# QCSPs on finite groups

## Work in Progress

K. Kearnes [1] B. Larose [2] B. Martin [3] Á. Szendrei [1]

[1]Boulder, CO

[2]LACIM, UQAM, Montréal

[3]Durham, UK

Joint Mathematics Meetings Denver, January 2020

# A decision problem: $QCSP(\mathbf{G})$

Let $\mathbf{G} = \langle G; \cdot, 1\rangle$ be a finite group.

**$QCSP(\mathbf{G})$**

- *Instance: a sentence* $\forall y_1 \exists x_1 \cdots \forall y_n \exists x_n \, \Phi$*,*
  *where* $\Phi$ *is a conjunction of term equations over* $\mathbf{G}$*;*
- *Problem: Is the sentence true ?*

# A decision problem: $QCSP(\mathbf{G})$

Let $\mathbf{G} = \langle G; \cdot, 1 \rangle$ be a finite group.

**$QCSP(\mathbf{G})$**

- *Instance: a sentence $\forall y_1 \exists x_1 \cdots \forall y_n \exists x_n \, \Phi$, where $\Phi$ is a conjunction of term equations over $\mathbf{G}$;*
- *Problem: Is the sentence true ?*

A typical instance of $QCSP(\mathbf{G})$:

$$\forall x \exists y \forall z \exists w \begin{cases} x^3 y^2 & = & z \\ z^5 & = & 1 \\ x^{-1} z^{-4} & = & y^3 w^6 \end{cases}$$

# A decision problem: *QCSP*(**G**)

Let $\mathbf{G} = \langle G; \cdot, 1 \rangle$ be a finite group.

### *QCSP*(**G**)

- *Instance: a sentence* $\forall y_1 \exists x_1 \cdots \forall y_n \exists x_n\, \Phi$*,*
  *where* $\Phi$ *is a conjunction of term equations over* $\mathbf{G}$*;*
- *Problem: Is the sentence true ?*

A typical instance of *QCSP*(**G**):

$$\forall x \exists y \forall z \exists w \begin{cases} x^3 y^2 & = & z \\ z^5 & = & 1 \\ x^{-1} z^{-4} & = & y^3 w^6 \end{cases}$$

*Complexity*: How hard is this ?

# Another decision problem: $QCSP_c(\mathbf{G})$

Let $\mathbf{G} = \langle G; \cdot, 1 \rangle$ be a finite group.

**$QCSP_c(\mathbf{G})$**

- *Instance: a sentence* $\forall y_1 \exists x_1 \cdots \forall y_n \exists x_n \, \Phi$,
  *where* $\Phi$ *is a conjunction of polynomial equations over* $\mathbf{G}$;
- *Problem: Is the sentence true ?*

# Another decision problem: $QCSP_c(\mathbf{G})$

Let $\mathbf{G} = \langle G; \cdot, 1 \rangle$ be a finite group.

## $QCSP_c(\mathbf{G})$

- *Instance: a sentence $\forall y_1 \exists x_1 \cdots \forall y_n \exists x_n \, \Phi$, where $\Phi$ is a conjunction of polynomial equations over $\mathbf{G}$;*
- *Problem: Is the sentence true ?*

A typical instance of $QCSP_c(\mathbf{G})$ (here $c, d, e, f, g \in \mathbf{G}$):

$$\forall x \exists y \forall z \exists w \begin{cases} cx^3dy^2 & = & ez \\ z^5 & = & f \\ x^{-1}z^{-4} & = & w^2y^3g \end{cases}$$

# Another decision problem: $QCSP_c(\mathbf{G})$

Let $\mathbf{G} = \langle G; \cdot, 1 \rangle$ be a finite group.

**$QCSP_c(\mathbf{G})$**

- *Instance: a sentence $\forall y_1 \exists x_1 \cdots \forall y_n \exists x_n \, \Phi$, where $\Phi$ is a conjunction of polynomial equations over $\mathbf{G}$;*
- *Problem: Is the sentence true ?*

A typical instance of $QCSP_c(\mathbf{G})$ (here $c, d, e, f, g \in \mathbf{G}$):

$$\forall x \exists y \forall z \exists w \begin{cases} cx^3dy^2 & = & ez \\ z^5 & = & f \\ x^{-1}z^{-4} & = & w^2y^3g \end{cases}$$

*Complexity*: How hard is this ?

# Context

- the above problems are (logspace-equivalent to) a special case of the general QCSP problem $QCSP(\Gamma)$ where $\Gamma$ is a set of finitary relations on a finite domain;

# Context

- the above problems are (logspace-equivalent to) a special case of the general QCSP problem $QCSP(\Gamma)$ where $\Gamma$ is a set of finitary relations on a finite domain;
- on the other hand, $QCSP(\mathbf{G})$ and $QCSP_c(\mathbf{G})$ generalise the problems $CSP(\mathbf{G})$ and $CSP_c(\mathbf{G})$ (by forbidding the use of $\forall$):

# Context

- the above problems are (logspace-equivalent to) a special case of the general QCSP problem $QCSP(\Gamma)$ where $\Gamma$ is a set of finitary relations on a finite domain;
- on the other hand, $QCSP(\mathbf{G})$ and $QCSP_c(\mathbf{G})$ generalise the problems $CSP(\mathbf{G})$ and $CSP_c(\mathbf{G})$ (by forbidding the use of $\forall$):
  - $CSP(\mathbf{G})$: is a given system of term equations over $\mathbf{G}$ satisfiable ?

# Context

- the above problems are (logspace-equivalent to) a special case of the general QCSP problem $QCSP(\Gamma)$ where $\Gamma$ is a set of finitary relations on a finite domain;
- on the other hand, $QCSP(\mathbf{G})$ and $QCSP_c(\mathbf{G})$ generalise the problems $CSP(\mathbf{G})$ and $CSP_c(\mathbf{G})$ (by forbidding the use of $\forall$):
  - $CSP(\mathbf{G})$: is a given system of term equations over **G** satisfiable ?
    - Trivial (set every variable to 1)

# Context

- the above problems are (logspace-equivalent to) a special case of the general QCSP problem $QCSP(\Gamma)$ where $\Gamma$ is a set of finitary relations on a finite domain;
- on the other hand, $QCSP(\mathbf{G})$ and $QCSP_c(\mathbf{G})$ generalise the problems $CSP(\mathbf{G})$ and $CSP_c(\mathbf{G})$ (by forbidding the use of $\forall$):
  - $CSP(\mathbf{G})$: is a given system of term equations over **G** satisfiable ?
    - Trivial (set every variable to 1)
  - $CSP_c(\mathbf{G})$: is a given system of polynomial equations over **G** satisfiable ?

# Context

- the above problems are (logspace-equivalent to) a special case of the general QCSP problem $QCSP(\Gamma)$ where $\Gamma$ is a set of finitary relations on a finite domain;
- on the other hand, $QCSP(\mathbf{G})$ and $QCSP_c(\mathbf{G})$ generalise the problems $CSP(\mathbf{G})$ and $CSP_c(\mathbf{G})$ (by forbidding the use of $\forall$):
  - $CSP(\mathbf{G})$: is a given system of term equations over **G** satisfiable ?
    - Trivial (set every variable to 1)
  - $CSP_c(\mathbf{G})$: is a given system of polynomial equations over **G** satisfiable ?
    - in P if **G** is Abelian, NP-c otherwise. (Goldmann, Russell, 2002).

# Context

- the above problems are (logspace-equivalent to) a special case of the general QCSP problem $QCSP(\Gamma)$ where $\Gamma$ is a set of finitary relations on a finite domain;
- on the other hand, $QCSP(\mathbf{G})$ and $QCSP_c(\mathbf{G})$ generalise the problems $CSP(\mathbf{G})$ and $CSP_c(\mathbf{G})$ (by forbidding the use of $\forall$):
  - $CSP(\mathbf{G})$: is a given system of term equations over **G** satisfiable ?
    - Trivial (set every variable to 1)
  - $CSP_c(\mathbf{G})$: is a given system of polynomial equations over **G** satisfiable ?
    - in P if **G** is Abelian, NP-c otherwise. (Goldmann, Russell, 2002).
    - Intriguing (same authors): deciding satisfiability of a *single* equation is NP-c for non-solvable groups, in P for nilpotent groups (and otherwise still open).

*****

# Context, continued

- because our problems are equivalent to problems of the form $QCSP(\Gamma)$, known tools can be used:

# Context, continued

- because our problems are equivalent to problems of the form $QCSP(\Gamma)$, known tools can be used:
- complexity is controlled by the **onto** polymorphisms of the constraint relations (BBCJK, 2009):

# Context, continued

- because our problems are equivalent to problems of the form $QCSP(\Gamma)$, known tools can be used:
- complexity is controlled by the **onto** polymorphisms of the constraint relations (BBCJK, 2009):
- in our context, the constraint relation is $\gamma_{\mathbf{G}} = \{(x, y, z) : xy = z\}$ together with singleton unary relations for $QCSP_c(\mathbf{G})$, and thus the "polymorphisms" are:

# Context, continued

- because our problems are equivalent to problems of the form $QCSP(\Gamma)$, known tools can be used:
- complexity is controlled by the **onto** polymorphisms of the constraint relations (BBCJK, 2009):
- in our context, the constraint relation is $\gamma_{\mathbf{G}} = \{(x, y, z) : xy = z\}$ together with singleton unary relations for $QCSP_c(\mathbf{G})$, and thus the "polymorphisms" are:
  - the onto group homomorphisms $f : \mathbf{G}^n \to \mathbf{G}$ for $QCSP(\mathbf{G})$,

# Context, continued

- because our problems are equivalent to problems of the form $QCSP(\Gamma)$, known tools can be used:
- complexity is controlled by the **onto** polymorphisms of the constraint relations (BBCJK, 2009):
- in our context, the constraint relation is $\gamma_{\mathbf{G}} = \{(x, y, z) : xy = z\}$ together with singleton unary relations for $QCSP_c(\mathbf{G})$, and thus the "polymorphisms" are:
  - the onto group homomorphisms $f : \mathbf{G}^n \to \mathbf{G}$ for $QCSP(\mathbf{G})$,
  - the idempotent group homomorphisms $f : \mathbf{G}^n \to \mathbf{G}$ for $QCSP_c(\mathbf{G})$, i.e. satisfying $f(x, x, \ldots, x) = x$ for all $x \in G$.

*****

# Preliminaries

- In general $QCSP(\Gamma)$ is in Pspace;

# Preliminaries

- In general $QCSP(\Gamma)$ is in Pspace;
- if the onto polymorphisms are essentially unary then $QCSP(\Gamma)$ is Pspace-complete (BBCJK, 2009);

# Preliminaries

- In general $QCSP(\Gamma)$ is in Pspace;
- if the onto polymorphisms are essentially unary then $QCSP(\Gamma)$ is Pspace-complete (BBCJK, 2009);
- If $\mathbf{G}$ is non-Abelian, $QCSP_c(\mathbf{G})$ is NP-hard;

# Preliminaries

- In general $QCSP(\Gamma)$ is in Pspace;
- if the onto polymorphisms are essentially unary then $QCSP(\Gamma)$ is Pspace-complete (BBCJK, 2009);
- If $\mathbf{G}$ is non-Abelian, $QCSP_c(\mathbf{G})$ is NP-hard;
  - because of $CSP_c(\mathbf{G})$

# Preliminaries

- In general $QCSP(\Gamma)$ is in Pspace;
- if the onto polymorphisms are essentially unary then $QCSP(\Gamma)$ is Pspace-complete (BBCJK, 2009);
- If $\mathbf{G}$ is non-Abelian, $QCSP_c(\mathbf{G})$ is NP-hard;
  - because of $CSP_c(\mathbf{G})$
- Clearly $QCSP_c(\mathbf{G})$ is always as hard as $QCSP(\mathbf{G})$.

*****

# A tractable case

**Theorem**

*If* $\mathbf{G}$ *is Abelian, then both* $QCSP(\mathbf{G})$ *and* $QCSP_c(\mathbf{G})$ *are in P.*

# A tractable case

**Theorem**

*If $\mathbf{G}$ is Abelian, then both QCSP$(\mathbf{G})$ and QCSP$_c(\mathbf{G})$ are in P.*

*Proof:* If $\mathbf{G}$ is Abelian, then the Maltsev operation

$$M(x, y, z) = x - y + z$$

is an idempotent group homomorphism $M : \mathbf{G}^3 \to \mathbf{G}$. By BBCJK, 2009, the presence of a Maltsev polymorphism guarantees tractability. $\square$

# A tractable case

**Theorem**

*If **G** is Abelian, then both QCSP(**G**) and $QCSP_c$(**G**) are in P.*

*Proof:* If **G** is Abelian, then the Maltsev operation

$$M(x, y, z) = x - y + z$$

is an idempotent group homomorphism $M : \mathbf{G}^3 \to \mathbf{G}$. By BBCJK, 2009, the presence of a Maltsev polymorphism guarantees tractability. □

- At the moment we have no other tractable cases (and there are probably no others (?))

# A hardness criterion

## Definition

Let **G** be a group, and let $\theta$ be a relation on $G$. We say that $\theta$ is **definable** on **G** if it can be defined using $\gamma_{\mathbf{G}}$ and $=$ using conjunction, and the existential and universal quantifiers.

# A hardness criterion

## Definition

Let **G** be a group, and let $\theta$ be a relation on $G$. We say that $\theta$ is **definable** on **G** if it can be defined using $\gamma_{\mathbf{G}}$ and $=$ using conjunction, and the existential and universal quantifiers.

- Alternatively, $\theta$ is definable if and only if it is invariant under all onto group homomorphisms $f : \mathbf{G}^n \to \mathbf{G}$.

# A hardness criterion

**Definition**

Let $\mathbf{G}$ be a group, and let $\theta$ be a relation on $G$. We say that $\theta$ is **definable** on $\mathbf{G}$ if it can be defined using $\gamma_{\mathbf{G}}$ and $=$ using conjunction, and the existential and universal quantifiers.

- Alternatively, $\theta$ is definable if and only if it is invariant under all onto group homomorphisms $f : \mathbf{G}^n \to \mathbf{G}$.
- For instance, if $\theta$ is the congruence determined by the center $Z(\mathbf{G})$, then it is definable:

$$\theta = \{(x, y) : \forall z,\ xy^{-1}z = zxy^{-1}\}.$$

# A hardness criterion, continued

- Let $\theta$ be an equivalence relation on $G$, let $f$ be an operation on $G$ that preserves $\theta$. Let $f^\theta$ denote the operation induced by $f$ on the $\theta$-blocks, i.e.

$$f^\theta(x_1/\theta, \ldots, x_n/\theta) = f(x_1, \ldots, x_n)/\theta.$$

# A hardness criterion, continued

- Let $\theta$ be an equivalence relation on $G$, let $f$ be an operation on $G$ that preserves $\theta$. Let $f^\theta$ denote the operation induced by $f$ on the $\theta$-blocks, i.e.

$$f^\theta(x_1/\theta, \ldots, x_n/\theta) = f(x_1, \ldots, x_n)/\theta.$$

## Lemma

*Let $\theta \neq G^2$ be a definable equivalence relation on $\mathbf{G}$. If $f^\theta$ is essentially unary for every onto homomorphism $f : \mathbf{G}^n \to \mathbf{G}$ then QCSP$(\mathbf{G})$ is Pspace-complete.*

# A hardness criterion, continued

- Let $\theta$ be an equivalence relation on $G$, let $f$ be an operation on $G$ that preserves $\theta$. Let $f^\theta$ denote the operation induced by $f$ on the $\theta$-blocks, i.e.

$$f^\theta(x_1/\theta, \dots, x_n/\theta) = f(x_1, \dots, x_n)/\theta.$$

**Lemma**

*Let $\theta \neq G^2$ be a definable equivalence relation on $\mathbf{G}$. If $f^\theta$ is essentially unary for every onto homomorphism $f : \mathbf{G}^n \to \mathbf{G}$ then QCSP$(\mathbf{G})$ is Pspace-complete.*

*Proof:* This is a straightforward application of results from BBCJK, 2009 and Chen, Mayr 2016. $\square$

# Strategy

- It seems reasonable at this point to aim for a proof of Pspace-hardness for $QCSP(\mathbf{G})$ for any non-Abelian group;

# Strategy

- It seems reasonable at this point to aim for a proof of Pspace-hardness for $QCSP(\mathbf{G})$ for any non-Abelian group;
- A possible strategy: if a definable quotient of $\mathbf{G}$ is onto-trivial, by our criterion $QCSP(\mathbf{G})$ is Pspace-complete;

# Strategy

- It seems reasonable at this point to aim for a proof of Pspace-hardness for $QCSP(\mathbf{G})$ for any non-Abelian group;
- A possible strategy: if a definable quotient of $\mathbf{G}$ is onto-trivial, by our criterion $QCSP(\mathbf{G})$ is Pspace-complete;
- Hence it would be interesting to characterise groups that are

# Strategy

- It seems reasonable at this point to aim for a proof of Pspace-hardness for $QCSP(\mathbf{G})$ for any non-Abelian group;
- A possible strategy: if a definable quotient of **G** is onto-trivial, by our criterion $QCSP(\mathbf{G})$ is Pspace-complete;
- Hence it would be interesting to characterise groups that are
  - *onto-trivial*, i.e. whose onto homomorphisms are all essentially unary;

# Strategy

- It seems reasonable at this point to aim for a proof of Pspace-hardness for $QCSP(\mathbf{G})$ for any non-Abelian group;
- A possible strategy: if a definable quotient of $\mathbf{G}$ is onto-trivial, by our criterion $QCSP(\mathbf{G})$ is Pspace-complete;
- Hence it would be interesting to characterise groups that are
  - *onto-trivial*, i.e. whose onto homomorphisms are all essentially unary;
  - *idempotent trivial*, i.e. whose idempotent homomorphisms are are projections.

# Strategy

- It seems reasonable at this point to aim for a proof of Pspace-hardness for $QCSP(\mathbf{G})$ for any non-Abelian group;
- A possible strategy: if a definable quotient of $\mathbf{G}$ is onto-trivial, by our criterion $QCSP(\mathbf{G})$ is Pspace-complete;
- Hence it would be interesting to characterise groups that are
  - *onto-trivial*, i.e. whose onto homomorphisms are all essentially unary;
  - *idempotent trivial*, i.e. whose idempotent homomorphisms are are projections.
- Stumbling blocks: direct products, nilpotent groups ..... (more on this later);

# Strategy

- It seems reasonable at this point to aim for a proof of Pspace-hardness for *QCSP*($\mathbf{G}$) for any non-Abelian group;
- A possible strategy: if a definable quotient of $\mathbf{G}$ is onto-trivial, by our criterion *QCSP*($\mathbf{G}$) is Pspace-complete;
- Hence it would be interesting to characterise groups that are
  - *onto-trivial*, i.e. whose onto homomorphisms are all essentially unary;
  - *idempotent trivial*, i.e. whose idempotent homomorphisms are are projections.
- Stumbling blocks: direct products, nilpotent groups ..... (more on this later);
- *from now on, most of the work is group-theoretic.*

# Strategy

- It seems reasonable at this point to aim for a proof of Pspace-hardness for *QCSP*($\mathbf{G}$) for any non-Abelian group;
- A possible strategy: if a definable quotient of $\mathbf{G}$ is onto-trivial, by our criterion *QCSP*($\mathbf{G}$) is Pspace-complete;
- Hence it would be interesting to characterise groups that are
  - *onto-trivial*, i.e. whose onto homomorphisms are all essentially unary;
  - *idempotent trivial*, i.e. whose idempotent homomorphisms are are projections.
- Stumbling blocks: direct products, nilpotent groups ..... (more on this later);
- *from now on, most of the work is group-theoretic.*
- Notation: $[\mathbf{A}, \mathbf{B}] =$ subgroup generated by the $aba^{-1}b^{-1}$; $\mathbf{G}' = [\mathbf{G}, \mathbf{G}]$.

# Onto homomorphisms: a crucial result

## Definition

Let $\mathbf{G}$ be a group. Let $f : \mathbf{G}^n \to \mathbf{G}$ be an onto homomorphism.
For each $1 \leq i \leq n$, let

- $f_i(x) = f(1, 1, \ldots, 1, x, 1, \ldots, 1)$ ($x$ in $i - th$ position),
- let $\mathbf{A}_i$ be the image of $f_i$ in $\mathbf{G}$.

# Onto homomorphisms: a crucial result

## Definition

Let **G** be a group. Let $f : \mathbf{G}^n \to \mathbf{G}$ be an onto homomorphism.
For each $1 \leq i \leq n$, let

- $f_i(x) = f(1, 1, \ldots, 1, x, 1, \ldots, 1)$ ($x$ in $i - th$ position),
- let $\mathbf{A}_i$ be the image of $f_i$ in **G**.

The following observations are fairly straightforward:

## Lemma

# Onto homomorphisms: a crucial result

## Definition

Let $\mathbf{G}$ be a group. Let $f : \mathbf{G}^n \to \mathbf{G}$ be an onto homomorphism.
For each $1 \leq i \leq n$, let

- $f_i(x) = f(1, 1, \ldots, 1, x, 1, \ldots, 1)$ ($x$ in $i - th$ position),
- let $\mathbf{A}_i$ be the image of $f_i$ in $\mathbf{G}$.

The following observations are fairly straightforward:

## Lemma

1. *Each $f_i$ is an endomorphism of* $\mathbf{G}$, *and* $f(x_1, \ldots, x_n) = f_1(x_1) \cdots f_n(x_n)$;

# Onto homomorphisms: a crucial result

## Definition

Let $\mathbf{G}$ be a group. Let $f : \mathbf{G}^n \to \mathbf{G}$ be an onto homomorphism.
For each $1 \leq i \leq n$, let

- $f_i(x) = f(1, 1, \ldots, 1, x, 1, \ldots, 1)$ ($x$ in $i - th$ position),
- let $\mathbf{A}_i$ be the image of $f_i$ in $\mathbf{G}$.

The following observations are fairly straightforward:

## Lemma

1. *Each $f_i$ is an endomorphism of $\mathbf{G}$, and* $f(x_1, \ldots, x_n) = f_1(x_1) \cdots f_n(x_n)$;
2. $\bigvee \mathbf{A}_i = \mathbf{G}$;

# Onto homomorphisms: a crucial result

## Definition

Let $\mathbf{G}$ be a group. Let $f : \mathbf{G}^n \to \mathbf{G}$ be an onto homomorphism.
For each $1 \leq i \leq n$, let

- $f_i(x) = f(1, 1, \ldots, 1, x, 1, \ldots, 1)$ ($x$ in $i-th$ position),
- let $\mathbf{A}_i$ be the image of $f_i$ in $\mathbf{G}$.

The following observations are fairly straightforward:

## Lemma

1. *Each $f_i$ is an endomorphism of $\mathbf{G}$, and* $f(x_1, \ldots, x_n) = f_1(x_1) \cdots f_n(x_n)$;
2. $\bigvee \mathbf{A}_i = \mathbf{G}$;
3. $[\mathbf{A}_i, \mathbf{A}_j] = 1$ *and* $\mathbf{A}_i \cap \mathbf{A}_j \leq Z(\mathbf{G})$ *if* $i \neq j$;

# Onto homomorphisms: a crucial result

## Definition

Let $\mathbf{G}$ be a group. Let $f : \mathbf{G}^n \to \mathbf{G}$ be an onto homomorphism.
For each $1 \leq i \leq n$, let

- $f_i(x) = f(1, 1, \ldots, 1, x, 1, \ldots, 1)$ ($x$ in $i - th$ position),
- let $\mathbf{A}_i$ be the image of $f_i$ in $\mathbf{G}$.

The following observations are fairly straightforward:

## Lemma

1. *Each $f_i$ is an endomorphism of $\mathbf{G}$, and* $f(x_1, \ldots, x_n) = f_1(x_1) \cdots f_n(x_n)$*;*
2. $\bigvee \mathbf{A}_i = \mathbf{G}$*;*
3. $[\mathbf{A}_i, \mathbf{A}_j] = 1$ *and* $\mathbf{A}_i \cap \mathbf{A}_j \leq Z(\mathbf{G})$ *if* $i \neq j$*;*
4. *if $f_j$ is onto then* $\mathbf{A}_i \leq Z(\mathbf{G})$ *for all* $i \neq j$*.*

# Onto homomorphisms: a crucial result, continued

**Theorem**

*Let* **G** *be a group. Then the following are equivalent:*

# Onto homomorphisms: a crucial result, continued

## Theorem

*Let* **G** *be a group. Then the following are equivalent:*

1. **G** *is directly indecomposable;*

# Onto homomorphisms: a crucial result, continued

**Theorem**

*Let* $\mathbf{G}$ *be a group. Then the following are equivalent:*

1. $\mathbf{G}$ *is directly indecomposable;*
2. *for each onto* $f : \mathbf{G}^n \to \mathbf{G}$ *there exists some* $i$ *such that* $f_i$ *is onto;*

# Onto homomorphisms: a crucial result, continued

**Theorem**

*Let* $\mathbf{G}$ *be a group. Then the following are equivalent:*

1. $\mathbf{G}$ *is directly indecomposable;*
2. *for each onto* $f : \mathbf{G}^n \to \mathbf{G}$ *there exists some* $i$ *such that* $f_i$ *is onto;*
3. *for any homomorphic images* $\mathbf{H}_i$ *of* $\mathbf{G}$*, if* $\mathbf{G}$ *is a homomorphic image of* $\prod \mathbf{H}_i$ *then there exists some* $i$ *such that* $\mathbf{H}_i \simeq \mathbf{G}$*.*

# Onto homomorphisms: a crucial result, continued

**Theorem**

*Let* $\mathbf{G}$ *be a group. Then the following are equivalent:*

1. $\mathbf{G}$ *is directly indecomposable;*
2. *for each onto* $f : \mathbf{G}^n \to \mathbf{G}$ *there exists some* $i$ *such that* $f_i$ *is onto;*
3. *for any homomorphic images* $\mathbf{H}_i$ *of* $\mathbf{G}$*, if* $\mathbf{G}$ *is a homomorphic image of* $\prod \mathbf{H}_i$ *then there exists some* $i$ *such that* $\mathbf{H}_i \simeq \mathbf{G}$*.*

Notes on proof:

# Onto homomorphisms: a crucial result, continued

**Theorem**

*Let $\mathbf{G}$ be a group. Then the following are equivalent:*

1. $\mathbf{G}$ *is directly indecomposable;*
2. *for each onto* $f : \mathbf{G}^n \to \mathbf{G}$ *there exists some* $i$ *such that* $f_i$ *is onto;*
3. *for any homomorphic images* $\mathbf{H}_i$ *of* $\mathbf{G}$*, if* $\mathbf{G}$ *is a homomorphic image of* $\prod \mathbf{H}_i$ *then there exists some* $i$ *such that* $\mathbf{H}_i \simeq \mathbf{G}$*.*

Notes on proof:

- the non-trivial part is (1) $\implies$ (2), rest is easy;

# Onto homomorphisms: a crucial result, continued

## Theorem

*Let* **G** *be a group. Then the following are equivalent:*

1. **G** *is directly indecomposable;*
2. *for each onto* $f : \mathbf{G}^n \to \mathbf{G}$ *there exists some* $i$ *such that* $f_i$ *is onto;*
3. *for any homomorphic images* $\mathbf{H}_i$ *of* **G**, *if* **G** *is a homomorphic image of* $\prod \mathbf{H}_i$ *then there exists some* $i$ *such that* $\mathbf{H}_i \simeq \mathbf{G}$.

Notes on proof:

- the non-trivial part is $(1) \implies (2)$, rest is easy;
- main idea for $\neg(2) \implies \neg(1)$: iterate applications of all the $f_i$ on **G** to produce a non-trivial normal retract, i.e. a non-trivial direct factor.

# Characterisation of onto-trivial groups

## Theorem

*Let* $\mathbf{G}$ *be a group,* $|G| > 2$*. Then the following are equivalent:*

# Characterisation of onto-trivial groups

## Theorem

*Let* **G** *be a group,* $|G| > 2$. *Then the following are equivalent:*

1. **G** *is 2-idempotent trivial;*

# Characterisation of onto-trivial groups

**Theorem**

*Let* $\mathbf{G}$ *be a group,* $|G| > 2$. *Then the following are equivalent:*

1. $\mathbf{G}$ *is 2-idempotent trivial;*
2. $\mathbf{G}$ *is idempotent-trivial;*

# Characterisation of onto-trivial groups

**Theorem**

*Let* $\mathbf{G}$ *be a group,* $|G| > 2$. *Then the following are equivalent:*

1. $\mathbf{G}$ *is 2-idempotent trivial;*
2. $\mathbf{G}$ *is idempotent-trivial;*
3. $\mathbf{G}$ *is onto-trivial;*

# Characterisation of onto-trivial groups

**Theorem**

*Let* $\mathbf{G}$ *be a group,* $|G| > 2$. *Then the following are equivalent:*

1. $\mathbf{G}$ *is 2-idempotent trivial;*
2. $\mathbf{G}$ *is idempotent-trivial;*
3. $\mathbf{G}$ *is onto-trivial;*
4. $\mathbf{G}$ *is directly indecomposable, and if* $\alpha : \mathbf{G} \to Z(\mathbf{G})$ *then* $\alpha = 1$*;*

# Characterisation of onto-trivial groups

## Theorem

*Let* $\mathbf{G}$ *be a group,* $|G| > 2$. *Then the following are equivalent:*

1. $\mathbf{G}$ *is 2-idempotent trivial;*
2. $\mathbf{G}$ *is idempotent-trivial;*
3. $\mathbf{G}$ *is onto-trivial;*
4. $\mathbf{G}$ *is directly indecomposable, and if* $\alpha : \mathbf{G} \to Z(\mathbf{G})$ *then* $\alpha = 1$*;*
5. $\mathbf{G}$ *is directly indecomposable, and* $gcd(\mathbf{G}/\mathbf{G}', Z(\mathbf{G})) = 1$.

# Characterisation of onto-trivial groups

## Theorem

*Let* $\mathbf{G}$ *be a group,* $|G| > 2$*. Then the following are equivalent:*

1. $\mathbf{G}$ *is 2-idempotent trivial;*
2. $\mathbf{G}$ *is idempotent-trivial;*
3. $\mathbf{G}$ *is onto-trivial;*
4. $\mathbf{G}$ *is directly indecomposable, and if* $\alpha : \mathbf{G} \to Z(\mathbf{G})$ *then* $\alpha = 1$*;*
5. $\mathbf{G}$ *is directly indecomposable, and gcd*$(\mathbf{G}/\mathbf{G}', Z(\mathbf{G})) = 1$*.*

- (4) $\implies$ (3): easy, use “crucial” result and Lemma;

# Characterisation of onto-trivial groups

## Theorem

*Let* $\mathbf{G}$ *be a group,* $|G| > 2$. *Then the following are equivalent:*

1. $\mathbf{G}$ *is 2-idempotent trivial;*
2. $\mathbf{G}$ *is idempotent-trivial;*
3. $\mathbf{G}$ *is onto-trivial;*
4. $\mathbf{G}$ *is directly indecomposable, and if* $\alpha : \mathbf{G} \to Z(\mathbf{G})$ *then* $\alpha = 1$*;*
5. $\mathbf{G}$ *is directly indecomposable, and* $gcd(\mathbf{G}/\mathbf{G}', Z(\mathbf{G})) = 1$.

- (4) $\implies$ (3): easy, use "crucial" result and Lemma;
- (1) $\implies$ (4):

# Characterisation of onto-trivial groups

## Theorem

*Let* $\mathbf{G}$ *be a group,* $|G| > 2$. *Then the following are equivalent:*

1. $\mathbf{G}$ *is 2-idempotent trivial;*
2. $\mathbf{G}$ *is idempotent-trivial;*
3. $\mathbf{G}$ *is onto-trivial;*
4. $\mathbf{G}$ *is directly indecomposable, and if* $\alpha : \mathbf{G} \to Z(\mathbf{G})$ *then* $\alpha = 1$*;*
5. $\mathbf{G}$ *is directly indecomposable, and* $gcd(\mathbf{G}/\mathbf{G}', Z(\mathbf{G})) = 1$.

- (4) $\implies$ (3): easy, use "crucial" result and Lemma;
- (1) $\implies$ (4):
  - if $\mathbf{G}$ is decomposable it admits a non-trivial idempotent binary;

# Characterisation of onto-trivial groups

**Theorem**

*Let $\mathbf{G}$ be a group, $|G| > 2$. Then the following are equivalent:*

1. $\mathbf{G}$ *is 2-idempotent trivial;*
2. $\mathbf{G}$ *is idempotent-trivial;*
3. $\mathbf{G}$ *is onto-trivial;*
4. $\mathbf{G}$ *is directly indecomposable, and if* $\alpha : \mathbf{G} \to Z(\mathbf{G})$ *then* $\alpha = 1$*;*
5. $\mathbf{G}$ *is directly indecomposable, and* $gcd(\mathbf{G}/\mathbf{G}', Z(\mathbf{G})) = 1$*.*

- (4) $\implies$ (3): easy, use "crucial" result and Lemma;
- (1) $\implies$ (4):
  - if $\mathbf{G}$ is decomposable it admits a non-trivial idempotent binary;
  - if $1 \neq \alpha : \mathbf{G} \to Z(\mathbf{G})$ then $\sigma(x) = x\alpha(x) \in Aut(\mathbf{G})$ and then $f(x, y) = \sigma^{-1}(x\alpha(y))$ is a non-trivial binary idempotent.

# Characterisation of onto-trivial groups

**Theorem**

*Let* $\mathbf{G}$ *be a group,* $|G| > 2$*. Then the following are equivalent:*

1. $\mathbf{G}$ *is 2-idempotent trivial;*
2. $\mathbf{G}$ *is idempotent-trivial;*
3. $\mathbf{G}$ *is onto-trivial;*
4. $\mathbf{G}$ *is directly indecomposable, and if* $\alpha : \mathbf{G} \to Z(\mathbf{G})$ *then* $\alpha = 1$*;*
5. $\mathbf{G}$ *is directly indecomposable, and* $gcd(\mathbf{G}/\mathbf{G}', Z(\mathbf{G})) = 1$.

- (4) $\implies$ (3): easy, use “crucial” result and Lemma;
- (1) $\implies$ (4):
  - if $\mathbf{G}$ is decomposable it admits a non-trivial idempotent binary;
  - if $1 \neq \alpha : \mathbf{G} \to Z(\mathbf{G})$ then $\sigma(x) = x\alpha(x) \in Aut(\mathbf{G})$ and then $f(x, y) = \sigma^{-1}(x\alpha(y))$ is a non-trivial binary idempotent.
- These groups are non-Abelian, e.g. centreless directly indecomposable groups; there are others, e.g. $SL_n(\mathbb{F})$.

# A first hardness result

**Theorem**

*If* $\mathbf{G}$ *is a directly indecomposable non-Abelian group, then* $QCSP(\mathbf{G})$ *is Pspace-complete.*

# A first hardness result

**Theorem**

*If* **G** *is a directly indecomposable non-Abelian group, then QCSP*(**G**) *is Pspace-complete.*

*Proof:* Let $f : \mathbf{G}^n \to \mathbf{G}$ be onto; by our ”crucial” result, **G** indecomposable implies there exists an index $j$ such that $f_j$ in onto. By our remarks in the Lemma, it follows that $\mathbf{A}_i \leq Z(\mathbf{G})$ for all $i \neq j$. Then

$$f^{\theta}(x_1\mathbf{Z}, \ldots, x_n\mathbf{Z}) = f(x_1, \ldots, x_n)\mathbf{Z} = f_1(x_1)\cdots f_n(x_n)\mathbf{Z} = f_j(x_j)\mathbf{Z}$$

so $f^{\theta}$ is essentially unary. We saw earlier that the congruence $\theta$ associated to $Z(\mathbf{G})$ is definable, and $\theta \neq G^2$ since **G** is not Abelian; hence by our hardness criterion, we are done. □

# A second hardness result

**Lemma**

*If $\mathbf{G}$ is centerless then QCSP($\mathbf{G}$) is Pspace-complete.*

# A second hardness result

**Lemma**

*If* $\mathbf{G}$ *is centerless then QCSP*$(\mathbf{G})$ *is Pspace-complete.*

*Sketch of proof:*

# A second hardness result

**Lemma**

*If* $\mathbf{G}$ *is centerless then QCSP*$(\mathbf{G})$ *is Pspace-complete.*

*Sketch of proof:*

- Induction on the number of direct factors; if $\mathbf{G}$ indecomposable previous result applies;

# A second hardness result

**Lemma**

*If* $\mathbf{G}$ *is centerless then* $QCSP(\mathbf{G})$ *is Pspace-complete.*

*Sketch of proof:*

- Induction on the number of direct factors; if $\mathbf{G}$ indecomposable previous result applies;
- fix an onto $f : \mathbf{G}^n \to \mathbf{G}$;

# A second hardness result

**Lemma**

*If* $\mathbf{G}$ *is centerless then QCSP*$(\mathbf{G})$ *is Pspace-complete.*

*Sketch of proof:*

- Induction on the number of direct factors; if $\mathbf{G}$ indecomposable previous result applies;
- fix an onto $f : \mathbf{G}^n \to \mathbf{G}$;
- *Krull-Remak-Schmidt Theorem*: asserts the uniqueness of *internal* direct decomposition of $\mathbf{G}$ into indecomposable factors $\mathbf{H}_j$;

# A second hardness result

## Lemma

*If $\mathbf{G}$ is centerless then QCSP$(\mathbf{G})$ is Pspace-complete.*

*Sketch of proof:*

- Induction on the number of direct factors; if $\mathbf{G}$ indecomposable previous result applies;
- fix an onto $f : \mathbf{G}^n \to \mathbf{G}$;
- *Krull-Remak-Schmidt Theorem*: asserts the uniqueness of *internal* direct decomposition of $\mathbf{G}$ into indecomposable factors $\mathbf{H}_j$;
- arguing on the $\mathbf{H}_j$ as we did with the $\mathbf{A}_i$, and because $\mathbf{G}$ centreless, we obtain another decomposition of $\mathbf{G}$;

# A second hardness result

**Lemma**

*If* $\mathbf{G}$ *is centerless then QCSP*$(\mathbf{G})$ *is Pspace-complete.*

*Sketch of proof:*

- Induction on the number of direct factors; if $\mathbf{G}$ indecomposable previous result applies;
- fix an onto $f : \mathbf{G}^n \to \mathbf{G}$;
- *Krull-Remak-Schmidt Theorem*: asserts the uniqueness of *internal* direct decomposition of $\mathbf{G}$ into indecomposable factors $\mathbf{H}_j$;
- arguing on the $\mathbf{H}_j$ as we did with the $\mathbf{A}_i$, and because $\mathbf{G}$ centreless, we obtain another decomposition of $\mathbf{G}$;
- by using Remak again, we obtain that each $f_i$ preserves each $\mathbf{H}_j$; ( “easy” reduction if a $\mathbf{H}_j$ is a hom image of another)

# A second hardness result

## Lemma

*If* $\mathbf{G}$ *is centerless then* $QCSP(\mathbf{G})$ *is Pspace-complete.*

*Sketch of proof:*

- Induction on the number of direct factors; if $\mathbf{G}$ indecomposable previous result applies;
- fix an onto $f : \mathbf{G}^n \to \mathbf{G}$;
- *Krull-Remak-Schmidt Theorem*: asserts the uniqueness of *internal* direct decomposition of $\mathbf{G}$ into indecomposable factors $\mathbf{H}_j$;
- arguing on the $\mathbf{H}_j$ as we did with the $\mathbf{A}_i$, and because $\mathbf{G}$ centreless, we obtain another decomposition of $\mathbf{G}$;
- by using Remak again, we obtain that each $f_i$ preserves each $\mathbf{H}_j$; ( "easy" reduction if a $\mathbf{H}_j$ is a hom image of another)
- hence we may quotient out (any) one of the $\mathbf{H}_j$.

# A second hardness result, continued

## Definition

Let $\mathbf{G}$ be a group. $Z^i(\mathbf{G})$, the *$i$-th center of* $\mathbf{G}$, is:

# A second hardness result, continued

## Definition

Let $\mathbf{G}$ be a group. $Z^i(\mathbf{G})$, the *$i$-th center of* $\mathbf{G}$, is:

- $Z^1(\mathbf{G}) = Z(\mathbf{G})$,

# A second hardness result, continued

## Definition

Let $\mathbf{G}$ be a group. $Z^i(\mathbf{G})$, the *i-th center of* $\mathbf{G}$, is:

- $Z^1(\mathbf{G}) = Z(\mathbf{G})$,
- for all $i \geq 1$, $Z^{i+1}(\mathbf{G})$ is the inverse image of $Z(\mathbf{G}/Z^i(\mathbf{G}))$ under the natural homomorphism from $\mathbf{G}$ onto $\mathbf{G}/Z^i(\mathbf{G})$.

# A second hardness result, continued

## Definition

Let **G** be a group. $Z^i(\mathbf{G})$, the *i-th center of* **G**, is:

- $Z^1(\mathbf{G}) = Z(\mathbf{G})$,
- for all $i \geq 1$, $Z^{i+1}(\mathbf{G})$ is the inverse image of $Z(\mathbf{G}/Z^i(\mathbf{G}))$ under the natural homomorphism from **G** onto $\mathbf{G}/Z^i(\mathbf{G})$.

## Definition

The group **G** is **nilpotent** if $Z^i(\mathbf{G}) = \mathbf{G}$ for some $i \geq 1$.

# A second hardness result, continued

## Definition

Let $\mathbf{G}$ be a group. $Z^i(\mathbf{G})$, the *i-th center of* $\mathbf{G}$, is:

- $Z^1(\mathbf{G}) = Z(\mathbf{G})$,
- for all $i \geq 1$, $Z^{i+1}(\mathbf{G})$ is the inverse image of $Z(\mathbf{G}/Z^i(\mathbf{G}))$ under the natural homomorphism from $\mathbf{G}$ onto $\mathbf{G}/Z^i(\mathbf{G})$.

## Definition

The group $\mathbf{G}$ is **nilpotent** if $Z^i(\mathbf{G}) = \mathbf{G}$ for some $i \geq 1$.

## Lemma

# A second hardness result, continued

## Definition

Let $\mathbf{G}$ be a group. $Z^i(\mathbf{G})$, the *i-th center of* $\mathbf{G}$, is:

- $Z^1(\mathbf{G}) = Z(\mathbf{G})$,
- for all $i \geq 1$, $Z^{i+1}(\mathbf{G})$ is the inverse image of $Z(\mathbf{G}/Z^i(\mathbf{G}))$ under the natural homomorphism from $\mathbf{G}$ onto $\mathbf{G}/Z^i(\mathbf{G})$.

## Definition

The group $\mathbf{G}$ is **nilpotent** if $Z^i(\mathbf{G}) = \mathbf{G}$ for some $i \geq 1$.

## Lemma

- *A group is* not *nilpotent iff* $\mathbf{G}/Z^i(\mathbf{G})$ *is centreless (non-trivial) for some* $i \geq 1$*;*

# A second hardness result, continued

## Definition

Let $\mathbf{G}$ be a group. $Z^i(\mathbf{G})$, the *i-th center of* $\mathbf{G}$, is:

- $Z^1(\mathbf{G}) = Z(\mathbf{G})$,
- for all $i \geq 1$, $Z^{i+1}(\mathbf{G})$ is the inverse image of $Z(\mathbf{G}/Z^i(\mathbf{G}))$ under the natural homomorphism from $\mathbf{G}$ onto $\mathbf{G}/Z^i(\mathbf{G})$.

## Definition

The group $\mathbf{G}$ is **nilpotent** if $Z^i(\mathbf{G}) = \mathbf{G}$ for some $i \geq 1$.

## Lemma

- *A group is* not *nilpotent iff* $\mathbf{G}/Z^i(\mathbf{G})$ *is centreless (non-trivial) for some* $i \geq 1$*;*
- *The congruence associated to* $Z^i(\mathbf{G})$ *is definable for all* $i \geq 1$*.*

# A second hardness result, continued

**Theorem**

*Let* $\mathbf{G}$ *be a non-nilpotent group. Then* $QCSP(\mathbf{G})$ *is Pspace-complete.*

# A second hardness result, continued

**Theorem**

*Let* $\mathbf{G}$ *be a non-nilpotent group. Then QCSP*$(\mathbf{G})$ *is Pspace-complete.*

*Proof:* Immediate by the previous results. $\square$