Enumeration of Schur rings over small groups

Matan Ziv-Av

Ben Gurion University of the Negev

ATCAGC 2014

Schur rings

Definition

A Schur ring (briefly, S-ring) over a group G is a subring $\mathcal{A}$ of the group ring $\mathbb{C}[G]$ such that exists a partition s of G satisfying:

1. $\underline{s}$ is a basis of $\mathcal{A}$ (as a vector space over $\mathbb{C}$).
2. $\{e\} \in s$.
3. $X^{-1} \in s$ for all $X \in s$.

For $X \subseteq G$, $X^{-1} = \{x^{-1} | x \in X\}$ and $\underline{X} = \sum_{x \in X} x$ is an element of $\mathbb{C}[G]$.

For t a set of subsets of G, $\underline{t} = \{\underline{X} | X \in t\}$.

Proposition

A subring with unity $\mathcal{A}$ of $\mathbb{C}[G]$ is a Schur ring if it is closed under componentwise multiplication and componentwise inverse.

Association schemes I

Definition

An association scheme is a pair $\mathfrak{M} = (\Omega, R)$, where R is a partition of Ω^2, $R = \{R_0, \dots, R_d\}$, such that

AS1 $\forall i \in [0, d] \exists i' \in [0, d] R_i^{-1} = R_{i'}$

AS2 $\Delta \in R$

AS3 $\forall i, j, k \in [0, d] \forall (x, y) \in R_k$
$|\{z \in \Omega | (x, z) \in R_i \wedge (z, y) \in R_j\}| = p_{ij}^k$

Here $\Delta = \{(a, a) | a \in \Omega\}$ is the diagonal (or complete reflexive) relation.
For a relation R, $R^{-1} = \{(y, x) | (x, y) \in R\}$.
Usually we denote $R_0 = \Delta$.
The rank of the scheme is $d + 1$, the number of basic relations.

Association schemes II

- The R_i's are called basic relations of $\mathfrak{M}$.
- The graphs $\Gamma_i = (\Omega, R_i)$ are called basic graphs of $\mathfrak{M}$.
- Their adjacency matrices A_i form the first standard basis of the corresponding coherent algebra.
- An association scheme $\mathfrak{N}$ with basic relations $S_0, \dots, S_t$ is a merging of $\mathfrak{M}$ if each S_i is a union of basic relations of $\mathfrak{M}$.
- A special case of merging: algebraic merging.
- More details about kinds of automorphisms and mergings can be found in "Association schemes on 28 points..." by Klin et al.

Association schemes III

Example

If G is a transitive permutation group acting on set Ω, then $(\Omega, 2 - orb(G))$ is an association scheme.

- For a permutation group G acting on Ω, $2 - orb(G)$ is the set of orbits of G in its induced action on $\Omega \times \Omega$.
- These orbits are called 2-orbits (or orbitals).
- Such a scheme is called Schurian.
- There are also non-Schurian association schemes (the smallest example is on 15 points).

Connection between Schur rings and association schemes

- An association scheme is called thin if all of its basic graphs are of valency 1.
- Generic example: $(\Omega, 2 - orb(G))$ for a regular permutation group G acting on Ω.
- There is a correspondence between Schur rings over G and mergings of the thin association scheme $(G, 2 - orb(G))$ (where we take a regular action of G upon itself).
- This correspondence allows us to use tools that enumerate merging of association schemes for the enumeration of Schur rings.

Known results

- Hanaki and Miyamoto classified association schemes with small number of vertices.
- The smallest number of vertices without full classification is 35.
- Available at `http://math.shinshu-u.ac.jp/~hanaki/as/`.
- This includes all S-rings.
- S. Reichard and C. Pech announced classification of all Schur rings for groups of order up to 47.

Theoretical and Computational results

- All S-rings over a cyclic group of prime order were explicitly listed (Klin, Pöchel).
- All those S-rings are Schurian, so all cyclic groups of prime order are Schur groups.
- A recent result: a cyclic group is a Schur group if and only if its order is one of p^k, pq^k, $2qp^k$, pqr, $2pqr$ for distinct primes p, q, r (Evdokimov, Kovács, Ponomarenko).
- For non-cyclic abelian groups: If such a group is Schur, it is in one of nine families (Evdokimov, Kovács, Ponomarenko).
- Some results for non abelian groups:
  - For $p \geq 5$, a p-group is Schur if and only if it is cyclic (Pöschel).
  - A_5 and $AGL_1(8)$ are not Schur Group (Klin, Z).

New results

- Enumeration of S-rings over groups of order up to 63.
- Calculation for groups of order 63 in a few weeks.
- Calculation for groups of order 64 requires different methods.
- In the results we consider S-rings up to isomorphism of association schemes.
- This means that two S-rings over different groups (of the same order) may be isomorphic.

Number of S-rings for each order

Ord	#	non Schurian
3	2	0
4	4	0
5	3	0
6	8	0
7	4	0
8	21	0
9	12	0
10	11	0
11	4	0
12	58	0
13	6	0

Ord	#	non Schurian
14	16	0
15	21	0
16	204	9
17	5	0
18	91	1
19	6	0
20	83	0
21	32	0
22	16	0
23	4	0
24	654	23

Ord	#	non Schurian
25	36	4
26	22	0
27	123	1
28	111	0
29	6	0
30	185	0
31	8	0
32	4212	553
33	27	0
34	17	0
35	41	0

Number of S-rings for each order

Ord	#	non Schurian
36	1259	73
37	9	0
38	23	1
39	44	0
40	936	31
41	8	0
42	293	3
43	8	0
44	107	0

Ord	#	non Schurian
45	245	0
46	16	1
47	4	0
48	16426	3309
49	93	35
50	237	27
51	35	0
52	169	2
53	6	0

Ord	#	non Schurian
54	2020	276
55	48	0
56	1271	46
57	43	1
58	21	0
59	4	0
60	2780	47
61	12	0
62	32	1

Number of Schur groups

Ord	nA+nS	nA+S	A+nS	A+S
16	7	2	2	3
18	2	1	0	2
24	11	1	0	3
25	0	0	1	1
27	2	0	0	3
32	1	43	4	3
36	1	9	1	3
38	1	0	0	1
40	10	1	0	3
42	5	0	0	1

Ord	nA+nS	nA+S	A+nS	A+S
46	1	0	0	1
48	47	0	3	2
49	0	0	1	1
50	2	1	1	1
52	2	1	0	2
54	11	1	0	3
56	10	0	0	3
57	1	0	0	1
60	9	2	0	2
62	1	0	0	1

- Groups are counted according to Schurity and abelianess.
- Only for orders where non-Schurian S-rings exist are listed.

Weisfeiler-Leman algorithm

- Given a partition t of G there is a partition s that is finer than t such that s defines an S-ring over G and s is the coarsest of all such partitions.
- s is called (coherent) closure of t.
- The WL algorithm is an algorithm for calculating s given t.
- It works by repeatedly calculating $\underline{x} \cdot \underline{y}$ for cells of t and splitting cells as necessary, until all those products split no more cells.
- The runtime is polynomial (in $|G|$).

Algorithm for enumeration of S-rings

- A simple algorithm:
  - Start with S-ring of rank 2.
  - For each basic set (of size more than 1), split it into two cells in every possible way and calculate the closure of each such partition.
  - Repeat previous step for each new S-ring found.
- The above algorithm cannot be used for groups of orders above 40.
- For example for the group of order 61, the initial partition is into cells of sizes 1 and 60.
- There are 2^{59} ways to split the cell of size 60 into two.

Main optimization of the algorithm - good sets

- First appearance in computer package COCO (Faradžev, Klin).
- Only run first step of the algorithm: a set X can be a basic set of an S-ring only if $\underline{X} \cdot \underline{X}$ does not split X.
- Not every set is a candidate for a good set. Only symmetric sets ($X^{-1} = X$) and antisymmetric sets ($X \cap X^{-1} = \emptyset$).
- For a group G with l elements of order 2 and k elements of order larger than 2, the number of symmetric candidates is $2^{l+\frac{k}{2}}$. The number of antisymmetric candidates is $3^{\frac{k}{2}}$.
- Once a set passes the first step we can run the complete WL algorithm for it, and see if it is really a basic set of some S-ring.
- When splitting a cell in the algorithm for enumeration, we only need to split into sets which can be basic sets.

Some examples of the numbers involved

- For the group A_5:
  - There are $2^{59} \simeq 10^{18}$ sets.
  - $l = 15$, $k = 44$, so there are $2^{37} + 3^{22} \simeq 10^{11}$ candidates for good sets.
  - Of those, only 4410 are basic sets.
- For the group Z_{60}:
  - There are $2^{59} \simeq 10^{18}$ sets.
  - $l = 1$, $k = 58$, so there are $2^{30} + 3^{29} \simeq 10^{14}$ candidates.
  - Of those only 3770 are basic sets.
- For the non-abelian group of order 55:
  - There are $2^{54} \simeq 10^{16}$ sets.
  - $l = 0$, $k = 54$, so there are $2^{27} + 3^{27} \simeq 10^{13}$ candidates.
  - Of those, only 2906 are good sets.

More examples of the numbers involved

- In fact, the group with the largest number of basic sets (among groups of order ≤ 62) is E_{2^5} of order 32. It has 638664 basic sets, and the enumeration of S-rings runs for a about a week.
- One group of order 54 has 195727 basic sets.
- All other groups (of orders up to 62) have small number of basic sets, and the enumeration is quite quick.
- The group with the largest number of S-rings (of groups of order up to 62) is $G = D_8 \times S_3$ of order 48. There are 13433 S-rings over G, up to isomorphism.

Available tools

- COCO
  - Written by Faradžev, Klin using computer language C for DOS, ported to UNIX by A. Brouwer.
  - Monolithic - searches for good sets and runs the enumeration with the results. Does not save intermediate results.
  - Written with a very small system in mind, so has very strict limits on number of good sets.
  - Hard to change those limits.
- COCO-II
  - A GAP package written by C. Pech and S. Reichard.
  - Another optimization - looks for good sets up to action of $Aut(G)$.
  - The search for good sets and the enumeration using those sets can be easily separated.
  - GAP is an interpreter, and is really slow in running the WL algorithm.

New tool

- Search for good sets and basic sets.
  - Written in C.
  - The search space can be arbitrarily divided among different threads/processes.
  - Dynamic programming: if X and Y differ by one element, calculating $\underline{Y} \cdot \underline{Y}$ is much faster if we know $\underline{X} \cdot \underline{X}$.
  - Pre-calculating products of the form $x(y+z)$.
- Enumerating S-rings.
  - Written in GAP.
  - Calculating up to $Aut(G)$.
  - Caching results of calculations of the form $\underline{X} \cdot \underline{Y}$ as well as results of WL algorithm.

Comparison of performance

- E_{2^4}:
  - COCO finds 3126 good sets immediately takes ??? minutes to enumerate all S-rings.
  - COCO-II takes about 6 seconds.
  - New tool takes about one second.
- A_5:
  - COCO cannot complete task.
  - COCO-II takes about 1 month.
  - New tool: about 20 hours CPU time split across 11 CPUS with a total of 30 cores takes about 1 hour (wall time).
- Non-abelian group of order 55:
  - COCO cannot complete task.
  - COCO-II takes about 4 years (extrapolation).
  - New tool: About 300 CPU hours, 10 hours on 30 CPU cores.

References

Bannai, E.; Ito, T. Algebraic combinatorics. I. Association schemes. The Benjamin/Cummings Publishing Co., Inc., Menlo Park, CA, 1984.

Evdokimov S.; Kovács I.; Ponomarenko I. On schurity of finite abelian groups. arXiv:1309.0989.

http://www.gap-system.org

http://math.shinshu-u.ac.jp/~hanaki/as/

Klin, M.; Muzychuk, M.; Pech, C.; Woldar, A.; Zieschang, P.-H. Association schemes on 28 points as mergings of a half-homogeneous coherent configuration. European J. Combin. 28, 2007, 1994-2025.

Klin, M.; Ziv-Av M. Enumeration of Schur Rings over the Group A_5 In: V.P. Gerdt et al. (Eds.): CASC 2013, LNCS 8136, pp. 219–230, 2013. http://link.springer.com/content/pdf/10.1007/978-3-319-02297-0_19.pdf

Pech, C.; Reichard, S. Enumerating Set Orbits In: M. Klin et al, Algorithmic Algebraic Combinatorics and Gröbner Bases (Springer-Verlag Berlin Heidelberg, 2009) pp. 31–65.

Wielandt, H. Finite permutation groups (Translated from the German by R. Bercov). Academic Press, New York, 1964.