Fancy divisibility in group theory

Anton A. Klyachko

Linear equations

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1x + b_1y + \dots = 0 \\ a_2x + b_2y + \dots = 0 \\ \qquad\qquad \dots\dots\dots \end{cases}$$

Linear equations

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1 x + b_1 y + \cdots = 0 \\ a_2 x + b_2 y + \cdots = 0 \\ \qquad\qquad\qquad \ldots\ldots\ldots \end{cases}$$

If it has less equations than unknowns, then ...

Linear equations

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1x + b_1y + \cdots = 0 \\ a_2x + b_2y + \cdots = 0 \\ \hfill \ldots\ldots\ldots \end{cases}$$

If it has less equations than unknowns, then

Linear equations

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1x + b_1y + \cdots = 0 \\ a_2x + b_2y + \cdots = 0 \\ \qquad\qquad \ldots\ldots\ldots \end{cases}$$

If it has less equations than unknowns, then the number of solutions is ...

Linear equations

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1x + b_1y + \cdots = 0 \\ a_2x + b_2y + \cdots = 0 \\ \qquad\qquad \ldots\ldots\ldots \end{cases}$$

If it has less equations than unknowns, then the number of solutions is

Linear equations

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1x + b_1y + \cdots = 0 \\ a_2x + b_2y + \cdots = 0 \\ \qquad\qquad \cdots\cdots\cdots \end{cases}$$

If it has less equations than unknowns, then the number of solutions is divisible by p.

Solomon's theorem

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1x + b_1y + \dots = 0 \\ a_2x + b_2y + \dots = 0 \\ \qquad\qquad \dots\dots\dots \end{cases}$$

If it has less equations than unknowns, then the number of solutions is divisible by p.

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1x + b_1y + \dots = 0 \\ a_2x + b_2y + \dots = 0 \\ \qquad\qquad \dots\dots\dots \end{cases}$$

If it has less equations than unknowns, then the number of solutions is divisible by p.

What about groups?

Solomon's theorem

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1x + b_1y + \cdots = 0 \\ a_2x + b_2y + \cdots = 0 \\ \qquad\qquad \ldots\ldots\ldots \end{cases}$$

If it has less equations than unknowns, then the number of solutions is divisible by p.
What about groups? $\mathbb{Z}/p\mathbb{Z}$ is a group...

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1x + b_1y + \cdots = 0 \\ a_2x + b_2y + \cdots = 0 \\ \qquad\qquad \cdots\cdots\cdots \end{cases}$$

If it has less equations than unknowns, then the number of solutions is divisible by p.

What about groups? $\mathbb{Z}/p\mathbb{Z}$ is a group...

Louis Solomon's theorem (1969)

If a system of coefficient-free equations over a group G has less equations than unknowns, then the number of solutions is

...

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1x + b_1y + \cdots = 0 \\ a_2x + b_2y + \cdots = 0 \\ \qquad\qquad\quad \ldots\ldots\ldots \end{cases}$$

If it has less equations than unknowns, then the number of solutions is divisible by p.

What about groups? $\mathbb{Z}/p\mathbb{Z}$ is a group...

Louis Solomon's theorem (1969)

If a system of coefficient-free equations over a group G has less equations than unknowns, then the number of solutions is

Solomon's theorem

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1 x + b_1 y + \dots = 0 \\ a_2 x + b_2 y + \dots = 0 \\ \qquad\qquad\quad \dots\dots\dots \end{cases}$$

If it has less equations than unknowns, then the number of solutions is divisible by p.

What about groups? $\mathbb{Z}/p\mathbb{Z}$ is a group...

Louis Solomon's theorem (1969)

If a system of coefficient-free equations over a group G has less equations than unknowns, then the number of solutions is divisible by $|G|$.

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1x + b_1y + \cdots = 0 \\ a_2x + b_2y + \cdots = 0 \\ \qquad\qquad \ldots\ldots\ldots \end{cases}$$

If it has less equations than unknowns, then the number of solutions is divisible by p.
What about groups? $\mathbb{Z}/p\mathbb{Z}$ is a group. . .

Louis Solomon's theorem (1969)

If a system of coefficient-free equations over a group G has less equations than unknowns, then the number of solutions is divisible by $|G|$.

$$\begin{cases} x^2y^3[x,z]\cdots = 1 \\ \qquad\qquad \ldots\ldots\ldots \end{cases}$$

Corollary-Example (K & Anna Mkrtchyan)

Corollary-Example-Definition (K & Anna Mkrtchyan)

We say that two elements of a group belong to the same *tribe* if their squares are equal.

$$S_3 = \{\ e, (12), (23), (13), \qquad (123), \qquad (321)\ \}$$

Our squares are e. Our squares are (321). Our squares are (123).

Corollary-Example-Definition (K & Anna Mkrtchyan)

We say that two elements of a group belong to the same *tribe* if their squares are equal. Clearly, the total size of all tribes is the order of the group.

$$S_3 = \{\ e, (12), (23), (13), \qquad (123), \qquad (321)\ \}$$

Our squares are e. Our squares are (321). Our squares are (123).

$$4 + 1 + 1 = 6 \quad \text{(it is obvious)}$$

Corollary-Example-Definition (K & Anna Mkrtchyan)

We say that two elements of a group belong to the same *tribe* if their squares are equal. Clearly, the total size of all tribes is the order of the group. It is less obvious that

$$S_3 = \{\ e, (12), (23), (13), \qquad (123), \qquad (321)\ \}$$

Our squares are e. Our squares are (321). Our squares are (123).

$$4 + 1 + 1 = 6 \quad \text{(it is obvious)}$$

Tribes

Corollary-Example-Definition (K & Anna Mkrtchyan)

We say that two elements of a group belong to the same *tribe* if their squares are equal. Clearly, the total size of all tribes is the order of the group. It is less obvious that *the sum of 2013th powers of tribe sizes is a multiple of the order of the group.*

$$S_3 = \{\ e, (12), (23), (13), \quad (123), \quad (321)\ \}$$

Our squares are e. Our squares are (321). Our squares are (123).

$$4 + 1 + 1 = 6 \quad \text{(it is obvious)}$$

$$4^{2013} + 1^{2013} + 1^{2013} \quad \text{is divisible by 6} \quad \text{(it is less obvious)}$$

Tribes. Magic trick revealed

Corollary-Example-Definition (K & Anna Mkrtchyan)

We say that two elements of a group belong to the same *tribe* if their squares are equal. Clearly, the total size of all tribes is the order of the group. It is less obvious that
the sum of 2013th powers of tribe sizes is a multiple of the order of the group.

Tribes. Magic trick revealed

Corollary-Example-Definition (K & Anna Mkrtchyan)

We say that two elements of a group belong to the same *tribe* if their squares are equal. Clearly, the total size of all tribes is the order of the group. It is less obvious that
the sum of 2013th powers of tribe sizes is a multiple of the order of the group.

Proof. $x_1^2 = \cdots = x_{2013}^2$.

Tribes. Magic trick revealed

Corollary-Example-Definition (K & Anna Mkrtchyan)

We say that two elements of a group belong to the same *tribe* if their squares are equal. Clearly, the total size of all tribes is the order of the group. It is less obvious that
the sum of 2013th powers of tribe sizes is a multiple of the order of the group.

Proof. $x_1^2 = \cdots = x_{2013}^2$.
A solution is a tuple $(g_1, \ldots, g_{2013})$ such that all g_is belong to the same tribe.

Tribes. Magic trick revealed

Corollary-Example-Definition (K & Anna Mkrtchyan)

We say that two elements of a group belong to the same *tribe* if their squares are equal. Clearly, the total size of all tribes is the order of the group. It is less obvious that
the sum of 2013th powers of tribe sizes is a multiple of the order of the group.

Proof. $x_1^2 = \cdots = x_{2013}^2$.
A solution is a tuple $(g_1, \ldots, g_{2013})$ such that all g_is belong to the same tribe. The number of solutions is the sum of 2013th powers of tribe sizes.

Tribes. Magic trick revealed

Corollary-Example-Definition (K & Anna Mkrtchyan)

We say that two elements of a group belong to the same *tribe* if their squares are equal. Clearly, the total size of all tribes is the order of the group. It is less obvious that *the sum of 2013th powers of tribe sizes is a multiple of the order of the group.*

Proof. $x_1^2 = \cdots = x_{2013}^2$.
A solution is a tuple $(g_1, \ldots, g_{2013})$ such that all g_is belong to the same tribe. The number of solutions is the sum of 2013th powers of tribe sizes. On the other hand, the number of equations is less than that of unknowns. So, the statement is a corollary of the Solomon theorem.

Corollary-Example-Definition (K & Anna Mkrtchyan)

We say that two elements of a group belong to the same *tribe* if their squares are equal. Clearly, the total size of all tribes is the order of the group. It is less obvious that *the sum of 2013th powers of tribe sizes is a multiple of the order of the group.*

Proof. $x_1^2 = \cdots = x_{2013}^2$.
A solution is a tuple $(g_1, \dots, g_{2013})$ such that all g_is belong to the same tribe. The number of solutions is the sum of 2013th powers of tribe sizes. On the other hand, the number of equations is less than that of unknowns. So, the statement is a corollary of the Solomon theorem.
2013 is an arbitrary positive integer;

Corollary-Example-Definition (K & Anna Mkrtchyan)

We say that two elements of a group belong to the same *tribe* if their squares are equal. Clearly, the total size of all tribes is the order of the group. It is less obvious that *the sum of 2013th powers of tribe sizes is a multiple of the order of the group.*

Proof. $x_1^2 = \cdots = x_{2013}^2$.
A solution is a tuple $(g_1, \ldots, g_{2013})$ such that all g_is belong to the same tribe. The number of solutions is the sum of 2013th powers of tribe sizes. On the other hand, the number of equations is less than that of unknowns. So, the statement is a corollary of the Solomon theorem.
2013 is an arbitrary positive integer; the squares (in the definition of tribes) can also be replaced by any positive integer powers.

A discouraging example

$$z = (x^{-1}zx)(y^{-1}zy)$$

Solutions in the symmetric group $G = S_3$.

A discouraging example

$$z = (x^{-1}zx)(y^{-1}zy)$$

Solutions in the symmetric group $G = S_3$.

With $z = 1$, there are 36 solutions (x and y can be arbitrary).

A discouraging example

$$z = (x^{-1}zx)(y^{-1}zy)$$

Solutions in the symmetric group $G = S_3$.

With $z = 1$, there are 36 solutions (x and y can be arbitrary).

With $z = (123)$, there are $3 \cdot 3 = 9$ solutions (x and y are arbitrary transpositions).

A discouraging example

$$z = (x^{-1}zx)(y^{-1}zy)$$

Solutions in the symmetric group $G = S_3$.

With $z = 1$, there are 36 solutions (x and y can be arbitrary).

With $z = (123)$, there are $3 \cdot 3 = 9$ solutions (x and y are arbitrary transpositions).

With $z = (321)$, there are also 9 solutions.

A discouraging example

$$z = (x^{-1}zx)(y^{-1}zy)$$

Solutions in the symmetric group $G = S_3$.

With $z = 1$, there are 36 solutions (x and y can be arbitrary).

With $z = (123)$, there are $3 \cdot 3 = 9$ solutions (x and y are arbitrary transpositions).

With $z = (321)$, there are also 9 solutions.

If z is a transposition, then there are no solutions (by parity).

A discouraging example

$$z = (x^{-1}zx)(y^{-1}zy)$$

Solutions in the symmetric group $G = S_3$.

With $z = 1$, there are 36 solutions (x and y can be arbitrary).

With $z = (123)$, there are $3 \cdot 3 = 9$ solutions (x and y are arbitrary transpositions).

With $z = (321)$, there are also 9 solutions.

If z is a transposition, then there are no solutions (by parity).

Thus, the total amount of solutions is $36 + 2 \cdot 9$.

A discouraging example

$$z = (x^{-1}zx)(y^{-1}zy)$$

Solutions in the symmetric group $G = S_3$.

With $z = 1$, there are 36 solutions (x and y can be arbitrary).

With $z = (123)$, there are $3 \cdot 3 = 9$ solutions (x and y are arbitrary transpositions).

With $z = (321)$, there are also 9 solutions.

If z is a transposition, then there are no solutions (by parity).

Thus, the total amount of solutions is $36 + 2 \cdot 9$.

This is (and must be) divisible by $|G| = 6$ but not divisible by $|G|^2$ (though the number of equations is two less than that of unknowns).

Back to high school

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1 x + b_1 y + \cdots = 0 \\ a_2 x + b_2 y + \cdots = 0 \\ \hfill \dots\dots\dots \end{cases}$$

The number of solutions is divisible by p if
there are less equations than unknowns.

Back to high school

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1 x + b_1 y + \cdots = 0 \\ a_2 x + b_2 y + \cdots = 0 \\ \qquad\qquad \dots\dots\dots \end{cases}$$

The number of solutions is divisible by p if
~~there are less equations than unknowns~~. the rank of the matrix

$$\begin{pmatrix} a_1 & b_1 & \dots \\ a_2 & b_2 & \dots \\ \dots & \dots & \dots \end{pmatrix}$$

is less than the number of unknowns.

A system of coefficient-free equations over a group G

$$\begin{cases} x^3y^3x^{-1}y[x,y]=1 \\ \\ (x,y^2)^5=1 \end{cases}$$

The *exponent-sum matrix*

$$A=\begin{pmatrix} 2 & 4 \\ 5 & 10 \end{pmatrix}$$

a_{ij} is the sum of exponents of ith unknown in jth equation.

Gordon–Rodriguez-Villegas theorem

A system of coefficient-free equations over a group G

$$\begin{cases} x^3y^3x^{-1}y[x,y] = 1 \\ (x,y^2)^5 = 1 \end{cases}$$

The *exponent-sum matrix*

$$A = \begin{pmatrix} 2 & 4 \\ 5 & 10 \end{pmatrix}$$

a_{ij} is the sum of exponents of ith unknown in jth equation.

Theorem (Cameron Gordon & Fernando Rodriguez-Villegas, 2012)

If rank A is less than the number of unknowns, then the number of solutions is divisible by $|G|$.

Non-homogeneous linear equations

A system of homogeneous linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1x + b_1y + \dots = 0 \\ a_2x + b_2y + \dots = 0 \\ \qquad\qquad\quad \dots\dots\dots \end{cases}$$

The number of solutions is divisible by p if the rank of the matrix

$$\begin{pmatrix} a_1 & b_1 & \dots \\ a_2 & b_2 & \dots \\ \dots & \dots & \dots \end{pmatrix}$$

is less than the number of unknowns.

Non-homogeneous linear equations

A system of ~~homogeneous~~ linear equations over $\mathbb{Z}/p\mathbb{Z}$:

$$\begin{cases} a_1x + b_1y + \dots = \alpha_1 \\ a_2x + b_2y + \dots = \alpha_2 \\ \qquad\qquad\qquad \dots\dots\dots \end{cases}$$

The number of solutions is divisible by p if the rank of the matrix

$$\begin{pmatrix} a_1 & b_1 & \dots \\ a_2 & b_2 & \dots \\ \dots & \dots & \dots \end{pmatrix}$$

is less than the number of unknowns.

Over arbitrary group G, this corresponds to equations with coefficients.

Equations with coefficients

A system of coefficient-free equations over a group G

$$\begin{cases} x^3y^3x^{-1}y[x,y] = 1 \\ (x,y^2)^5 = 1 \end{cases}$$

The *exponent-sum matrix* $A = \begin{pmatrix} 2 & 4 \\ 5 & 10 \end{pmatrix}$

a_{ij} is the sum of exponents of ith unknown in jth equation.

Theorem (Cameron Gordon & Fernando Rodriguez-Villegas, 2012)

If rank A is less than the number of unknowns, then the number of solutions is divisible by $|G|$.

Equations with coefficients

A system of ~~coefficient-free~~ equations over a group $G \ni a, b, c, \dots$

$$\begin{cases} x^3 a y^3 x^{-1} b y [x, y] c = 1 \\ (xd, y^2)^5 = 1 \end{cases}$$

The *exponent-sum matrix* $A = \begin{pmatrix} 2 & 4 \\ 5 & 10 \end{pmatrix}$

a_{ij} is the sum of exponents of ith unknown in jth equation.

Theorem (FALSE!!!)

If rank A is less than the number of unknowns, then the number of solutions is divisible by $|G|$.

$[x, a] = 1$. The exponent-sum matrix is 0 but
$|\{solutions\}| = |C(a)| < |G|$

A system of ~~coefficient-free~~ equations over a group $G \ni a, b, c, \ldots$

$$\begin{cases} x^3ay^3x^{-1}by[x,y]c = 1 \\ (xd, y^2)^5 = 1 \end{cases}$$

The *exponent-sum matrix* $A = \begin{pmatrix} 2 & 4 \\ 5 & 10 \end{pmatrix}$

a_{ij} is the sum of exponents of ith unknown in jth equation.

Theorem (K & Anna Mkrtchyan)

If rank A is less than the number of unknowns, then the number of solutions is divisible by $|C(\{a, b, \ldots\})|$.

$C(X)$ is the centraliser of a set X.

Theorem (K & Anna Mkrtchyan)

If rank(exponent-sum matrix) is less than the number of unknowns, then the number of solutions is divisible by $|C(\{a, b, \dots\})|$.

Roots of subgroups

Theorem (K & Anna Mkrtchyan)

If rank(exponent-sum matrix) is less than the number of unknowns, then the number of solutions is divisible by $|C(\{a, b, \ldots\})|$.

Corollary (K & Anna Mkrtchyan)

The number of elements of a group G whose squares belong to a given subgroup H is always divisible by $|H|$.

Theorem (K & Anna Mkrtchyan)

If rank(exponent-sum matrix) is less than the number of unknowns, then the number of solutions is divisible by $|C(\{a, b, \dots\})|$.

Corollary (K & Anna Mkrtchyan)

The number of elements of a group G whose squares belong to a given subgroup H is always divisible by $|H|$.

Proof. Suppose that $H = C(D)$ for some $D \subseteq G$.
$\{[x^2, d] = 1 \ : d \in D\}$.

Theorem (K & Anna Mkrtchyan)

If rank(exponent-sum matrix) is less than the number of unknowns, then the number of solutions is divisible by $|C(\{a, b, \dots\})|$.

Corollary (K & Anna Mkrtchyan)

The number of elements of a group G whose squares belong to a given subgroup H is always divisible by $|H|$.

Proof. Suppose that $H = C(D)$ for some $D \subseteq G$.
$\{[x^2, d] = 1 \ : d \in D\}$. rank $A = 0$ is less than the number of unknowns (one).

Theorem (K & Anna Mkrtchyan)

If rank(exponent-sum matrix) is less than the number of unknowns, then the number of solutions is divisible by $|C(\{a, b, \ldots\})|$.

Corollary (K & Anna Mkrtchyan)

The number of elements of a group G whose squares belong to a given subgroup H is always divisible by $|H|$.

Proof. Suppose that $H = C(D)$ for some $D \subseteq G$.
$\{[x^2, d] = 1 \ : d \in D\}$. rank $A = 0$ is less than the number of unknowns (one).

Exercise

If H is a subgroup of a group G, then there exists an overgroup $\widehat{G} \supseteq G, D, B$ such that, in $\widehat{G}$, $H = C(D)$ and $G = C(B)$.

Corollary (K & Anna Mkrtchyan)

The number of elements of a group G whose squares belong to a given subgroup H is always divisible by $|H|$.

Corollary (K & Anna Mkrtchyan)

The number of elements of a group G whose cubes belong to a given subgroup H is always divisible by $|H|$.

Corollary (K & Anna Mkrtchyan)

The number of elements of a group G whose 2013th powers belong to a given subgroup H is always divisible by $|H|$.

Corollary (K & Anna Mkrtchyan)

The number of elements of a group G whose squares belong to a given subgroup H is always divisible by $|H|$.

The number of homomorphisms $f\colon \mathbb{Z} \to G$ such that $f(2\mathbb{Z}) \subseteq H$ is divisible by $|H|$.

Roots of subgroups generalised

Corollary (K & Anna Mkrtchyan)

The number of elements of a group G whose squares belong to a given subgroup H is always divisible by $|H|$.

The number of homomorphisms $f\colon \mathbb{Z} \to G$ such that $f(2\mathbb{Z}) \subseteq H$ is divisible by $|H|$.

Generalisation (K & Anna Mkrtchyan)

Suppose that H is a subgroup of a group G and W is a subgroup (or a subset) of a finitely generated group F with infinite abelianisation F/F'. Then the number of homomorphisms $f\colon F \to G$ such that $f(W) \subseteq H$ is always divisible by $|H|$.

First-order formulae

An arbitrary first-order formula φ over a group $G \ni a, b, \ldots$:

$$\forall z \exists t \left(z^2 y x^2 a t^{-2} x^2 y z b (xy)^5 = 1 \vee t[x, y]^2 \neq 1 \wedge (x^2 y^2 a)^3 \neq 1 \right)$$

First-order formulae

An arbitrary first-order formula φ over a group $G \ni a, b, \ldots$:

$$\forall z \exists t \left(z^2 y x^2 a t^{-2} x^2 y z b (xy)^5 = 1 \vee t[x, y]^2 \neq 1 \wedge (x^2 y^2 a)^3 \neq 1 \right)$$

We are free:) We are bound:(We are just elements of G.

First-order formulae

An arbitrary first-order formula φ over a group $G \ni a, b, \ldots$:

$$\forall z \exists t \left(z^2 y x^2 a t^{-2} x^2 y z b (xy)^5 = 1 \vee t[x,y]^2 \neq 1 \wedge (x^2 y^2 a)^3 \neq 1 \right)$$

We are free:) We are bound:(We are just elements of G.
Left-hand sides of atomic subformulae:

$$z^2 y x^2 a t^{-2} x^2 y z b (xy)^5, \quad t[x,y]^2, \quad (x^2 y^2 a)^3.$$

An arbitrary first-order formula φ over a group $G \ni a, b, \ldots$:

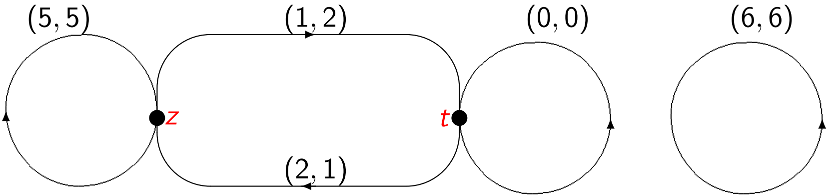
$$\forall z \exists t \left(z^2 y x^2 a t^{-2} x^2 y z b (xy)^5 = 1 \vee t[x,y]^2 \neq 1 \wedge (x^2 y^2 a)^3 \neq 1\right)$$

We are free:) We are bound:(We are just elements of G.

Left-hand sides of atomic subformulae:

$$z^2 y x^2 a t^{-2} x^2 y z b (xy)^5, \quad t[x,y]^2, \quad (x^2 y^2 a)^3.$$

The (generalised) digraph $\Gamma(\varphi)$:



Exponent-sum matrix

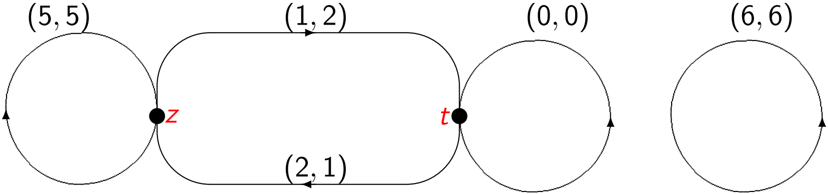
An arbitrary first-order formula φ over a group $G \ni a, b, \ldots$:

$$\forall z \exists t \left(z^2 y x^2 a t^{-2} x^2 y z b (xy)^5 = 1 \vee t[x, y]^2 \neq 1 \wedge (x^2 y^2 a)^3 \neq 1 \right)$$

An arbitrary first-order formula φ over a group $G \ni a, b, \ldots$:

$$\forall z \exists t \left(z^2 y x^2 a t^{-2} x^2 y z b (xy)^5 = 1 \vee t[x, y]^2 \neq 1 \wedge (x^2 y^2 a)^3 \neq 1\right)$$

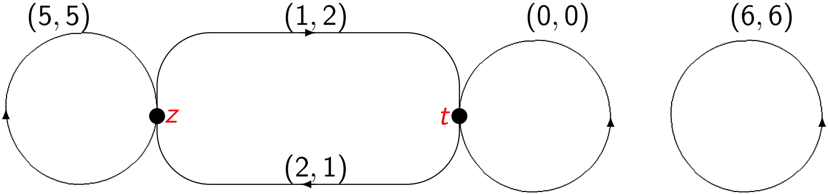
The (generalised) digraph $\Gamma(\varphi)$:



An arbitrary first-order formula φ over a group $G \ni a, b, \ldots$:

$$\forall z \exists t \left(z^2 y x^2 a t^{-2} x^2 y z b (xy)^5 = 1 \vee t[x, y]^2 \neq 1 \wedge (x^2 y^2 a)^3 \neq 1 \right)$$

The (generalised) digraph $\Gamma(\varphi)$:



The signed sums along generating cycles:

$$(5, 5); \quad (1, 2) + (2, 1) = (3, 3); \quad (0, 0); \quad (6, 6).$$

The *exponent-sum matrix* $A(\varphi) = \begin{pmatrix} 5 & 5 \\ 3 & 3 \\ 0 & 0 \\ 6 & 6 \end{pmatrix}$

Main theorem

An arbitrary first-order formula φ over a group $G \ni a, b, \dots$:

$$\forall z \exists t \left(z^2 y x^2 a t^{-2} x^2 y z b (xy)^5 = 1 \vee t[x,y]^2 \neq 1 \wedge (x^2 y^2 a)^3 \neq 1 \right)$$

Main theorem

An arbitrary first-order formula φ over a group $G \ni a, b, \ldots$:

$$\forall z \exists t \left(z^2 y x^2 a t^{-2} x^2 y z b (xy)^5 = 1 \vee t[x, y]^2 \neq 1 \wedge (x^2 y^2 a)^3 \neq 1 \right)$$

Main theorem

An arbitrary first-order formula φ over a group $G \ni a, b, \ldots$:

$$\forall z \exists t \left(z^2 y x^2 a t^{-2} x^2 y z b (xy)^5 = 1 \vee t[x,y]^2 \neq 1 \wedge (x^2 y^2 a)^3 \neq 1\right)$$

$$\text{The } \textit{exponent-sum matrix } A(\varphi) = \begin{pmatrix} 5 & 5 \\ 3 & 3 \\ 0 & 0 \\ 6 & 6 \end{pmatrix}$$

Theorem (K & Anna Mkrtchyan)

If $\operatorname{rank}(A(\varphi))$ is less than the number of unknowns, then the number of tuples of elements satisfying φ is divisible by $|C(\{a, b, \ldots\})|$.

Theorem (K & Anna Mkrtchyan)

If $\operatorname{rank}(A(\varphi))$ is less than the number of unknowns, then the number of tuples of elements satisfying φ is divisible by $|C(\{a, b, \dots\})|$.

Calculation-free version (K & Anna Mkrtchyan)

If

$$\#(\textit{proper occurrences of bound variables}) + \\ + \#(\textit{components of } \Gamma(\varphi)) < \#(\textit{variables}),$$

then the number of tuples of elements satisfying φ is divisible by $|C(\{a, b, \dots\})|$.

Proof.

$$\operatorname{rank}(A(\varphi)) \leqslant \#(\textit{rows}) = \dots - (\textit{the Euler characteristic of } \Gamma).$$

Theorem (K & Anna Mkrtchyan)

If $\mathrm{rank}(A(\varphi))$ is less than the number of unknowns, then the number of tuples of elements satisfying φ is divisible by $|C(\{a, b, \dots\})|$.

The order of any group divides, e.g. the following numbers:

Some applications

Theorem (K & Anna Mkrtchyan)

If $\mathrm{rank}(A(\varphi))$ is less than the number of unknowns, then the number of tuples of elements satisfying φ is divisible by $|C(\{a, b, \dots\})|$.

The order of any group divides, e.g. the following numbers:

- the number of pairs of noncommuting elements whose product of squares is a cube

Some applications

Theorem (K & Anna Mkrtchyan)

If $\mathrm{rank}(A(\varphi))$ is less than the number of unknowns, then the number of tuples of elements satisfying φ is divisible by $|C(\{a, b, \dots\})|$.

The order of any group divides, e.g. the following numbers:

- the number of pairs of noncommuting elements whose product of squares is a cube

Some applications

Theorem (K & Anna Mkrtchyan)

If $\mathrm{rank}(A(\varphi))$ is less than the number of unknowns, then the number of tuples of elements satisfying φ is divisible by $|C(\{a, b, \dots\})|$.

The order of any group divides, e.g. the following numbers:

- the number of pairs of noncommuting elements whose product of squares is a cube of a noncentral element;
- the number of pairs of noncommuting elements whose product of squares is a cube if the cube of their product lies in the centre;

Some applications

Theorem (K & Anna Mkrtchyan)

If $\operatorname{rank}(A(\varphi))$ is less than the number of unknowns, then the number of tuples of elements satisfying φ is divisible by $|C(\{a, b, \dots\})|$.

The order of any group divides, e.g. the following numbers:

- the number of pairs of noncommuting elements whose product of squares is a cube of a noncentral element;
- the number of pairs of noncommuting elements whose product of squares is a cube if the cube of their product lies in the centre;
- the number of pairs of elements such that either the product of their squares is a cube or their commutator is not a square;

Some applications

Theorem (K & Anna Mkrtchyan)

If $\mathrm{rank}(A(\varphi))$ is less than the number of unknowns, then the number of tuples of elements satisfying φ is divisible by $|C(\{a, b, \dots\})|$.

The order of any group divides, e.g. the following numbers:

- the number of pairs of noncommuting elements whose product of squares is a cube of a noncentral element;
- the number of pairs of noncommuting elements whose product of squares is a cube if the cube of their product lies in the centre;
- the number of pairs of elements such that either the product of their squares is a cube or their commutator is not a square;
- ...

Conjugation theorems

A system of coefficient-free conditions (over a group $G \ni a, b, \dots$)

$$\begin{cases} x^3y^3x^{-1}y[x,y] \sim a \\ \\ (x,y^2)^5 \sim b \end{cases}$$

$$A = \begin{pmatrix} 2 & 4 \\ 5 & 10 \end{pmatrix}$$

Conjugation theorems

A system of coefficient-free conditions (over a group $G \ni a, b, \dots$)

$$\begin{cases} x^3y^3x^{-1}y[x,y] \sim a \\ \\ (x,y^2)^5 \sim b \end{cases}$$

$$A = \begin{pmatrix} 2 & 4 \\ 5 & 10 \end{pmatrix}$$

Theorem (Cameron Gordon & Fernando Rodriguez-Villegas, 2012)

If rank A is less than the number of unknowns, then the number of solutions is divisible by $|G|$ (where $\sim$ stands for conjugation).

Conjugation theorems

A system of coefficient-free conditions (over a group $G \ni a, b, \dots$)

$$\begin{cases} x^3y^3x^{-1}y[x,y] \sim a \\ \\ (x, y^2)^5 \sim b \end{cases}$$

$$A = \begin{pmatrix} 2 & 4 \\ 5 & 10 \end{pmatrix}$$

Theorem (Cameron Gordon & Fernando Rodriguez-Villegas, 2012)

If rank A is less than the number of unknowns, then the number of solutions is divisible by $|G|$ (where $\sim$ stands for conjugation).

Theorem (K & Anna Mkrtchyan)

If rank A is less than the number of unknowns, then the number of solutions is divisible by $|G|$ (where $\sim$ stands for simultaneous conjugation).

- A. Klyachko, A. Mkrtchyan, How many tuples of group elements have a given property? arXiv:1205.2824
- A question from Mathoverflow
- Another question from Mathoverflow

Thank you!