MULTIVALUED GROUPS AND SCHUR RINGS

A. V. VASIL'EV AND I. N. PONOMARENKO

Abstract. We study finite involutive multivalued groups associated with Schur rings. Their reduced valency is shown to equal the least common multiple of the sizes of the basic sets of the corresponding ring. We prove that the double-coset group associated with a complemented subgroup of a finite group is isomorphic to a Schur multivalued group over the complement. In particular, every coset multivalued group is a Schur multivalued group. Using affine Schur rings, we construct families of pairwise nonisomorphic commutative multivalued groups over elementary abelian groups. We obtain asymptotic bounds for the sizes of these families and prove that the proportion of double-coset groups in them tends to zero.

Keywords: multivalued group, Schur ring, coset group, double-coset group, permutation group.

1. Introduction

The theory of multivalued groups goes back to a construction of Buchstaber and Novikov [4]; a survey of its main results and applications is given in [1]. Natural examples of multivalued groups arise in topology [2], algebra and dynamics [3, 6], and algebraic combinatorics [7,19]. Two important sources of examples are the coset and double-coset constructions. In the former, a finite group acts by automorphisms on another finite group, and the elements of the resulting multivalued group are the orbits of this action. In the latter, the elements of the multivalued group are the double cosets of a subgroup of a finite group. We denote the classes of coset and double-coset multivalued groups by $\mathfrak{K}_{coset}$ and $\mathfrak{K}_{bicoset}$, respectively.

In this note, we study multivalued groups arising from Schur rings. This construction is part of the general theory of combinatorial algebras [5]; here we clarify its relationship with double-coset groups and construct a family in which the proportion of double-coset groups tends to zero. A Schur ring over a finite group G can be defined as a subspace $\mathcal{A}$ of the group algebra $\mathbb{C}G$, that contains the identities 1_G and $\sum_{g\in G} g$ for ordinary and componentwise multiplications, respectively, and is closed under both multiplications and the linear extension of the map $g \mapsto g^{-1}$. A definition in terms of a partition of the group is given in Section 3.

Wielandt developed the theory of Schur rings in connection with permutation groups containing a regular subgroup; see [17, Chapter IV]. Schur rings are now used in the theory of Cayley graphs [9], algebraic combinatorics [12], algebraic coding theory [18], algorithmic problems in group and graph theory [13], and other areas of mathematics (see, in particular, the survey [11]).

In Theorem 3.2, we apply the construction of [5] to Schur rings. The normalized sums of their basic sets form a basis of the group algebra of an involutive multivalued group, whose reduced valency is the least common multiple of the sizes of these sets

(Theorem 3.2). A multivalued group isomorphic to one obtained in this way from an S-ring over G will be called a Schur multivalued group over G.

Every coset multivalued group is a Schur multivalued group (Corollary 4.2). More generally, if a subgroup L of a finite group K has a complement G, then the double-coset group of the pair (K, L) is isomorphic to a Schur multivalued group over G (Theorem 4.1). For the class $\mathfrak{K}_{\rm schur}$ of all Schur multivalued groups, we have the inclusions

$$\mathfrak{K}_{coset} \subsetneq \mathfrak{K}_{bicoset} \cap \mathfrak{K}_{schur} \subsetneq \mathfrak{K}_{schur}. \tag{1.1}$$

The first inclusion is strict by Example 3.4; the strictness of the second follows from the theorem below. It provides families of Schur multivalued groups of bounded order whose sizes grow subexponentially and in which the proportion of double-coset groups tends to zero.

Theorem. *For every prime power $q \geq 3$, there exists a family $\mathfrak{K}(q)$ of pairwise nonisomorphic involutive multivalued groups with the following properties:*

1. *Each group in $\mathfrak{K}(q)$ has order at most $\lfloor (q+3)/2 \rfloor$ and reduced valency at least $q-1$, and is a Schur multivalued group over an elementary abelian group of order q^2.*
2. *$|\mathfrak{K}(q)| = \exp(\Theta(\sqrt{q}))$ as $q \to \infty$.*
3. *The proportion of double-coset groups in $\mathfrak{K}(q)$ tends to 0 as $q \to \infty$.*

Section 2 collects the basic definitions and properties of multivalued groups. Schur multivalued groups are introduced in Section 3, and their relationship with double-coset groups is established in Section 4. The theorem in the introduction follows from Theorems 5.1 and 5.3 and the estimate for the number of partitions given in the proof of the latter.

2. Multivalued groups

2.1. **Definition.** Let X be a finite nonempty set, let n be a positive integer, and let $X^{(n)}$ be the set of all n-multisets of elements of X. An n-valued group structure on X is specified by a multiplication $\cdot : X \times X \to X^{(n)}$ and an inversion map $\star : X \to X$ satisfying the conditions below. We write the product of $x, y \in X$ as

$$x \cdot y = [(x \cdot y)_1, \ldots, (x \cdot y)_n].$$

Multiplication extends to multisets in the natural way. It is required to be associative: for all $x, y, z \in X$, the following equality of n^2-multisets holds:

$$(x \cdot y) \cdot z = x \cdot (y \cdot z).$$

We also assume that there is an identity element $e \in X$ for multiplication, that is,

$$x \cdot e = e \cdot x = [\underbrace{x, \ldots, x}_{n}]$$

for all $x \in X$. The inverse $x^\star$ satisfies $e \in x \cdot x^\star$ and $e \in x^\star \cdot x$. The number $|X|$ is called the order of the multivalued group $\mathfrak{X}$.

For $x, y, z \in X$, let $m^z_{x,y}$ denote the multiplicity of z in the multiset $x \cdot y$. Setting $p^z_{x,y} = m^z_{x,y}/n$, we obtain the group algebra of the multivalued group $\mathfrak{X}$: it is the complex vector space with basis X and multiplication $xy = \sum_z p^z_{x,y} z$. We call the number

$$\nu(\mathfrak{X}) = \min\{N \in \mathbb{N} : N p^z_{x,y} \in \mathbb{Z} \text{ for all } x, y, z \in X\}$$

the *reduced valency*. Thus, $\nu(\mathfrak{X})$ is the least common multiple of the positive denominators of the rational numbers $p^z_{x,y}$ written in lowest terms.

Following [5], we use a normalized notion of isomorphism of multivalued groups that allows the valencies to differ. Namely, a bijection $f : X \to X'$, $x \mapsto x'$, is an *isomorphism* from an n-valued group $\mathfrak{X}$ to an n'-valued group $\mathfrak{X}'$ with underlying set X' if

$$(x^\star)' = (x')^\star \quad \text{and} \quad p^z_{x,y} = p^{z'}_{x',y'} \tag{2.1}$$

for all $x, y, z \in X$ (in particular, $f(e) = e'$). If $n = n'$, the latter equality is equivalent to the usual preservation of multiset multiplication. The valency n is not an invariant of isomorphism as defined here, whereas the reduced valency is.

In accordance with [5, Definition 1.2], a multivalued group $\mathfrak{X}$ is called *involutive* if

$$(x^\star)^\star = x, \quad e \in x \cdot y \iff y = x^\star, \quad m^e_{x,x^\star} = m^e_{x^\star,x}, \quad (x \cdot y)^\star = y^\star \cdot x^\star.$$

The first and last conditions mean that $\star$ is an involutive anti-isomorphism of the group algebra of $\mathfrak{X}$.

A subset $Y \subseteq X$ is called a *subgroup* of the multivalued group $\mathfrak{X}$ if $e \in Y$, $Y^\star = Y$, and $x \cdot y$ consists of elements of Y for all $x, y \in Y$. The restricted operations give Y an n-valued group structure.

2.2. **Double-coset groups.** Let K be a finite group and L a subgroup of order n. Following [1, Section 6], let $X = L\backslash K/L$ be the set of double cosets, and define an n-valued multiplication by

$$m^z_{x,y} = |\{\ell \in L : Lk_1\ell k_2 L = z\}|,$$

where $x = Lk_1L$ and $y = Lk_2L$. With this multiplication, X becomes an n-valued group $\mathfrak{X}$ with identity element L and inversion $(LkL)^\star = Lk^{-1}L$, $k \in K$. We call $\mathfrak{X}$ the *double-coset* group associated with the pair (K, L). Note that $\star$ is an involution on X and $(x \cdot y)^\star = y^\star \cdot x^\star$. The uniqueness of the inverse and the equalities

$$m^L_{x,x^\star} = |L \cap k^{-1}Lk|, \qquad m^L_{x^\star,x} = |L \cap kLk^{-1}|$$

for $x = LkL$ imply that $\mathfrak{X}$ is involutive.

For the double-coset group of (K, L), let $\overline{K}$ denote the permutation group on the set $L\backslash K$ of right cosets induced by right multiplication in K. Note that $\overline{K}$ is the image of the action of K in the symmetric group; this action need not be faithful.

Lemma 2.1. *The permutation group $\overline{K}$ has degree $\sum_{x\in X}(p^e_{x^\star,x})^{-1}$. It is primitive*[1] *if and only if the multivalued group $\mathfrak{X}$ has no nontrivial proper subgroups.*

Proof. The degree of $\overline{K}$ is $|K : L| = \sum_{x\in X} c(x)$, where $c(x)$ is the number of right cosets of L contained in x. Let $x = LkL$. Then $c(x) = |LkL|/|L|$. The standard formula for the size of a double coset gives

$$n\,c(x) = |LkL| = \frac{|L| \cdot |L|}{|L \cap kLk^{-1}|} = \frac{n^2}{m^e_{x^\star,x}} = \frac{n}{p^e_{x^\star,x}}.$$

Thus $c(x) = (p^e_{x^\star,x})^{-1}$, as required.

Let us prove the second assertion of the lemma. It is clear if $L = K$. Suppose that $L < K$. The action of K on $L\backslash K$ is primitive exactly when L is a maximal subgroup of K. The subgroups H with $L \le H \le K$ are in bijection with the

[1]Here we also regard the group of degree 1 as primitive.

subgroups of the double-coset group: to H we associate the set of double cosets contained in H, and to a subgroup Y of $\mathfrak{X}$ we associate the union $\bigcup_{x\in Y} x$. Hence the absence of intermediate subgroups between L and K is equivalent to the absence of subgroups Y with $\{L\} \subsetneq Y \subsetneq X$. □

We conclude this section with an important special case of double-coset groups. Let G and A be finite groups and let $\varphi : A \to \mathrm{Aut}(G)$ be a homomorphism. Set $K = G \rtimes_\varphi A$ and $L = \{1\} \rtimes A$. Identifying $L\backslash K$ with G, we see that the right action of K on $L\backslash K$ induces on G the action generated by right translations and the automorphisms in $\varphi(A)$. The double cosets in $L\backslash K/L$ correspond to the $\varphi(A)$-orbits on G. Following [1], we call the resulting multivalued group on the set of $\varphi(A)$-orbits the *coset* group of the triple (G, A, φ).

3. Schur multivalued groups

3.1. **Schur rings.** We recall the definition of an S-ring. Let G be a finite group. A subalgebra $\mathcal{A}$ of the group algebra $\mathbb{C}G$ is called a *Schur ring*, or an *S-ring*, over G (see [16,17]) if there exists a partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of G such that $\{1_G\} \in \mathcal{S}$, $R^{-1} \in \mathcal{S}$ for every $R \in \mathcal{S}$, and

$$\mathcal{A} = \mathrm{Span}_{\mathbb{C}}\{\underline{R} : R \in \mathcal{S}\}, \tag{3.1}$$

where $\underline{R} = \sum_{g\in R} g$. The classes of the partition $\mathcal{S}$ are called the basic sets of $\mathcal{A}$.

Note that $\mathcal{S}$ is uniquely determined by the algebra $\mathcal{A}$. The largest S-ring over G corresponds to the discrete partition of G and is equal to $\mathbb{C}G$. If $G \neq 1$, the smallest S-ring corresponds to the partition with two classes $\{1_G\}$ and $G^\# = G \setminus \{1_G\}$; this S-ring is called trivial.

Example 3.1. [16]; see also [17, Section 21]. *Let K be a subgroup of the symmetric group* $\mathrm{Sym}(G)$ *containing the permutations $x \mapsto xg$, $x \in G$, for every $g \in G$. Let $\mathcal{S}$ be the partition of G into the orbits of the stabilizer $K_1 = K_{1_G}$ of 1_G. Then the subspace $\mathcal{A}$ defined by (3.1) is an S-ring over G. We denote it by $\mathfrak{L}(G, K_1)$.*

It follows from (3.1) that the elements $\underline{R}$, $R \in \mathcal{S}$, form a linear basis of $\mathcal{A}$. In particular, the product of two such elements is a linear combination

$$\underline{R}\,\underline{S} = \sum_{T\in\mathcal{S}} c^T_{R,S}\underline{T} \tag{3.2}$$

with nonnegative integer coefficients $c^T_{R,S}$. These coefficients are called the structure constants of the S-ring and satisfy the identities

$$|T|c^T_{R,S} = |R|c^R_{T,S^{-1}} \quad \text{and} \quad \sum_T |T|c^T_{R,S} = |R||S| \tag{3.3}$$

for all $R, S, T \in \mathcal{S}$. It is easy to check that $c^T_{R,S}$ is the number of representations of a fixed $t \in T$ as $t = gh$, with $g \in R$ and $h \in S$. Note that

$$d(R) = c^{1_G}_{R,R^{-1}} = |R|$$

is positive, and the sum of these numbers over all $R \in \mathcal{S}$ equals the order of G (to simplify notation, here and below we write 1_G instead of $\{1_G\}$ in the superscript). Moreover, $d(R) = d(R^{-1})$.

For each $A = \sum_{T\in\mathcal{S}} a_T\underline{T}$ in $\mathcal{A}$, set

$$A^* = \sum_{T\in\mathcal{S}} \bar{a}_T\underline{T^{-1}},$$

where $\bar{a}_T$ is the complex conjugate of a_T. The bijection $A \mapsto A^*$, $A \in \mathcal{A}$, is a semilinear involutive antiautomorphism of $\mathcal{A}$: $(AB)^* = B^*A^*$ and $(A^*)^* = A$. The map

$$\varepsilon : \mathcal{A} \to \mathbb{C}, \quad \sum_T a_T \underline{T} \mapsto \sum_T a_T |T|,$$

is a one-dimensional representation and satisfies $\varepsilon(A^*) = \overline{\varepsilon(A)}$.

3.2. **Construction.** We construct a multivalued group from an S-ring $\mathcal{A}$. Set

$$n = \mathrm{LCM}\{|R| : R \in \mathcal{S}\} \quad \text{and} \quad X = \{x_R : R \in \mathcal{S}\}, \tag{3.4}$$

where $x_R = \frac{1}{|R|}\underline{R}$. Define n-valued multiplication on X by prescribing the multiplicity $m^z_{x,y}$ of $z = x_T$ in the product $x \cdot y$ of $x = x_R$ and $y = x_S$ as follows:

$$m^z_{x,y} = n \cdot \frac{|T|\, c^T_{R,S}}{|R|\,|S|}. \tag{3.5}$$

Using the identities (3.3), one readily checks that $m^z_{x,y}$ is a nonnegative integer and $\sum_z m^z_{x,y} = n$. Finally, set $(x_R)^\star = x_{R^{-1}}$.

Theorem 3.2. *With the notation above, the triple $\mathfrak{X} = \mathfrak{X}(\mathcal{A}) = (X, \cdot, \star)$ is an involutive n-valued group, and $\nu(\mathfrak{X}) = n$.*

Proof. Set $p^T_{R,S} = m^z_{x,y}/n$. The established properties of $m^z_{x,y}$ and the definition of n imply that $np^T_{R,S}$ is a nonnegative integer and $\sum_T p^T_{R,S} = 1$. The associativity of multivalued multiplication follows from the associativity of multiplication in $\mathcal{A}$ and the equalities

$$x_R x_S = \sum_{T \in \mathcal{S}} p^T_{R,S} x_T.$$

The identity is $x_{\{1_G\}} = 1_G$. Since

$$p^{1_G}_{R,S} = \begin{cases} 1/|R|, & \text{if } S = R^{-1}, \\ 0, & \text{if } S \neq R^{-1}, \end{cases}$$

the inverse is unique and equals $x_{R^{-1}}$. The equality $|R| = |R^{-1}|$ gives equality of the multiplicities of the identity in $x_R \cdot x_{R^{-1}}$ and $x_{R^{-1}} \cdot x_R$. The property $(AB)^* = B^*A^*$ ensures that the involution is compatible with multiplication. Thus the group is involutive.

All the numbers $np^T_{R,S}$ are integers, so $\nu(\mathfrak{X})$ divides n. On the other hand, the normalized multiplicities include $p^{1_G}_{R,R^{-1}} = 1/|R|$ for every $R \in \mathcal{S}$. Hence each $|R|$ divides $\nu(\mathfrak{X})$, and therefore n divides $\nu(\mathfrak{X})$. Thus $\nu(\mathfrak{X}) = n$. □

Definition 3.3. *We call $\mathfrak{X}(\mathcal{A})$ the multivalued group associated with the S-ring $\mathcal{A}$. A group $\mathfrak{X}$ is called a Schur multivalued group over G if it is isomorphic to $\mathfrak{X}(\mathcal{A})$ for some S-ring $\mathcal{A}$ over G.*

The following example shows that S-rings over different groups may give rise to isomorphic Schur multivalued groups.

Example 3.4. *Let $\mathcal{A}$ be the trivial S-ring over a group G of order $m > 1$. Formula (3.4) and Theorem 3.2 show that $\mathfrak{X} := \mathfrak{X}(\mathcal{A})$ is an $(m-1)$-valued group of order 2. Its multiplicities (3.5) depend only on m, not on G. Thus $\mathfrak{X}$ is a Schur multivalued group over every group G of order m.*

Moreover, $\mathfrak{X}$ is a double-coset group: it is isomorphic to the group associated with the pair $(\mathrm{Sym}(m), \mathrm{Sym}(m-1))$, where $\mathrm{Sym}(m-1)$ is a point stabilizer in the natural action of $\mathrm{Sym}(m)$. Indeed, both multivalued groups have two elements, and the normalized multiplicity of the identity in the square of the nonidentity element is $1/(m-1)$.

If m is divisible by two distinct primes p and q, then $\mathfrak{X}$ is not a coset group. Otherwise, it would arise from a transitive action of a group of automorphisms on the nonidentity elements of a group G of order m. However, G contains elements of orders p and q, which cannot belong to the same orbit of a group of automorphisms.

3.3. **Isomorphisms.** Isomorphic multivalued groups can also arise from different S-rings over the same group. To describe this phenomenon, we recall the notion of an algebraic isomorphism.

Let $\mathcal{A}$ and $\mathcal{A}'$ be S-rings over groups G and G', respectively. An isomorphism of complex algebras $\varphi : \mathcal{A} \to \mathcal{A}'$ is called an *algebraic isomorphism*[2] if it maps the standard basis of $\mathcal{A}$ onto the standard basis of $\mathcal{A}'$. In this case, for every $R \in \mathcal{S}(\mathcal{A})$ there is a unique $R' \in \mathcal{S}(\mathcal{A}')$ such that $\varphi(\underline{R}) = \underline{R'}$. Moreover,

$$\{1_G\}' = \{1_{G'}\}, \quad (R^{-1})' = (R')^{-1}, \quad c^T_{R,S} = c^{T'}_{R',S'}$$

for all $R, S, T \in \mathcal{S}(\mathcal{A})$. Therefore, (3.4) and (3.5) show that an algebraic isomorphism φ induces an isomorphism $x_R \mapsto x_{R'}$, $R \in \mathcal{S}(\mathcal{A})$, of the associated multivalued groups, thus proving the following statement.

Proposition 3.5. *If $\mathcal{A}$ and $\mathcal{A}'$ are algebraically isomorphic S-rings, then the multivalued groups $\mathfrak{X}(\mathcal{A})$ and $\mathfrak{X}(\mathcal{A}')$ are isomorphic and have the same reduced valency.*

In Section 5, we construct a family of S-rings over an elementary abelian group of order q^2 whose number of pairwise algebraically nonisomorphic representatives grows as $\exp(\Theta(\sqrt{q}))$ when $q \to \infty$.

4. Double-coset multivalued groups in the context of Schur rings

Let K be a finite group. The double cosets of a subgroup L of K form a partition of K closed under taking inverses. The linear span of their sums is closed under multiplication in $\mathbb{C}K$. However, the double coset containing the identity of K is L, rather than $\{1_K\}$. Thus, if $L \neq 1_K$, this partition does not define an S-ring over K in the usual sense. According to the definition in [10, Section 3], such a partition defines only a pseudo-S-ring over K. We show that, under an additional assumption on L, the corresponding multivalued group $\mathfrak{X}$ is associated with a suitable Schur ring.

Suppose that L has a complement G in K, that is,

$$K = L\,G \quad \text{and} \quad G \cap L = 1.$$

Then each $k \in K$ has a unique factorization $k = \ell g$, where $\ell \in L$ and $g \in G$. This defines a bijection

$$\pi : L\backslash K \longrightarrow G, \qquad \pi(Lg) = g.$$

Via this bijection, the permutation group $\overline{K}$ defined in Section 2.2 can be identified with the group of all permutations $\overline{k} \in \mathrm{Sym}(G)$ determined by $k \in K$ through

$$g^{\overline{k}} = \pi(Lgk), \quad g \in G,\ k \in K.$$

[2]Combinatorial isomorphisms of S-rings are defined as isomorphisms of the corresponding Cayley schemes.

Let N be the kernel of the corresponding action of K on G. Then $\overline{K}_{1_G} \cong L/N$. Moreover, $\overline{K} \cong K/N$ contains the right regular subgroup G. Thus Example 3.1 defines the S-ring

$$\mathcal{A}(K, L) = \mathfrak{L}(G, \overline{K}_{1_G}).$$

In general, this S-ring depends on the choice of the complement G; this choice is suppressed in the notation $\mathcal{A}(K, L)$.

Theorem 4.1. *Let L be a subgroup of a finite group K, and let G be a complement to L in K. Then the double-coset group of the pair (K, L) is isomorphic to the multivalued group associated with the S-ring $\mathcal{A}(K, L)$ over G.*

Proof. Set $X = L\backslash K/L$. For each $x \in X$, let

$$\pi(x) = \{\pi(Lk) : k \in x\},$$

where π is defined above. If $x = LgL$, then the right cosets of L contained in x are $Lg\ell$, $\ell \in L$. Thus the sets $\pi(x)$, $x \in X$, are precisely the $\overline{K}_{1_G}$-orbits, that is, the basic sets of $\mathcal{A}(K, L)$. We verify that for all $x, y, z \in X$,

$$\frac{m^z_{x,y}}{n} = \frac{|T|\, c^T_{R,S}}{|R|\,|S|}, \tag{4.1}$$

where $n = |L|$, $R = \pi(x)$, $S = \pi(y)$, and $T = \pi(z)$. To this end, choose $g \in \pi(x)$ and count in two ways the set Ω of all pairs $(\ell, h) \in L \times S$ such that $g\ell h \in z$.

For each fixed $h \in S$, the number of $\ell \in L$ with $g\ell h \in z$ is $m^z_{x,y}$, since $LgL = x$ and $LhL = y$. Therefore,

$$|\Omega| = |S| m^z_{x,y}.$$

On the other hand, set $r = \pi(Lg\ell) \in R$. Since $g\ell = \ell' r$ for some $\ell' \in L$, the condition $g\ell h \in z$ is equivalent to $rh \in z \cap G = T$. For each fixed $r \in R$, the number of $\ell \in L$ such that $\pi(Lg\ell) = r$ is $|L|/|R|$. The number of pairs $(r, h) \in R \times S$ with $rh \in T$ is $|T| c^T_{R,S}$. Consequently,

$$|\Omega| = \frac{|L|}{|R|}\, |T| c^T_{R,S}.$$

Comparing the two expressions for $|\Omega|$ yields (4.1).

To complete the proof, note that the bijection $x \mapsto x_{\pi(x)}$, $x \in X$, is an isomorphism from $\mathfrak{X}$ to $\mathfrak{X}(\mathcal{A}(K, L))$. Indeed, the equality in (2.1) for the normalized multiplicities follows from (4.1), and preservation of the involution follows from $\pi(x^\star) = x^{-1} \cap G = (x \cap G)^{-1} = \pi(x)^{-1}$. □

Let a finite group A act on a finite group G via a homomorphism $\varphi : A \to \mathrm{Aut}(G)$. In the semidirect product $K = G \rtimes_\varphi A$, the naturally embedded subgroup G is a complement to $L = \{1_G\} \rtimes A$. Hence Theorem 4.1 gives the following.

Corollary 4.2. *The coset multivalued group of the triple (G, A, φ) is isomorphic to the multivalued group associated with the S-ring $\mathfrak{L}(G, \varphi(A))$ over G. In particular, every coset multivalued group is a Schur multivalued group.*

5. A family of multivalued groups that are not double-coset groups

5.1. **Affine S-rings.** We use the S-ring construction of [8, Theorem 1]. Let $\mathbb{F}$ be a finite field of order q, let $G = (\mathbb{F}^2, +)$, and let $L = \{\lambda I_2 : \lambda \in \mathbb{F}^\times\}$ be the group of scalar matrices. The affine group $K = G \rtimes L$ acts on G, with G acting by translations and L by scalar multiplication. Consider the S-ring $\mathcal{A}_0 = \mathfrak{L}(G, L)$ and its S-subrings.

The nonidentity basic sets of $\mathcal{A}_0$ are the one-dimensional $\mathbb{F}$-subspaces of $\mathbb{F}^2$ with zero removed. There are $q+1$ such sets; each has size $q-1$ and satisfies $-R = R$. For any two such sets R, S,

$$\underline{R} \cdot \underline{S} = \begin{cases} \underline{G^\# \setminus (R \cup S)}, & \text{if } R \neq S; \\ (q-1)\,\underline{0_G} + (q-2)\underline{R}, & \text{if } R = S, \end{cases} \tag{5.1}$$

where $G^\# = G \setminus \{0_G\}$.

We construct an S-subring of $\mathcal{A}_0$ corresponding to a partition $\pi = (k_1, \ldots, k_a)$ of $q+1$, where

$$a \geq 1, \qquad k_1 \geq k_2 \geq \ldots \geq k_a \geq 1, \qquad \sum_{i=1}^{a} k_i = q+1.$$

Choose a partition $\mathcal{P}$ of the set $\mathcal{S}_0^\#$ of nonidentity basic sets into classes $\mathcal{P}_u$ of size k_u, $1 \leq u \leq a$. Let R_u be the union of the sets in $\mathcal{P}_u$; thus

$$|R_u| = (q-1)k_u, \quad 1 \leq u \leq a. \tag{5.2}$$

A direct calculation using (5.1) shows that, for $1 \leq u, v \leq a$,

$$\underline{R_u}\underline{R_v} = \begin{cases} (k_u - 1)k_v\,\underline{R_u} + k_u(k_v - 1)\underline{R_v} \\ \qquad + k_u k_v\,\underline{S_{u,v}} & \text{if } u \neq v, \\ (q-1)k_u\,\underline{0_G} + [q - 2 + (k_u - 1)(k_u - 2)]\,\underline{R_u} \\ \qquad + k_u(k_u - 1)\,\underline{S_{u,u}} & \text{if } u = v, \end{cases} \tag{5.3}$$

where $S_{u,v} = G^\# \setminus (R_u \cup R_v)$. Set $R_0 = \{0_G\}$. Then the $\mathbb{C}$-vector space

$$\mathcal{A}(q, \pi) = \mathrm{Span}_{\mathbb{C}}\{\underline{R_u} : 0 \leq u \leq a\}$$

is a commutative S-ring over G. Its basic sets are $R_0, R_1, \ldots, R_a$. Its structure constants are determined solely by $k_1, \ldots, k_a$. Hence its algebraic isomorphism class depends only on π and not on the choice of $\mathcal{P}$. We call $\mathcal{A}(q, \pi)$ the *affine* S-ring over a group of order q^2 corresponding to the partition π.

5.2. **Construction.** Applying Theorem 3.2 to affine S-rings yields the following multivalued groups.

Theorem 5.1. *Let q be a prime power and let $\pi = (k_1, \ldots, k_a)$ be a partition of $q+1$. Then the multivalued group $\mathfrak{X}(q, \pi)$ with elements*

$$x_u = \frac{1}{|R_u|}\underline{R_u}, \qquad 0 \leq u \leq a,$$

associated with the S-ring $\mathcal{A}(q, \pi)$ is commutative, has the identity map as its involution, and has reduced valency

$$n = (q-1) \cdot \mathrm{LCM}\{k_1, \ldots, k_a\}.$$

For $1 \le i, j \le a$, the multiplicities are given by the following formulas; multiplication by x_0 is determined by the identity axiom:

$$i \neq j: \qquad m_{x_i,x_j}^{x_u} = \frac{n}{q-1} \cdot \begin{cases} 0 & \text{if } u = 0, \\ k_u - 1 & \text{if } u \in \{i, j\}, \\ k_u & \text{if } u \notin \{0, i, j\}, \end{cases}$$

$$i = j: \qquad m_{x_i,x_i}^{x_u} = \frac{n}{(q-1)k_i} \cdot \begin{cases} 1 & \text{if } u = 0, \\ q - 2 + (k_i - 1)(k_i - 2) & \text{if } u = i, \\ k_u(k_i - 1) & \text{if } u \notin \{0, i\}. \end{cases}$$

For fixed q, the multivalued groups $\mathfrak{X}(q, \pi)$ and $\mathfrak{X}(q, \pi')$ are isomorphic if and only if $\pi = \pi'$.

Proof. The first part follows from Theorem 3.2 and formulas (5.2) and (5.3). Now let $f : \mathfrak{X}(q, \pi) \to \mathfrak{X}(q, \pi')$ be an isomorphism. Then $a = a'$, $f(x_0) = x'_0$, and there exists a permutation σ of $\{1, \dots, a\}$ such that $f(x_i) = x'_{\sigma(i)}$. Preservation of the normalized multiplicities gives

$$\frac{1}{(q-1)k_i} = \frac{m_{x_i,x_i}^{x_0}}{n} = \frac{m_{x'_{\sigma(i)},x'_{\sigma(i)}}^{x'_0}}{n'} = \frac{1}{(q-1)k'_{\sigma(i)}}.$$

Hence $k_i = k'_{\sigma(i)}$ for all i. Since the parts of both partitions are listed in nonincreasing order, $\pi = \pi'$. The converse follows from the explicit formulas for the multiplicities. □

Remark 5.2. *Under the assumptions and notation of Theorem 5.1, suppose that $q \ge 3$ and $k_i \ge 2$ for every $1 \le i \le a$. The formulas for the multiplicities imply that $m_{x_i,x_i}^{x_j} > 0$ for every $1 \le i \le a$ and every $0 \le j \le a$. Thus any subgroup containing at least one x_i, $i \neq 0$, contains all elements of $\mathfrak{X}(q, \pi)$. Consequently, $\mathfrak{X}(q, \pi)$ has no subgroups Y with $\{x_0\} \subsetneq Y \subsetneq X$.*

We show that, among the groups $\mathfrak{X}(q, \pi)$ for which all parts of π are at least 2, the proportion of double-coset groups tends to zero as $q \to \infty$.

Theorem 5.3. *Let $q \ge 3$ be a prime power. Let $\mathfrak{K}(q)$ be a set of representatives of the isomorphism classes of the groups $\mathfrak{X}(q, \pi)$ for which all parts of π are at least 2, and let $\mathfrak{K}_0(q)$ be its subset of double-coset groups. There exist absolute constants $c_1, c_2 > 0$ such that*

$$|\mathfrak{K}(q)| \ge 2^{c_1\sqrt{q}} \quad \text{and} \quad |\mathfrak{K}_0(q)| \le 2^{c_2(\log q)^2}. \tag{5.4}$$

In particular, the ratio $\frac{|\mathfrak{K}_0(q)|}{|\mathfrak{K}(q)|}$ tends to 0 as $q \to \infty$.

Proof. Applying the formula for the number of partitions π in which every part is at least 2 (see [15, p. 500]), we obtain the following asymptotic formula for the number of multivalued groups in $\mathfrak{K}(q)$:

$$|\mathfrak{K}(q)| \sim \frac{C_1}{(q+1)^{3/2}} 2^{C_2\sqrt{q+1}}$$

for some absolute constants $C_1, C_2 > 0$. This proves the first inequality in (5.4).

We now bound $|\mathfrak{K}_0(q)|$. By Lemma 2.1 and the formulas in Theorem 5.1, the permutation group $\overline{K}$ corresponding to a double-coset multivalued group $\mathfrak{X} \in \mathfrak{K}_0(q)$ has degree

$$\sum_{x \in X} \frac{1}{p^{x_0}_{x,x^\star}} = 1 + \sum_{i=1}^{a} (q-1)k_i = q^2,$$

where X is the underlying set of $\mathfrak{X}$. By Remark 5.2 and Lemma 2.1, this permutation group is primitive. Since conjugate subgroups of $\mathrm{Sym}(q^2)$ give rise to isomorphic multivalued groups, a coarse upper bound for $|\mathfrak{K}_0(q)|$ is the number of conjugacy classes of all primitive permutation groups of degree q^2.

By [14, Theorem I], the number of conjugacy classes of primitive groups of degree d is at most $d^{C\mu(d)}$, where $\mu(d)$ is the largest exponent in the prime factorization of d and C is an absolute constant. If $q = p^f$, then $\mu(q^2) = 2f \le 2\log_2 q$. Consequently,

$$|\mathfrak{K}_0(q)| \le (q^2)^{C\mu(q^2)} \le 2^{4C(\log_2 q)^2}.$$

This proves the second inequality in (5.4). □

Acknowledgments

The research of A. V. Vasil'ev was carried out within the framework of the Sobolev Institute of Mathematics project FWNF-2026-0017.

References

[1] V. M. Buchstaber, *n-valued groups: theory and applications*, Mosc. Math. J. **6** (2006), no. 1, 57–84.
[2] V. M. Buchstaber and A. N. Kholodov, *Topological constructions connected with many-valued formal groups*, Math. USSR-Izv. **20** (1983), no. 1, 1–25.
[3] V. M. Buchstaber and M. I. Kornev, *Algebraic n-valued groups, cubics, and Wendt matrices*, Mat. Sb. **217** (2026), no. 8, 29–86 (Russian).
[4] V. M. Buchstaber and S. P. Novikov, *Formal groups, power systems and Adams operators*, Math. USSR-Sb. **13** (1971), no. 1, 80–116.
[5] V. M. Buchstaber, A. M. Vershik, S. A. Evdokimov, and I. N. Ponomarenko, *Combinatorial algebras and multivalued involutive groups*, Funct. Anal. Appl. **30** (1996), no. 3, 158–162.
[6] V. M. Buchstaber and A. P. Veselov, *Conway topograph,* $\mathrm{PGL}_2(\mathbb{Z})$*-dynamics and two-valued groups*, Russian Math. Surveys **74** (2019), no. 3, 387–430.
[7] J. Guo, I. Ponomarenko and A. V. Vasil'ev, *On multivalued groups of order 3*, Sci. China Math. **68** (2025), no. 8, 1969–1978.
[8] A. Hanaki, T. Hirai, and I. Ponomarenko, *On a huge family of non-Schurian Schur rings*, Electron. J. Combin. **29** (2022), no. 2, P2.14.
[9] M. H. Klin and R. Pöschel, *The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings*, Algebraic Methods in Graph Theory (Szeged, 1978), Vols. I, II, Colloq. Math. Soc. János Bolyai, vol. 25, North-Holland, Amsterdam–New York, 1981, pp. 405–434.
[10] M. E. Muzychuk, *The structure of rational Schur rings over cyclic groups*, European J. Combin. **14** (1993), no. 5, 479–490.
[11] M. E. Muzychuk and I. Ponomarenko, *Schur rings*, European J. Combin. **30** (2009), no. 6, 1526–1539.
[12] M. E. Muzychuk and G. Ryabov, *Constructing linked systems of relative difference sets via Schur rings*, Des. Codes Cryptogr. **92** (2024), no. 9, 2615–2637.
[13] I. Ponomarenko and A. Vasil'ev, *Testing isomorphism of central Cayley graphs over almost simple groups in polynomial time*, Zap. Nauchn. Sem. POMI **455** (2017), 154–180.
[14] L. Pyber and A. Shalev, *Asymptotic results for primitive permutation groups*, J. Algebra **188** (1997), no. 1, 103–124.

[15] J. Sándor, D. S. Mitrinović, and B. Crstici, *Handbook of Number Theory I*, Springer, Dordrecht, 2006.
[16] I. Schur, *Zur Theorie der einfach transitiven Permutationsgruppen*, Sitzungsber. Preuss. Akad. Wiss. Phys.-Math. Kl. (1933), 598–623.
[17] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York–London, 1964.
[18] Y. Wu, J. Y. Hyun, and Y. Lee, *Characterization of p-ary functions in terms of association schemes and its applications*, J. Combin. Theory Ser. A **187** (2022), 105576.
[19] P. V. Yagodovskii, *Representations of multivalued groups on graphs*, Russian Math. Surveys **57** (2002), no. 1, 173–174.

Sobolev Institute of Mathematics, Siberian Branch of the Russian Academy of Sciences, 4 Akademika Koptyuga Avenue, Novosibirsk 630090, Russia
Email address: vasand@math.nsc.ru

St. Petersburg Department of Steklov Mathematical Institute of the Russian Academy of Sciences, 27 Fontanka Embankment, St. Petersburg 191023, Russia
Email address: inp@pdmi.ras.ru