Enumeration of groups

(and quasigroups, semigroups, ...)

and quandles

1
10
3330
178981952
2483527537094825
14325590003318891522275680
50976900301814584087291487087214170039
155682086691137947272042502251643461917498835481022016

1
5
24
188
1915
28634
1627672
3684030417
105978177936292

1
1
3
7
22
73
298
1581
11079
102771
1275419
21101335
469250886

1
2
5
14
51
267
2328
56092
10494213
494873672891

1	1	1	2	1	2	1	5	2	2
1	5	1	2	1	14	1	5	1	5
2	2	1	15	2	2	5	4	1	4
1	51	1	2	1	14	1	2	2	14
1	6	1	4	2	2	1	52	2	5
1	5	1	15	2	13	2	2	1	13
1	2	4	267	1	4	1	5	1	4
1	50	1	2	3	4	1	6	1	52
15	2	1	15	1	2	1	12	1	10
1	4	2	2	1	231	1	5	2	16

David Stanovský

Charles University

Groups

(A000001)

10	1	1	1	2	1	2	1	5	2	2
20	1	5	1	2	1	14	1	5	1	5
30	2	2	1	15	2	2	5	4	1	4
40	1	51	1	2	1	14	1	2	2	14
50	1	6	1	4	2	2	1	52	2	5
60	1	5	1	15	2	13	2	2	1	13
70	1	2	4	267	1	4	1	5	1	4
80	1	50	1	2	3	4	1	6	1	52
90	15	2	1	15	1	2	1	12	1	10
100	1	4	2	2	1	231	1	5	2	16

Groupoids

(A001329)

1	1
2	10
3	3330
4	178981952
5	2483527537094825
6	14325590003318891522275680
7	50976900301814584087291487087214170039
8	155682086691137947272042502251643461917498835481022016

Quasigroups

(A057991)

1	1
2	1
3	5
4	35
5	1411
6	1130531
7	12198455835
8	2697818331680661
9	15224734061438247321497
10	2750892211809150446995735533513
11	19464657391668924966791023043937578299025

Semigroups

(A027851)

1	1
2	5
3	24
4	188
5	1915
6	28634
7	1627672
8	3684030417
9	105978177936292

Groupoids

(A001329)

1	1
2	10
3	3330
4	178981952
5	2483527537094825
6	14325590003318891522275680
7	50976900301814584087291487087214170039
8	155682086691137947272042502251643461917498835481022016

$$\# \leq n^{n^2}$$

$$\# \geq \frac{n^{n^2}}{n!} \geq n^{n^2-n}$$

Semigroups

(A027851)

1	1
2	5
3	24
4	188
5	1915
6	28634
7	1627672
8	3684030417
9	105978177936292

$$\boxed{\text{folklore(?): } \# \geq n^{(1-\varepsilon)n^2}}$$

	$1 \ldots m$	$m+1 \ldots n$
$1 \ldots m$	1	1
$m+1 \ldots n$	1	$\leq m$

Quasigroups

(A057991)

1	1
2	1
3	5
4	35
5	1411
6	1130531
7	12198455835
8	2697818331680661
9	15224734061438247321497
10	2750892211809150446995735533513
11	19464657391668924966791023043937578299025

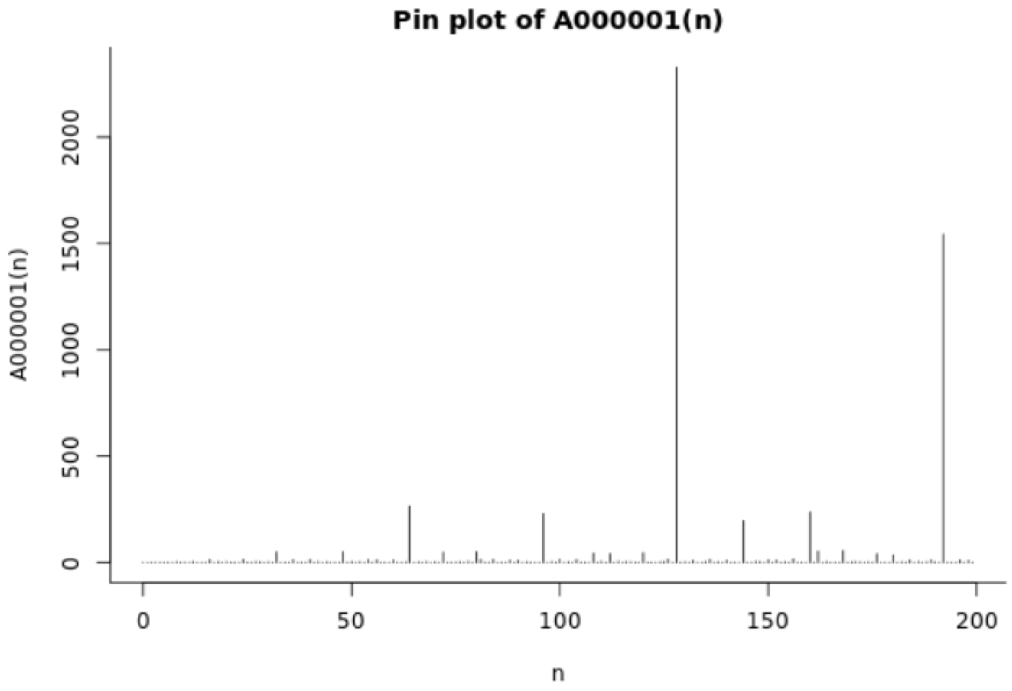
[Marshall Hall 1948]

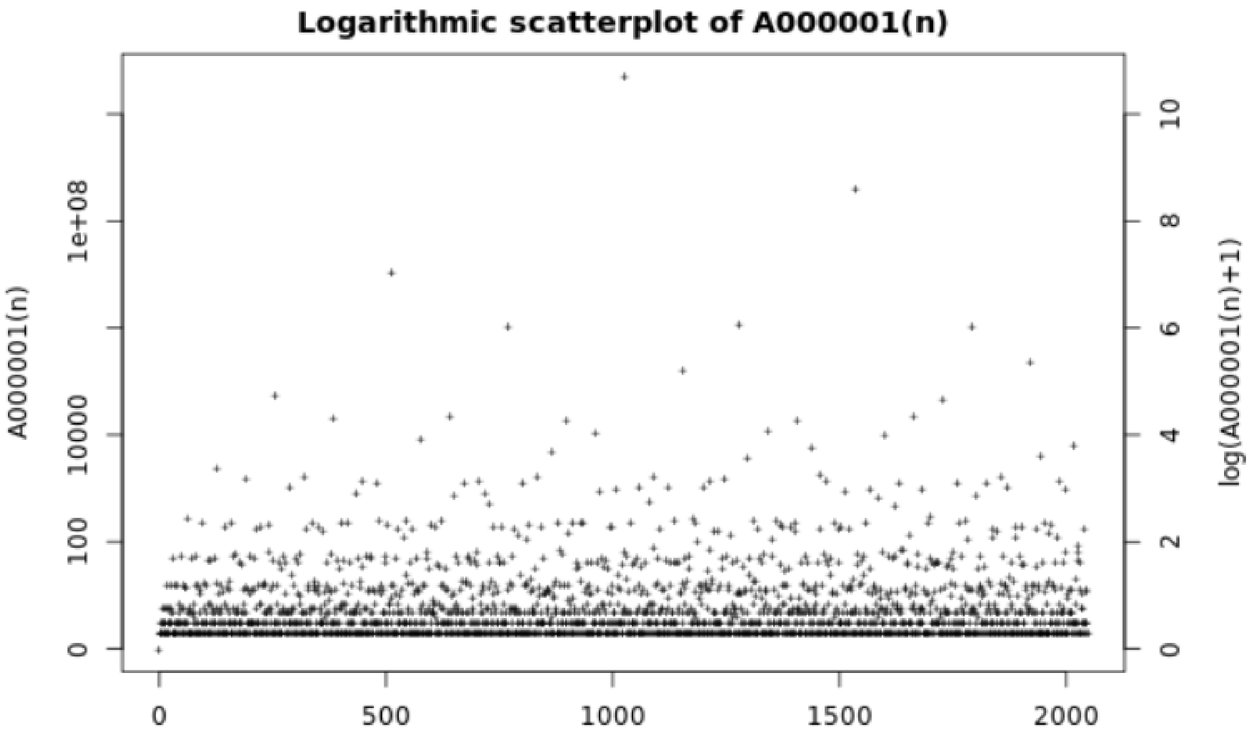
$$\# \geq n^{\frac{1}{2}n^2 - O(n)}$$

Groups

(A000001)

10	1	1	1	2	1	2	1	5	2	2
20	1	5	1	2	1	14	1	5	1	5
30	2	2	1	15	2	2	5	4	1	4
40	1	51	1	2	1	14	1	2	2	14
50	1	6	1	4	2	2	1	52	2	5
60	1	5	1	15	2	13	2	2	1	13
70	1	2	4	267	1	4	1	5	1	4
80	1	50	1	2	3	4	1	6	1	52
90	15	2	1	15	1	2	1	12	1	10
100	1	4	2	2	1	231	1	5	2	16
	1	4	1	14	2	2	1	45	1	6
	2	43	1	6	1	5	4	2	1	47
128	2	2	1	4	5	16	1	2328	2	4
	1	10	1	2	5	15	1	4	1	11
	1	2	1	197	1	2	6	5	1	13
	1	12	2	4	2	18	1	2	1	238
	1	55	1	5	2	2	1	57	2	4
	5	4	1	4	2	42	1	2	1	37
	1	4	2	12	1	6	1	4	13	4
200	1	1543	1	2	2	12	1	10	1	52
	2	2	2	12	2	2	2	51	1	12
	1	5	1	2	1	177	1	2	2	15
	1	6	1	197	6	2	1	15	1	4
	2	14	1	16	1	4	2	4	1	208
	1	5	67	5	2	4	1	12	1	15
256	1	46	2	2	1	56092	1	6	1	15
	2	2	1	39	1	4	1	4	1	30
	1	54	5	2	4	10	1	2	4	40
	1	4	1	4	2	4	1	1045	2	4
300	2	5	1	23	1	14	5	2	1	49


Pin plot of A000001(n)
A000001(n)
0
500
1000
1500
2000
0
50
100
150
200
n


Logarithmic scatterplot of A000001(n)
A000001(n)
0
100
10000
1e+08
log(A000001(n)+1)
0
2
4
6
8
10
0
500
1000
1500
2000

Groups of order 2^n

(A000679)

1	1
2	2
3	5
4	14
5	51
6	267
7	2328
8	56092
9	10494213
10	49487367289

Groups of order 2^n, $\log_2$ scale

($\log_2$ A000679)

1	0.0
2	1.0
3	2.3
4	3.8
5	5.7
6	8.1
7	11.2
8	15.8
9	23.3
10	38.8

p-groups: order $n = p^k$

[Graham Higman 1960]

- quasipolynomial: $\# \sim 2^{c(logn)^3}$
- $\# \geq p^{\frac{2}{27}k^2(k-6)}$

  by constructing many factors of the form $FG_r/\langle x^{p^2}, [x,y]^p, [[x,y],z]\rangle$
- $\# \leq p^{\frac{1}{6}k(k^2-1)}$

  by counting polycyclic presentations (based on subnormal series with cyclic factors)

[Charles Sims 1965]

- $c = \frac{2}{27}$
- $\# \leq p^{\frac{2}{27}k^3+o(k^3)}$ $(\sim \frac{1}{4}$ of the book$)$

general groups: order $n = \prod p_i^{k_i}$, denote $K = \max k_i$

[László Pyber 1993]

- $\# \leq n^{(\frac{2}{27}+o(1))K^2}$ $(\sim \frac{1}{2}$ of the book$)$

The book: [Blackburn, Neumann, Venkataraman: Enumeration of finite groups].

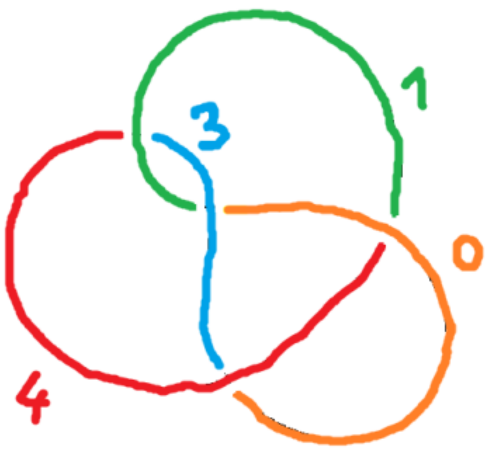
Quandles

A binary algebra $(Q, *)$ is called a *quandle* if

- $x * x = x$
- all left translations $L_x(y) = x * y$ are automorphisms.

Motivation:

- algebra (group conjugation, affine forms), geometry (symmetric spaces), math physics (discrete solutions to the Yang-Baxter equation), ...
- coloring invariants of knots:



by $(\mathbb{Z}_5, 2x - y)$.

From groups to quandles (examples)

A binary algebra $(Q, *)$ is called a *quandle* if

- $x * x = x$
- all left translations $L_x(y) = x * y$ are automorphisms.

Affine quandles: A abelian group, $f \in \mathrm{Aut}(A)$ $\rightsquigarrow$ $\mathrm{Aff}(A, f) = (A, *)$

$$x * y = (1 - f)(x) + f(y)$$

Conjugation quandles: G group $\rightsquigarrow$ $\mathrm{Cjg}(G) = (G, *)$ with

$$x * y = xyx^{-1}$$

From quandles to permutation groups

A binary algebra $(Q, *)$ is called a *quandle* if

- $x * x = x$
- all left translations $L_x(y) = x * y$ are automorphisms.

(left) multiplication group: $\mathrm{LMlt}(Q) = \langle L_x : x \in Q \rangle \trianglelefteq \mathrm{Aut}(Q)$

(left) displacement group: $\mathrm{Dis}(Q) = \langle L_x L_y^{-1} : x, y \in Q \rangle \trianglelefteq \mathrm{LMlt}(Q)$

A quandle Q is called *connected* if $\mathrm{LMlt}(Q)$ acts transitively.

Quandles

(A181769)

1	1
2	1
3	3
4	7
5	22
6	73
7	298
8	1581
9	11079
10	102771
11	1275419
12	21101335
13	469250886

Quandles

(A181769)

1	1
2	1
3	3
4	7
5	22
6	73
7	298
8	1581
9	11079
10	102771
11	1275419
12	21101335
13	469250886

[Blackburn 2013]

$\# \leq 2^{1.56n^2+o(n^2)}$

$\# \geq 2^{\frac{1}{4}n^2-o(n^2)}$

[Ashford, Riordan 2017]

$\# \leq 2^{\frac{1}{4}n^2+o(n^2)}$

semigroups, quasigroups >> # quandles >> # groups

Connected quandles

(A181771)

10	1	0	1	1	3	2	5	3	8	1
20	9	10	11	0	7	9	15	12	17	10
30	9	0	21	42	34	0	65	13	27	24
40	29	17	11	0	15	73	35	0	13	33
50	39	26	41	9	45	0	45			

Quasigroup quandles

(A177886)

10	1	0	1	1	3	0	5	2	8	0
20	9	1	11	0	5	9	15	0	17	3
30	7	0	21	2	34	0	62	7	27	0
40	29	8	11	0	15	9	35	0	13	6
50	39	0	41	9	36	0	45			

1	0	1	1	3	2	5	3	8	1
9	10	11	0	7	9	15	12	17	10
9	0	21	42	34	0	65	13	27	24
29	17	11	0	15	73	35	0	13	33
39	26	41	9	45	0	45			

Connected and quasigroup quandles

10 20 30 40 50

1	0	1	1	3	2	5	3	8	1
9	10	11	0	7	9	15	12	17	10
9	0	21	42	34	0	65	13	27	24
29	17	11	0	15	73	35	0	13	33
39	26	41	9	45	0	45			

1	0	1	1	3	0	5	2	8	0
9	1	11	0	5	9	15	0	17	3
7	0	21	2	34	0	62	7	27	0
29	8	11	0	15	9	35	0	13	6
39	0	41	9	36	0	45			

[Etingof, Soloviev, Guralnik 2001]
(# of order p) $= p - 2$

[McCarron / Hulpke, Vojtěchovský, S. 2016]
(# of size $2p$) $= 0$, except 6, 10

[ESG / Graña / Nagy]
order p, $p^2 \Rightarrow$ affine
quasigroup of order 2^k where $k < 6$ or $k = 7 \Rightarrow$ affine

Joyce-Blackburn representation

[Vojtěchovský, Yang 2019]

Let G be a permutation group on a set X. There is a 1-1 correspondence between

- *quandles on X with $\mathrm{LMlt}(Q) = G$*
- *quandle envelopes over G*, i.e., tuples $(\rho_x : x \in X/G)$ such that $\rho_x \in Z(G_x)$ and $\langle \bigcup \rho_x^G \rangle = G$

Isomorphism theorem: $G \leq S_X$ up to conjugacy, ρ_x up to .....

Joyce-Blackburn representation

[Vojtěchovský, Yang 2019]

Let G be a permutation group on a set X. There is a 1-1 correspondence between

- *quandles on X with* $\mathrm{LMlt}(Q) = G$
- *quandle envelopes over G*, i.e., tuples $(\rho_x : x \in X/G)$ such that $\rho_x \in Z(G_x)$ and $\langle \bigcup \rho_x^G \rangle = G$

Isomorphism theorem: $G \leq S_X$ up to conjugacy, ρ_x up to .....

It defines a group action on envelopes, but it is difficult to handle. Hence,

- imprecise handling $\rightsquigarrow$ asymptotic upper bounds [Blackburn] [AR]
- computer calculations with subgroups of S_n $\rightsquigarrow$ enumeration up to 12
- computer calculations with *transitive* subgroups of S_n $\rightsquigarrow$ enumeration of *connected* quandles up to 47
- theory of transitive groups $\rightsquigarrow$ theorems [ESG] [G] [Nagy] [HSV] ...
- separate handling of special cases $\rightsquigarrow$ enumeration for 13 and more

	quandles	2-reductive medial quandles	difference	
1	1	1	0	
2	1	1	0	
3	3	2	1	
4	7	5	2	
5	22	15	7	
6	73	55	18	
7	298	246	52	
8	1581	1398	183	
9	11079	10301	778	
10	102771	98532	4239	4.12%
11	1275419	1246479	28940	2.23%
12	21101335	20837171	264164	1.25%
13	469250886	466087624	3163262	0.67%
14		13943041873		
15		563753074915		
16		30784745506212		

Reductive quandles

[Jedlička, Pilitowska, S., Zamojska-Dzienio 2015] [Bonatto, S. 2025]

A quandle is called *n-reductive* if composition of any n right translations is a constant mapping, i.e., $R_{x_1} \circ \ldots \circ R_{x_n} = c$.

In particular, *2-reductive* means $(yx_1)x_2 = (zx_1)x_2$.

Theorem. [BS]

A quandle is n-reductive if and only if it is strongly solvable of length $\leq n$.

Reductive quandles

[Jedlička, Pilitowska, S., Zamojska-Dzienio 2015] [Bonatto, S. 2025]

A quandle is called *n-reductive* if composition of any n right translations is a constant mapping, i.e., $R_{x_1} \circ \ldots \circ R_{x_n} = c$.

In particular, *2-reductive* means $(yx_1)x_2 = (zx_1)x_2$.

Theorem. [BS]
A quandle is n-reductive if and only if it is strongly solvable of length $\leq n$.

Enumeration of medial 2-reductive quandles [JPSZ]:

- representing medial quandles as disjoint union of affine quandles
- leads to a manageable isomorphism theorem
- in the 2-reductive case, Burnside's orbit counting can be used

Conjecture. There are 'very few' non-reductive quandles.

Question. Is strong solvability related to explosion in the number of models, in some general sense?