QUANTUM SPACES ASSOCIATED TO MULTIPERMUTATION SOLUTIONS OF LEVEL TWO

TATIANA GATEVA-IVANOVA AND SHAHN MAJID

Abstract. We study finite set-theoretic solutions (X, r) of the Yang-Baxter equation of square-free multipermutation type. We show that each such solution over $\mathbb{C}$ with multipermutation level two can be put in diagonal form with the associated Yang-Baxter algebra $\mathcal{A}(\mathbb{C}, X, r)$ having a q-commutation form of relations determined by complex phase factors. These complex factors are roots of unity and all roots of a prescribed form appear as determined by the representation theory of the finite abelian group $\mathcal{G}$ of left actions on X. We study the structure of $\mathcal{A}(\mathbb{C}, X, r)$ and show that they have a $\bullet$-product form 'quantizing' the commutative algebra of polynomials in $|X|$ variables. We obtain the $\bullet$-product both as a Drinfeld cotwist for a certain canonical 2-cocycle and as a braided-opposite product for a certain crossed $\mathcal{G}$-module (over any field k). We provide first steps in the noncommutative differential geometry of $\mathcal{A}(k, X, r)$ arising from these results. As a byproduct of our work we find that every such level 2 solution (X, r) factorises as $r = f \circ \tau \circ f^{-1}$ where τ is the flip map and (X, f) is another solution coming from X as a crossed $\mathcal{G}$-set.

1. Introduction

Let V be a vector space of a field k. It is well-known that the 'Yang-Baxter equation' (YBE) on an invertible linear map $R : V \otimes V \to V \otimes V$,

$$R_{12}R_{23}R_{12} = R_{23}R_{12}R_{23}$$

(where $R_{i,j}$ denotes R acting in the i, j place in $V \otimes V \otimes V$) provide a linear representation of the braid group on tensor powers of V. When $R^2 = \mathrm{id}$ one says that the solution is involutive, and in this case one has a representation of the symmetric group on tensor powers. We say that R is of cotwist form if $R = FF_{21}^{-1}$ for some invertible linear map $F : V \otimes V \to V \otimes V$. Such a form of R always obeys the YBE and is always involutive. Associated to each solution of the YBE are several algebraic constructions, among them the 'quantum space' $k_R[V]$ which is nothing but the tensor algebra on V modulo the ideal generated by the image of $\mathrm{id} - R$. If $\{x_i\}$ are a basis of V then $k_R[V]$ is the free associative algebra generates by the x_i modulo the ideal generated by $x_i x_j - \cdot R(x_i \otimes x_j)$ where $\cdot$ on the right denotes product in the free associative algebra.

Date: June 2008/Ver 2.

1991 *Mathematics Subject Classification.* Primary 81R50, 16W50, 16S36.

Key words and phrases. Yang-Baxter, semigroups, quantum groups, graphs, noncommutative geometry.

The first author is partially supported by Isaac Newton Institute, UK, the ICTP, Trieste, and Grant MI 1503/2005 of the Bulgarian National Science Fund of the Ministry of Education and Science.

Next, a particularly nice class of solutions is provided by set-theoretic solutions where X is a set, $r : X \times X \to X \times X$ obeys similar relations on $X \times X \times X$. Of course, each such solution extends linearly to $V = kX$ with matrices in this natural basis having only entries from 0,1 and many other nice properties. In this case there is a semigroup $S(X, r)$ generated by X with relations $xy = \cdot r(x, y)$ (where $\cdot$ denotes product in the free semigroup) and the semigroup algebra $kS(X, r) = k_R[V]$. There is a canonical action of $S(X, r)$ on X by permutations and hence of $k_R[V]$ on V. The algebra $k_R[V]$ when defined in the basis X is the 'Yang-Baxter algebra' $\mathcal{A}(k, X, r)$ associated to (X, r), but $k_R[V]$ is defined independently of any basis of V and may be computed in some other more convenient one.

In this paper we look at the special properties of linear solutions obtained in this way when r is a finite square-free multipermutation solution of level 2. Precise details of what this means will be recalled in the preliminaries but, briefly, such solutions are involutive and have the property that the permutation group $\mathcal{G}(X, r)$, defined as the image in $\mathrm{Sym}(X)$ of $S(X, r)$ acting by permutations on X, is abelian. We show over the field $k = \mathbb{C}$ that then (i) the linear extension has a cotwist form and (ii) there exists a basis Y of V in which R has a diagonal form in the sense that R is the vector space flip map but with further coefficients in this basis. This is achieved (Theorem4.9) in Section 4 using Fourier theory on the finite groups $\mathcal{G}_i$ which are the restrictions of $\mathcal{G}$ to its orbits in X. The necessary methods in the context of finite abelian groups are first developed in Section 3 before applying to each $\mathcal{G}_i$.

The basis $Y = \{y^i_\eta\}$ which we obtain here for the span of each orbit X_i is labelled by characters on $\mathcal{G}_i$. Writing the diagonal coefficients of R in this basis as $q_{i,\eta,j,\zeta}$, say, the quantum algebra $\mathcal{A}(\mathbb{C}, X, r)$ takes a 'q-commutation' relations form

$$y^i_\eta y^j_\zeta = q_{i,\eta,j,\zeta} y^j_\zeta y^i_\eta; \quad q_{i,\eta,j,\zeta} = \frac{\chi_\zeta(\sigma^i_j)}{\chi_\eta(\sigma^j_i)}$$

where $\sigma^j_i \in \mathrm{Sym}(X_i)$ is a certain fixed permutation for each ordered pair i, j and χ_η, χ_ζ denote characters on $\mathcal{G}_i, \mathcal{G}_j$. Relations with q-factors are typical in the simplest models of noncommutative geometry (for example the 'quantum plane' [M]) but now the factors are particular roots of unity with values determined by the group characters.

Such factors are also typical in quantum mechanics (the 'Weyl form' of the Heisenberg commutation relations) and in Section 6 we provide a general picture of $\mathcal{A}(k, X, r)$ as 'quantisation' in the sense of a deformed $\bullet$-product on the vector space of the commutative algebra $k[V]$ (the symmetric algebra on V which we view as polynomials in any fixed basis of V as $|X|$ variables). We obtain this $\bullet$ product in analogy with the Moyal product in quantum mechanics, using modern Drinfeld cotwist methods. The form of R ensures that this is possible but we find a natural expression of $\bullet$ in Proposition 6.4 as such a cotwist with respect to a canonical cocycle on $\mathcal{H}^* \times \mathcal{H}$ where $\mathcal{H} = \prod_i \mathcal{G}_i$. This is a finite group version of the canonical symplectic structure on $V^* \oplus V$ in quantum theory. We then find a second expression (now over a general field k) of the same $\bullet$-product in terms of the braided-opposite algebra to $k[V]$ in the braided category of crossed $\mathcal{G}$-modules, Proposition 6.9.

An immediate consequence of our work is that $\mathcal{A}(k, X, r)$ is not only an algebra but a Hopf algebra in a certain symmetric monoidal category with braiding induced by R. Moreover, the infinitesimal translations afforded by this braided coproduct provide braided differential operators or 'vector fields' which define a noncommtuative differential structure on the algebra. We show, equivalently, that there is a natural exterior algebra of differential forms $(\Omega(\mathcal{A}(k, X, r)), \mathrm{d})$ obtained by extending $\bullet$ to differential forms. In this way we provide the first stage of the noncommutative differential geometry of $\mathcal{A}(k, X, r)$ for the class of (X, r) under study.

In Section 7 we end with a short epilogue to our work. Namely, the 'cotwist' form of R turns out to have a set-theoretic analogue $r = f \circ \tau \circ f^{-1}$ where $f : X \times X \to X \times X$ is itself a set-theoretic solution (X, f) and $\tau(x, y) = (y, x)$. It is the (non-involutive) braiding associated to X as a crossed $\mathcal{G}$-set. We provide (Proposition 7.1) necessary and sufficient conditions for this which include (and do not allow much more than) (X, r) square-free involutive of multipermutation level 2.

2. Preliminaries on set-theoretic solutions

There are many works on set-theoretic solutions and related structures, of which a relevant selection for the interested reader is [ESS, GB, GI, GI04, GIM1, GIM2, GJO, JO, LYZ, R, T, V]. In this section we recall basic notions and results which will be used in the paper. We shall use the terminology, notation and some results from our previous works, [GI, GIM1, GIM2].

Definition 2.1. Let X be a nonempty set (not necessarily finite) and let $r : X \times X \longrightarrow X \times X$ be a bijective map. We refer to it as a *quadratic set*, and denote it by (X, r). The image of (x, y) under r is presented as

$$r(x, y) = ({}^x y, x^y). \tag{2.1}$$

The formula (2.1) defines a "left action" $\mathcal{L} : X \times X \longrightarrow X$, and a "right action" $\mathcal{R} : X \times X \longrightarrow X$, on X as:

$$\mathcal{L}_x(y) = {}^x y, \quad \mathcal{R}_y(x) = x^y, \tag{2.2}$$

for all $x, y \in X$. The map r is *nondegenerate*, if the maps $\mathcal{R}_x$ and $\mathcal{L}_x$ are bijective for each $x \in X$. In this paper we shall consider only the case where r is nondegenerate. As a notational tool, we shall sometimes identify the sets $X \times X$ and X^2, the set of all monomials of length two in the free semigroup $\langle X \rangle$.

Definition 2.2. (1) r is *square-free* if $r(x, x) = (x, x)$ for all $x \in X$.

(2) r is *a set-theoretic solution of the Yang-Baxter equation* or, shortly *a solution* (YBE) if the braid relation

$$r^{12} r^{23} r^{12} = r^{23} r^{12} r^{23}$$

holds in $X \times X \times X$, where the two bijective maps $r^{ii+1} : X^3 \longrightarrow X^3$, $1 \leq i \leq 2$ are defined as $r^{12} = r \times \mathrm{id}_X$, and $r^{23} = \mathrm{id}_X \times r$. In this case we shall refer to (X, r) also as a *a braided set*.

(3) A braided set (X, r) with r involutive is called *a symmetric set*.

To each quadratic set (X, r) we associate canonical algebraic objects generated by X and with quadratic defining relations $\Re = \Re(r)$ defined by

$$xy = zt \in \Re(r), \quad \text{whenever} \quad r(x, y) = (z, t). \tag{2.3}$$

Definition 2.3. Let (X, r) be a quadratic set.

(i) The semigroup $S = S(X, r) = \langle X; \Re(r)\rangle$, with a set of generators X and a set of defining relations $\Re(r)$, is called *the semigroup associated with* (X, r).

(ii) The *group* $G = G(X, r)$ *associated with* (X, r) is defined as $G = G(X, r) = {}_{gr}\langle X; \Re(r)\rangle$

(iii) For arbitrary fixed field k, *the* k*-algebra associated with* (X, r) is defined as $\mathcal{A} = \mathcal{A}(k, X, r) = k\langle X; \Re(r)\rangle$. ($\mathcal{A}(k, X, r)$ is isomorphic to the monoidal algebra $kS(X, r)$).

(iv) To each nondegenerate braided set (X, r) we also associate a permutation group, called *the group of left action* and denoted $\mathcal{G} = \mathcal{G}(X, r)$, see Definition 2.6.

If (X, r) is a solution, then $S(X, r)$, resp. $G(X, r)$, resp. $\mathcal{A}(k, X, r)$ is called the *Yang-Baxter semigroup*, resp. the *Yang-Baxter group*, resp. the *Yang-Baxter algebra* associated to (X, r).

Example 2.4. For arbitrary nonempty set X with $|X| \geq 2$, *the trivial solution* (X, r) is defined as $r(x, y) = (y, x)$, for all $x, y \in X$. It is clear that (X, r) is the trivial solution *iff* ${}^x y = y$, and $x^y = x$, for all $x, y \in X$, or equivalently $\mathcal{L}_x = \mathrm{id}_X = \mathcal{R}_x$ for all $x \in X$. In this case $S(X, r)$ is the free abelian monoid, $G(X, r)$ is the free abelian group, $\mathcal{A}(k, X, r)$ the algebra of commutative polynomials in X, and $\mathcal{G}(X, r) = \{\mathrm{id}_X\}$.

Remark 2.5. Suppose (X, r) is a nondegenerate quadratic set. It is well known, see for example [GIM1], that (X, r) is a braided set (i.e. r obeys the YBE) *iff* the following conditions hold

$$\mathbf{l1}: \quad {}^x({}^y z) = {}^{{}^x y}({}^{x^y} z), \qquad \mathbf{r1}: \quad (x^y)^z = (x^{{}^y z})^{y^z},$$

$$\mathbf{lr3}: \quad ({}^x y)^{({}^{x^y}(z))} = {}^{(x^{{}^y z})}(y^z),$$

for all $x, y, z \in X$.

Clearly, conditions **l1**, imply that for each nondegenerate braided set (X, r) the assignment: $x \longrightarrow \mathcal{L}_x, x \in X$ extends canonically to a group homomorphism

$$\mathcal{L} : G(X, r) \longrightarrow \mathrm{Sym}(X), \tag{2.4}$$

which defines *the canonical left action of* $G(X, r)$ *on the set* X. Analogously **r1** implies *a canonical right action of* $G(X, r)$ *on* X.

Definition 2.6. [GIM1] Let (X, r) be a nondegenerate braided set, $\mathcal{L} : G(X, r) \longrightarrow \mathrm{Sym}(X)$ be the canonical group homomorphism defined via the left action. The image $\mathcal{L}(G(X, r))$ is denoted by $\mathcal{G}(X, r)$. We call it *the (permutation) group of left actions*.

The permutation group $\mathcal{G}(X, r)$ will be of particular importance in the present paper.

Remark 2.7. Suppose X is a finite set, then $\mathcal{G} = \mathcal{L}(S(X, r))$. Indeed, $\mathcal{G}$ is generated as a semigroup by the images $\mathcal{L}_x$ of all $x \in X$ and their inverses. Each $\mathcal{L}_x$ is a permutation of finite order, say m_x. Then its inverse (in $\mathcal{G}$) is simply $(\mathcal{L}_x)^{m_x - 1}$. So $\mathcal{G}$ is generated as a semigroup by the set $\{\mathcal{L}_x, \mathcal{L}_{(x^{m_x - 1})} \mid x \in X\} \subseteq \mathcal{L}(S(X, r))$.

The following conditions were introduced and studied in [GI, GIM1, GIM2]:

Definition 2.8. Let (X, r) be a quadratic set.

(1) [GI, GIM1] (X, r) is called *cyclic* if the following conditions are satisfied

$$\textbf{cl1}: \quad {}^{y^x}x = {}^{y}x \quad \text{for all } x, y \in X; \qquad \textbf{cr1}: \quad x^{{}^{x}y} = x^{y}, \quad \text{for all } x, y \in X;$$
$$\textbf{cl2}: \quad {}^{{}^{x}y}x = {}^{y}x, \quad \text{for all } x, y \in X; \qquad \textbf{cr2}: \quad x^{y^x} = x^{y} \quad \text{for all } x, y \in X.$$

We refer to these conditions as *cyclic conditions*.

(2) Condition **lri** is defined as

$$\textbf{lri:} \quad ({}^{x}y)^{x} = y = {}^{x}(y^{x}) \text{ for all } \quad x, y \in X.$$

In other words **lri** holds if and only if (X, r) is nondegenerate and $\mathcal{R}_x = \mathcal{L}_x^{-1}$ and $\mathcal{L}_x = \mathcal{R}_x^{-1}$

In this paper the class of *nondegenerate square-free symmetric sets of finite order* will be of special interest. The following result is extracted from [GIM1], Theorem 2.34, where more equivalent conditions are pointed out. Note that in our considerations below (unless we indicate the contrary) the set X is not necessarily of finite order.

Fact 2.9. [GIM1]. *Suppose (X, r) is nondegenerate, involutive and square-free quadratic set (not necessarily finite). Then the following conditions are equivalent: (i) (X, r) is a set-theoretic solution of the Yang-Baxter equation; (ii) (X, r) satisfies* **l1***; (iii) (X, r) satisfies* **r1***; (iv) (X, r) satisfies* **lr3**.

In this case (X, r) is cyclic and satisfies **lri**.

Corollary 2.10. *Every nondegenerate square-free symmetric set (X, r) is uniquely determined by the left action $\mathcal{L} : X \times X \longrightarrow X$, more precisely,*

$$r(x, y) = (\mathcal{L}_x(y), \mathcal{L}_y^{-1}(x)).$$

Furthermore it is cyclic.

Let (X, r) be a braided set. Clearly, if Y is an r-invariant subset of (X, r), r induces a solution (Y, r_Y), where $r_Y = r_{|Y \times Y}$. We call (Y, r_Y) *the restricted solution (on Y)*. Suppose (X, r) is square-free symmetric set. Then each G-orbit under the left action of G on X is also a right G-orbit and therefore it is an r-invariant subset.

2.1. **Nondegenerate square-free symmetric sets of finite order.** In the case when (X, r) is a square-free symmetric sets of finite order the algebras $\mathcal{A}(X, r)$ provided new classes of Noetherian rings [GI94, GI96-1], Gorentstein (Artin-Schelter regular) rings [GI96-2, GI00, GI04] and so forth. Artin-Schelter regular rings were introduced in [AS] and are of particular interest. The algebras $\mathcal{A}(X, r)$ are similar in spirit to the quadratic algebras associated to linear solutions particularly studied in [M], but have their own remarkable properties. The semigroups $S(X, r)$ for a general braided set (X, r) were studied particularly in [GIM1] with a systematic theory of 'exponentiation' from the set to the semigroup by means of the 'actions' $\mathcal{L}_x, \mathcal{R}_x$ (which in the process become a matched pair of semigroup actions) somewhat in analogy with the Lie theoretic exponentiation in [M90].

We shall recall some basic facts and recent results needed in this paper. Suppose (X, r) is a nondegenerate square-free symmetric set of finite order, $G = G(X, r), \mathcal{G} =$

$\mathcal{G}(X,r)$ in notation as above. Note that the group G acts nontransitively on X. This follows from the decomposition theorem of Rump, [R].

Let $X_1, \cdots, X_t$ be the set of orbits of the left action of G on X. These are r-invariant subsets of X, and each $(X_i, r_i), 1 \leq i \leq t$, where r_i is the restriction $r_i = r_{|X_i \times X_i}$, is also square-free symmetric sets.

For each $i, 1 \leq i \leq t$, we denote by $\mathcal{G}_i$ the subgroups of $\mathrm{Sym}(X_i)$ generated by the set of all restrictions $\mathcal{L}_{x|X_i}$:

$$\mathcal{G}_i = {}_{gr}\langle \mathcal{L}_{x|X_i} \mid x \in X \rangle$$

Note that $\mathcal{G}_i$ acts transitively on X_i for $1 \leq i \leq t$. In general $\mathcal{G}_i$ is not a subgroup of $\mathcal{G}$. Rather, there are canonical group surjections $\mathcal{G} \to \mathcal{G}_i$ of restriction to X_i and a canonical inclusion $\mathcal{G} \subseteq \prod_{1 \leq i \leq t} \mathcal{G}_i$.

The notions of retraction of symmetric sets and multipermutation solutions were introduced in the general case in [ESS], where (X,r) is not necessarily finite, or square-free. In [GI], [GIM1], [GIM2] are studied especially the multipermutation square-free solutions of finite order, we recall some notions and results. Let (X,r) be a nondegenerate symmetric set. An equivalence relation $\sim$ is defined on X as

$$x \sim y \quad \textit{iff} \quad \mathcal{L}_x = \mathcal{L}_y.$$

In this case we also have $\mathcal{R}_x = \mathcal{R}_y$,

We denote by $[x]$ the equivalence class of $x \in X$, $[X] = X/_\sim$ is the set of equivalence classes.

Lemma 2.11. [GIM1] *Let (X,r) be a nondegenerate symmetric set.*

(1) *The left and the right actions of X onto itself induce naturally left and right actions on the retraction $[X]$, via*

$$^{[\alpha]}[x] := [^{\alpha}x] \quad [\alpha]^{[x]} := [\alpha^x], \textit{ for all } \alpha, x \in X.$$

(2) *The new actions (as usual) define a canonical map $r_{[X]} : [X] \times [X] \longrightarrow [X] \times [X]$ where $r_{[X]}([x],[y]) = ({}^{[x]}[y], [x]^{[y]})$.*
(3) *$([X], r_{[X]})$ is a nondegenerate symmetric set. Furthermore,*
(4) *(X,r) cyclic $\Longrightarrow$ $([X], r_{[X]})$ cyclic.*
(5) *(X,r) is **lri** $\Longrightarrow$ $([X], r_{[X]})$ is **lri**.*
(6) *(X,r) square-free $\Longrightarrow$ $([X], r_{[X]})$ square-free.*

Definition 2.12. [ESS] The solution $Ret(X,r) = ([X],[r])$ is called the *retraction of* (X,r). For all integers $m \geq 1$, $Ret^m(X,r)$ is defined recursively as $Ret^m(X,r) = Ret(Ret^{m-1}(X,r))$.

(X,r) is *a multipermutation solution of level* m, if m is the minimal number (if any), such that $Ret^m(X,r)$ is the trivial solution on a set of one element. In this case we write $mpl(X,r) = m$. By definition (X,r) is *a multipermutation solution of level* 0 *iff* X is a one element set.

The following conjecture was made by the first author in 2004.

Conjecture 2.13. [GI]

(1) *Every nondegenerate square-free symmetric set (X, r) of finite order is retractable.*
(2) *Every nondegenerate square-free symmetric set (X, r) of finite order n is a multipermutation solution, with $mpl(X, r) < n$.*

A more recent conjecture states

Conjecture 2.14. [GI08] *Suppose (X, r) is a nondegenerate square-free multipermutation solution of finite order n. Then $mpl(X) < \log_2 n$.*

Evidence for this conjecture and more recent results on multipermutation square-free symmetric sets in the general case can be found in [CGI].

The following results are of significant importance for our paper and can be deduced from the results in [GIM2]. We give a sketch of the proofs

Proposition 2.15. *Let (X, r) be a nondegenerate square-free symmetric set of finite order, $X_i, 1 \leq i \leq t$ the set of all $G(X, r)$-orbits in X enumerated so that $X_1, \cdots, X_{t_0}$ is the set of all nontrivial orbits (if any). Then the following are equivalent.*

(1) *(X, r) is a multipermutation solution of level 2*
(2) *$t_0 \geq 1$ and for each $j, 1 \leq j \leq t_0$, $x, y \in X_j$ implies $\mathcal{L}_x = \mathcal{L}_y$.*
(3) *$t_0 \geq 1$ and for each $x \in X$ the permutation $\mathcal{L}_x$ is an r-automorphism, i.e. $\mathcal{G}(X, r) \subseteq Aut(X, r)$.*

Proof. If there are no nontrivial orbits then $mpl(X, r) = 1$ since all elements act the same way, i.e. $([X], r_{[X]})$ is the 1-element solution. Assuming $t_0 \geq 1$, $mpl(X, r) = 2$ means $mpl([X], r_{[X]}) = 1$, which means $[^x y] = [y]$ for all $x, y \in X$, i.e.

$$\mathcal{L}_y = \mathcal{L}_{^x y}, \quad \forall x, y \in X. \tag{2.5}$$

Note that for every pair $x, y \in X$, x, y belong to the same orbit X_i *iff* $y = \mathcal{L}_u(x)$, for some $u \in S(X, r)$. This gives (2.5) $\iff$ (2). Meanwhile, [GIM2, Lemma 2.7] provides (2.5) $\iff$ (3). □

Theorem 2.16. *Let (X, r) be a nondegenerate square-free symmetric set of multipermutation level 2 and finite order, and X_i orbits as in Proposition 2.15. Let $(X_i, r_i), 1 \leq i \leq t$ be the restricted solution. Then:*

(1) *$\mathcal{G}(X, r)$ is a nontrivial abelian group.*
(2) *Each $(X_i, r_i), 1 \leq i \leq t_0$ is a trivial solution. Clearly in the case $t_0 < t$, each (X_j, r_j), with $t_0 \leq j \leq t$ is a one element solution.*
(3) *For any ordered pair $i, j, 1 \leq i \leq t_0, 1 \leq j \leq t$, such that X_j acts nontrivially on X_i, every $x \in X_j$ acts via the same permutation $\sigma_i^j \in \mathrm{Sym}(X_i)$ which is a product of disjoint cycles of equal length $d = d_i^j$*

$$\sigma_i^j = (x_1 \cdots x_d)(y_1 \cdots y_d) \cdots (z_1 \cdots z_d),$$

where each element of X_i occurs exactly once. Here d_i^j is an invariant of the pair X_j, X_i.

(4) X *is* a strong twisted union $X = X_1 \natural X_2 \natural \cdots \natural X_t$, *(see the definition in* [GIM1]*).*

Proof. The proof of part (1) is given immediately following [GIM2, Lemma 5.25]. Briefly, write (2.5) as $\mathcal{L}_y = \mathcal{L}_{y^x}$ for all x, y using **lri** (see Fact 2.9), and then use **l1**. By Proposition 2.15(2) and (X, r) square-free one has ${}^y x = {}^x x = x$, for all $x, y \in X_i$ which implies part (2) here. The implication $mpl(X, r) = 2 \Longrightarrow$ (3) can be read off from [GIM2, Thms. 5.22, 5.24]. The reader can deduce it also from Proposition 2.15(2) and the fact that $\mathcal{G}$ is an abelian group of permutations acting transitively on each orbit X_i. $mpl(X, r) = 2 \Longleftrightarrow$ (4) follows from [GIM2, Thm. 5.24]. □

We note that the converse to part (1) stated in [GIM2, Thm. 5.24] is incorrect (there was a gap in the proof in this direction). Indeed, $\mathcal{G}$ a nontrivial abelian group does not require multipermutation level 2, see [CGI] for an example.

3. Representations of finite abelian groups and diagonalization over $\mathbb{C}$

In this section we shall recall some facts from representation theory of finite abelian groups. $\mathbb{C}^\times$ will denote the multiplicative group of nonzero complex numbers. C_p will denote a cyclic group of finite order p, where p is a positive integer. We shall write also $C_p = \langle u \rangle$ to denote that C_p is generated by u. A will denote an abelian group of finite order N. We recall some facts, from the representation theory of finite abelian groups, which can be extracted from the literature, see for example [C08] and [C].

Theorem 3.1. *Let A be a finite abelian group. Then*

$$A = C_{p_1} \times C_{p_2} \times \cdots \times C_{p_s}, \tag{3.1}$$

where $p_1 \cdots, p_s$ are positive integers, $p_i \mid p_{i+1}$, for $1 \leq i \leq s-1$.

It is not difficult to verify that the integer s in the presentation (3.1) is *minimal* with the property that A can be presented as a direct product of s cyclic groups. In addition the condition that p_i divides p_{i+1}, for $1 \leq i \leq s-1$ guarantees that the presentation (3.1) is unique, so Theorem 3.1 is a stronger version of the *Basis theorem for abelian groups*, (where originally the condition $p_i \mid p_{i+1}$, is not imposed) see [D].

We choose a set of generators

$$\mathbb{B} = \{u_1, \cdots, u_s\} \tag{3.2}$$

where $C_{p_i} = \langle u_i \rangle, 1 \leq i \leq s$. Every element $a \in A$ can be presented as

$$a = u_1^{m_1} u_2^{m_2} \cdots u_s^{m_s}, \quad \text{with} \quad 0 \leq m_i \leq p_i - 1, \quad \forall i, 1 \leq i \leq s. \tag{3.3}$$

where the multi-index s-tuple $\mathbf{m} = (m_1, m_2, \ldots, m_s)$ is uniquely determined by a and we refer to it as the *coordinates of a with respect to* $\mathbb{B}$. Here $\mathbb{B}$ is called *a basis for the abelian group A*. If we consider A as a $\mathbb{Z}$-module, with operation $+$, then $\mathbb{B}$ behaves as a free-module basis.

Denote by $\Lambda = \Lambda(A)$ the multi-indexing set

$$\Lambda = \{\mathbf{m} = (m_1, m_2, \cdots, m_s) \mid 0 \leq m_i \leq p_i - 1, \quad 1 \leq i \leq s\} \tag{3.4}$$

Clearly, $\mid \Lambda \mid = \mid A \mid = N$. Note that, in general, the choice of $\mathbb{B}$ is not unique, but Λ is uniquelly determined by the presentation (3.1).

In the setting of finite abelian grous the notion of a character is simple and pleasant to work with. As a reference one can use for example [C]. We recall some basic definitions and results.

Definition 3.2. In the context of abelian groups and for our purposes, a *character* χ on an abelian group A can be defined simply as a group homomorphism $\chi : A \to \mathbb{C}^\times$, i.e. as a 1-dimensional representation.

Note that these are *irreducible characters* from the point of view of the general theory (and that in general a character on an arbitrary group is defined as the trace of a representation). We will not need the general theory here.

Since A is a finite group of order N, then every $a \in A$, satisfies $a^N = 1$, so $\chi(a^N) = \chi(a)^N = 1$, therefore $\chi(a)$ is a root of unity of order dividing N.

The set A^* of (irreducible) characters is a group called the dual of A. Suppose p is a positive integer, $C_p = \langle g \rangle$. Let θ be a primitive p-th root of unity. Then the dual C_p^* is itself a cyclic group of order p generated by the character $\chi^{(p)}$, with $\chi^{(p)}(g) = \theta$, so $C_p^* \cong C_p$. In this case every character χ is a group homomorphism

$$C_p \to \langle \theta \rangle.$$

More generally, if A is a finite abelian group, presented as (3.1), then

$$A^* = C_{p_1}^* \times C_{p_2}^* \times \cdots \times C_{p_s}^* \cong C_{p_1} \times C_{p_2} \times \cdots \times C_{p_s} = A. \tag{3.5}$$

Note that the isomorphism $A^* \cong A$ is not canonical, since it depends on the decomposition of A as a direct product and on the choice of primitive p_k-th roots of unity θ_k for each $1 \leq k \leq s$. Once this choice is made, we can use our same indexing set Λ to label elements of A^*:

$$\chi(u_k) = \theta_k^{\eta_k} \tag{3.6}$$

where $\eta = (\eta_1, \cdots, \eta_s) \in \Lambda$ denotes the s-tuple of coordinates of $\chi = \chi_\eta$.

Suppose now that $A \subseteq \mathrm{Sym}(Z)$ is an abelian group of permutations acting *transitively* on a finite set Z. Under the assumptions and notations as above, we recall some elementary properties which will be useful for our results, see [C], [C08].

Fact 3.3. (1) *For every $x \in Z$ the stabilizer* $\mathrm{Stab}(x)$ *is the identity permutation $e = \mathrm{id}_Z$.*

(2) *Let $x_1 \in Z$, then the map $A \longrightarrow Z$ defined as $A \ni \pi \mapsto \pi(x_1)$ is a bijection. Therefore we can consider Z as the set*

$$Z = \{\pi(x_1) \mid \pi \in A\}$$

In particular,

$$\mid Z \mid = \mid A \mid = N = \prod_{1 \leq k \leq s} p_k$$

Fix an arbitrary $x_1 \in Z$. We know that its stabilizer is trivial. An arbitrary $z \in X$, can be presented as $z = \pi(x_1)$, for some $\pi \in A$, since the group A acts transitively on X. This permutation π is uniquely determined by z, indeed $\pi(x_1) = \rho(x_1)$ implies $\rho^{-1}\pi(x_1) = x_1$, and therefore $\rho^{-1}\pi \in \mathrm{Stab}(x_1) = \{e\}$. Hence $\rho = \pi$. Hence there is a 1-1 correspondence between Z and A provided by $z = \pi(x_1)$. Hence the coordinates $\mathbf{m} = \mathbf{m}_\pi = (m_1, \cdots, m_s)$ of $\pi \in A$ in our basis can also be viewed as coordinates of the corresponding element

$$Z = \{x_{\mathbf{m}} \mid \mathbf{m} \in \Lambda\}; \quad x_{\mathbf{m}_\pi} = \pi(x_1)$$

In this way the set Λ also indexes elements of Z.

Finally, we often use $N \times N$ permutation matrices, so it will be convenient to order Λ linearly. This induces an enumeration of A, A^*, Z as we have seen. Let $<$ be the lexicographic order on Λ. $<$ is a linear ordering on a finite set, so we can enumerate Λ accordingly,

$$\mathbf{m}^{(1)} = (0, \cdots, 0) < \mathbf{m}^{(2)} = (1, \cdots, 0) < \cdots < \mathbf{m}^{(N)} = (p_1 - 1, \cdots, p_s - 1).$$

We can then refer to our enumerated elements by their position. Thus

$$x_j = x_{\mathbf{m}^{(j)}} = \pi_j(x_1), \quad \chi_j(u_k) = \theta_k^{m_k^{(j)}} \tag{3.7}$$

where $\mathbf{m}^{(j)} = (m_1^{(j)}, \cdots, m_s^{(j)})$. Clearly, this is equivalent to our previous multi-index enumeration, and one has $x_1 < x_2 < \cdots x_N$ as the induced ordering on Z.

Let V be the N dimensional $\mathbb{C}$-vector space spanned by Z. Then the action of each permutation $\pi \in A$ on Z can be extended to linear automorphism T_π of V and the action of A on Z canonically extends to action of the group algebra $\mathbb{C}A$ on V. This induces a matrix representation of A via permutation matrices.

Let $P = P(\pi)$ be the matrix of the automorphism T_π. w.r.t. the basis $Z = \{x_1, x_2, \cdots, x_N\}$. Then P is a permutation matrix with entries

$$P_{ij} = \begin{cases} 1 & \text{if} \quad \pi x_i = x_j \\ 0 & \text{else} \end{cases}$$

As usual, $\overline{\theta}$ denotes the complex conjugate of $\theta \in \mathbb{C}$.

Theorem 3.4. *In notation as above, suppose χ is an irreducible character of A. Then*

$$y_\chi = \sum_{1 \le i \le N} \overline{\chi(\pi_i)} x_i \tag{3.8}$$

is a simultaneous eigenvector for all $\rho \in A$. More precisely, there is an equality

$$P(\rho) y_\chi = \chi(\rho) y_\chi. \tag{3.9}$$

Proof. We know that for all $\pi \in A$, $\theta = \chi(\pi) \in \mathbb{C}$ is a root of unity, thus $\theta\overline{\theta} = 1$, and $\overline{\theta} = \theta^{-1}$. This implies

$$\overline{\chi(\pi)} = (\chi(\pi))^{-1} = \chi(\pi^{-1}). \tag{3.10}$$

Now we use (3.7), (3.10) to present y_χ as

$$y_\chi = \sum_{1 \le i \le N} \overline{\chi(\pi_i)} x_i = \sum_{1 \le i \le N} \chi(\pi_i^{-1}) \pi_i(x_1) \tag{3.11}$$

For each $i, 1 \leq i \leq N$ we set $\rho\pi_i = \sigma_i$. Then

$$\pi_i^{-1} = \sigma_i^{-1}\rho \quad \chi(\pi_i^{-1}) = \chi(\sigma_i^{-1})\chi(\rho) \tag{3.12}$$

We apply (3.10) and (3.12) to deduce the equalities

$$\begin{aligned} P(\rho)y_\chi &= P(\rho).\textstyle\sum_{1\leq i\leq N}\chi(\pi_i^{-1})\pi_i(x_1) \\ &= \quad \textstyle\sum_{1\leq i\leq N}\chi(\pi_i^{-1})\rho\pi_i(x_1) \\ &= \textstyle\sum_{1\leq i\leq N}[\chi(\sigma_i^{-1})\chi(\rho)]\sigma_i(x_1) \\ &= \chi(\rho)\textstyle\sum_{1\leq i\leq N}\chi(\sigma_i^{-1})\sigma_i(x_1) \\ &= \qquad \chi(\rho)y_\chi \end{aligned} \tag{3.13}$$

The last equality follows from the equalities of sets

$$\{\sigma_i, 1 \leq i \leq N\} = \{\pi_i, 1 \leq i \leq N\}.$$

□

4. Complete Datum of multipermutation solution of level two and explicit formulae for the diagonlization

In this section (X, r) denotes a finite nondegenerate square-free symmetric set of multipermutation level 2. We shall use the notation of Section 2. As usual $G = G(X, r)$, $S = S(X, r)$ and $\mathcal{G} = \mathcal{G}(X, r)$, are respectively the associated YB group, YB monoid, and the permutation group of (X, r). $X_1, \cdots, X_t$ are the G-orbits or equivalently the $\mathcal{G}$-orbits in X.

By the Decomposition Theorem [R], $t \geq 2$. By Proposition 2.15 there is at least one nontrivial orbit X_i, and we enumerate the orbits so that $X_1 \cdots X_{t_0}$ is the set of all nontrivial orbits in X $(1 \leq t_0 \leq t)$. The restrictions (X_i, r_i) $1 \leq i \leq t_0$ are trivial solutions and all elements $x \in X_i$ are equivalent. In the case when $t_0 < t$, (X_i, r_i) are one element solutions for all $t_0 < i \leq t$.

We recall from Section 2 that for $1 \leq i \leq t$, $\mathcal{G}_i$ is the subgroup of $\mathrm{Sym}(X_i)$ generated by the set $\{\mathcal{L}_{x|X_i} \mid x \in X\}$. As sets we also have

$$\mathcal{G}_i = \{\mathcal{L}_{u|X_i} \mid u \in G(X, r)\} = \mathcal{G}_{|X_i}.$$

The $\mathcal{G}_i$ are 1-element groups for $t_0 < i \leq t$.

Remark 4.1. By Remark 2.7 every element g of $\mathcal{G}$ (respectively of $\mathcal{G}_i$) has a presentation as $g = \mathcal{L}_u, u \in S$ (respectively as $g = \mathcal{L}_{u|X_i}, u \in S$).

Under our assumption the group $\mathcal{G}$ is abelian. Hence each $\mathcal{G}_i$ is an abelian group of permutations acting transitively on X_i, $1 \leq i \leq t_0$. It is known, see Section 3, that in this case there is an equality of orders $\mid \mathcal{G}_i \mid = \mid X_i \mid$.

We shall use the results of the previous section (adjusted to our concrete notation for the left actions). In particular, for each $i, 1 \leq i \leq t_0$, $\mathcal{G}_i$ is a direct product of cyclic subgroups (see Theorem 3.1)

$$\mathcal{G}_i = (\mathcal{L}_{u_{i1}|X_i}) \times (\mathcal{L}_{u_{i2}|X_i}) \times \cdots \times (\mathcal{L}_{u_{is_i}|X_i}), \tag{4.1}$$

where for $1 \leq k \leq s_i$, the orders p_{ik} of $\mathcal{L}_{u_{ik}|X_i}$ satisfy

$$p_{ik} \mid p_{ik+1}, \quad 1 \leq k \leq s_i - 1. \tag{4.2}$$

Moreover, for each $i, 1 \leq i \leq t_0$, s_i, is the least integer such that $\mathcal{G}_i$ is generated by s_i elements, and by the above remark we can without loss of generality choose all $u_{ik} \in S = S(X, r), 1 \leq k \leq s_i$ (but not necessarily $u_{ij} \in X$.) The integer s_i and the finite sequence $p_{i1}, \cdots, p_{is_i}$ in (4.1), (4.2) are invariants of the data (X_i, r) and are uniquelly determined for each $i, 1 \leq i \leq t_0$. Note that the set $\{\mathcal{L}_{x|X_i} \mid x \in X\}$ generates the group $\mathcal{G}_i$, but it is not necessarily a minimal set of generators.

Definition 4.2. For $1 \leq i \leq t_0$ we fix a presentation as in (4.1). We call the set $\mathbb{B}_i = \{u_{i1}, \cdots, u_{is_i}\}$ *a basis of labels for* $\mathcal{G}_i$. We shall assume that $u_{ik} \in S, 1 \leq k \leq s_i$ (see Remark 4.1).

We know that each $g \in \mathcal{G}_i$ has a unique presentation in terms of the basis elements:

$$g = \prod_{1 \leq k \leq s_i} (\mathcal{L}_{u_{ik}|X_i})^{m_{g,k}}, \quad \text{where} \quad 0 \leq m_{g,k} \leq p_{ik} - 1. \tag{4.3}$$

Definition 4.3. We call the s_i-tuple $\mathbf{m_g} = (\mathbf{m_{g,1}}, \cdots, \mathbf{m_{g,s_i}})$ the *coordinates of* $g \in \mathcal{G}_i$.

Consider the vector spaces $V = \mathrm{Span}_{\mathbb{C}} X$, $V_i = \mathrm{Span}_{\mathbb{C}} X_i, 1 \leq i \leq t$. Clearly (since X is a basis of V), for each $u \in S$ the map $\mathcal{L}_u \in \mathrm{Sym}(X)$ extends canonically to a linear automorphism on V, denoted $\tilde{\mathcal{L}}_u$. It is a standard fact that these can be extended to representations of the group algebra $\mathbb{C}\mathcal{G}$ on $V = SpanX$, and since each $V_i, 1 \leq i \leq s$ is invariant, this representation canonically induces representations of $\mathbb{C}\mathcal{G}_i$ on V_i.

We shall apply the results of the previous section to find a basis Y_i of V_i , $1 \leq i \leq t_0$ on which $\mathcal{G}_i$ acts diagonally. In the cases $t_0 < j \leq t$ we simply set $Y_j = X_j$. Then, clearly, the set $Y = \bigcup_{1 \leq i \leq t} Y_i$ is a basis of V on which the group $\mathcal{G}$ acts diagonally.

To each multipermutation solution (X, r) with $mpl(X, r) = 2$ and in notation as above, we associated the following datum $\mathbb{D}$ below. The results Theorems 4.7, 4.9, and Corollary 4.8 will give: i) Explicit coordinates of a new basis Y_i w.r.t initial basis X_i of $\mathbb{C}X_i$ in terms of the datum $\mathbb{D}$. The new basis will have the feature that the linear solution R associated to r is diagonal. ii) Explicitly presented form of the diagonal coefficients of R.

Definition 4.4. For $1 \leq i \leq t_0$, we define *the complete datum* $\mathbb{D}_i$ *of* X_i as $(X_i, \mathbb{B}_i, \mathcal{P}_i, \Theta^i, \mathcal{M}_i)$ where:

(1) $\mathbb{B}_i = \{u_{i1}, \cdots, u_{is_i}\}$ is a basis as in Definition 4.2.
(2) $\mathcal{P}_i = \{p_{i1}, \cdots, p_{is_i}\}$, where p_{ik} is the order of $\mathcal{L}_{u_{ik}|X_i}, 1 \leq k \leq s_i$. Note that
$$N_i = p_{i1} \cdots p_{is_i} = \mid X_i \mid = \mid \mathcal{G}_i \mid$$
by the results of the previous section.

(3) $\Theta^i = \{\theta_{i1}, \cdots, \theta_{is_i}\}$ where θ_i is a chosen primitive p_{is_i}–th root of unity and

$$\theta_{ik} = (\theta_i)^{\frac{p_{is_i}}{p_{ik}}}, \quad 1 \leq k \leq s_i.$$

Clearly, each θ_{ik} is a primitive p_{ik}–th root of unity.

(4) $\mathcal{M}_i = \{\mathbf{m}_i^j \mid 1 \leq j \leq t\}$ where $\mathbf{m}_i^j = (m_{i1}^j, \cdots, m_{is_i}^j)$ denotes the coordinates in our basis of the element $\sigma_i^j \in \mathcal{G}_i$ for the action of any element of X_j on X_i (see Theorem 2.16).

(5) $\mathbb{D} = \mathbb{D}(X, r) = (\mathbb{D}_1, \cdots, \mathbb{D}_t)$ is *a complete datum of* (X, r).

In the particular case, when $i > t_0$, i.e. X_i is a one element set and (for completeness) we define $\mathbb{D}_i = (X_i, \{1\}, \{1\}, \{1\}, \{1\})$.

From the $\mathcal{P}_i$ part of the datum for each i, $1 \leq i \leq t$, we also have an associated space

$$\Lambda_i = \{\mathbf{m} = (m_1, \cdots, m_{s_i}) \mid 0 \leq m_k \leq p_{ik} - 1,\ 1 \leq k \leq s_i\}$$

for the range of coordinates in our basis $\mathbb{B}_i$. Clearly, $\mid \Lambda_i \mid = N_i$. Every element of $\mathcal{G}_i$ can be written with coordinates $\mathbf{m}_g \in \Lambda_i$ as in Definition 4.3. As explained in Section 3 this induces also coordinates on X_i once we fix an element $x_{i1} \in X_i$, and it induces coordinates for $\mathcal{G}_i^*$ given the data Θ^i. Thus, given $\eta = (\eta_1, \cdots, \eta_{s_i}) \in \Lambda_i$ the corresponding character is

$$\chi(\mathcal{L}_{u_{i1}|X_i}) = \theta_{i1}^{\eta_1}, \quad \chi(\mathcal{L}_{u_{i2}|X_i}) = \theta_{i2}^{\eta_2}, \quad \cdots, \quad \chi(\mathcal{L}_{u_{is_i}|X_i}) = \theta_{is_i}^{\eta_{s_i}} \tag{4.4}$$

Notation 4.5. Let $\eta \in \Lambda_i$, and $\chi_\eta \in \mathcal{G}_i^*$ the corresponding character as in 4.4. The simultaneous eigenvector vector y_{χ_η}, see Theorem 3.4 and (3.8), will be denoted y_η^i.

Finally, in order to have explicit formulae, we enumerate Λ_i as in Section 3. We enumerate the corresponding elements of $\mathcal{G}_i$ as $\mathrm{id} = \pi_1 < \cdots < \pi_{N_i}$ and the elements of X_i as $x_{i1} < x_{i2} < \cdots < x_{iN_i}$. As in the proof of Theorem 3.4 we then have explicitly

$$y_\eta^i = y_{\chi_\eta} = \sum_{1 \leq j \leq N_i} \chi_\eta(\pi_j^{-1}) x_{ij} \tag{4.5}$$

for the explicit change from a basis X_i to the new basis $Y_i = \{y_\eta^i \mid \eta \in \Lambda_i\}$. Here $x_{ij} = \pi_j(x_{i1})$. We can also write this formula as a sum over $\pi \in \mathcal{G}_i$ (without enumeration).

Lemma 4.6. *In notation and enumeration as above, let* $\eta = (\eta_1, \cdots, \eta_{s_i}) \in \Lambda_i$. *Denote*

$$\lambda_1 = (\theta_{i1})^{\eta_1}, \quad \lambda_2 = (\theta_{i2})^{\eta_2}, \cdots, \quad \lambda_{s_i} = (\theta_{is_i})^{\eta_{s_i}}.$$

The simultaneous eigenvector y^i_η has the following explicit coordinates with respect to the basis X_i (given in the form of a vertical "block-vector"):

$$y^i_\eta = \left[\begin{array}{c} (\lambda_{s_i})^{p_{is_i}-1}B_{s_i-1} \\ \hline \vdots \\ \hline (\lambda_{s_i})^2 B_{s_i-1} \\ \hline (\lambda_{s_i})B_{s_i-1} \\ \hline B_{s_i-1} \end{array}\right], \tag{4.6}$$

where the vectors B_k are determined recursively as follows.

$$B_1 = \left[\begin{array}{c} \lambda_1^{p_{i1}-1} \\ \vdots \\ \lambda_1^2 \\ \lambda_1 \\ 1 \end{array}\right],$$

and for $2 \leq k \leq s_i$, one has

$$B_k = \left[\begin{array}{c} (\lambda_k)^{p_{ik}-1}B_{k-1} \\ \hline \vdots \\ \hline (\lambda_k)^2 B_{k-1} \\ \hline \lambda_k B_{k-1} \\ \hline B_{k-1} \end{array}\right]$$

In particular, for $\eta^1 = (0, 0, \cdots, 0)$ one has

$$y^i_{\eta^1} = \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{bmatrix},$$

The following theorem is mainly an elaboration of Theorem 3.4 in terms of the fixed datum and the enumeration of X induced from the action of $\mathcal{G}$.

Theorem 4.7. *Let (X, r) be a finite nondegenerate square-free symmetric set and notations as in Section 2. We assume that (X, r) is a nontrivial solution. Let $V = \mathbb{C}X = \oplus_i V_i$ where $V_i = \mathbb{C}X_i$. Then*

1. *The left action of of the finite group $\mathcal{G}$ on X, extends canonically to a representation of the group algebra $\mathbb{C}\mathcal{G}$ on V. Each $V_i, 1 \leq i \leq t$, is invariant under this representation. Moreover, suppose there exists a basis Y of V on which $\mathcal{G}$ acts diagonally. Then $\mathcal{G}$ is abelian.*
2. *Suppose that (X, r) has $mpl(X, r) = 2$ and datum $\mathbb{D}$. Then:*
   (a) *The set $Y_i = \{y^i_\eta \mid \eta \in \Lambda_i\}$ is a basis of V_i on which $\mathcal{G}_i$ acts diagonally. The set $Y = \bigcup Y_i$, is a basis of V on which the group $\mathcal{G}$ acts diagonally.*
   (b) *The elements of Y_i are simultaneous eigenvectors of all $g \in \mathcal{G}_i$, with eigenvalues $\mu^g_{i,\eta}$ determined from the coordinates $\mathbf{m}_g$,*

$$g.y^i_\eta = \mu^g_{i,\eta} y^i_\eta, \quad \mu^g_{i,\eta} = \chi_\eta(g) = \prod_{1 \leq k \leq s_i} (\theta^{\eta_k}_{ik})^{m_{g,k}}. \tag{4.7}$$

Proof. Part (1) collects some classical facts. Note that by its definition as a subgroup of $\mathrm{Sym}(X)$, the group $\mathcal{G}$ acts faithfully on V. In the basis Y the matrices for the elements of $\mathcal{G}$, being diagonal, all commute. Since they also form a faithful representation, the group $\mathcal{G}$ must be abelian. Part (2) is an elaboration of Theorem 3.4 in the present context. □

The next corollary follows straightforwardly from Theorem 4.7. Using direct information from the datum $\mathbb{D}$ it gives explicitly the coefficients which occur in the Main Theorem 4.9.

Recall that each ordered pair X_j, X_i defines uniquely the s_i-tuple $\mathbf{m}^j_i = (m^j_{i,1}, \cdots, m^j_{i,s_i}) \in \mathcal{M}_i$. (These are the coordinates of any element $\mathcal{L}_{x|X_i}$ when $x \in X_j$).

Corollary 4.8. *In the hypothesis of Theorem 4.7. Let i, j be integers $1 \leq i, j \leq t$. Then all $x \in X_j$ act in the same way as*

$$\mathcal{L}_x y^i_\eta = \mu^j_{i,\eta} y^i_\eta; \quad \mu^j_{i,\eta} = \chi_\eta(\sigma^j_i) = \prod_{1 \leq k \leq s_i} (\theta^{\eta_k}_{ik})^{m^j_{i,k}}. \tag{4.8}$$

where $\mathbf{m}^j_i \in \mathcal{M}_i$ is from our datum. In particular, $\mu^j_{i,\eta} = 1$, whenever $j = i$, so

$$\mathcal{L}_x y^i_\eta = y^i_\eta, \quad \forall x \in X_i.$$

We are now ready to prove our main theorem.

Theorem 4.9. *Let (X, r) be a finite nondegenerate square-free symmetric set of order n, with $mpl(X, r) = 2$, and datum $\mathbb{D}$. For each $i, 1 \leq i \leq t$, let Y_i be the basis of V_i determined by Theorem 4.7. Then the linear extension $R : V \otimes V \longrightarrow V \otimes V$, of the solution r to kX has the form*

$$R(y^i_\eta \otimes y^j_\zeta) = \frac{\mu^i_{j,\zeta}}{\mu^j_{i,\eta}}\, y^i_\eta \otimes y^j_\zeta.$$

Proof. Note first that as a linear extension of the map r, the automorphism R satisfies

$$R(z \otimes x) = {}^z x \otimes z^x. \tag{4.9}$$

Note also that since **lri** holds, action from the right is inverse to action from the left, and that under our assumptions this left action has the form ${}^z x = \sigma^j_i(x)$ if $z \in X_j$ and $x \in X_i$. Hence we merely need to compute

$$\begin{aligned}
R(y^i_\eta \otimes y^j_\zeta) &= \sum_{\substack{\pi\in\mathcal{G}_i\\ \rho\in\mathcal{G}_j}} \chi_\eta(\pi^{-1})\chi_\zeta(\rho^{-1}) R(\pi(x_{i1}) \otimes \rho(x_{j1})) \\
&= \sum_{\substack{\pi\in\mathcal{G}_i\\ \rho\in\mathcal{G}_j}} \chi_\eta(\pi^{-1})\chi_\zeta(\rho^{-1})\ {}^{\pi(x_{i1})}\rho(x_{j1}) \otimes \pi(x_{i1})^{\rho(x_{j1})} \\
&= \sum_{\substack{\pi\in\mathcal{G}_i\\ \rho\in\mathcal{G}_j}} \chi_\eta(\pi^{-1})\chi_\zeta(\rho^{-1})(\sigma^i_j\rho)(x_{j1}) \otimes ((\sigma^j_i)^{-1}\pi)(x_{i1}) \\
&= \sum_{\substack{\pi'\in\mathcal{G}_i\\ \rho'\in\mathcal{G}_j}} \chi_\eta(\pi'^{-1}(\sigma^j_i)^{-1})\chi_\zeta(\rho'^{-1}\sigma^i_j)\rho'(x_{j1}) \otimes \pi'(x_{i1}) \\
&= \chi_\eta((\sigma^j_i)^{-1})\chi_\zeta(\sigma^i_j) \sum_{\substack{\pi'\in\mathcal{G}_i\\ \rho'\in\mathcal{G}_j}} \chi_\zeta(\rho'^{-1})\rho'(x_{j1}) \otimes \chi_\eta(\pi'^{-1})\pi'(x_{i1}) \\
&= \frac{\chi_\zeta(\sigma^i_j)}{\chi_\eta(\sigma^j_i)} y^j_\zeta \otimes y^i_\eta
\end{aligned}$$

where we use the definition (4.5) and linearity of R. We change the summation over π, ρ to summation over $\pi' = (\sigma^j_i)^{-1}\pi$ and $\rho' = \sigma^i_j\rho$ (if one runs over $\mathcal{G}_i$ and $\mathcal{G}_j$ respectively then so does the other). We then use that the characters are group homomorphisms, identifying the result as stated. □

We do not know if only $mpl(X, r) = 2$ solutions are diagonalisable in this way but in the next section we give an example in support of that conjecture as well as 'forward' examples of Theorem 4.9.

5. Worked out examples

In this section we illustrate the results on Section 4 on some nontrivial examples. The first example was suggested by Peter Cameron.

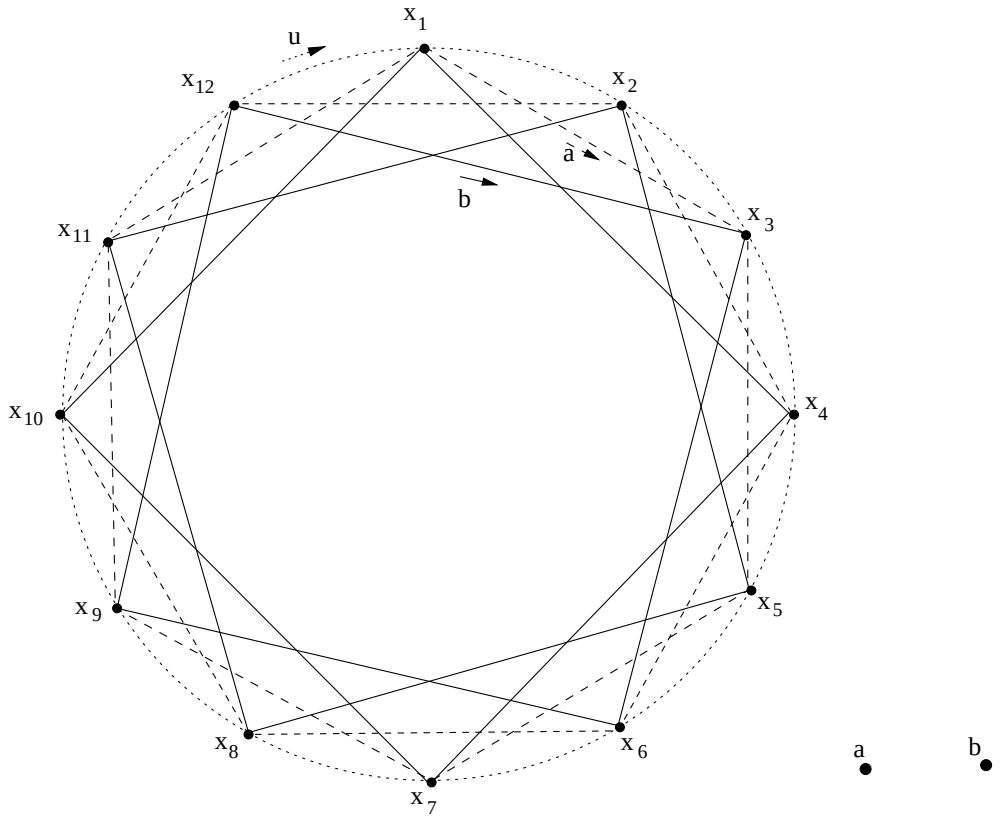

FIGURE 1. Graph for Example 5.1. Arrows show left actions on the set $X = \{x_1, \cdots x_{12}\} \cup \{a\} \cup \{b\}$.

Example 5.1. Let (X, r) be the square-free symmetric set defined as follows.

$$\begin{aligned} X &= \{x_1, x_2, \cdots, x_{12}, a, b\} \\ \mathcal{L}_a &= (x_1x_3x_5x_7x_9x_{11})(x_2x_4x_6x_8x_{10}x_{12}) \\ \mathcal{L}_b &= (x_1x_4x_7x_{10})(x_2x_5x_8x_{11})(x_3x_6x_9x_{12}) \\ \mathcal{L}_{x_i} &= \mathrm{id}_X \quad 1 \le i \le 12. \end{aligned}$$

The graph for this example is shown in Figure 1.

In this case $\mathcal{G} = {}_{gr}\langle \mathcal{L}_a, \mathcal{L}_b \rangle$, and X splits into 3 $\mathcal{G}$-orbits: $X_1 = \{x_i \mid 1 \le i \le 12\}$, $X_2 = \{a\}, X_3 = \{b\}$. Clearly, $\mathcal{G}_1 = \mathcal{G}$. Note that $(\mathcal{L}_a)^3 = (\mathcal{L}_b)^2$, so we can not present $\mathcal{G}_1$ as a direct product of the cyclic groups $\langle \mathcal{L}_a \rangle$ and $\langle \mathcal{L}_a \rangle$. One can use as a basis for $\mathcal{G}_1$ the element $u = a^2b^3$. More precisely,

$$\mathcal{G}_1 = \langle \mathcal{L}_u \rangle, \quad \mathcal{L}_a = (\mathcal{L}_u)^2, \quad \mathcal{L}_b = (\mathcal{L}_u)^3,$$

$\mathcal{L}_u = (x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}x_{11}x_{12})$ is a cycle of length 12. The datum $\mathbb{D}(X,r)$ is:

$$s_1 = 1, \quad \mathbb{B}_1 = \{u\}, \quad \mathcal{P}_1 = \{12\}$$

$$\Theta^1 = \{\theta\} \quad \text{where } \theta \text{ is a chosen primitive 12–th root of unity}$$

$$\mathcal{M}_1 = \{\mathbf{m}_1^2, \mathbf{m}_1^3\} \quad \text{where} \quad \mathbf{m}_1^2 = (2), \mathbf{m}_1^3 = (3)$$

$$\mathbb{D}_1 = (X_i, \mathbb{B}_1, \mathcal{P}_1, \Theta^1, \mathcal{M}_1),\ \mathbb{D}_2 = (X_2, \{1\}, \{1\}, \{1\}, \{1\}),\ \mathbb{D}_3 = (X_3, \{1\}, \{1\}, \{1\}, \{1\})$$

$$\mathbb{D} = \mathbb{D}(X,r) = (\mathbb{D}_1, \mathbb{D}_2, \mathbb{D}_3)$$

$$\Lambda_1 = \{k \mid 0 \leq k \leq 11\}$$

Here instead of $y_\eta^1, \eta \in \Lambda_1$ we shall simply write $y_k, 1 \leq k \leq 11$, $y_1^2 = a, y_1^3 = b$. Note that this enumeration agrees with our convention in Section 4. Then y_k, in coordinates with respect to the basis X_1 of V_1 and written as the transpose of a row vector is

$$y_k = \left[(\theta^k)^{11} \ \cdots \ (\theta^k)^2 \ \theta^k \ 1\right]^t$$

Furthermore, one has

$$R(a \otimes y_k) = \theta^{2k}\, y_k \otimes a, \quad R(b \otimes y_k) = \theta^{3k}\, y_k \otimes b$$

$$R(y_j \otimes y_k) = y_k \otimes y_j, \qquad R(a \otimes b) = b \otimes a, \quad \forall k, j, 1 \leq k, j \leq 12$$

Example 5.2. Let (X,r) be the square-free symmetric set defined as follows.

$$X = X_1 \bigcup X_2 \bigcup X_3, \qquad X_1 = \{a_i \mid 1 \leq i \leq 18\}$$

$$X_2 = \{b_j \mid 1 \leq j \leq 16\}, \quad X_3 = \{c_k \mid 1 \leq k \leq 8\}$$

The solution r is defined via the left actions:

$$\mathcal{L}_{a_i} = \tau.\upsilon, \quad 1 \leq i \leq 18; \quad \mathcal{L}_{b_j} = \rho.\omega, \quad 1 \leq j \leq 16; \quad \mathcal{L}_{c_k} = \pi.\sigma, \quad 1 \leq k \leq 8$$

where the permutations $\pi, \rho, \sigma, \tau, \upsilon, \omega$ are given below.

$$\pi = \pi_0\pi_1\pi_2\pi_3\pi_4\pi_5, \quad \text{where} \quad \pi_k = (a_{3k+1}\ a_{3k+2}\ a_{3k+3}), \qquad 0 \leq k \leq 5$$

$$\rho = \rho_1\rho_2\rho_3, \quad \text{where} \quad \rho_m = (a_m\ a_{m+3}\ a_{m+2.3}\ \cdots\ a_{m+5.3}), \quad 1 \leq m \leq 3$$

$$\tau = \tau_0\tau_1\tau_2\tau_3, \quad \text{where} \quad \tau_j = (b_{4k+1}\ b_{4k+2}\ b_{4k+3}\ b_{4k+4}), \qquad 0 \leq k \leq 3$$

$$\sigma = \sigma_1\sigma_2\sigma_3\sigma_4, \quad \text{where} \quad \sigma_m = (b_m\ b_{m+4}\ b_{m+2.4}\ b_{m+3.4}), \qquad 1 \leq m \leq 4$$

$$\upsilon = \upsilon_0\upsilon_1\upsilon_2\upsilon_3, \quad \text{where} \quad \upsilon_m = (c_{2k+1}\ c_{2k+2}), \qquad 0 \leq k \leq 3$$

$$\omega = \omega_1\omega_2, \quad \text{where} \quad \omega_m = (c_m\ c_{m+2}\ c_{m+2.2}\ c_{m+3.2}), \qquad 1 \leq m \leq 2$$

The graph for this example is given in Figure 2.

Clearly, $\mathcal{G} = {}_{gr}\langle \mathcal{L}_{a_1}, \mathcal{L}_{b_1}, \mathcal{L}_{c_1} \rangle$ and the $\mathcal{G}$-orbits in X are exactly X_1, X_2, X_3. This time each of the restricted groups $\mathcal{G}_i, 1 \leq \imath \leq 3$ is nontrivial and differs from $\mathcal{G}$.

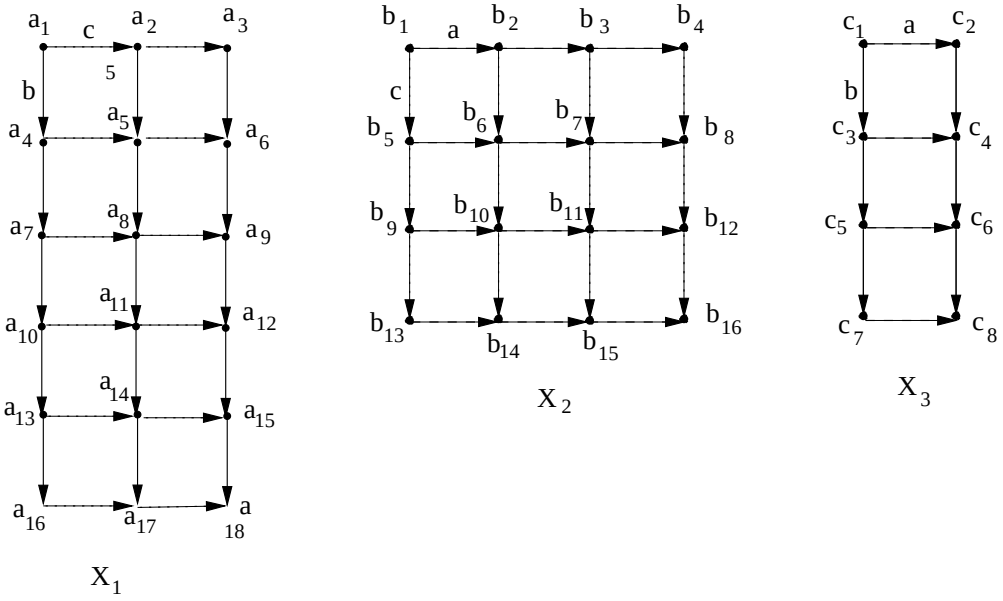

FIGURE 2. Graph for Example 5.2. Arrows show left actions on the set $X = X_1 \cup X_2 \cup X_3$.

More precisely, one has

$$\mathcal{L}_{a|X_1} = e, \quad \mathcal{L}_{b|X_1} = \rho, \quad \mathcal{L}_{c|X_1} = \pi, \quad \forall a \in X_1,\ b \in X_2,\ c \in X_3$$

$$\mathcal{G}_1 = \langle \pi \rangle \times \langle \rho \rangle, \quad \pi^3 = e, \quad \rho^6 = e.$$

In the usual notation one has:

$$s_1 = 2, \quad \mathbb{B}_1 = \{u_{11} = c_1, u_{12} = b_1\}, \quad \mathcal{P}_1 = \{3, 6\},$$

$$\Theta^1 = \{\theta_{11} = (\theta)^2, \theta_{12} = \theta\}, \quad \text{where } \theta \text{ is a chosen primitive 6–th root of unity,}$$

$$\mathcal{M}_1 = \{\mathbf{m}_1^2 = (0,1), \quad \mathbf{m}_1^3 = (1,0)\}, \quad \mathbb{D}_1 = (X_1, \mathbb{B}_1, \mathcal{P}_1, \Theta^1, \mathcal{M}_1);$$

$$\Lambda_1 = \{(\eta_1, \eta_2) \mid 0 \le \eta_1 \le 2, \quad 0 \le \eta_2 \le 5\}.$$

On X_2 one has

$$\mathcal{L}_{a|X_2} = \tau, \quad \mathcal{L}_{b|X_2} = e, \quad \mathcal{L}_{c|X_2} = \sigma, \quad \forall a \in X_1,\ b \in X_2,\ c \in X_3$$

$$\mathcal{G}_2 = \langle \tau \rangle \times \langle \sigma \rangle \quad \tau^4 = e \quad \sigma^4 = e$$

$$s_2 = 2 \quad \mathbb{B}_2 = \{u_{21} = a_1, u_{22} = c_1\}, \quad \mathcal{P}_2 = \{4, 4\}$$

$$\Theta^2 = \{\theta_{21} = i,\ \theta_{22} = i\} \quad \text{(here we chose as a primitive 4–th root of unity simply } i \in \mathbb{C})$$

$$\mathcal{M}_2 = \{\mathbf{m}_2^1 = (1,0), \quad \mathbf{m}_2^3 = (0,1)\} \quad \mathbb{D}_2 = (X_1, \mathbb{B}_2, \mathcal{P}_2, \Theta^2, \mathcal{M}_2);$$

$$\Lambda_2 = \{(\eta_1, \eta_2) \mid 0 \le \eta_1, \eta_2 \le 3\}$$

Finally,

$$\mathcal{L}_{a|X_3} = \upsilon, \quad \mathcal{L}_{b|X_3} = \omega, \quad \mathcal{L}_{c|X_3} = e, \quad \forall a \in X_1,\ b \in X_2,\ c \in X_3$$

$$\mathcal{G}_3 = \langle \upsilon \rangle \times \langle \omega \rangle, \quad \upsilon^2 = e, \quad \omega^4 = e$$

Furthermore,

$$s_3 = 2, \quad \mathbb{B}_3 = \{u_{31} = a_1, u_{32} = b_1\}, \quad \mathcal{P}_3 = \{2, 4\}$$

$$\Theta^3 = \{\theta_{31} = i^2 = -1, \theta_{32} = i\}$$

$$\mathcal{M}_3 = \{\mathbf{m}_3^1 = (1, 0), \quad \mathbf{m}_2^3 = (0, 1)\}$$

$$\mathbb{D}_3 = (X_3, \mathbb{B}_3, \mathcal{P}_3, \Theta^3, \mathcal{M}_3);$$

$$\Lambda_3 = \{(\eta_1, \eta_2) \mid 0 \leq \eta_1 \leq 1, 0 \leq \eta_2 \leq 3\}$$

$$\mathbb{D} = \mathbb{D}(X, r) = (\mathbb{D}_1, \mathbb{D}_2, \mathbb{D}_3)$$

We can compute all y_η^i, $1 \leq i \leq 3, \eta \in \Lambda_i$, via the recursive formulae in Lemma 4.6. For example, the 18 entries of $y_{(1,1)}^1$ written as a transposed row vector are

$$\begin{aligned} y_{(1,1)}^1 &= \left[\theta^5\theta^4\ \ \theta^5\theta^2\ \ \theta^5\ \ \theta^4\theta^4\ \ \theta^4\theta^2\ \ \theta^4\ \ \theta^3\theta^4\ \ \theta^3\theta^2\ \ \theta^3\ \ \theta^2\theta^4\ \ \theta^2\theta^2\ \ \theta^2\ \ \theta\theta^4\ \ \theta\theta^2\ \ \theta\ \ \theta^4\ \ \theta^2\ \ 1\right]^t \\ &= \left[\theta^3\ \ \theta\ \ \theta^5\ \ \theta^2\ \ 1\ \ \theta^4\ \ \theta\ \ \theta^5\ \ \theta^3\ \ 1\ \ \theta^4\ \ \theta^2\ \ \theta^5\ \ \theta^3\ \ \theta\ \ \theta^4\ \ \theta^2\ \ 1\right]^t \end{aligned}$$

The above two examples illustrate our main Theorem 4.9 as well as our explicit methods developed in Section 4. In the converse direction to Theorem 4.9, we can ask:

Question 5.3. *Suppose that (X, r) is a square-free nondegenerate symmetric set of finite order n, X_i orbits of $G(X, r)$, $V = \mathbb{C}X$ and $V_i = \mathbb{C}X_i$. Suppose that there exists a basis Y of V with $Y = \cup Y_i$, each Y_i a basis of V_i, such that the linear extension R of r has the form*

$$R(y_i \otimes y_j) = \mu_{ij} y_j \otimes y_i, 1 \leq i, j \leq n, \quad \mu_{ij} \in \mathbb{C}^\times.$$

Can we conclude that (X, r) is a multipermutation solution with $mpl(X, r) = 2$?

We provide an example in support of an affirmative answer here. This will be a square-free symmetric set (X, r) with $mpl(X, r) = 3$ for which it is impossible to find a new basis Y of the diagonal form stated. From the list of solutions of order ≤ 4 in [GI94] it is not difficult to verify that $|X| \leq 4$ implies that $mpl(X, r) \leq 2$, hence such an example must have order at least $|X| = 5$, see also [CGI]. A method for constructing higher permutation level examples is in [CGI] and we use one of these.

Example 5.4. [CGI] Let (X, r) be the square-free symmetric set of order 5 defined as follows.

$$X = \{x_1, x_2, x_3, x_4, a\}$$

$$\mathcal{L}_a = (x_1x_2x_3x_4), \quad \mathcal{L}_{x_1} = \mathcal{L}_{x_3} = (x_2x_4), \quad \mathcal{L}_{x_2} = \mathcal{L}_{x_4} = (x_1x_3)$$

$$\mathcal{G} = {}_{gr}\langle \mathcal{L}_a, \mathcal{L}_{x_1}, \mathcal{L}_{x_2} \rangle = {}_{gr}\langle \mathcal{L}_a, \mathcal{L}_{x_2} \rangle = {}_{gr}\langle (x_1x_2x_3x_4), (x_1x_3) \rangle \simeq D_8,$$

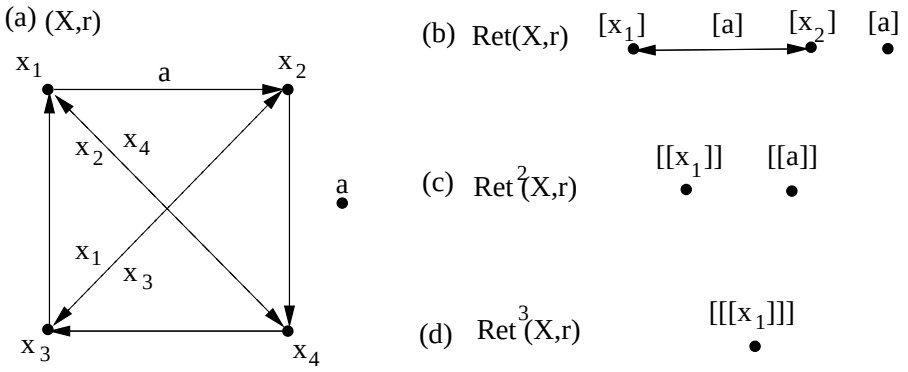

FIGURE 3. Graphs for Example 5.4. Arrows show left actions on the set $X = \{x_1, x_2, x_3, x_4\} \cup \{a\}$ in part (a). The first retract is shown in part (b). The second retract (c) is the trivial solution. The third retract (d) is the 1-element solution. Hence $mpl(X, r) = 3$.

where D_8 is the Dihedral group of order 8 with generators of order 4 and 2 as exhibited.

In this case the orbits are $X_1 = \{x_1, x_2, x_3, x_4\}$, $X_2 = \{a\}$. It is straightforward to see that the retract $Ret(X, r) = ([X], r_{[X]})$ satisfies

$$[X] = \{[x_1], [x_2], [a]\}, \quad \mathcal{L}_{[a]} = ([x_1][x_2]), \quad \mathcal{L}_{[x_1]} = \mathcal{L}_{[x_2]} = \mathrm{id}_{[X]}$$

so $mpl(Ret(X, r)) = 2$ and thus $mpl(X, r) = 3$. The graph for this example is shown in Figure 3.

Now assume that there is a basis $Y = Y_1 \bigcup \{a\}$ fulfilling the conditions in Conjecture 5.3. Let $Y_1 = \{y_1, y_2, y_3, y_4\} \subset V_1$. So we assume that

$$R(a \otimes y_i) = \lambda_i y_i \otimes a; \quad \lambda_i \in \mathbb{C}^\times, \quad 1 \le i \le 4 \tag{5.1}$$

and

$$R(y_i \otimes y_j) = \mu_{ij} y_j \otimes y_i; \quad \mu_{ij} \in \mathbb{C}^\times, \quad 1 \le i \le 4. \tag{5.2}$$

Each $y_i \in Y_1$ is some linear combination $y_i = \sum_j \alpha_j x_j$ (say) but the right action on a is trivial, so

$$R(a \otimes y_i) = R(a \otimes \sum \alpha_j x_j) = \sum \alpha_j R(a \otimes x_j) = \sum \alpha_j \, {}^a(x_j) \otimes a = \mathcal{L}_a(y_i) \otimes a.$$

Hence we require $\mathcal{L}_a y_i \otimes a = \lambda_i y_i \otimes a$. Hence $\mathcal{L}_a y_i = \lambda_i y_i$. So each $y_i \in Y$ is an eigenvector of $P(a)$ – the permutation matrix of the cycle $(x_1 x_2 x_3 x_4)$. Since the latter has four eigenvectors and these have distinct eigenvalues, this determines Y_1 up to normalisation and order. Without loss of generality we can therefore take

$$Y_1 = \left\{ y_0 = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \quad y_1 = \begin{pmatrix} -\imath \\ -1 \\ \imath \\ 1 \end{pmatrix}, \quad y_2 = \begin{pmatrix} -1 \\ 1 \\ -1 \\ 1 \end{pmatrix}, \quad y_3 = \begin{pmatrix} \imath \\ -1 \\ -\imath \\ 1 \end{pmatrix} \right\}$$

in terms of the basis X_1. We compute R in basis Y_1 in two steps;

$$z_1 = x_1 + x_3, \quad z_2 = x_1 - x_3, \quad t_1 = x_2 + x_4, \quad t_2 = x_2 - x_4$$

$$R(z_1 \otimes z_2) = z_2 \otimes z_1, \quad R(z_1 \otimes t_1) = t_1 \otimes z_1, \quad R(z_1 \otimes t_2) = -t_2 \otimes z_1$$

$$R(z_2 \otimes t_1) = -t_1 \otimes z_2, \quad R(z_2 \otimes t_2) = t_2 \otimes z_2, \quad R(t_1 \otimes t_2) = t_2 \otimes t_1$$

and then

$$y_0 = z_1 + t_1, \quad y_1 = -\imath z_2 - t_2, \quad y_2 = -z_1 + t_1, \quad y_3 = \imath z_2 - t_2$$

$$R(y_1 \otimes y_2) = R((\imath z_2 + t_2) \otimes (z_1 - t_1)) = \imath z_1 \otimes z_2 + \imath t_1 \otimes z_2 - z_1 \otimes t_2 - t_1 \otimes t_2$$

$$y_2 \otimes y_1 = (z_1 - t_1) \otimes (\imath z_2 + t_2) = \imath z_1 \otimes z_2 + z_1 \otimes t_2 - \imath t_1 \otimes z_2 - t_1 \otimes t_2$$

Now, by our assumption $R(y_1 \otimes y_2) = \mu(y_2 \otimes y_1)$. Here $\mu = \mu_{12}$. Hence, comparing, we need

$$(\mu - 1)(\imath z_1 \otimes z_2) - (\mu + 1)\imath(t_1 \otimes z_2) + (\mu + 1)(z_1 \otimes t_2) - (\mu - 1)(t_1 \otimes t_2) = 0$$

which requires both $\mu + 1 = 0$ and $\mu - 1 = 0$, which is not possible.

6. Structure of $\mathcal{A}(k, X, r)$

Let $R : V \otimes V \to V \otimes V$ be an invertible solution of the QYBE over a field k. The quantum space associated to this data is the algebra $k_R[V]$ defined as a quotient of the tensor algebra TV modulo the ideal generated by elements of the form $v \otimes w - R(v \otimes w)$. This definition is basis-independent but in the case $V = kX$ and R the linear extension of a set-theoretic solution it is clear that $k_R[V]$ computed in this basis becomes the quantum algebra $\mathcal{A}(k, X, r)$.

On the other hand it is immediate from the form of R found in the main theorem above (Theorem 4.9) that for a finite square-free multipermutation solution r of level 2 the vector space $V = \mathbb{C}X$ has a new basis of generators $\{y^i_\eta \mid 1 \leq i \leq t,\ \eta \in \Lambda_i\}$ in which the relations of $\mathbb{C}_R[V]$ take the diagonal form

$$y^i_\eta . y^j_\zeta = \frac{\mu^i_{j,\zeta}}{\mu^j_{i,\eta}} y^j_\zeta . y^i_\eta,\ 1 \leq i \leq j \leq t,\ \eta \in \Lambda_i,\ \zeta \in \Lambda_j, \tag{6.1}$$

where the complex numbers $\mu^i_{j,\eta}$ etc., are roots of unity defined explicitly in (4.8). When $i = j$ we require $\eta < \zeta$ but note that due to the properties of the coefficients μ we have in in fact that

$$y^i_\eta y^i_\zeta = y^i_\zeta y^i_\eta, \quad \eta < \zeta \in \Lambda_i, \quad 1 \leq i \leq t. \tag{6.2}$$

Since the change from the X to the new Y basis does not change the algebra, clearly this algebra is also isomorphic to the quantum algebra $\mathcal{A}(\mathbb{C}, X, r)$. This is our first immediate corollary.

In this section we give two points of view on the further particular structure of $\mathcal{A}(k, X, r)$ in the form $k_R[V]$ for our solutions of mulitpermutation level 2. The first result concerns its structure as a cotwist indicated by the particular 'ratio' form of R in Theorem 4.9.

6.1. **Generalities on diagonal cotwist quantum algebras.** We will use Hopf algebra methods but the Hopf algebras here will be group algebras and therefore we will give the general theory of cotwists at this level. Let H be a group and $\mathcal{F} : H \times H \to k^\times$ a 2-cocycle in the sense

$$\mathcal{F}(a, bc)\mathcal{F}(b, c) = \mathcal{F}(a, b)\mathcal{F}(ab, c), \quad \mathcal{F}(e, a) = 1, \quad \forall a, b, c \in H$$

(here e is the group identity and one can deduce that $F(a, e) = 1$ holds as well). Let $\mathcal{A}$ be a H-graded algebra (so $\mathcal{A} = \oplus_{a\in H}\mathcal{A}_a$ into graded components, $1 \in \mathcal{A}_e$ and $\mathcal{A}_a\mathcal{A}_b \subseteq \mathcal{A}_{ab}$). Then the vector space of A acquires a new associative product $\bullet$, say, with

$$f \bullet g = \mathcal{F}(|f|, |g|)fg$$

on homogeneous elements $f, g \in \mathcal{A}$ of degree $|f|, |g|$. The right hand side uses the old product. We obtain new algebra $\mathcal{A}^{\mathcal{F}}$ covariant under the Drinfeld-cotwisted quantum group $(kH)_{\mathcal{F}}$. As a Hopf algebra the latter is the same as the group algebra kH but with a cotriangular structure $\mathcal{F}_{21}\mathcal{F}^{-1}$ (the product here in a certain convolution algebra). This means that the natural category in which $\mathcal{A}^{\mathcal{F}}$ lives is that of H-graded spaces but with a non-trivial symmetry (i.e. involutive brading) Ψ given by a ratio of $\mathcal{F}$ and its inverse transpose. We refer to [M95] for details.

Now suppose that V is a vector space of dimension n with basis $Y = \{y_i\}$ and R a solution with diagonal entries ρ_{ij} in the sense

$$R(y_i \otimes y_j) = \rho_{ij}y_j \otimes y_i.$$

The indices i, j in this subsection will become multi-indices $(i, \eta), (j, \zeta)$ etc in our application. We suppose further that $\rho_{ij} = F_{ij}/F_{ji}$ for some F_{ij}. Note that since R is involutive we have $\rho_{ji} = \rho_{ij}^{-1}$ and the above form provides a natural special case of this. Let $k[Y]$ (the algebra of polynomials $k[y_1, \cdots, y_n]$ in the basis) be graded by $H = \mathbb{Z}^n$, the free abelian group on generators g_i, with the H-degree of y_i being g_i.

Next, we define

$$\mathcal{F}(g_{i_1} \cdots g_{i_k}, g_{j_1} \cdots g_{j_l}) = \prod_{a=1}^{k}\prod_{b=1}^{l} F_{i_a j_b}$$

This extends to negative powers by the use of $F^{-1}_{i_a j_b}$ if one or other (but not both) of the relevant g_{i_a} or g_{j_b} occurs inverted in the sequence. It is easy to see that this defines a bicharacter on $\mathbb{Z}^n$ and hence in particular a 2-cocycle on it. A bicharacter on a group means $\mathcal{F}(ab, c) = \mathcal{F}(a, c)\mathcal{F}(b, c)$ and $\mathcal{F}(a, bc) = \mathcal{F}(a, b)\mathcal{F}(a, c)$ for any a, b, c in the group.

Applying the cotwist construction now gives the algebra $k[Y]^{\mathcal{F}}$ with the same vector space as $k[Y]$ and the new product

$$(y_{i_1}y_{i_2} \cdots y_{i_k}) \bullet (y_{j_1}y_{j_2} \cdots y_{j_l}) = \left(\prod_{a=1}^{k}\prod_{b=1}^{l} F_{i_a j_b}\right) y_{i_1}y_{i_2} \cdots y_{i_k}y_{j_1}y_{j_2} \cdots y_{j_l}. \tag{6.3}$$

Proposition 6.1. *Suppose that $R : V \otimes V \to V \otimes V$ has a diagonal 'ratio' form in a basis $\{y_i\}$. Then $k_R[V]$ is isomorphic to $k[Y]^{\mathcal{F}}$, i.e. a cocycle cotwist of the commutative polynomial algebra $k[Y]$.*

Proof. The $n(n-1)/2$ relations of $k_R[V]$ in basis $\{y_i\}$ are of the form $y_i.y_j = \rho_{ij}y_j.y_i$ and since the coefficients in our case are clearly invertible they allow all words on the generators to be put in standard form in terms of basis $\{y_1^{s_1}\cdots y_n^{s_n}\}$. We identify the vector space of $k_R[V]$ with that of $k[Y]^{\mathcal{F}}$ in this way. One may then verify that the products coincide. Thus $y_i \bullet y_j = F_{ij}y_iy_j = F_{ij}y_jy_i = \frac{F_{ij}}{F_{ji}}y_j \bullet y_i$ as required in degree 2. Hence there is an algebra epimorphism $k_R[V] \to k[Y]^{\mathcal{F}}$. Since their bases coincide in each degree, this is an isomorphism. □

By definition, an exterior differential calculus $(\Omega(\mathcal{A}), \mathrm{d})$ on an algebra $\mathcal{A}$ means an associative $\mathbb{N}$-graded algebra Ω generated by degrees $\Omega^0 = \mathcal{A}$ and Ω^1, and $\mathrm{d} : \Omega^m \to \Omega^{m+1}$ obeying $\mathrm{d}^2 = 0$ and a graded Leibniz rule for its action on products.

Corollary 6.2. *$k_R[V]$ has a natural exterior differential calculus $(\Omega_R(V), \mathrm{d})$ with basis $\mathrm{d}y_i$ over $k_R[V]$ and relations*

$$\mathrm{d}y_i \cdot y_j = \rho_{ij}y_j.\mathrm{d}y_i, \quad \forall i,j, \quad \mathrm{d}y_i \cdot \mathrm{d}y_j + \rho_{ij}\mathrm{d}y_j \cdot \mathrm{d}y_i = 0, \quad \forall i \le j.$$

Moreover, the partial derivative operators $\partial^i : k_R[V] \to k_R[V]$ defined by $\mathrm{d}f = \sum_i (\partial^i f)\mathrm{d}y_i$ are right-handed braided derivations in the sense:

$$\partial^i(f \cdot (y_{j_1}\cdots y_{j_l})) = f \cdot \partial^i(y_{j_1}\cdots y_{j_l}) + \left(\prod_{b=1}^{l}\rho_{ij_b}\right)(\partial^i f)\cdot(y_{j_1}\cdots y_{j_l})$$

on f and homogeneous $y_{j_1}\cdots y_{j_l}$ in $k_R[V]$. The product here is the noncommutative one of $k_R[V]$.

Proof. We apply the cotwisting theory above to the usual exterior algebra $\Omega(k[Y])$ generated by the commutative y_i and the graded-commutative $\mathrm{d}y_i$. This retains the $\mathbb{Z}^n$-grading where d is given degree 0 (so $\mathrm{d}y_i$ has the same degree as y_i) and is therefore an H-comodule algebra as before. Cotwisting now gives $y_i \bullet \mathrm{d}y_j = F_{ij}y_i\mathrm{d}y_j = \frac{F_{ij}}{F_{ji}}\mathrm{d}y_j \bullet y_i$ as before. Similarly for the relations between the $\mathrm{d}y_i$. We define this algebra $\Omega(k[Y])^{\mathcal{F}}$ to be the exterior calculus on $k_R[V] = k[Y]^{\mathcal{F}}$. The map d is unchanged at the level of the unchanged underlying vector spaces. Finally, we identify this exterior calculus with product $\bullet$ with the abstract algebra $\Omega_R(V)$ generated by $y_i, \mathrm{d}y_i$ as stated, by identifying the natural bases as before. The product in the abstract algebra is now the noncommutative one (without explicitly writing $\bullet$). The relations imply that in $\Omega_R(V)$,

$$\mathrm{d}y_i.(y_{j_1}\cdots y_{j_l}) = \left(\prod_{a=1}^{l}\rho_{ij_a}\right)y_{j_1}\cdots y_{j_l}\mathrm{d}y_i$$

from which the behaviour of the partial derivatives follows. □

Another feature of $k_R[V]$ is its braided Hopf algebra structure as follows. We have explained that as a cotwist it 'lives' in the category of H-graded spaces but with a nontrivial braiding (in our case a symmetry) built from ρ. The braiding on monomials is

$$\Psi(y_{i_1}\cdots y_{i_k}\otimes y_{j_1}\cdots y_{j_l}) = \left(\prod_{a=1}^{k}\prod_{b=1}^{l}\rho_{i_aj_b}\right)y_{j_1}\cdots y_{j_l}\otimes y_{i_1}\cdots y_{i_k}$$

Working in this category, $k_R[V]$ necessarily has an additive coproduct $\underline{\Delta} y_i = y_i \otimes 1 + 1 \otimes y_i$ which expresses addition on the underlying braided space just as the usual $k[Y]$ has an ordinary Hopf algebra structure with additive coproduct. We refer to [M95, Ch 10] for the general theory. (In our case since R is involutive there is no other R'-operator as in the general theory of braided linear spaces.)

Proposition 6.3. *In the context above with $k_R[V]$ viewed as a 'braided linear space' the braided derivatives ∂^i canonically defined by*

$$\underline{\Delta} f(y) = f \otimes 1 + \sum_i \partial^i(f) \otimes y_i + \cdots$$

(where we drop terms with higher products of y_i on the right) coincide with the partial derivatives above obtained by cotwisting.

Proof. As a Hopf algebra in a (symmetric) braided category we extend $\underline{\Delta}$ to products by

$$\underline{\Delta}(fg) = (\underline{\Delta} f)(\underline{\Delta} g) = \sum f_{(1)} \Psi(f_{(2)} \otimes g_{(1)}) g_{(2)}$$

using the notation $\underline{\Delta} f = \sum f_{(1)} \otimes f_{(2)}$. Expanding as stated, this becomes

$$(f \otimes 1 + \partial^i f \otimes y_i + \cdots)(g \otimes 1 + \partial^i g \otimes y_i + \cdots) = fg \otimes 1 + f\partial^i g \otimes y_i + \partial^i f \Psi(y_i \otimes g) + \cdots$$

which gives the same results for $\partial^i(fg)$ as above. Since the values of both on generators are $\partial^i y_j = \delta^i{}_j$ (the Kronecker delta-function), the partial derivatives coincide. There are explicit formulae for the braided derivatives in terms of 'braided integer matrices' generalizing the notion of q-integers, see [M95]. □

Similar calculus and braided Hopf algebra structures on $k_R[V]$ were found in greater generality in the 1990s in a 'braided approach to noncommutative geometry' [M95], without assuming that R is involutive or of cotwist form. However, in the special case of a diagonal cotwist solutiion as above the formulae are rather simpler and, moreover, we are able to obtain the constructions quite explicitly on the underlying vector spaces rather than in terms of arguments by generators and relations as in the literature.

All of the above apply in view of Theorem 4.9 to $\mathbb{C}_R[V]$ with R obtained from a finite square-free set-theoretic solution of multipermutation level 2. We set

$$F_{(i,\eta),(j,\zeta)} = \mu^i_{j,\zeta} \tag{6.4}$$

where our basis of V is now written as $\{y^i_\eta\}$, i.e. labelled by the multi-index (i,η) in place of i above. We have explained that $\mathbb{C}_R[V]$ is $\mathcal{A}(\mathbb{C}, X, r)$ written as a quadratic algebra and Proposition 6.1 asserts that this is a $\bullet$-product 'quantisation' of $\mathbb{C}[V]$ (the usual polynomial algebra with our basis as generators). The relations of the differential calculus on $\mathcal{A}(\mathbb{C}, X, r)$ from Corollary 6.2 are

$$\mathrm{d}y^i_\eta . y^j_\zeta = \frac{\mu^i_{j,\zeta}}{\mu^j_{i,\eta}} y^j_\zeta . \mathrm{d}y^i_\eta, \quad (\mathrm{d}y^i_\eta).(\mathrm{d}y^j_\zeta) + \frac{\mu^i_{j,\eta}}{\mu^j_{i,\eta}} (\mathrm{d}y^j_\zeta).(\mathrm{d}y^i_\eta) = 0, \tag{6.5}$$

(we take $i \le j$ in the second set of relations and where $i = j$ then $\eta < \zeta$). The algebra is moreover a Hopf algebra in a certain symmetric monoidal category with additive coproduct in the generators as in Proposition 6.3. Note that $\mathcal{A}(\mathbb{C}, X, r)$, as a semigroup algebra, also has an ordinary bialgebra structure with coproduct

$\Delta x = x \otimes x$ on $x \in X$. This is a different coproduct from the additive braided coproduct $\underline{\Delta}$ on the same algebra.

6.2. **Canonical cotwist structure of $\mathcal{A}(\mathbb{C}, X, r)$.** While the above generalities apply in our case, they do not make use of the specific structure of the diagonal basis $\{y^i_\eta\}$. Here we provide the same $\bullet$ product for our particular quantum algebra $\mathbb{C}_R[V]$ (and hence $\mathcal{A}(\mathbb{C}, X, r)$) as a different cotwist, this time with finite grading group and a canonical cocycle on it.

We let

$$H = \prod_{1\le i\le t} \mathcal{G}_i^* \times \prod_{1\le i\le t} \mathcal{G}_i = \mathcal{H}^* \times \mathcal{H}$$

and we let V be H-graded as follows. We let the component V_i have $\mathcal{H}$-grade $\prod_{1\le j\le t} \sigma_j^i$ and define the $\mathcal{H}^*$-grading equivalently as an action of $\mathcal{H}$. This action is just the action of each $\mathcal{G}_i$ on each V_i (with trivial action on V_j if $j \ne i$). Because the group H is abelian the grading extends to $\mathbb{C}[V]$ (by which we mean the symmetric algebra on V, i.e. the free commutative algebra of polynomials in a fixed basis).

Note that these definitions are basis-independent. However, the bases where the actions of the $\mathcal{G}_i$ are diagonal are just those where the basis elements have homogeneous grade under $\mathcal{H}^*$ and hence under the action of H. This is precisely our $\{y^i_\eta\}$ basis constructed in Section 4. The basis elements here have degree

$$|y^i_\eta| = (\chi_\eta, \gamma^i) \in H; \quad \gamma^i = \prod_{1\le j\le t} \sigma^i_j.$$

Next, on each subgroup $\mathcal{G}_i^* \times \mathcal{G}_i$ there is a canonical 2-cocycle

$$\mathcal{F}((\chi, g), (\chi', h)) = \chi'(g), \quad \forall \chi, \chi' \in \mathcal{G}_i^*,\ g, h \in \mathcal{G}_i$$

which similarly extends for each i to define a 2-cocycle $\mathcal{F}$ on H.

Proposition 6.4. *Let (X, r) be a finite square-free multipermutation solution of level 2 and let $V = \mathbb{C}X$ be H-graded as above. Then the canonical 2-cocycle $\mathcal{F}$ on H induces a cotwist quantization $\mathbb{C}[V]^{\mathcal{F}}$ isomorphic to $\mathbb{C}_R[V]$ and hence to $\mathcal{A}(\mathbb{C}, X, r)$.*

Proof. We compute in the homogeneous basis

$$\begin{aligned}
(y^{i_1}_{\eta_1} \cdots y^{i_k}_{\eta_k}) \bullet (y^{j_1}_{\zeta_1} \cdots y^{j_l}_{\zeta_l}) &= \mathcal{F}(\chi_{\eta_1}\gamma^{i_1} \cdots \chi_{\eta_k}\gamma^{i_k}, \chi_{\zeta_1}\gamma^{j_1} \cdots \chi_{\zeta_l}\gamma^{j_l}) y^{i_1}_{\eta_1} \cdots y^{i_k}_{\eta_k} y^{j_1}_{\zeta_1} \cdots y^{j_l}_{\zeta_l} \\
&= (\chi_{\zeta_1} \cdots \chi_{\zeta_l})(\gamma^{i_1} \cdots \gamma^{i_k}) y^{i_1}_{\eta_1} \cdots y^{i_k}_{\eta_k} y^{j_1}_{\zeta_1} \cdots y^{j_l}_{\zeta_l} \\
&= \chi_{\zeta_1}(\sigma^{i_1}_{j_1} \cdots \sigma^{i_k}_{j_1}) \cdots \chi_{\zeta_l}(\sigma^{i_1}_{j_l} \cdots \sigma^{i_k}_{j_l}) y^{i_1}_{\eta_1} \cdots y^{i_k}_{\eta_k} y^{j_1}_{\zeta_1} \cdots y^{j_l}_{\zeta_l} \\
&= \left(\prod_{a=1}^{k} \prod_{b=1}^{l} \chi_{\zeta_b}(\sigma^{i_a}_{j_b}) \right) y^{i_1}_{\eta_1} \cdots y^{i_k}_{\eta_k} y^{j_1}_{\zeta_1} \cdots y^{j_l}_{\zeta_l}
\end{aligned}$$

We write expressions in the group H where the various factors $\mathcal{G}_i$ and $\mathcal{G}_j^*$ all mutually commute. We view the product of characters in the second line here as a single character in $\mathcal{H}^*$ but the evaluation of a factor χ_{ζ_b} is 1 except on elements in the corresponding $\mathcal{G}_{j_b}$. Hence writing out the products of the $\gamma^{i_a} = \sigma_1^{i_a} \cdots \sigma_t^{i_a}$ and collecting the factors living in each $\mathcal{G}_{j_b}$ gives the third line. Using that χ_{ζ_b} is a character gives the last expression. We recognise $\mu^{i_a}_{j_b\zeta_b}$ in the product, i.e. the same factors $F_{(i_a,\eta_a),(j_b,\zeta_b)}$ as in the previous section and the same form of product

(6.3) in terms of such factors. Hence we again obtain the algebra $\mathcal{A}(\mathbb{C}, X, r)$ in the $\{y^i_\eta\}$ generators. □

These results express $\mathcal{A}(\mathbb{C}, X, r)$ as a kind of 'quantisation' of the commutative polynomial algebra $\mathbb{C}[V]$ (indeed, the form of H and the cocycle on it are a finite version of the similar ideas that apply to the Moyal product in quantum mechancs). We similarly find the same formulae (6.5) for the quantum differential calculus and for the braiding. In the present setting, however, we learn that these constructions are all H-graded since we have constructed them in a symmetric monoidal category of H-graded spaces.

Moreover, they are canonically defined independent of any basis. The only subtlety is that other elements such as those of our original basis X will not be homogeneous. However, we can think of the H-grading equivalently as a *coaction* of the group Hopf algebra $\mathbb{C}H$ where everything is extended linearly as a map $\Delta_R : V \to V \otimes \mathbb{C}H$ (the axioms for this map are dual to the axioms of an action $H^* \times V \to V$ and are equivalent to such an action as H here is finite). On homogeneous elements we have $\Delta_R v = v \otimes |v|$ and we extend this linearly. We also understand the cocycle now as a map $\mathcal{F} : \mathbb{C}H \otimes \mathbb{C}H \to \mathbb{C}$ which is the same map as before but extended linearly. The bullet product is defined now as

$$f \bullet g = f^{(1)} g^{(2)} \mathcal{F}(f^{(2)} \otimes g^{(2)}); \quad \Delta_R f = \sum f^{(1)} \otimes f^{(2)} \tag{6.6}$$

where we use an 'explicit' notation for $\Delta_R f \in V \otimes H$. Provided we linearise everything in this way, we are free to change bases. In particular, we could now use the original basis X. Then we recover the following result:

Corollary 6.5. *$\mathcal{A}(\mathbb{C}, X, r)$ can be built on the same vector space as $\mathbb{C}[V]$ where $V = \mathbb{C}X$ (i.e. the polynomial algebra on $|X|$ variables labelled by $x \in X$) with bullet product*

$$x \bullet y = x\mathcal{L}_x(y), \quad \forall x, y \in X$$

Proof. We compute $\mathbb{C}[V]^{\mathcal{F}}$ in the basis X with the explanations above that our previous maps are extended linearly. The coaction of $\mathbb{C}H$ on $V = \mathbb{C}X$ corresponding to our previous H-grading has the form

$$x \mapsto \frac{1}{N_i} \sum_{\pi \in \mathcal{G}_i} \pi(x) \otimes \left(\sum_{\eta \in \Lambda_i} \chi_\eta(\pi^{-1}) \chi_\eta \right) \gamma^i. \tag{6.7}$$

Here the γ^i part of the grading is the same on the entire space V_i hence unaffected by the change of basis. The Fourier transform relating the $\{\pi(x_{i1})\}$ basis to the $\{y^i_\eta\}$ has an inverse and we use this to compute the coaction $y^i_\eta \mapsto y^i_\eta \otimes |y^i_\eta|$ in the former basis as stated in (6.7). One may verify this directly from $y^i_\eta = \sum_\pi \chi_\eta(\pi^{-1})\pi(x_{i1})$ and the identity $\sum_\pi \chi_\eta(\pi)\chi(\pi^{-1}) = \delta_{\chi,\chi_\eta}|\mathcal{G}_i|$. Armed with this coaction, for $x \in X_i$, $y \in X_j$ we have,

$$x \bullet y = \frac{1}{N_i N_j} \sum_{\pi \in \mathcal{G}_i \rho \in \mathcal{G}_j} \pi(x)\rho(y) \sum_{\eta \in \Lambda_i \zeta \in \Lambda_j} \chi_\eta(\pi^{-1}) \chi_\zeta(\rho^{-1}) \mathcal{F}(\chi_\eta \gamma^i, \chi_\zeta \gamma^j) = x\sigma^i{}_j(y)$$

after a short computation. Here $\mathcal{F}(\chi_\eta \gamma^i, \chi_\zeta \gamma^j) = \chi_\zeta(\gamma^i) = \chi_\zeta(\sigma^i_j)$. □

We remark that while it is easy to see directly that the stated formula for $\bullet$ gives the right relations $x \bullet y = ({}^x y) \bullet (x^y)$ on the generators, it is not *apriori* obvious that $\bullet$ extends to a well-defined associative product in the same vector space as $\mathbb{C}[V]$ and this is what the twisting theory ensures (it follows from $\mathcal{F}$ a 2-cocycle). In the X basis we also have differential calculus readily computed in the same way as

$$x \bullet \mathrm{d}y = (\mathrm{d}^x y) \bullet x^y, \quad \mathrm{d}x \bullet \mathrm{d}y = (\mathrm{d}^x y) \bullet (\mathrm{d}x^y) \tag{6.8}$$

with $\mathrm{d}^2 = 0$ and d respecting the H-grading, part which includes that d commutes with the action of each restriction $\mathcal{G}_i$ and hence with the left action. Dropping the $\bullet$ symbol, this defines the exterior differential calculus $(\Omega(\mathcal{A}(\mathbb{C}, X, r)), \mathrm{d})$ for our quantum space. The symmetry Ψ on the generators is just r itself.

Finally, we explain how the above results extend to any field k. The trick is that by the time we allow the linear span of characters in $\mathbb{C}\mathcal{H}^* \subseteq \mathbb{C}H = \mathbb{C}\mathcal{H}^* \otimes \mathbb{C}\mathcal{H}$ we are in fact working with *all* functions on $\mathcal{H}$ – we do not need to use the basis provided by the characters and can hence dispense with the characters all together. Thus, $\mathbb{C}\mathcal{H}^* = \mathbb{C}(\mathcal{H})$ in a canonical way as Hopf algebras. The latter denotes the Hopf algebra of functions on $\mathcal{H}$ (this works for any finite group). In this second form, we can now simply work with $k(\mathcal{H})$ for a general field. It is the Hopf algebra dual of $k\mathcal{H}$; we refer to [M95] for an introduction. One can in fact introduce characters over k but we do not need to if we use these Hopf algebra methods. Thus, instead of the group H above we now work with the Hopf algebra

$$H = k(\mathcal{H}) \otimes k\mathcal{H}.$$

The Hopf algebra $k(\mathcal{H})$ has a basis $\{\delta_h \mid h \in \mathcal{H}\}$ where δ_h is the Kronecker δ-function $\delta_h(h') = 1$ if $h = h'$ and otherwise 0. We explained in general above that the $\mathcal{H}^*$-part of the grading was dual to the action of $\mathcal{H}$ on $V = kX$ which on each $V_i = kX_i$ is given by the action of $\mathcal{G}_i$. The $\mathcal{H}$ part of the grading is by the element γ^i as before. Thus the coaction $V \to V \otimes H$ given simply by

$$\Delta_R v = \sum_{\pi \in \mathcal{G}_i} \pi.v \otimes (\delta_\pi \otimes \gamma^i), \quad \forall\ v \in V_i.$$

where $\delta_\pi \in k(\mathcal{G}_i)$ is viewed in $k(\mathcal{H}) = \otimes_{1 \le i \le t} k(\mathcal{G}_i)$. This agrees with our previous formula (6.7) in the case where $k = \mathbb{C}$ since

$$\frac{1}{|\mathcal{G}_i|} \sum_{\eta \in \Lambda_i} \chi_\eta(\pi^{-1}) \chi_\eta = \delta_\pi$$

when the linear combination of characters on the left is viewed as a function on $\mathcal{G}_i$.

Next, as Hopf algebra 2-cocycle $\mathcal{F} : H \otimes H \to k$ we take the linear map

$$\mathcal{F}((f \otimes h) \otimes (f' \otimes h')) = \epsilon(f)\epsilon(h') f'(h), \quad f, f' \in k(\mathcal{H}), \quad h, h' \in k\mathcal{H} \tag{6.9}$$

where the map $\epsilon(f) = f(e)$ (evaluation as the group identity) and $\epsilon(h) = 1$ for all $h \in \mathcal{H} \subset k\mathcal{H}$. The k-valued linear map ϵ is called the counit of the relevant Hopf algebra. We refer to [M95, Chapter 2.3] for the formal definitions and axioms obeyed by $\mathcal{F}, \epsilon$ as linear maps. The cotwisting theory applies to produce an associative algebra with $\bullet$-product (6.6) but now on the vector space of $k[V]$ over a general field.

Proposition 6.6. *Let (X,r) be a finite square-free multipermutation solution of level 2, and let $V = kX$ be an H-comodule by Δ_R as above, where $H = k(\mathcal{H}) \otimes k\mathcal{H}$. Then the Hopf algebra 2-cocycle $\mathcal{F}$ in (6.9) induces a cotwist $k[V]^{\mathcal{F}}$ isomorphic to $k_R[V]$ and hence to $\mathcal{A}(k,X,r)$.*

Proof. The computation of the $\bullet$ product is the same as before but proceeds more cleanly without the use of characters. We compute in the basis X. For $x \in X_i$, $y \in X_j$, we have

$$x \bullet y = \sum_{\substack{\pi \in \mathcal{G}_i \\ \rho \in \mathcal{G}_j}} \pi(x)\rho(y)\mathcal{F}((\delta_\pi \otimes \gamma^i) \otimes (\delta_\rho \otimes \gamma^j)) = \sum_{\substack{\pi \in \mathcal{G}_i \\ \rho \in \mathcal{G}_j}} \pi(x)\rho(y)\epsilon(\delta_\pi)\epsilon(\gamma^j)\delta_\rho(\gamma^i) = x\sigma_j^i(y)$$

as before. Remember that δ_ρ is viewed as a function on $\mathcal{H}$ but is sensitive only to the part of γ^i that lives in $\mathcal{G}_j$, where it has value δ_{ρ,σ_j^i}. We then find as observed before that $x \bullet y = ({}^x y) \bullet (x^y)$ as required in degree 2. Also, by construction, the algebra $k[V]^{\mathcal{F}}$ has the same Hilbert series as $k[V]$. As $\mathcal{A}(k,X,r)$ also has the same Hilbert series when (X,r) is a symmetric set, see [GB, Thm. 1.3] and [GI, Thm. 9.7], we conclude that the epimorphism $\mathcal{A}(k,X,r) \to k[V]^{\mathcal{F}}$ is an isomorphism. □

In the same way, it is clear that we have $(\Omega(\mathcal{A}(k,X,r)), \mathrm{d})$ with the same formulae as before in the X basis. One also has a monoidal symmetry Ψ defined over k (it is built from $\mathcal{F}$ and its 'convolution inverse', see [M95, Chapter 3]) with respect to which $\mathcal{A}(k,X,r)$ is a Hopf algebra in a symmetric monoidal category.

6.3. **Structure of $\mathcal{A}(k,X,r)$ as a braided-opposite algebra.** Here we present a different point of view on the structure of $\mathcal{A}(k,X,r)$. We use Hopf algebra methods which do not require characters and in this context we prefer to work with $\mathcal{G}(X,r) \subseteq \mathcal{H}$ rather than the bigger group. We also then do not need to assume that X is finite. Initially, let $\mathcal{G}$ be any group.

Definition 6.7. A set X is a crossed $\mathcal{G}$-set if there is a map $|\ | : X \to \mathcal{G}$ (the grading) and an action of $\mathcal{G}$ on X such that $|g.x| = g|x|g^{-1}$ for all $g \in \mathcal{G}$ and $x \in X$.

The notion goes back to Whitehead but is also part of the modern theory of quantum groups. The linear span $V = kX$ becomnes a 'crossed $\mathcal{G}$-module' and this is the same thing in the case of $\mathcal{G}$ finite as V a module under the quantum double $D(\mathcal{G})$ of the group algebra of $\mathcal{G}$, see [M95] for an introduction. Its category of modules is strictly braided and so is the category of crossed $\mathcal{G}$-modules (for any group). In algebraic terms we require V to be both $\mathcal{G}$-graded as a vector space and to enjoy an action of $\mathcal{G}$, and the two to be compatible. The grading can be viewed as a coaction $V \to V \otimes k\mathcal{G}$ of the Hopf algebra $k\mathcal{G}$ which we write explicitly as $v \mapsto \Delta_R(v) = \sum v^{(1)} \otimes v^{(2)} \in V \otimes k\mathcal{G}$, as we have seen at the end of the previous section. Let us write the action of $\mathcal{G}$ and hence of $k\mathcal{G}$ as usual from the left to conform with notations in the paper. Then the braiding in the category of crossed modules $\Psi^D_{V,W} : V \otimes W \to W \otimes V$ can be written as

$$\Psi^D(v \otimes w) = \sum v^{(2)}.w \otimes v^{(1)} \tag{6.10}$$

Lemma 6.8. *Let (X, r) be a square-free involutive set-theoretic solution of multi-permutation level 2. Then X is a crossed $\mathcal{G}$-set, where $\mathcal{G}$ is the group defined in Section 2, and $|x| = \mathcal{L}_x$.*

Proof. If X is finite, we know from Theorem 2.16 that $\mathcal{G}$ is abelian, but the same is true even if X is infinite (we will prove this in passing in the next section, see (7.2)). Since the group $\mathcal{G}$ is Abelian we require for a crossed module that the grade of an element is not changed by the action of $\mathcal{G}$. In the finite case the grade $\mathcal{L}_x$ is constant on each orbit X_i and by definition the action of $\mathcal{G}$ does not take us out of an orbit. One can show by direct computation that $\mathcal{L}_x$ does not change if one acts on x by an element of $\mathcal{G}$ even if X is infinite (see (7.3)). □

Hence V is a crossed $\mathcal{G}$-module and one may verify that so is $k[V]$, the polynomial algebra on any fixed basis of V (it is defined invariantly as the symmetric algebra on V and in that formulation does not require V to be finite-dimensional). The grade of any monomial is the product of the grades of each generator in the monomial and in this way $k[V]$ becomes $\mathcal{G}$-graded (we need that $\mathcal{G}$ is Abelian). The algebra also has an action of $\mathcal{G}$ inherited from the action on V. In this way $k[V]$ is an algebra in the braided category of crossed $\mathcal{G}$-modules.

Finally, for any algebra $\mathcal{A}$ over k in a k-linear braided category there is an opposite algebra $\mathcal{A}^{\underline{op}}$ with 'opposite product' which we denote $\bullet$ built on the same object but with

$$\bullet = \cdot\Psi$$

where $\cdot$ denotes the original product of $\mathcal{A}$.

Proposition 6.9. *Let $V = kX$ for (X, r) as in the lemma above and finite, and view $k[V]$ in the braided category of crossed $\mathcal{G}$-modules. Then $\mathcal{A}(k, X, r) \cong k[V]^{\underline{op}}$.*

Proof. The opposite product in the category of crossed modules has the form

$$f \bullet g = \cdot(f^{(2)}.g \otimes f^{(1)}) = (f^{(2)}.g)f^{(1)} = f^{(1)}(f^{(2)}.g), \quad \forall f, g \in k[V],$$

where we use that the initial algebra is commutative and Ψ^D from (6.10). If we compute this in our X basis we find

$$x \bullet y = x\mathcal{L}_x(y) = x\,{}^x y.$$

It is easy to see (see remarks above) that this implies $x \bullet y = {}^x y \bullet x^y$ as required. The above construction ensures that the algebra $k[V]^{\underline{op}}$ is associative and is built on the same vector space as $k[V]$ in each degree as taking the opposite product does not change the degree. At least in the case of finite X it follows that this algebra is isomorphic to $\mathcal{A}(k, X, r)$ by the same arguments as in the proof of Proposition 6.6. □

We do not attempt the proof with infinite (X, r) here but we note $k[V]^{\underline{op}}$ is defined and associative even in this case. In the finite case, we obtain $\mathcal{A}(k, X, r)$ on the vector space of $k[V]$ with the same $\bullet$ product as in Proposition 6.6 but this time we understand its product as the 'braided-opposite', which is a novel approach to 'quantisation' via braided categories. Moreover, this approach works even for infinite X provided $\mathcal{G}$ remains abelian. From this point of view also, the classical exterior algebra $(\Omega(k[V]), \mathrm{d})$ is $\mathcal{G}$-graded and has an action of $\mathcal{G}$ by declaring that

it commutes with d. In this way it too lies in the braided category of crossed $\mathcal{G}$-modules and has a braided opposite product. The axioms of a differential exterior algebra in noncommutative geometry do not make use of any braiding (they make sense in any monoidal category with suitable additive and k-linear structure), hence we can view the entire construction in the braided category of crossed $\mathcal{G}$-modules. Now, if $\mathcal{A}$ in a braided category has differential exterior algebra (Ω, d) then one can show by braid-diagram methods [M95] that $\mathcal{A}^{\underline{op}}$ has differential exterior algebra $(\Omega^{\underline{op}}, \mathrm{d})$ where we use the graded braided opposite coproduct (the term 'graded' here refers to the $\mathbb{Z}_2$ grading in terms of odd or even differential forms and entails an additional sign according to the degree). Hence we can 'quantise' the classical exterior algebra to obtain one on $k[V]^{\underline{op}}$ by using the graded braided-opposite product which, since the initial algebra and exterior algebra are (graded) commutative, comes out as

$$f \bullet \mathrm{d}g = f^{(1)}\mathrm{d}(f^{(2)}.g), \quad \mathrm{d}f \bullet \mathrm{d}g = (\mathrm{d}f^{(1)})\mathrm{d}(f^{(2)}.g).$$

This gives the same calculus (6.8) when applied to $\mathcal{A}(k, X, r)$. Once again, these constructions are basis-independent. Over $\mathbb{C}$, we can compute it in the $\{y^i_\eta\}$ basis if we prefer with the same result (6.5). Similarly, the monoidal symmetry Ψ with respect to which $\mathcal{A}(\mathbb{C}, X, r)$ was a Hopf algebra as in Section 6.1 can also be expressed in terms of Ψ^D and its inverse if one wishes to use this approach.

Remark 6.10. Motivated by the above, we note that if we are not interested in linking up with our original diagonalisation problem, we can also redo Proposition 6.6 using $\mathcal{G}$ in place of $\mathcal{H}$ provided $\mathcal{G}$ is finite. We define V to be a $H = k(\mathcal{G}) \otimes k\mathcal{G}$-comodule by

$$\Delta_R(x) = \sum_{g \in \mathcal{G}} g(x) \otimes (\delta_g \otimes \mathcal{L}_x)$$

and we define the canonical 2-cocycle $\mathcal{F} : H \otimes H \to k$ by the same formula as in (6.9) but now with $f, f' \in k(\mathcal{G})$ and $h, h' \in k\mathcal{G}$. We obtain that $\mathcal{A}(k, X, r)$ is the cotwist of $k[V]^{\mathcal{F}}$ under the coaction of $k(\mathcal{G}) \otimes k\mathcal{G}$ by a similar computation to that in Proposition 6.6.

Proposition 6.9 when $\mathcal{G}$ is finite is then equivalent to this version of the cotwist by the action of $\mathcal{G}$. Thus, a coaction of $k(\mathcal{G})$ on a vector space V is equivalent to an action of $k\mathcal{G}$. Hence a coaction of $k(\mathcal{G}) \otimes k\mathcal{G}$ is equivalent to an action of $k\mathcal{G}$ and a coaction of $k\mathcal{G}$. In our case where $\mathcal{G}$ is abelian these make V into a crossed $k\mathcal{G}$-module which evidently is the linearization of the crossed $\mathcal{G}$-set in Lemma 6.8.

Going the other way, one could similarly view the $k(\mathcal{H}) \otimes k\mathcal{H}$ coaction in Proposition 6.6 as making V and hence $k[V]$ into a crossed $\mathcal{H}$-module. The coaction is given by the $\mathcal{H}$ grade of V_i as γ^i which is just the image of the $\mathcal{G}$-grade used above under the canonical inclusion $\mathcal{G} \subseteq \mathcal{H}$, while the action is the action of $\mathcal{G}_i$ on V_i which pulls back to the $\mathcal{G}$ action under this inclusion. Therefore we necessarily obtain the same Ψ^D from this crossed module as the one used in Proposition 6.9, and hence the same braided-opposite algebra even though the category is slightly different.

7. Epilogue

In the course of our study of $A(k,X,r)$ we observed in Lemma 6.8 that for (X,r) a finite square-free of multipermutation level 2 the set X is a crossed $\mathcal{G}$-set. As such it acquires a braiding of which the linearisation is Ψ^D in (6.10). The underlying braiding, which we denote f, is, however, set-theoretic. Hence we have the following result at the level of (X,r) analogous to our cotwisting result for $\mathcal{A}(k,X,r)$. We can state and verify it directly in maximal generality. We let τ denote the 'flip' map $\tau(x,y)=(y,x)$.

Proposition 7.1. *Let (X,r) be a nondegenerate quadratic set and define an associated non-degenerate quadratic set (X,f) where*

$$f: X\times X\to X\times X,\quad f(x,y)=({}^{x}y,x).$$

Then

(1) $r=f\circ\tau\circ f^{-1}$ iff r *is involutive with* **lri** *(or* iff r *is involutive and cyclic).*
(2) *Suppose r has* **lri**. *Then any two of the following imply the third and (1):*
   (a) ${}^{({}^{x}y)}z={}^{x}z$ *for all $x,y,z\in X$*
   (b) *f obeys the YBE*
   (c) *r obeys the YBE*
(3) *Suppose that r is square free. Then the above hold* iff (X,r) *is a symmetric set of multipermutation level ≤ 2.*

Proof. First, note that since r is nondegenerate each $\mathcal{L}_y$ is invertible hence so is f, with $f^{-1}(x,y)=(y,(\mathcal{L}_y)^{-1}x)$. The right actions associated to f are by the identity map which is also invertible and its left actions are the same as for r and hence each are invertible. Hence (X,f) is a nondegenerate quadratic set.

For part (1), writing out $r=f\circ\tau\circ f^{-1}$, we require $(\mathcal{L}_y)^{-1}x=x^y$, i.e. $x={}^{y}(x^y)$, which is equivalent to **lri** by [GIM1, Lemma 2.19], and we require ${}^{(\mathcal{L}_y)^{-1}x}y={}^{x}y$ which now reduces to the **cl1**. Thus, if r has the form stated, clearly it is involutive and **lri** holds, while conversely if r is involutive and obeys **lri** then by [GIM1, Prop. 2.25] it is cyclic and hence has the form stated. Similarly if r is cyclic and involutive then by [GIM1, Prop. 2.25] **lri** holds.

For part (2), we first compute directly that

$$\text{YBE for } f \;\Leftrightarrow {}^{x}({}^{y}z)={}^{({}^{x}y)}({}^{x}z),\quad \forall x,y,z\in X. \tag{7.1}$$

Hence, if **l1** is assumed (for example if r obeys the YBE), this condition becomes ${}^{({}^{x}y)}({}^{x^y}z)={}^{({}^{x}y)}({}^{x}z)$, which by nondegeneracy holds if and only if the condition (a) holds (we do not in fact need to assume **lri** or the full YBE in this direction).

If instead we assume **lri** and (a). Then **l1**, **l2**, **lr3** (the conditions for r to obey the YBE) each reduce to ${}^{x}({}^{y}z)={}^{y}({}^{x}z)$ for all $x,y,z\in X$. Similarly the above condition (7.1) reduces to this same commutativity condition. Hence under the assumption of **lri** and (a) for r:

$$\text{YBE for } r\Leftrightarrow \mathcal{L}_x\mathcal{L}_y=\mathcal{L}_y\mathcal{L}_x,\ \forall\ x,y\in X\Leftrightarrow \text{YBE for } f. \tag{7.2}$$

Moreover, (2)(a) implies that (X,r) is cyclic and hence if **lri** also holds then part (1) applies.

For (3), the argument is similar to the proof in Proposition 2.15, but we will be careful now to allow X infinite. Thus, condition $mpl(X,r) \leq 2$ means $\mathcal{L}_{[y]} = \mathcal{L}_{[y']}$ for all y, y' (so that the second retract is trivial), i.e. ${}^{[y]}[x] = {}^{[y']}[x]$ for all y, y', x. Equality here is in $[X]$, i.e. ${}^{({}^{y}x)}z = {}^{({}^{y'}x)}z$ for all y, y', x, z. If (X,r) is square-free then this is equivalent to ${}^{({}^{y}x)}z = {}^{x}z$ (in one direction, set $y' = x$) as in (2.5). Hence under the assumption of **lri** and square-free,

$$mpl(X,r) \leq 2 \quad \Leftrightarrow {}^{x^y}z = {}^{x}z, \quad \forall x, y, z \in X. \tag{7.3}$$

In this case, if we assume (2) then by (2)(c) (X,r) also obeys the YBE and by (1) it is involutive. Conversely, if (X,r) is a square-free involutive solution of the YBE then it is necessarily **lri** by [GIM1, Cor. 2.31] and if $mpl(X,r) \leq 2$ then by the above, (2)(a) holds as well as (2)(c). Hence all conditions hold. Note that in this case the group $\mathcal{G}(X,r)$ is abelian by (7.2) without assuming that (X,r) is finite as in Theorem 2.16(1). □

Acknowledgements. The first author would like warmly to thank José Gómez-Torrecillas for suggesting in 2006 the problem of investigating when $\mathcal{A}(\mathbb{C}, X, r)$ has a diagonal form of relations. She would also like warmly to thank Peter Cameron for valuable and fruitful discussions and for his beautiful explanation of the elementary theory of characters, essential to the present version of the paper. The work was completed while the first author was attending the Isaac Newton Institute Programme on Combinatorics and Statistical Mechanics (CSM) 2008, she thanks the Isaac Newton Institute for local support and for the inspiring working atmosphere. Finally, she thanks the ICTP in Trieste for support during the first stage of the project.

References

[AS] Artin, M. and Schelter, W., *Graded algebras of global dimension 3*, Adv. Math. **66** (1987), 171–216.

[C] Peter J. Cameron, *Permutation Groups*, Cambridge University Press **45** (1999) 220pp.

[C08] Peter J. Cameron, *Introduction to Algebra*, Oxford University Press (2008) 337pp.

[CGI] Cameron, P and Gateva-Ivanova, T. , Multipermutation solutions of YBE, Preprint, 2008.

[D] Douglas, J., *On the Basis Theorem for finite abelian groups: IV*, Proc. National Academy of Sciences of U.S.A. **39** (1953), 307–310.

[ESS] Etingof, P., Schedler, T. and Soloviev, A., *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. **100** (1999), 169–209.

[GI94] Gateva-Ivanova, T., *Noetherian properties of skew polynomial rings with binomial relations*, Trans. Amer. Math. Soc. **343** (1994), 203–219.

[GI96-1] Gateva-Ivanova, T., *Skew polynomial rings with binomial relations*, J. Algebra **185** (1996), 710–753.

[GI96-2] Gateva-Ivanova, T., *Regularity of the skew polynomial rings with binomial relations*, Preprint (1996).

[GI00] Gateva-Ivanova, T., *Set theoretic solutions of the Yang-Baxter equation*, Mathematics and education in Mathematics, Proc. of the Twenty Ninth Spring Conference of the Union of Bulgarian Mathematicians, Lovetch (2000), 107-117.

[GI04] T. Gateva-Ivanova, *Quantum binomial algebras, Artin-Schelter regular rings, and solutions of the Yang-Baxter equations*, Serdica Math. J. **30** (2004), 431-470.

[GI] Gateva-Ivanova, T., *A combinatorial approach to the set-theoretic solutions of the Yang-Baxter equation*, J.Math.Phys., **45** (2004), 3828–3858.

[GI08] Gateva-Ivanova, T.. *Set-theoretic solutions of YBE, a combinatorial approach* - Talk to the seminar Combinatorics and Statistical Mechanics, Isaac Neuton Institute, March 2008.

[GIM1] T. Gateva-Ivanova, T. and Majid, S., *Matched pairs approach to set theoretic solutions of the Yang-Baxter equation*, J. Algebra 319 (2008) 1462-1529.

[GIM2] T. Gateva-Ivanova, T. and Majid, S., *Set Theoretic Solutions of the Yang-Baxter Equations, Graphs and Computations*, J. Symb. Comp. 42 (2007) 1079-1112.

[GB] Gateva-Ivanova, T. and Van den Bergh, M., *Semigroups of I-type*, J. Algebra **206** (1998), 97–112.

[GJO] Gateva-Ivanova, T., Jespers, E. and Okninski, J., *Quadratic algebras of skew polynomial type and underlying semigroups*, arXiv:math.RA/0210217 v1; J.Algebra, **270** (2003), 635-659.

[JO] Jespers, E. and Okninski, J., *Binomial Semigroups*, J. Algebra **202** (1998), 250–275.

[LYZ] Lu, J., Yan, M. and Zhu, Y., *On the set-theoretical Yang-Baxter equation*, Duke Math. J. **104** (2000), 1–18.

[M90] Majid, S., Matched pairs of Lie groups associated to solutions of the Yang-Baxter equations. *Pac. J. Math.*, **141** (1990) 311–332.

[M95] Majid, S., *Foundations of quantum group theory*, Cambridge Univ. Press (1995).

[M] Manin, Yu., Quantum Groups and Non Commutative Geometry Montreal University Report No. CRM- 1561, 1988

[R] Rump, W., *A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation*, Advances in Mathematics, **193** (2005), 40–55.

[T] Takeuchi, M., *Survey on matched pairs of groups. An elementary approach to the ESS-LYZ theory*, Banach Center Publ. **61** (2003), 305–331.

[V] Veselov, A.P., Yang-Baxter maps: dynamical point of view, arXiv:math/0612814v1 [math.QA]

TGI: Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia 1113, Bulgaria, S.M: Queen Mary, University of London, School of Mathematics, Mile End Rd, London E1 4NS, UK

E-mail address: tatianagateva@yahoo.com, tatyana@aubg.bg, s.majid@qmul.ac.uk