Möbius function in finite groups: some computation and application

SandGAL2019

Cremona June 10-13

Francesca Dalla Volta

Milano-Bicocca

(Joint work (in progress) with Martino Borello, Giovanni Zini)

The Möbius function on a PoSet

The Möbius function associated with a finite, partially-ordered set χ (poset) μ_χ is a map $\mu_\chi : \chi \times \chi \to \mathbb{Z}$ such that : $\mu_\chi(a, b) = 0$ unless $a \leq b$ when it is defined recursively by the equations

$$\mu_\chi(a, a) = 1$$

$$\sum_{a \leq c \leq b} \mu_\chi(a, c) = 0, \;\; a < b.$$

GENERALIZATION of the classical Möbius function of the number theory:

$\mu(n) = (-1)^r$ if n is the product of r distinct primes

$\mu(n) = 0$ if n is divisible by the square of a prime.

The Möbius function of a group G

Let G be a (finite) group; Denote by $\mathcal{P}(G)$ the subgroup lattice of G. The Möbius function of G is defined recursively by

$$\mu_G(G) = 1, \ \mu(H) = -\sum_{K\,:\,H<K\leq G} \mu_G(K)$$

for any $H < G$.

EXAMPLE 1. *If G is the cyclic infinite group, μ_G is the number theoretic Möbius function: if G_n is the subgroup of G of index n, $\mu_G(G_n) = \mu(n)$*

Beginning with generation of groups.

μ was introduced independently by Weisner (1935) and Hall(1936).

Hall: enumerates generating tuples of elements of G:

- $\sigma_n(G)$: number of ordered n-tuples of elements of G
- $\phi_n(H)$: number of ordered n-tuples of elements of G which generate $H \leq G$.

$$\sigma_n(G) = \sum_{H:H\leq G} \phi_n(H)$$

$$\phi_n(G) = \sum_{H,\, H\leq G} \sigma_n(H)\mu(H) = \sum_{H,\, H\leq G} |\, H\,|^n\, \mu(H)$$

(using Möbius inversion formula)

Great interest about Möbius function and related topics

- T. Hawkes, M. Isaacs, M. Özaydin (1989), Pahlings(1993): relation between the Möbius function on the Poset $\mathcal{P}(G)$ of the subgroups of a group G and the Möbius function λ of the lattice of conjugacy classes of subgroups of G:
  $[H] \leq [K]$ if $H \leq K^g$ for some $g \in G$
  For solvable groups, the following is true:

$$\mu_G(H) = \lambda_G([H])[N_{G'}(H) : G' \cap H]$$

  Is it the following true for non solvabe groups?NO

- Find some bound (or the exact value) for $\mu_G(1)$, when G is a classical group. (Shareshan Ph.D thesis, 1996): partial results, related to the reduced Euler characteristic for a simplicial complex;

- Denote by $Prob_G(n)$ the probability that n elements of G, (G finite) generate G. It is immediate:

$$Prob_G(n) = \frac{\phi_n(G)}{\mid G \mid^n} = \sum_{H \leq G} \frac{\mu_G(H)}{[G : H]^n}$$

It is possible to define a **complex function** (Boston, Mann 1996):

$$P_G(s) = \sum_{n \in \mathbb{N}} \frac{a_n(G)}{n^s},\ s \in \mathbb{C},$$

where

$$a_n(G) = \sum_{[G:H]=n} \mu_G(H)$$

$P_G(t) = Prob_G(t)$ **for** $t \in \mathbb{N}$

Going to profinite groups:

Definition 2. *A finitely generated profinite group is said to be positively generated if, for some k, the probability that k random elements generate G, is positive.*

In case of profinite groups, the sum becomes:

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

where H ranges over all open subgroups of G.

Mann conjectured that this sum is absolutely convergent in "some" half complex plane. This conjecture is implied by the following 2 facts:

– 1 the number $|\mu_G(H)|$ is bounded by a polynomial function in $[G : H]$;

– 2 the number $b_n(G)$ of subgroups H of index n satisfying $\mu_G(H) \neq 0$ grows at most polynomially in n.

1 and 2 were proved in the case of alternating and symmetric groups (Lucchini-Colombo- 2010);
Lucchini (2010): Actually 1 and 2 are true, if they are verified for almost finite simple groups.

- The structure of the group of units of the finite monoid of all cellular automata over the configuration space A^G, for a given finite set A and a finite group G (A. Castillo-Ramirez and M. Gadouleau, 2017)

The Möbius function for $G = PSL(3, 2^p)$

Alternating and symmetric groups done. Now? Other classical groups?

Not very much is known on the exact values of $\mu(H)$ when G is a simple group; up to our knowledge, the only infinite families of non-abelian simple groups for which the Möbius function is completely known are the following.

- The groups $PSL(2,q)$; for q prime for any prime power q (where also the groups $PGL(2,q)$ are completely worked out. (Downs 1991, Hall 1936)

- The Suzuki groups $Sz(q)$ for any odd power q of 2 (Down, Jones, 2016);

- The Ree groups $Ree(q)$ for any odd power q of 3 (Pierro, 2016);

- The 3-dimensional unitary groups $PSU(3,2^{2^n})$, $n > 0$ (Zini 2018);

For any of these families Mann's conjecture is verified.

Theorem 3. *(Borello, D.V., Zini) The Möbius function is completely known in case* $G = PSL(3, 2^p)$, p *prime number.*

H	elements of the plane stabilized by H	$\mu(H)$
G	-	1
$(E_{q^2} \rtimes C_{q-1}) \,.\, PSL(2,q)$	an $\mathbb{F}_q$-rational point	-1
$(E_{q^2} \rtimes C_{q-1}) \,.\, PSL(2,q)$	an $\mathbb{F}_q$-rational line	-1
$(C_{q-1} \times C_{q-1}) \rtimes Sym(3)$	an $\mathbb{F}_q$-rational triangle	-1
$C_{q^2+q+1} \rtimes C_3$	an $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$-rational triangle	-1
$PSL(3,2)$	a subplane of order 2	-1
$(E_q \,.\, E_{q^2}) \rtimes (C_{q-1} \times C_{q-1})$	an $\mathbb{F}_q$-rat. point P and an $\mathbb{F}_q$-rat.ℓ, $P \in \ell$	1
$GL(2,q)$	an $\mathbb{F}_q$-rat. P and an $\mathbb{F}_q$-rat. ℓ, $P \notin \ell$	1
$E_q \rtimes (C_{q-1} \times C_{q-1})$	two $\mathbb{F}_q$-rat. points and two $\mathbb{F}_q$	-1
$(C_{q-1} \times C_{q-1}) \rtimes C_2$	an $\mathbb{F}_q$-rati. triangle and one of its vert.	1
$(C_2 \times C_2) \rtimes Sym(3)$	a subp. Π of order 2 and a point of Π	1
$(C_2 \times C_2) \rtimes Sym(3)$	a subp. Π of order 2 and a line of Π	1
$C_7 \rtimes C_3$	a subplane Π of order 2 and a triangle not in Π	1
$C_4 \rtimes C_2$	a subplane Π of order 2, a P and an ℓ, $P \in \ell$	$-\frac{q}{2}$

Strategy?

- Through geometric arguments, to find the subgroups which are intersection of maximal subgroups (MAXINT); then .... a lot of calculations.

- Considering the action of G on geometric objects, to find conjugacy classes.

Why only maxint?

Theorem 4. *If H is not intersection of maximal subgroups, then $\mu(H) = 0$*

Remark 5. *It should be nice to have result for $PSL(n, q)$ in general (at least in order to understand if the Lucchini-Mann conjecture is true). At the moment we were not able. The problem seems to be actually difficult. Going back to Shareshan work (2000), just some general bound for $\mu(1, G)$ is given for several classes of classical groups*

Möbius function and other combinatorial object

1. Euler characteristic for the simplicial complex associated with a finite poset $\mathcal{P}$: the Möbius function can be used to compute the reduced Euler characteristic $\tilde{\chi}(\Delta(\mathcal{P}))$ of the order complex $\Delta(\mathcal{P})$ of $\mathcal{P}$. We give computation when $\mathcal{P}$ is the poset L_r of r-subgroups of $PGL(3, q)$

2. finding the maximum number d such that the direct product of d copies of $PSL(3, 2^p)$ may be generated by 2 elements, but this is no more true for $(d + 1)$ copies

3. Connection with Cellular Automata

1. Euler characteristic

prime r	$\tilde{\chi}(\Delta(L_r))$	prime r	$\tilde{\chi}(\Delta(L_r))$
$r \nmid \lvert PGL(3,q)\rvert$	0	$r \mid (q-1),\ r \notin \{2,3\}$	$-\frac{q^2(q^2+q+1)(q^2+q-3)}{3}$
$r \mid q$	$-(q^3-1)$	$r=2 \mid (q-1)$	$-\frac{q^2(q^2+q+1)(q^2+q-3)}{3}$
$3 \neq r \mid (q^2+q+1)$	$\frac{q^3(q-1)^2(q+1)}{3}$	$r=3 \mid (q-1)$	$-\frac{q^2(q^6-q^4+7q^3-7q-8)}{8}$
$2 \neq r \mid (q+1)$	$\frac{q^3(q^3-1)}{2}$		

2. Let $d_k(G)$ be the number of normal subgroups N of the free group F_k of finite rank k such that $F_k/N \cong G$. Then

$$d_k = \frac{1}{|aut(G)|} \sum_{H \leq G} \mu(H)|H|^k,$$

(Downs Jones 2016, Hall 1935). For instance, for $G = PSL(3, 2^p)$

$$d_2(G) = \frac{q^4 + q^3 + q^2 + q + 2)(q + 2)(q - 1)^3 - 3(q^2 + q + 1) - 107}{2p}$$

3. **Some word about the last point:**

- G is a finite group, A is a finite set, $CA(G : A)$ is the monoid of all the Cellular Automata over A^G.

- $ICA(G : A)$ the group of invertible (units) Cellular automata

- $[H]$ is the conjugacy class of the subgroup H;

- $B_{[H]} = \{x \in A^G : [G_x] = [H]\}$, $B_{[H]}$ is an union of orbits for the action of G over A^G

Theorem 6. *A. Castillo-Ramirez and M. Gadouleau, Let G be a finite group of order $n \geq 2$ and A a finite set of size $q \geq 2$. If H is a subgroup of order m,*

$$\mid B_{[H]} \mid = \mid [H] \mid \sum_{K \leq G} \mu(H, K)$$

Structure of ICA(G:A)

Theorem 7. *If G is a finite group of order n and A a finite set of size $q \geq 2$, denote by $[H_1], \ldots, [H_r]$ the different conjugacy classes of subgroups of G. Then*

$$ICA(G : A) \simeq \Pi_{i=1,\ldots r}((\frac{N_G(H_i)}{H_i}) \wr Sym(\alpha_i)$$

where $\alpha_i = \alpha_{[H_i]}(G : A) = \mid \mathcal{O}, \mathcal{O} \in B_{[H]} \mid$

Thank You

bibliography

1. N. Boston, A probabilistic generalization of the Riemann zeta function, in ??Analytic Number Theory, Proceedings of a Conference in Honor of Heini Halberstam,?? Vol. 1, Progress in Mathematics, Vol. 138, Birkhauser, Boston, 1996

2. A. Castillo-Ramirez and M. Gadouleau, Cellular Automata and Finite Groups, *Nat. Comput.*, DOI 10.1007/s11047-017-9640-3.

3. V.Colombo and A.Lucchini, On subgroups with non-zero Möbius numbers in the alternating and symmetric groups, *J.Algebra* **324** (9) (2010), 2464–2474.

4. P. Hall, The Eulerian functions of a group, *Quart. J. Math.* **7** (1) (1936), 134–151.

5. T. Hawkes, M. Isaacs, and M. Özaydin, On the Möbius function of a finte group, *Rocky Mountain J. Math.* **19** (4) (1989), 1003–1034.

6. A. Mann, Positively finitely generated groups, *Forum Math.* **8** (4) (1996), 429–459.

7. A. Mann, A probabilistic zeta function for arithmetic groups, *Internat. J. Algebra Comput.* **15** (5–6) (2005), 1053–1059.

8. H. Pahlings, On the Möbius function of a finte group, *Arch. Math. (Basel)* **60** (1) (1993), 7–14.

9. Weisner L. Weisner, Abstract theory of inversion of finite series, *Trans. Amer. Math. Soc.* **38** (3) (1935), 474–484.