S-Rings over the elementary abelian group of order 64

Sven Reichard

August 26, 2016

Outline

Preliminaries

Previously on G2S2

- Cayley objects, Cayley isomorphisms (Dobson)
- Group ring $\mathbb{C}[H]$, regular representation (Betten)
- Association schemes, adjacency algebra (Ponomarenko et al.)
- P-polynomial schemes and distance regular graphs (Ito)
- Coherent graphs (Ziv-Av)

The group ring

- Let G be a finite group.
- Let $\mathbb{C}[H]$ be the set of formal sums over H.
- Then $\mathbb{C}[H]$ forms a ring.

More formally

$\mathbb{C}[H]$ is the set of functions $\varphi : H \to \mathbb{C}$, together with the operations

- $(\varphi + \rho)(x) = \varphi(x) + \rho(x)$;
- $(\varphi \cdot \rho)(x) = \sum_{y \in H} \varphi(y)\rho(y^{-1}x)$ (convolution)
- $(\varphi \circ \rho)(x) = \varphi(x)\rho(x)$ (pointwise product)

for $\varphi, \rho \in \mathbb{C}[H]$, $x \in H$.
We also define $\varphi^{-1}(x) := \varphi(x^{-1})$

- For $x \in H$ we define $\underline{x} : H \to \mathbb{C}$ as

$$\underline{x}(y) = \delta_{x,y}.$$

- Then every $\phi \in \mathbb{C}[H]$ can be represented as

$$\phi = \sum_{x \in H} \phi(x)\underline{x}.$$

- For $x, y \in H$ we have

$$\underline{x} \cdot \underline{y} = \underline{x \cdot y}$$

- Hence we get an embedding of H into $\mathbb{C}[H]$.
- Therefore every ϕ can be considered a formal sum over H.

Simple quantities

- We extend this notation to subsets of H:
- For $S \subseteq H$ we let
$$\underline{S} = \sum_{x \in S} \underline{x}.$$
- So $\underline{S}$ is the characteristic function of S in H.
- We also write $S^{-1} := \left\{ s^{-1} \middle| s \in S \right\}$.

Definition of S-rings

A $\mathbb{C}$-submodule of $\mathbb{C}[H]$ is an S-ring if it closed under convolution, pointwise multiplication, and inversion, and contains the neutral elements $\underline{1}$ and $\underline{H}$.
For each S-ring $\mathcal{A}$ there is a unique partition

$$\mathcal{S} = \{S_0, S_1, \ldots, S_{d-1}\}$$

of H such that that

$$\mathcal{A} = \left\langle \underline{S_0}, \ldots, \underline{S_{d-1}} \right\rangle.$$

We call this the standard basis of $\mathcal{A}$. Any set appearing in such a basis is called *coherent* (cf. Ziv-Av).

Example

- Let $H = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.
- Then $\underline{0}, \underline{3}, \underline{\{1, 5\}}, \underline{\{2, 4\}}$ generate an S-ring over H.
- For example,

$$\underline{\{1, 5\}} \cdot \underline{\{2, 4\}} = \underline{\{1, 5\}} + 2 \cdot \underline{3}.$$

Correspondence of schemes and S-rings

- A partition of H generates an S-ring if and only if the corresponding Cayley relations $Cay(H, S_i)$ form an association scheme.
- This scheme is invariant under the left-regular action of H.
- Vice versa, a scheme W which admits a regular group of automorphisms is a Cayley scheme (by Sabidussi) and hence yields an S-ring $\mathcal{A}$.
- The adjacency algebra of W is just the regular representation of $\mathcal{A}$.

The isomorphism problem

- As was mentioned, it is desirable to classify S-rings over a given group H.
- This helps in solving the isomorphism problem of Cayley objects over H.
- There are standard catalogs of small abstract groups (up to isomorphism).
- Program: Enumerate S-rings over small groups.

Previous work

There have been three serious attempts to classify S-rings over all small groups.

- Fiedler (2003) $n \leq 31$.
- Pech, R (2007) $n \leq 47$.
- Ziv-Av (2013) $n \leq 63$.

- Why these numbers?
- For orders 32, 48, 64 there exist groups with many involutions and many automorphisms
- These are the elementary abelian groups E_{32} and E_{64}, as well as $3 \times E_{16}$.
- They are particularly difficult for current approaches.
- Ziv-Av stated: "For the groups of order 64 (especially for E_{64}) an innovative approach is necessary, as the current algorithms cannot finish the calculations in a reasonable time."
- This is the goal.

Algorithm outline

- All attempts so far used a similar general strategy:
- Any S-ring can be described by a partition of the group H.
- Determine all subsets of H which can appear as a simple quantity. (Coherent sets).
- Search for partitions of H consisting of coherent sets.
- Known symmetries were used to varying degrees.

Algorithm and results

- In the previous approaches all coherent sets needed to be kept in memory at some point.
- This is not feasible for $H = E_{64}$ since the total number is too big. (1,104,838,608,132)
- So an intermediate step was introduced.

Algorithm

- Enumerate all coherent sets, up to isomorphism.
- For each simple quantity, enumerate all compatible simple quantities.
- Extend each pair to independent generating sets.
- From each generating set construct an S-ring.
- Classify the S-rings up to isomorphism.

Enumerating simple quantities

- We need to consider all subsets of $H \setminus \{e\}$.
- We can use symmetries in $Aut(H) = \mathrm{GL}(6, 2)$.
- Use "orderly generation", canonicity test for subsets (Pech, R).

- For a coherent set S we have the condition that

$$|(\underline{S})^2(S)| = 1$$

- The product $(\underline{S})^2$ can be computed incrementally.
- Adding an element to S increases each value of $(\underline{S})^2$ by at most 2; this allows to prune the search.
- In the group ring we can compute products more efficiently than in general schemes.
- The search took around one week and found exactly 100 inequivalent coherent sets.

Enumerating pairs

- Given a simple quantity S we can find the smallest S-ring containing S. (Weisfeiler-Leman)
- Any set compatible with S has to be a subset of a basis element of that ring.
- A variation of the previous program was used.
- We only consider sets not exceeding S in size.
- 1242 pairs were found in 3 hours.

Enumerating bases

- From the compatible pairs we can construct all sets compatible with a given set.
- Among these we construct independent generating sets.
- Altogether we get approximately 400,000 such sets.
- Time taken: 9 hours.

Isomorphic rejection

- From each generating set we obtain an S-ring.
- We test the corresponding schemes for isomorphisms.
- Note: Schemes may be isomorphic even if S-rings are not (Cayley-) isomorphic.

Results

- There are 2082 S-rings over E_{64}, up to scheme isomorphism.
- 47 are primitive.
- 274 are non-schurian.
- 31 are both primitive and non-schurian.
- There are 10 non-schurian strongly regular graphs, with valencies 21, 27 and 28.

Correctness

- This is a reasonably large search using involved algorithms.
- There is a certain probability for error.
- "Lam principle": Ideally the results should be independently duplicated.
- However, we performed some plausibility checks.

Plausibility 1: Coherent sets

- The solutions consists of partitions of H.
- In the first step we enumerated all possible parts of size less than $|H|/2$.
- Each small class of a solution partition is isomorphic to one of these original sets.

Plausibility 2: Duality

- The group H is abelian.
- Hence all irreducible characters of H are linear.
- They form a group $\widehat{H} \cong H$.
- The characters can be extended to functions

$$\chi : \mathbb{C}[H] \to \mathbb{C}$$

Plausibility 2: Duality

- Given an S-ring $\mathcal{A} \subseteq \mathbb{C}[H]$ we define an equivalence relation on $\widehat{H}$:
- $\chi \sim \xi$ if $\chi|_{\mathcal{A}} = \xi|_{\mathcal{A}}$.
- Let Σ_i be the equivalence classes.
- Theorem: The $\underline{\Sigma_i}$ generate an S-ring $\widehat{\mathcal{A}}$ over $\widehat{H}$.

Plausibility 2: Duality

- The ranks of $\mathcal{A}$ and $\widehat{\mathcal{A}}$ coincide.
- $\widehat{\widehat{\mathcal{A}}} \cong \mathcal{A}$.
- The isomorphism $H \cong \widehat{H}$ gives us an S-ring over H isomorphic to $\widehat{\mathcal{A}}$.
- Hence the set of isomorphism classes of S-rings is closed under duality.

Results

- There are several known constructions of S-rings of order 64.
- Subschemes of Hamming and cyclotomic schemes.
- Constructions from "smaller" S-rings:
  - Semidirect products (Hirasaka)
  - Wedge (or generalized wreath) product (Muzychuk)
  - Exponentiation, primitive wreath product (Evdokimov-Ponomarenko)
- These can explain around 600 of the S-rings.

The Hamming scheme

- The n-dimensional cube Q_n is distance regular.
- The corresponding scheme is the Hamming scheme.
- It is invariant under the group of translations, which is a regular representation of E_{2^n}.
- Hence it can be considered as an S-ring.

The Hamming scheme

- The subschemes of the Hamming schemes were classified by Muzychuk (1985).
- In the case of $n = 6$ we get nine proper subschemes. All of them are schurian.
- Of those, three are primitive.
- Two strongly regular graphs of valencies 27 and 28.
- One distance regular graph of valency 21 and diameter 4.

Cyclotomic schemes

- Let F be a finite field. Let H be a subgroup of F^*, and let G be generated by H and $(F, +)$.
- The action of G on F yields a scheme and an S-ring over $(F, +)$.
- For $F = GF(64)$ we get schemes of rank $1 + k$, where $k|63$.

Outlook

- Understand the structure of the S-rings.
- Duplicate Ziv-Av's results on 48-63 vertices.
- Consider other groups of order 64.

Thank you!