non-trivial classes

Critical groups

Definition

$G \neq 1$ a group is called

1. critical if every $x \in G \setminus \{1\}$ is critical
2. plain [compound] if every $x \in G \setminus \{1\}$ is plain [compound]

- Critical groups represent an extreme situation.
  It is required that every non-trivial $\mathbb{N}$-class is critical
- We do not know immediately if critical groups exist
- If they exist, in principle, there are three possibilities:
  - every non-trivial class is compound
  - every non-trivial class is plain
  - there exist both plain and compound non-trivial classes

Partitions and existence of critical groups

Definition

A partition of $G \neq 1$ is a set $\mathscr{P}$ of non-trivial subgroups of G, such that every element $x \in G \setminus \{1\}$ belongs to a unique subgroup in $\mathscr{P}$.

If $|\mathscr{P}| = 1$, the partition is called trivial.

- The groups admitting a non-trivial partition are known (Kegel, Baer, Suzuki).
  Among them, we find the Frobenius groups. For instance, D_{2n} for n odd

Partitions and existence of critical groups

Definition

A partition of $G \neq 1$ is a set $\mathscr{P}$ of non-trivial subgroups of G, such that every element $x \in G \setminus \{1\}$ belongs to a unique subgroup in $\mathscr{P}$.
If $|\mathscr{P}| = 1$, the partition is called trivial.

- The groups admitting a non-trivial partition are known (Kegel, Baer, Suzuki).
  Among them, we find the Frobenius groups. For instance, D_{2n} for n odd

Partitions and existence of critical groups

Definition

A partition of $G \neq 1$ is a set $\mathscr{P}$ of non-trivial subgroups of G, such that every element $x \in G \setminus \{1\}$ belongs to a unique subgroup in $\mathscr{P}$.
If $|\mathscr{P}| = 1$, the partition is called trivial.

- The groups admitting a non-trivial partition are known (Kegel, Baer, Suzuki).
  Among them, we find the Frobenius groups. For instance, D_{2n} for n odd

Partitions and existence of critical groups

Definition

A partition of $G \neq 1$ is a set $\mathscr{P}$ of non-trivial subgroups of G, such that every element $x \in G \setminus \{1\}$ belongs to a unique subgroup in $\mathscr{P}$.
If $|\mathscr{P}| = 1$, the partition is called trivial.

- The groups admitting a non-trivial partition are known (Kegel, Baer, Suzuki).
  Among them, we find the Frobenius groups. For instance, D_{2n} for n odd

Proposition 1 (B. P. 2024)

A group admitting a non-trivial partition into cyclic subgroups of order a prime power with exponent at least 2 is critical

Proof.

- $\mathcal{P}$ a partition of G by cyclic subgroups of order a prime power with exponent at least 2.
- $x \in G \setminus \{1\} \Rightarrow$ there exists a unique $U \in \mathcal{P}$ such that $x \in U$. We show that $N[x] = U$. It follows that

$$[x]_{\mathrm{N}} = U \setminus \{1\}$$

and

$$\widehat{[x]_{\mathrm{N}}} = U = [x]_{\mathrm{N}} \cup \{1\}.$$

- By $|U| = p^r$, p prime, $r \geq 2$, we deduce x critical. □

Proposition 1 (B. P. 2024)

A group admitting a non-trivial partition into cyclic subgroups of order a prime power with exponent at least 2 is critical

Proof.

- $\mathcal{P}$ a partition of G by cyclic subgroups of order a prime power with exponent at least 2.
- $x \in G \setminus \{1\} \Rightarrow$ there exists a unique $U \in \mathcal{P}$ such that $x \in U$. We show that $N[x] = U$. It follows that

$$[x]_{\mathrm{N}} = U \setminus \{1\}$$

and

$$\widehat{[x]_{\mathrm{N}}} = U = [x]_{\mathrm{N}} \dot\cup \{1\}.$$

- By $|U| = p^r$, p prime, $r \geq 2$, we deduce x critical. $\square$

Proposition 1 (B. P. 2024)

A group admitting a non-trivial partition into cyclic subgroups of order a prime power with exponent at least 2 is critical

Proof.

- $\mathcal{P}$ a partition of G by cyclic subgroups of order a prime power with exponent at least 2.
- $x \in G \setminus \{1\} \Rightarrow$ there exists a unique $U \in \mathcal{P}$ such that $x \in U$. We show that $N[x] = U$. It follows that

$$[x]_{\mathrm{N}} = U \setminus \{1\}$$

and

$$\widehat{[x]_{\mathrm{N}}} = U = [x]_{\mathrm{N}} \cup \{1\}.$$

- By $|U| = p^r$, p prime, $r \geq 2$, we deduce x critical. □

Proposition 1 (B. P. 2024)

A group admitting a non-trivial partition into cyclic subgroups of order a prime power with exponent at least 2 is critical

Proof.

- $\mathcal{P}$ a partition of G by cyclic subgroups of order a prime power with exponent at least 2.
- $x \in G \setminus \{1\} \Rightarrow$ there exists a unique $U \in \mathcal{P}$ such that $x \in U$. We show that $N[x] = U$. It follows that

$$[x]_{\mathrm{N}} = U \setminus \{1\}$$

and

$$\widehat{[x]_{\mathrm{N}}} = U = [x]_{\mathrm{N}} \mathbin{\dot\cup} \{1\}.$$

- By $|U| = p^r$, p prime, $r \geq 2$, we deduce x critical. □

Proposition 1 (B. P. 2024)

A group admitting a non-trivial partition into cyclic subgroups of order a prime power with exponent at least 2 is critical

Proof.

- $\mathcal{P}$ a partition of G by cyclic subgroups of order a prime power with exponent at least 2.
- $x \in G \setminus \{1\} \Rightarrow$ there exists a unique $U \in \mathcal{P}$ such that $x \in U$. We show that $N[x] = U$. It follows that

$$[x]_{\mathrm{N}} = U \setminus \{1\}$$

and

$$\widehat{[x]_{\mathrm{N}}} = U = [x]_{\mathrm{N}} \mathbin{\dot\cup} \{1\}.$$

- By $|U| = p^r$, p prime, $r \geq 2$, we deduce x critical. □

Proposition 1 (B. P. 2024)

A group admitting a non-trivial partition into cyclic subgroups of order a prime power with exponent at least 2 is critical

Proof.

- $\mathcal{P}$ a partition of G by cyclic subgroups of order a prime power with exponent at least 2.
- $x \in G \setminus \{1\} \Rightarrow$ there exists a unique $U \in \mathcal{P}$ such that $x \in U$. We show that $N[x] = U$. It follows that

$$[x]_{\mathrm{N}} = U \setminus \{1\}$$

and

$$\widehat{[x]_{\mathrm{N}}} = U = [x]_{\mathrm{N}} \,\dot{\cup}\, \{1\}.$$

- By $|U| = p^r$, p prime, $r \geq 2$, we deduce x critical. □

Frobenius groups

Proposition

Let $C_{p^a} = \langle x \rangle$ and $C_{q^b} = \langle y \rangle$ with $p \neq q$ primes and $a, b \geq 2$ integers. Then

(*i*) the group $C_{p^a} \rtimes C_{q^b}$ defined by $x^y = x^r$, with $2 \leq r < p^a$ such that $p \nmid r$, is a Frobenius group with kernel C_{p^a} iff $q^b = |r|_{\mod p}$

(*ii*) the Frobenius groups in (*i*) exist iff $q^b \mid p - 1$.

- Note that $q^b \mid p - 1, b \geq 2 \Rightarrow p \notin \{2, 3\}$
- Since $4 = |7|_{\mod 5}$, $C_{25} \rtimes C_4$ defined by $x^y = x^7$ is Frobenius and thus, considering its partition by kernel and complements and using Proposition 1, we deduce that it is critical
- $\Longrightarrow$ critical groups do exist. Try to find all of them!

Frobenius groups

Proposition

Let $C_{p^a} = \langle x \rangle$ and $C_{q^b} = \langle y \rangle$ with $p \neq q$ primes and $a, b \geq 2$ integers. Then

- (i) the group $C_{p^a} \rtimes C_{q^b}$ defined by $x^y = x^r$, with $2 \leq r < p^a$ such that $p \nmid r$, is a Frobenius group with kernel C_{p^a} iff $q^b = |r|_{\mod p}$
- (ii) the Frobenius groups in (i) exist iff $q^b \mid p - 1$.

- Note that $q^b \mid p - 1, b \geq 2 \Rightarrow p \notin \{2, 3\}$
- Since $4 = |7|_{\mod 5}$, $C_{25} \rtimes C_4$ defined by $x^y = x^7$ is Frobenius and thus, considering its partition by kernel and complements and using Proposition 1, we deduce that it is critical
- $\Longrightarrow$ critical groups do exist. Try to find all of them!

Frobenius groups

Proposition

Let $C_{p^a} = \langle x \rangle$ and $C_{q^b} = \langle y \rangle$ with $p \neq q$ primes and $a, b \geq 2$ integers. Then

(*i*) the group $C_{p^a} \rtimes C_{q^b}$ defined by $x^y = x^r$, with $2 \leq r < p^a$ such that $p \nmid r$, is a Frobenius group with kernel C_{p^a} iff $q^b = |r|_{\mod p}$

(*ii*) the Frobenius groups in (*i*) exist iff $q^b \mid p - 1$.

- Note that $q^b \mid p - 1, b \geq 2 \Rightarrow p \notin \{2, 3\}$
- Since $4 = |7|_{\mod 5}$, $C_{25} \rtimes C_4$ defined by $x^y = x^7$ is Frobenius and thus, considering its partition by kernel and complements and using Proposition 1, we deduce that it is critical
- $\Longrightarrow$ critical groups do exist. Try to find all of them!

An easy fact

Using the fact that a plain critical element cannot have prime order, we deduce immediately

Remark

There exists no plain critical group

However, it remains the possibility to have both plain and compound classes in a critical group...

Local properties of critical groups

Lemma 1

Let G be a critical group and p a prime dividing $|G|$. Then, every element of order p is the power of an element of order p^2.
In particular, $p^2 \mid |G|$.

$\Downarrow$

Proposition 2 (B. P. 2024)

If G is a critical group, then G is compound critical

Local properties of critical groups

Lemma 1

Let G be a critical group and p a prime dividing $|G|$. Then, every element of order p is the power of an element of order p^2.
In particular, $p^2 \mid |G|$.

$$\Downarrow$$

Proposition 2 (B. P. 2024)

If G is a critical group, then G is compound critical

Local properties of critical groups

Lemma 1

Let G be a critical group and p a prime dividing $|G|$. Then, every element of order p is the power of an element of order p^2.
In particular, $p^2 \mid |G|$.

$\Downarrow$

Proposition 2 (B. P. 2024)

If G is a critical group, then G is compound critical

The characterization of critical groups

A surprising result

Main Theorem (B. P. 2024)

A group G is critical iff there exist p, q distinct primes, with p odd, and $a, b \geq 2$ integers such that
G is a Frobenius group with kernel $F \cong C_{p^a}$ and complement $H \cong C_{q^b}$

Since we know how to get all such Frobenius groups, we know all the possible critical groups

- The proof is elaborate and involves the theory of partitions
- For instance, a result on the Hughes-Thompson subgroup of the Sylow subgroups of a critical group

The characterization of critical groups

A surprising result

Main Theorem (B. P. 2024)

A group G is critical iff there exist p, q distinct primes, with p odd, and $a, b \geq 2$ integers such that
G is a Frobenius group with kernel $F \cong C_{p^a}$ and complement $H \cong C_{q^b}$

Since we know how to get all such Frobenius groups, we know all the possible critical groups

- The proof is elaborate and involves the theory of partitions
- For instance, a result on the Hughes-Thompson subgroup of the Sylow subgroups of a critical group

The characterization of critical groups

A surprising result

Main Theorem (B. P. 2024)

A group G is critical iff there exist p, q distinct primes, with p odd, and $a, b \geq 2$ integers such that
G is a Frobenius group with kernel $F \cong C_{p^a}$ and complement $H \cong C_{q^b}$

Since we know how to get all such Frobenius groups, we know all the possible critical groups

- The proof is elaborate and involves the theory of partitions
- For instance, a result on the Hughes-Thompson subgroup of the Sylow subgroups of a critical group

The characterization of critical groups

A surprising result

Main Theorem (B. P. 2024)

A group G is critical iff there exist p, q distinct primes, with p odd, and $a, b \geq 2$ integers such that
G is a Frobenius group with kernel $F \cong C_{p^a}$ and complement $H \cong C_{q^b}$

Since we know how to get all such Frobenius groups, we know all the possible critical groups

- The proof is elaborate and involves the theory of partitions
- For instance, a result on the Hughes-Thompson subgroup of the Sylow subgroups of a critical group

The characterization of critical groups

A surprising result

Main Theorem (B. P. 2024)

A group G is critical iff there exist p, q distinct primes, with p odd, and $a, b \geq 2$ integers such that G is a Frobenius group with kernel $F \cong C_{p^a}$ and complement $H \cong C_{q^b}$

Since we know how to get all such Frobenius groups, we know all the possible critical groups

- The proof is elaborate and involves the theory of partitions
- For instance, a result on the Hughes-Thompson subgroup of the Sylow subgroups of a critical group

Sylow subgroups of critical groups

- The Hughes-Thompson subgroup of a p-group P

$$H_p(P) := \langle x \in P : o(x) \neq p \rangle$$

Theorem (Kegel 1961)

A p-group P admits a non-trivial partition if and only if $H_p(P) \neq P$

Proposition 3 (B. P. 2024)

Let G be a critical group, p a prime dividing $|G|$ and $P \in \mathrm{Syl}_p(G)$. Then

- $H_p(P) = P$
- P admits only the trivial partition

Sylow subgroups of critical groups

- The Hughes-Thompson subgroup of a p-group P

$$H_p(P) := \langle x \in P : o(x) \neq p \rangle$$

Theorem (Kegel 1961)

A p-group P admits a non-trivial partition if and only if $H_p(P) \neq P$

Proposition 3 (B. P. 2024)

Let G be a critical group, p a prime dividing $|G|$ and $P \in \mathrm{Syl}_p(G)$. Then

- $H_p(P) = P$
- P admits only the trivial partition

Sylow subgroups of critical groups

- The Hughes-Thompson subgroup of a p-group P

$$H_p(P) := \langle x \in P : o(x) \neq p \rangle$$

Theorem (Kegel 1961)

A p-group P admits a non-trivial partition if and only if $H_p(P) \neq P$

Proposition 3 (B. P. 2024)

Let G be a critical group, p a prime dividing $|G|$ and $P \in \mathrm{Syl}_p(G)$. Then

- $H_p(P) = P$
- P admits only the trivial partition

Sketch of the proof of the Main Theorem

- A critical group G is necessarily compound and thus an EPPO non-cyclic group
- The neighbourhood closures of the non-trivial $\mathbb{N}$-classes give a partition $\mathcal{P}$ of G into maximal cyclic subgroups which turn out to be the Sylow subgroups of G
- The theorem by Hölder, Burnside, Zassenhaus characterizing the finite groups with cyclic Sylow subgroups in the EPPO case, implies that $\pi(G) = \{p, q\}$ with the p-Sylow subgroup normal
- The q-Sylow subgroup is selfnormalizing. By the presence of $\mathcal{P}$, this implies G to be a Frobenius group with the required structure

Sketch of the proof of the Main Theorem

- A critical group G is necessarily compound and thus an EPPO non-cyclic group
- The neighbourhood closures of the non-trivial $\mathtt{N}$-classes give a partition $\mathcal{P}$ of G into maximal cyclic subgroups which turn out to be the Sylow subgroups of G
- The theorem by Hölder, Burnside, Zassenhaus characterizing the finite groups with cyclic Sylow subgroups in the EPPO case, implies that $\pi(G) = \{p, q\}$ with the p-Sylow subgroup normal
- The q-Sylow subgroup is selfnormalizing. By the presence of $\mathcal{P}$, this implies G to be a Frobenius group with the required structure

Sketch of the proof of the Main Theorem

- A critical group G is necessarily compound and thus an EPPO non-cyclic group
- The neighbourhood closures of the non-trivial $\mathbb{N}$-classes give a partition $\mathcal{P}$ of G into maximal cyclic subgroups which turn out to be the Sylow subgroups of G
- The theorem by Hölder, Burnside, Zassenhaus characterizing the finite groups with cyclic Sylow subgroups in the EPPO case, implies that $\pi(G) = \{p, q\}$ with the p-Sylow subgroup normal
- The q-Sylow subgroup is selfnormalizing. By the presence of $\mathcal{P}$, this implies G to be a Frobenius group with the required structure

Thanks for your attention!

Thanks for your attention!

References

- D. Bubboloni, N. Pinzauti, *Critical classes of power graphs and reconstruction of directed power graphs*, arxiv/4620170 (2023)
- P. J. Cameron, *The power graph of a finite group, II*, Journal of Group Theory **13** (2010), 779–783
- P. J. Cameron, S. Ghosh, *The power graph of a finite group*, Discrete Mathematics **311** (2011), 1220–1222
- P. J. Cameron, *Graphs defined on groups*, International Journal of Group Theory, vol.**11** No. 2 (2022), 53–107