RANDOM GENERATION IN FINITE GROUPS

Mariapia Moscatiello

University of Padova

Young Researchers Algebra Conference 2019

Napoli
16th-18th September 2019

INTRODUCTION

- G finite group

INTRODUCTION

- G finite group
- $(x_k)_{k \in \mathbb{N}}$ sequence of uniformly distributed G - valued random variables

- G finite group
- $(x_k)_{k\in\mathbb{N}}$ sequence of uniformly distributed G - valued random variables

Define a random variable:

$$\tau_G = min\{k \geq 1 \mid \langle x_1, \ldots, x_k \rangle = G\}$$

- G finite group
- $(x_k)_{k\in\mathbb{N}}$ sequence of uniformly distributed G - valued random variables

Define a random variable:

$$\tau_G = min\{k \geq 1 \mid \langle x_1, \ldots, x_k \rangle = G\}$$

$$e(G) = \sum_{k\geq 0} kP\left(\tau_G = k\right)$$

Expectation of τ_G

INTRODUCTION

- G finite group
- $(x_k)_{k\in\mathbb{N}}$ sequence of uniformly distributed G - valued random variables

Define a random variable:

$$\tau_G = min\{k \geq 1 \mid \langle x_1, \ldots, x_k \rangle = G\}$$

$$e(G) = \sum_{k\geq 0} kP\left(\tau_G = k\right)$$

The expected number of elements of G which have to be drawn at random, with replacement, before a set of generators is found

Since $\tau_G > k \iff \langle x_1, \ldots, x_k \rangle \neq G$ we get

$$P(\tau_G > k) = 1 - P_G(k),$$

with $P_G(k) = \dfrac{|\{(g_1, \ldots, g_k) : \langle g_1, \ldots, g_k \rangle = G\}|}{|G|^k}$ the probability that k randomly chosen elements generate G

Since $\tau_G > k \iff \langle x_1, \ldots, x_k \rangle \neq G$ we get

$$P(\tau_G > k) = 1 - P_G(k),$$

with $P_G(k) = \dfrac{|\{(g_1, \ldots, g_k) : \langle g_1, \ldots, g_k \rangle = G\}|}{|G|^k}$ the probability that k randomly chosen elements generate G

$$\begin{aligned} e(G) &= \sum_{k\geq 1} kP\left(\tau_G = k\right) = \sum_{k\geq 1}\left(\sum_{m\geq k} P\left(\tau_G = m\right)\right) \\ &= \sum_{k\geq 1} P\left(\tau_G \geq k\right) = \sum_{k\geq 0} P\left(\tau_G > k\right) \\ &= \sum_{k\geq 0}\left(1 - P_G\left(k\right)\right) \end{aligned}$$

EXAMPLE

If $G = C_p$ is a cyclic group of prime order p, then τ_G is a geometric random variable of parameter $\frac{p-1}{p}$, so $e(C_p) = \frac{p}{p-1}$

EXAMPLE

Let $G = D_{2p}$ be the dihedral group of order $2p$ for an odd prime p

$$G = \langle x_1, \ldots, x_n \rangle \iff \exists\ 1 \leq i < j \leq n : x_i \neq 1 \ and \ x_j \notin \langle x_i \rangle$$

EXAMPLE

Let $G = D_{2p}$ be the dihedral group of order $2p$ for an odd prime p

$$G = \langle x_1, \ldots, x_n \rangle \iff \exists\ 1 \le i < j \le n : x_i \neq 1 \ and \ x_j \notin \langle x_i \rangle$$

- The number of trials needed to obtain $x \neq 1$ in G is a geometric random variable with parameter $\frac{2p-1}{2p}$ and expectation $E_0 = \frac{2p}{2p-1}$;

EXAMPLE

Let $G = D_{2p}$ be the dihedral group of order $2p$ for an odd prime p

$$G = \langle x_1, \ldots, x_n \rangle \Longleftrightarrow \exists\, 1 \leq i < j \leq n : x_i \neq 1 \text{ and } x_j \notin \langle x_i \rangle$$

- The number of trials needed to obtain $x \neq 1$ in G is a geometric random variable with parameter $\frac{2p-1}{2p}$ and expectation $E_0 = \frac{2p}{2p-1}$;
- With probability $p_1 = \frac{p}{2p-1}$, x has order 2 : the number of trials needed to find $y \notin \langle x \rangle$ is a geometric with expectation $E_1 = \frac{2p}{2p-2}$

EXAMPLE

Let $G = D_{2p}$ be the dihedral group of order $2p$ for an odd prime p

$$G = \langle x_1, \ldots, x_n \rangle \Longleftrightarrow \exists\, 1 \le i < j \le n : x_i \ne 1 \text{ and } x_j \notin \langle x_i \rangle$$

- The number of trials needed to obtain $x \ne 1$ in G is a geometric random variable with parameter $\frac{2p-1}{2p}$ and expectation $E_0 = \frac{2p}{2p-1}$;
- With probability $p_1 = \frac{p}{2p-1}$, x has order 2 : the number of trials needed to find $y \notin \langle x \rangle$ is a geometric with expectation $E_1 = \frac{2p}{2p-2}$
- With probability $p_2 = \frac{p-1}{2p-1}$, x has order p : the number of trials needed to find $y \notin \langle x \rangle$ is a geometric with expectation $E_2 = \frac{2p}{2p-p}$

EXAMPLE

Let $G = D_{2p}$ be the dihedral group of order $2p$ for an odd prime p

$$G = \langle x_1, \ldots, x_n \rangle \Longleftrightarrow \exists\, 1 \le i < j \le n : x_i \ne 1 \text{ and } x_j \notin \langle x_i \rangle$$

- The number of trials needed to obtain $x \ne 1$ in G is a geometric random variable with parameter $\frac{2p-1}{2p}$ and expectation $E_0 = \frac{2p}{2p-1}$;
- With probability $p_1 = \frac{p}{2p-1}$, x has order 2 : the number of trials needed to find $y \notin \langle x \rangle$ is a geometric with expectation $E_1 = \frac{2p}{2p-2}$
- With probability $p_2 = \frac{p-1}{2p-1}$, x has order p : the number of trials needed to find $y \notin \langle x \rangle$ is a geometric with expectation $E_2 = \frac{2p}{2p-p}$

$$e(D_{2p}) = E_0 + p_1 E_1 + p_2 E_2 = 2 + \frac{2p^2}{(2p-1)(2p-2)}$$

EXAMPLE

Let $G = D_{2p}$ be the dihedral group of order $2p$ for an odd prime p

$$G = \langle x_1, \dots, x_n \rangle \Longleftrightarrow \exists\, 1 \le i < j \le n : x_i \neq 1 \; and \; x_j \notin \langle x_i \rangle$$

- The number of trials needed to obtain $x \neq 1$ in G is a geometric random variable with parameter $\frac{2p-1}{2p}$ and expectation $E_0 = \frac{2p}{2p-1}$;
- With probability $p_1 = \frac{p}{2p-1}$, x has order 2 : the number of trials needed to find $y \notin \langle x \rangle$ is a geometric with expectation $E_1 = \frac{2p}{2p-2}$
- With probability $p_2 = \frac{p-1}{2p-1}$, x has order p : the number of trials needed to find $y \notin \langle x \rangle$ is a geometric with expectation $E_2 = \frac{2p}{2p-p}$

$$e(D_{2p}) = E_0 + p_1 E_1 + p_2 E_2 = 2 + \frac{2p^2}{(2p-1)(2p-2)}$$

In particular $e(Sym(3)) = \frac{29}{10}$

The Möbius function μ_G on the subgroup lattice of G is defined as:

$$\mu_G(G) = 1$$

$$\mu_G(H) = -\sum_{H<K} \mu_G(K), \quad \forall H < G$$

The Möbius function μ_G on the subgroup lattice of G is defined as:

$$\mu_G(G) = 1$$
$$\mu_G(H) = -\sum_{H<K} \mu_G(K), \quad \forall H < G$$

Theorem (P. Hall)

$$P_G(t) = \sum_{H \leq G} \frac{\mu_G(H)}{|G:H|^t}$$

MÖBIUS FUNCTION

The Möbius function μ_G on the subgroup lattice of G is defined as:

$$\mu_G(G) = 1$$

$$\mu_G(H) = -\sum_{H<K} \mu_G(K), \quad \forall H < G$$

Theorem (P. Hall)

$$P_G(t) = \sum_{H \leq G} \frac{\mu_G(H)}{|G:H|^t}$$

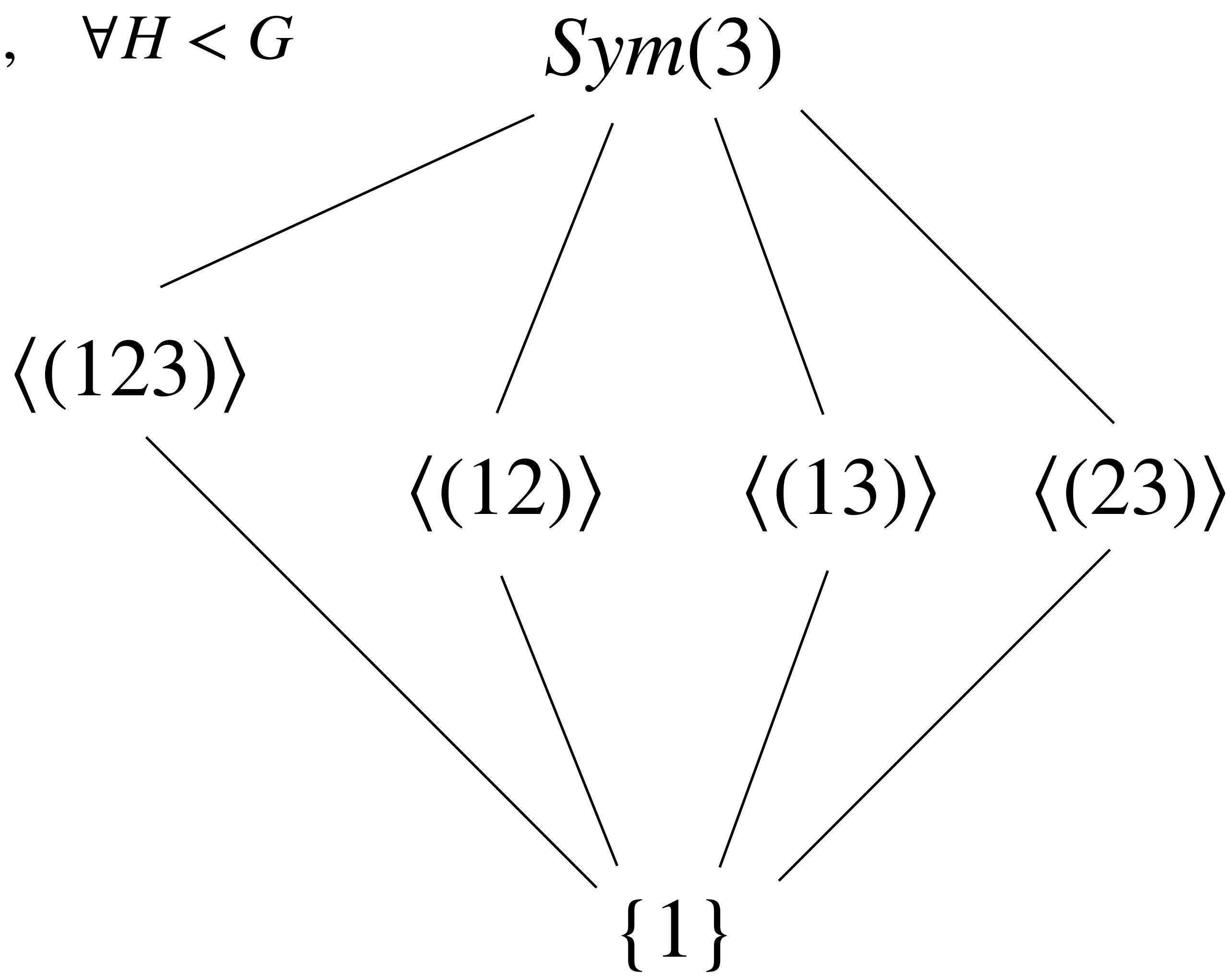
Theorem (A. Lucchini)

$$e(G) = -\sum_{H<G} \frac{\mu_G(H)|G|}{|G|-|H|}$$

EXAMPLE

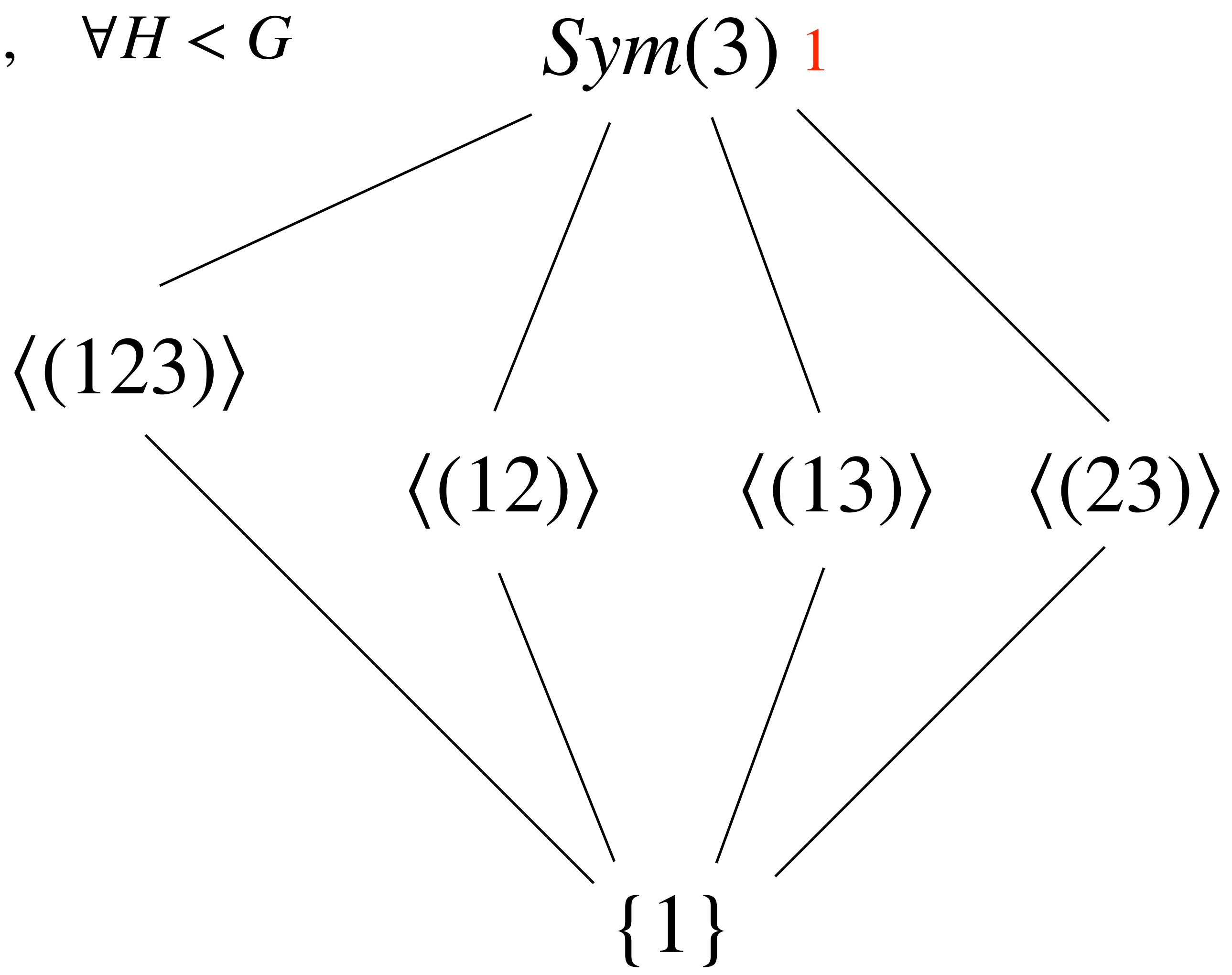
$$\mu_G(G) = 1$$

$$\mu_G(H) = -\sum_{H<K} \mu_G(K), \quad \forall H < G$$



$$\mu_G(G) = 1$$

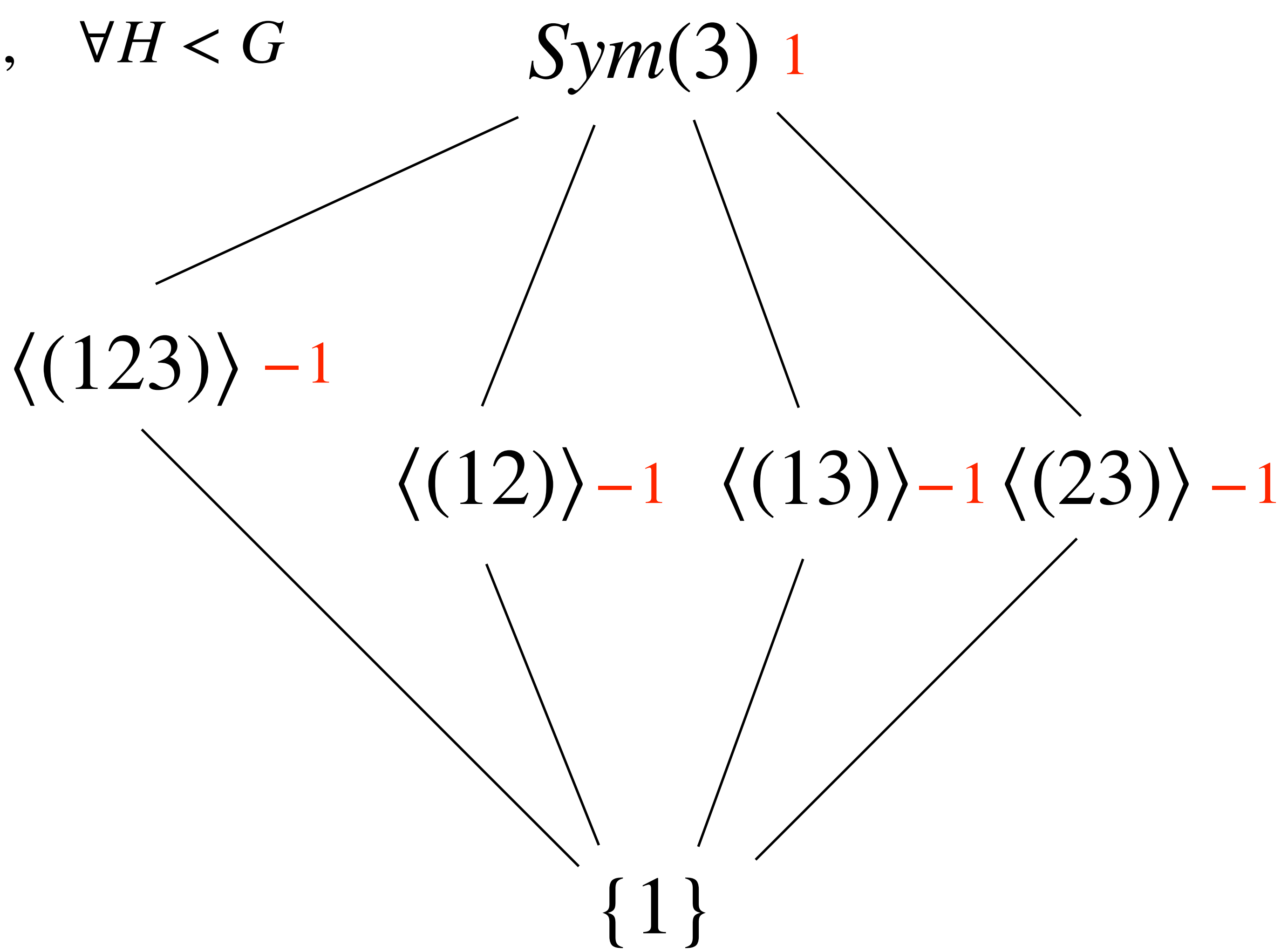
$$\mu_G(H) = -\sum_{H<K} \mu_G(K), \quad \forall H < G$$



EXAMPLE

$$\mu_G(G) = 1$$

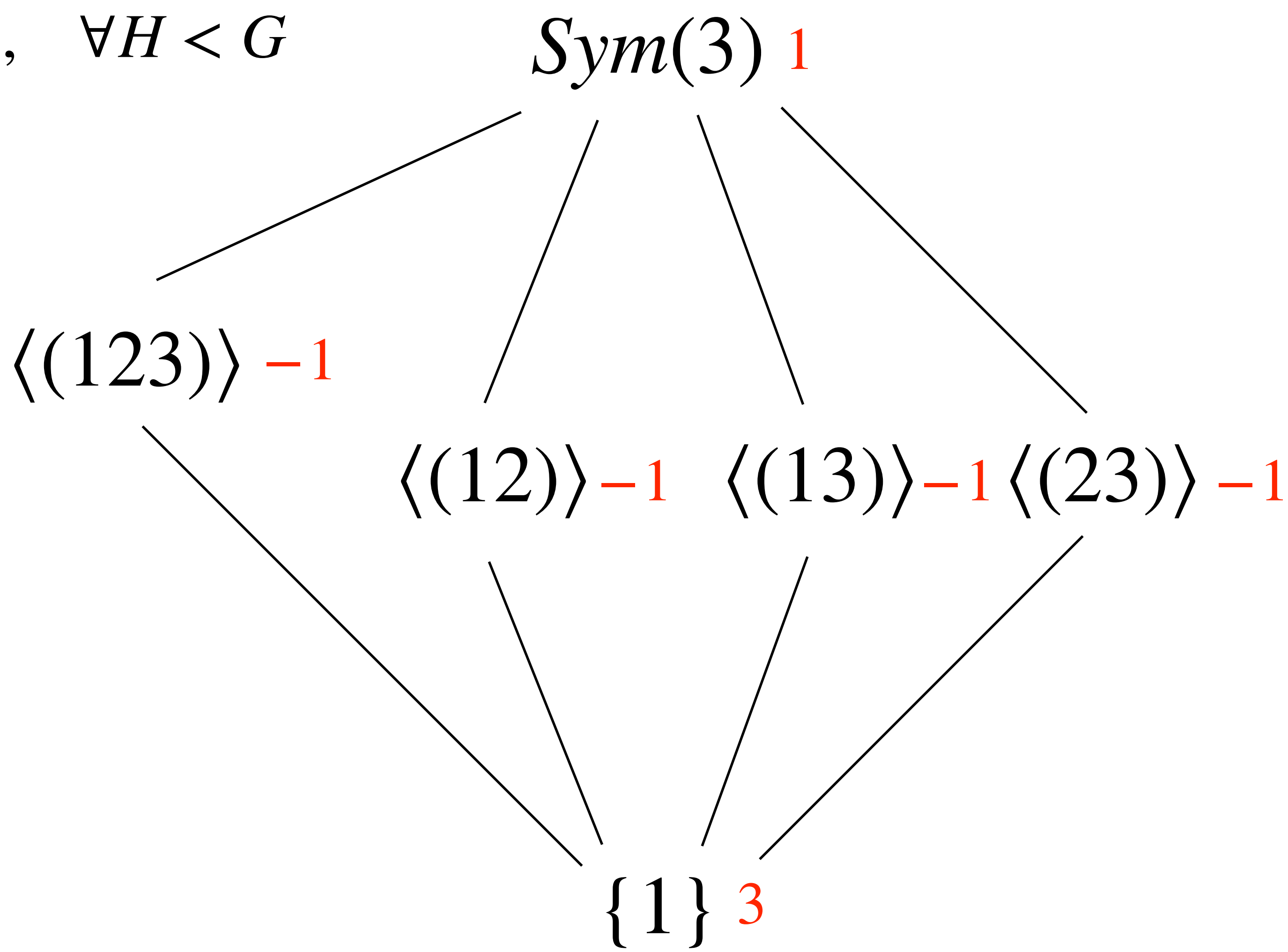
$$\mu_G(H) = -\sum_{H<K} \mu_G(K), \quad \forall H < G$$



EXAMPLE

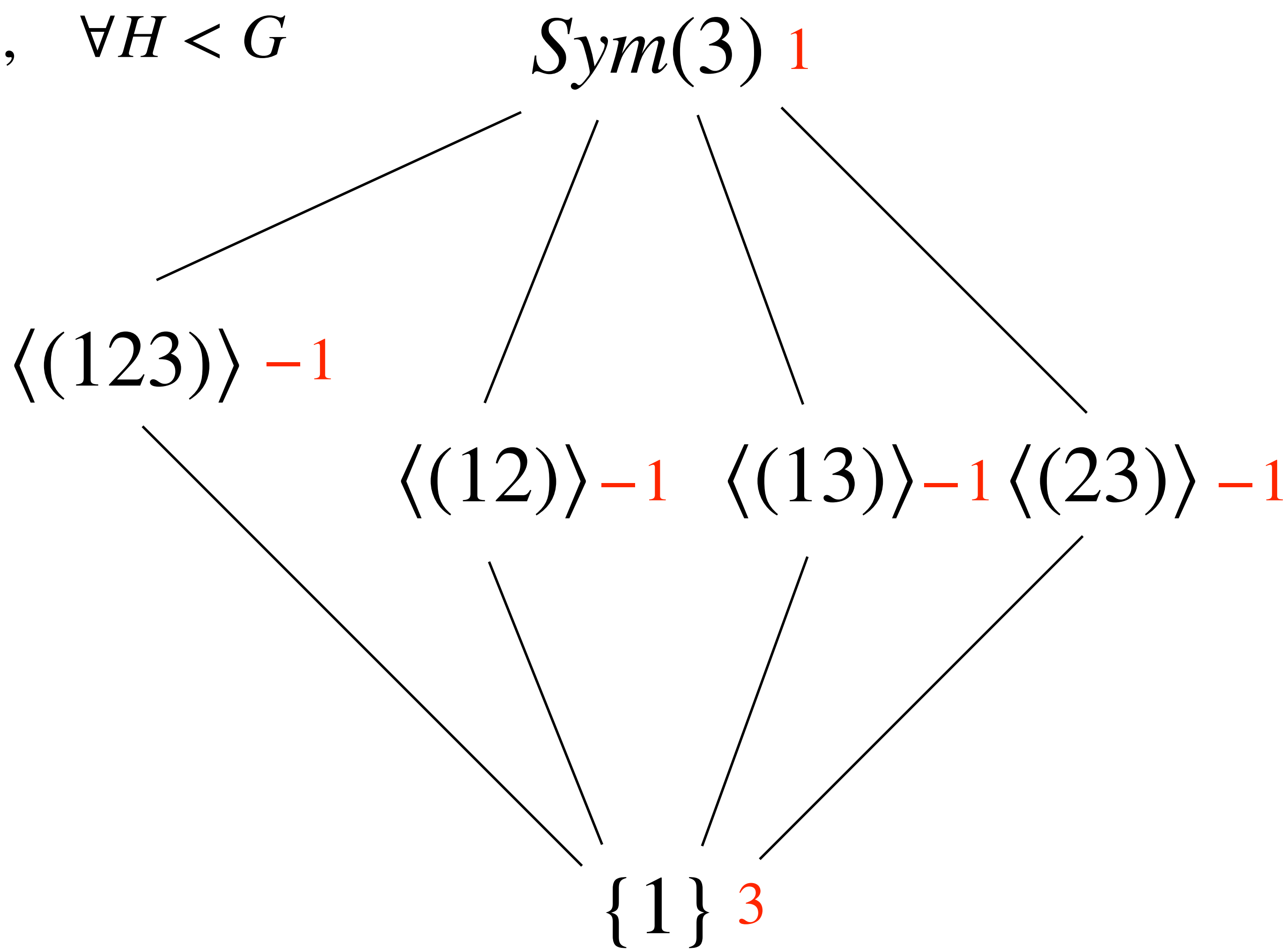
$$\mu_G(G) = 1$$

$$\mu_G(H) = -\sum_{H<K} \mu_G(K), \quad \forall H < G$$



$$\mu_G(G) = 1$$

$$\mu_G(H) = -\sum_{H<K} \mu_G(K), \quad \forall H < G$$



$$e(Sym(3)) = -\sum_{H<Sym(3)} \frac{\mu_{Sym(3)}(H)\,|Sym(3)|}{|Sym(3)| - |H|}$$

$$= -\frac{3\cdot 6}{6-1} + 3\cdot\frac{6}{6-2} + \frac{6}{6-3} = \frac{29}{10}$$

WHAT IS KNOWN

Dixon proved that $e(Sym(n)) \rightarrow 2.5 \; and \; e(Alt(n)) \rightarrow 2, n \rightarrow \infty$

WHAT IS KNOWN

Dixon proved that $e(Sym(n)) \to 2.5$ *and* $e(Alt(n)) \to 2,\ n \to \infty$

More generally for a finite, non abelian, simple group S, famous results of Dixon, Kantor-Lubotzky and Liebeck-Shalev establish that

$$P_S(2) \to 1,\ |S| \to \infty$$

From this one can deduce that $e(S) \to 2,\ |S| \to \infty$

WHAT IS KNOWN

Dixon proved that $e(Sym(n)) \to 2.5$ *and* $e(Alt(n)) \to 2,\ n \to \infty$

More generally for a finite, non abelian, simple group S, famous results of Dixon, Kantor-Lubotzky and Liebeck-Shalev establish that

$$P_S(2) \to 1,\ |S| \to \infty$$

From this one can deduce that $e(S) \to 2,\ |S| \to \infty$

Lucchini proved that for a non abelian, simple group S, $e(S) \leq e(Alt(6)) \sim 2.494$ and that for $n \geq 5,\ 2.5 \leq e(Sym(n)) \leq e(Sym(6)) \sim 2.8816$

WHAT IS KNOWN

Dixon proved that $e(Sym(n)) \to 2.5$ *and* $e(Alt(n)) \to 2,\ n \to \infty$

More generally for a finite, non abelian, simple group S, famous results of Dixon, Kantor-Lubotzky and Liebeck-Shalev establish that

$$P_S(2) \to 1,\ |S| \to \infty$$

From this one can deduce that $e(S) \to 2,\ |S| \to \infty$

Lucchini proved that for a non abelian, simple group S, $e(S) \leq e(Alt(6)) \sim 2.494$ and that for $n \geq 5,\ 2.5 \leq e(Sym(n)) \leq e(Sym(6)) \sim 2.8816$

Pomerance proved that for a finite nilpotent group G, then $e(G) \leq d(G) + \sigma$, where $\sigma \sim 2.1185$ is an absolute constant that is explicitly described in terms of the Riemann zeta function

A PROBABILISTIC VERSION OF AN OLD THEOREM

Theorem (R. Guralnick, A. Lucchini)

If all the Sylow subgroups of a finite group G can be generated by d elements, then the group G itself can be generated by $d+1$ elements

Theorem (R. Guralnick, A. Lucchini)

If all the Sylow subgroups of a finite group G can be generated by d elements, then the group G itself can be generated by $d+1$ elements

Theorem (A. Lucchini, MM 2017)

If all the Sylow subgroups of a finite group G can be generated by d elements, then

$$e(G) \leq d + \kappa$$

where $\kappa \sim 2.752394$ is an absolute constant that is explicitly described in terms of the Riemann zeta function and best possible in this context

Theorem (R. Guralnick, A. Lucchini)

If all the Sylow subgroups of a finite group G can be generated by d elements, then the group G itself can be generated by $d+1$ elements

Theorem (A. Lucchini, MM 2017)

If all the Sylow subgroups of a finite group G can be generated by d elements, then

$$e(G) \leq d + \kappa$$

where $\kappa \sim 2.752394$ is an absolute constant that is explicitly described in terms of the Riemann zeta function and best possible in this context

This result is an improvement of a bound already obtained by Lucchini

WHAT ABOUT A GENERALIZATION?

Theorem (A. Lucchini, MM 2017)

If all the Sylow subgroups of a finite group G can be generated by d elements, then

$$e(G) \leq d + \kappa$$

where $\kappa \sim 2.752394$ is an absolute constant that is explicitly described in terms of the Riemann zeta function and best possible in this context

Relaxing the hypotheses

Replace the fact that all the Sylow subgroups are d-generated, with the assumption that there exists a family of coprime index subgroup all d-generated

GENERALIZATION IN SOLUBLE CASE

Theorem (A. Lucchini, MM 2017)

If all the Sylow subgroups of a finite group G can be generated by d elements, then

$$e(G) \leq d + \kappa$$

where $\kappa \sim 2.752394$ is an absolute constant that is explicitly described in terms of the Riemann zeta function and best possible in this context

Theorem (A. Lucchini, MM 2019)

Let G be a finite soluble group. Assume that for every $p \in \pi(G)$ there exists a subgroup G_p such that p does not divide $|G : G_p|$ and $e(G_p) \leq d$.
Then $e(G) \leq d + 9$

If G is a p-subgroup of $\mathrm{Sym}(n)$, then G can be generated by $\lfloor n/p \rfloor$ elements

If G is a p-subgroup of $\mathrm{Sym}(n)$, then G can be generated by $\lfloor n/p \rfloor$ elements

Corollary

If G is a permutation group of degree n, $e(G) \leq \lfloor n/2 \rfloor + \kappa$, with $\kappa \sim 2.752395$

If G is a p-subgroup of $\mathrm{Sym}(n)$, then G can be generated by $\lfloor n/p \rfloor$ elements

Corollary

If G is a permutation group of degree n, $e(G) \leq \lfloor n/2 \rfloor + \kappa$, with $\kappa \sim 2.752395$

This bound is not best possible

If G is a p-subgroup of Sym(n), then G can be generated by $\lfloor n/p \rfloor$ elements

Corollary

If G is a permutation group of degree n, $e(G) \leq \lfloor n/2 \rfloor + \kappa$, with $\kappa \sim 2.752395$

This bound is not best possible

Theorem (A. Lucchini, MM 2017)

If G is a permutation group of degree n, then either G=Sym(3) and $e(G) = 2.9$ or $e(G) \leq \lfloor n/2 \rfloor + \tilde{\kappa}$, with $\tilde{\kappa} \sim 1.606695$

Theorem (A. Lucchini, MM 2017)

If G is a permutation group of degree n, then either G=Sym(3) and $e(G) = 2.9$ or $e(G) \leq \lfloor n/2 \rfloor + \tilde{\kappa}$, with $\tilde{\kappa} \sim 1.606695$

$\tilde{\kappa}$ is best possible

Theorem (A. Lucchini, MM 2017)

If G is a permutation group of degree n, then either G=Sym(3) and $e(G) = 2.9$ or $e(G) \leq \lfloor n/2 \rfloor + \tilde{\kappa}$, with $\tilde{\kappa} \sim 1.606695$

$\tilde{\kappa}$ is best possible

Let $m = \lfloor n/2 \rfloor$ and set

$$G_m = \begin{cases} Sym(2)^m, \eta = 0, & \textit{if } m \textit{ is even} \\ Sym(2)^{m-1} \times Sym(3), \eta = 1, & \textit{if } m \textit{ is odd} \end{cases}$$

$$e(G_m) = m + \sum_{j \geq 0} \left(\left(\prod_{1 \leq l \leq m} \left(1 - \frac{1}{2^{j+l}}\right) \left(1 - \frac{3}{3^{j+m}}\right)^{\eta} \right) \right)$$

For $m \geq 4$, $e(G_m) - m$ increase with m and $\lim_{m \to \infty} e(G_m) - m = \tilde{k}$

A DIFFERENT QUESTION HAVING SAME ORIGIN

A subset $X \subseteq G$ is a minimal generating set for G if X is a generating set for G and no proper subset of X is a generating set for G

A DIFFERENT QUESTION HAVING SAME ORIGIN

A subset $X \subseteq G$ is a minimal generating set for G if X is a generating set for G and no proper subset of X is a generating set for G

Example

$\{(1,2),(2,3),\ldots,(n-1,n)\}$ minimally generates $\mathrm{Sym}(n)$

A DIFFERENT QUESTION HAVING SAME ORIGIN

A subset $X \subseteq G$ is a minimal generating set for G if X is a generating set for G and no proper subset of X is a generating set for G

Example

$\{(1,2),(2,3),\ldots,(n-1,n)\}$ minimally generates $\mathrm{Sym}(n)$

Denote with $m(G)$ the largest size of a minimal generating set for G

A DIFFERENT QUESTION HAVING SAME ORIGIN

A subset $X \subseteq G$ is a minimal generating set for G if X is a generating set for G and no proper subset of X is a generating set for G

Example

$\{(1,2), (2,3), \ldots, (n-1, n)\}$ minimally generates $\mathrm{Sym}(n)$

Denote with $m(G)$ the largest size of a minimal generating set for G

Theorem (P. Cameron, P. Cara, J. Whiston)

If G is a subgroup of $\mathrm{Sym}(n)$, then $m(G) \leq n-1$. The equality holds if and only if G=$\mathrm{Sym}(n)$. In particular $m(\mathrm{Sym}(n))=n-1$

A DIFFERENT QUESTION HAVING SAME ORIGIN

Theorem (R. Guralnick, A. Lucchini)

If all the Sylow subgroups of a finite group G can be generated by d elements, then the group G itself can be generated by $d+1$ elements

A DIFFERENT QUESTION HAVING SAME ORIGIN

Theorem (R. Guralnick, A. Lucchini)

If all the Sylow subgroups of a finite group G can be generated by d elements, then the group G itself can be generated by $d+1$ elements

Denote with $d_p(G)$ the minimal cardinality of a generating set of a Sylow p-subgroup of G

A DIFFERENT QUESTION HAVING SAME ORIGIN

Theorem (R. Guralnick, A. Lucchini)

If all the Sylow subgroups of a finite group G can be generated by d elements, then the group G itself can be generated by $d+1$ elements

Denote with $d_p(G)$ the minimal cardinality of a generating set of a Sylow p-subgroup of G

Is it possible to bound $m(G)$ as a function of $d_p(G)$, with p running through the prime divisors of the order of G?

A DIFFERENT QUESTION HAVING SAME ORIGIN

Theorem (R. Guralnick, A. Lucchini)

If all the Sylow subgroups of a finite group G can be generated by d elements, then the group G itself can be generated by $d+1$ elements

Denote with $d_p(G)$ the minimal cardinality of a generating set of a Sylow p-subgroup of G

Is it possible to bound $m(G)$ as a function of $d_p(G)$, with p running through the prime divisors of the order of G?

Theorem (A. Lucchini, P. Spiga, MM 2019)

Let G be a finite soluble group. Then $m(G) \leq \sum_{p \in \pi(G)} d_p(G)$

A DIFFERENT QUESTION HAVING SAME ORIGIN

Theorem (R. Guralnick, A. Lucchini)

If all the Sylow subgroups of a finite group G can be generated by d elements, then the group G itself can be generated by $d+1$ elements

Denote with $d_p(G)$ the minimal cardinality of a generating set of a Sylow p-subgroup of G

Is it possible to bound $m(G)$ as a function of $d_p(G)$, with p running through the prime divisors of the order of G?

Theorem (A. Lucchini, P. Spiga, MM 2019)

Let G be a finite soluble group. Then $m(G) \leq \sum_{p \in \pi(G)} d_p(G)$

Is this result true for all finite group?

A DIFFERENT QUESTION HAVING SAME ORIGIN

Theorem (R. Guralnick, A. Lucchini)

If all the Sylow subgroups of a finite group G can be generated by d elements, then the group G itself can be generated by $d+1$ elements

Denote with $d_p(G)$ the minimal cardinality of a generating set of a Sylow p-subgroup of G

Is it possible to bound $m(G)$ as a function of $d_p(G)$, with p running through the prime divisors of the order of G?

Theorem (A. Lucchini, P. Spiga, MM 2019)

Let G be a finite soluble group. Then $m(G) \leq \sum_{p \in \pi(G)} d_p(G) = \delta(G)$

Is this result true for all finite group?

NOT TRUE FOR THE SYMMETRIC GROUP

Example (smallest degree for a negative answer)

$$m(\mathrm{Sym}(9)) = 8 > \sum_p d_p(Sym(9)) = 7$$

NOT TRUE FOR THE SYMMETRIC GROUP

Example (smallest degree for a negative answer)

$$m(\mathrm{Sym}(9))=8 > \sum_p d_p(Sym(9)) = 7$$

Theorem (A. Lucchini, P. Spiga, MM 2019)

$$\delta(Sym(n)) = \sum_{p\in\pi(Sym(n))} d_p(Sym(n)) = log\ 2 \cdot n + o(n)$$

NOT TRUE FOR THE SYMMETRIC GROUP

Example (smallest degree for a negative answer)

$$m(\mathrm{Sym}(9))=8 > \sum_p d_p(Sym(9)) = 7$$

Theorem (A. Lucchini, P. Spiga, MM 2019)

$$\delta(Sym(n)) = \sum_{p\in\pi(Sym(n))} d_p(Sym(n)) = log\ 2 \cdot n + o(n)$$

$m(\mathrm{Sym}(n))=n\text{-}1$

NOT TRUE FOR THE SYMMETRIC GROUP

Example (smallest degree for a negative answer)

$$m(\mathrm{Sym}(9))=8 > \sum_p d_p(Sym(9)) = 7$$

Theorem (A. Lucchini, P. Spiga, MM 2019)

$$\delta(Sym(n)) = \sum_{p\in\pi(Sym(n))} d_p(Sym(n)) = log\, 2 \cdot n + o(n)$$

$m(\mathrm{Sym}(n))=n$-1

Corollary

As $n \to \infty$, $m(Sym(n)) - \delta(Sym(n)) \to \infty$ and $m(Sym(n)) \leq \delta(Sym(n))$ is satisfies only by finitely many values of n

NOT TRUE FOR THE SYMMETRIC GROUP

Example (smallest degree for a negative answer)

$$m(\mathrm{Sym}(9))=8 > \sum_p d_p(Sym(9)) = 7$$

Theorem (A. Lucchini, P. Spiga, MM 2019)

$$\delta(Sym(n)) = \sum_{p\in\pi(Sym(n))} d_p(Sym(n)) = log\ 2 \cdot n + o(n)$$

$m(\mathrm{Sym}(n))=n$-1

Corollary

As $n \to \infty$, $m(Sym(n)) - \delta(Sym(n)) \to \infty$ and $m(Sym(n)) \leq \delta(Sym(n))$ is satisfies only by finitely many values of n

Theorem (A. Lucchini, P. Spiga, MM 2019)

For every positive real number $\eta > 1$, there exists a constant c such that $m(Sym(n)) \leq c(\delta(Sym(n)))^\eta$, for every $n \in \mathbb{N}$

CONJECTURE AND REDUCTION

Conjecture (A. Lucchini, P. Spiga, MM 2019)

There exist two constants c and η such that $m(G) \le c(\sum_p d_p(G))^\eta = c(\delta(G))^\eta$, for every finite group G

CONJECTURE AND REDUCTION

Conjecture (A. Lucchini, P. Spiga, MM 2019)

There exist two constants c and η such that $m(G) \leq c(\sum_p d_p(G))^\eta = c(\delta(G))^\eta$, for every finite group G

Theorem (A. Lucchini, P. Spiga, MM 2019)

If there are $\sigma \geq 1$ and $\eta \geq 2$ such that $m(X) - m(X/S) \leq \sigma \cdot |\pi(S)|^\eta$ for every composition factor S of G and for every almost simple group X with $\operatorname{soc} X = S$. Then

$$m(G) \leq \sigma(\sum_p d_p(G))^\eta = \sigma(\delta(G))^\eta$$

CONJECTURE AND REDUCTION

Conjecture (A. Lucchini, P. Spiga, MM 2019)

There exist two constants c and η such that $m(G) \leq c(\sum_p d_p(G))^\eta = c(\delta(G))^\eta$, for every finite group G

Theorem (A. Lucchini, P. Spiga, MM 2019)

If there are $\sigma \geq 1$ and $\eta \geq 2$ such that $m(X) - m(X/S) \leq \sigma \cdot |\pi(S)|^\eta$ for every composition factor S of G and for every almost simple group X with $\operatorname{soc} X = S$. Then

$$m(G) \leq \sigma(\sum_p d_p(G))^\eta = \sigma(\delta(G))^\eta$$

CONJECTURE AND REDUCTION

Conjecture (A. Lucchini, P. Spiga, MM 2019)

There exist two constants c and η such that $m(G) \leq c(\sum_p d_p(G))^\eta = c(\delta(G))^\eta$, for every finite group G

Theorem (A. Lucchini, P. Spiga, MM 2019)

If there are $\sigma \geq 1$ and $\eta \geq 2$ such that $m(X) - m(X/S) \leq \sigma \cdot |\pi(S)|^\eta$ for every composition factor S of G and for every almost simple group X with $\operatorname{soc} X = S$. Then

$$m(G) \leq \sigma(\sum_p d_p(G))^\eta = \sigma(\delta(G))^\eta$$

Reduced Conjecture (A. Lucchini, P. Spiga, MM 2019)

There exist two constants σ and η such that $m(X) - m(X/socX) \leq \sigma(|\pi(socX)|)^\eta$, for every finite almost simple group X

TOWARD A PROOF

Reduced Conjecture (A. Lucchini, P. Spiga, MM 2019)

There exist two constants σ and η such that $m(X) - m(X/socX) \leq \sigma(|\pi(socX)|)^{\eta}$, for every finite almost simple group X

Proposition <u>**Reduced Conjecture holds true for soc$X$ not of Lie type**</u>

There exists a constants such that, if X is a finite almost simple group and soc$X$ is not a simple group of Lie type, then $m(X) - m(X/socX) \leq \sigma(|\pi(socX)|)^2$

TOWARD A PROOF

Reduced Conjecture (A. Lucchini, P. Spiga, MM 2019)

There exist two constants σ and η such that $m(X) - m(X/socX) \leq \sigma(|\pi(socX)|)^{\eta}$, for every finite almost simple group X

Proposition <u>**Reduced Conjecture holds true for soc$X$ not of Lie type**</u>

There exists a constants such that, if X is a finite almost simple group and soc$X$ is not a simple group of Lie type, then $m(X) - m(X/socX) \leq \sigma(|\pi(socX)|)^2$

Conjecture holds true if there are no composition factor of Lie type

Corollary

There exists a constant σ such that if G has no composition factor of Lie type, then $m(G) \leq \sigma(\sum_p d_p(G))^2 = \sigma(\delta(G))^2$

WHAT ABOUT THE SIMPLE GROUPS OF LIE TYPE?

Theorem (J. Whiston, J. Saxl)

Let p be a prime number, then $m(PSL(2,p^r)) \leq max(6, \tilde{\pi}(r)+2)$, where $\tilde{\pi}(r)$ is the number of distinct prime divisors of r

WHAT ABOUT THE SIMPLE GROUPS OF LIE TYPE?

Theorem (J. Whiston, J. Saxl)

Let p be a prime number, then $m(PSL(2,p^r)) \leq max(6, \tilde{\pi}(r)+2)$, where $\tilde{\pi}(r)$ is the number of distinct prime divisors of r

$$\tilde{\pi}(r) \leq \tilde{\pi}(p^r - 1) \leq |\pi(PSL_2(p^r))|$$

WHAT ABOUT THE SIMPLE GROUPS OF LIE TYPE?

Theorem (J. Whiston, J. Saxl)

Let p be a prime number, then $m(PSL(2,p^r)) \leq max(6, \tilde{\pi}(r) + 2)$, where $\tilde{\pi}(r)$ is the number of distinct prime divisors of r

$$\tilde{\pi}(r) \leq \tilde{\pi}(p^r - 1) \leq |\pi(PSL_2(p^r))|$$

Corollary

$$m(PSL_2(p^r)) \leq |\pi(PSL_2(p^r))|^2$$

Reduced Conjecture holds true for $PSL_2(p^r)$

WHAT ABOUT THE SIMPLE GROUPS OF LIE TYPE?

Theorem (J. Whiston, J. Saxl)

Let p be a prime number, then $m(PSL(2,p^r)) \leq max(6, \tilde{\pi}(r) + 2)$, where $\tilde{\pi}(r)$ is the number of distinct prime divisors of r

$\tilde{\pi}(r) \leq \tilde{\pi}(p^r - 1) \leq |\pi(PSL_2(p^r))|$

Corollary

$m(PSL_2(p^r)) \leq |\pi(PSL_2(p^r))|^2$

Reduced Conjecture holds true for $PSL_2(p^r)$

P. J. Keen

$m(PSL_3(p^r))$, $m(SO(3,p^r))$, $m(SU(3,p^r))$ have linear bounds in terms of $\tilde{\pi}(r)$

WHAT ABOUT THE SIMPLE GROUPS OF LIE TYPE?

Theorem (J. Whiston, J. Saxl)

Let p be a prime number, then $m(PSL(2,p^r)) \leq max(6, \tilde{\pi}(r) + 2)$, where $\tilde{\pi}(r)$ is the number of distinct prime divisors of r

$$\tilde{\pi}(r) \leq \tilde{\pi}(p^r - 1) \leq |\pi(PSL_2(p^r))|$$

Corollary

$$m(PSL_2(p^r)) \leq |\pi(PSL_2(p^r))|^2$$

Reduced Conjecture holds true for $PSL_2(p^r)$

P. J. Keen

$m(PSL_3(p^r))$, $m(SO(3,p^r))$, $m(SU(3,p^r))$ have linear bounds in terms of $\tilde{\pi}(r)$

Let X an almost simple group with $socX = G_n(p^r)$ be a group of Lie type with rank n over $\mathbb{F}_{p^r}$. Is $m(X)$-$m(X/socX)$ polynomially bounded in terms of n and $\tilde{\pi}(r)$?

WHAT ABOUT THE SIMPLE GROUPS OF LIE TYPE?

Theorem (J. Whiston, J. Saxl)

Let p be a prime number, then $m(PSL(2,p^r)) \leq max(6, \tilde{\pi}(r) + 2)$, where $\tilde{\pi}(r)$ is the number of distinct prime divisors of r

$\tilde{\pi}(r) \leq \tilde{\pi}(p^r - 1) \leq |\pi(PSL_2(p^r))|$

Corollary

$m(PSL_2(p^r)) \leq |\pi(PSL_2(p^r))|^2$

Reduced Conjecture holds true for $PSL_2(p^r)$

P. J. Keen

$m(PSL_3(p^r))$, $m(SO(3,p^r))$, $m(SU(3,p^r))$ have linear bounds in terms of $\tilde{\pi}(r)$

Let X an almost simple group with $socX = G_n(p^r)$ be a group of Lie type with rank n over $\mathbb{F}_{p^r}$. Is $m(X)$-$m(X/socX)$ polynomially bounded in terms of n and $\tilde{\pi}(r)$?

If this question has an affirmative answer, both our conjectures would be true