Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Advances in Mathematics 193 (2005) 40–55
ADVANCES IN Mathematics
http://www.elsevier.com/locate/aim

A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation

Wolfgang Rump*

Institut für Algebra und Zahlentheorie, Universität Stuttgart Pfaffenwaldring 57, D-70550 Stuttgart, Germany

Received 28 August 2003; accepted 18 March 2004

Available online 20 July 2004

Communicated by P. Etingof
Dedicated to Professor C.M. Ringel on the occasion of his 60th birthday

Abstract

It is known that every skew-polynomial ring with generating set X and binomial relations in the sense of Gateva-Ivanova (Trans. Amer. Math. Soc. 343 (1994) 203) is an Artin-Schelter regular domain of global dimension $|X|$. Moreover, every such ring gives rise to a non-degenerate unitary set-theoretical solution $R : X^2 \to X^2$ of the quantum Yang-Baxter equation which fixes the diagonal of X^2. Gateva-Ivanova's conjecture (Talk at the International Algebra Conference, Miskolc, Hungary, 1996) states that conversely, every such solution R comes from a skew-polynomial ring with binomial relations. An equivalent conjecture (Duke Math. J. 100 (1999) 169) says that the underlying set X is R-decomposable. We prove these conjectures and construct an indecomposable solution R with $|X| = \infty$ which shows that an extension to infinite X is false.

MSC: primary: 81R50

Keywords: Yang-Baxter equation; Set-theoretical solution; Artin-Schelter regular; Cycle set

*Fax: +49-711-685-5322.
E-mail address: rump@mathematik.uni-stuttgart.de.

0001-8708/$ - see front matter
doi:10.1016/j.aim.2004.03.019

1. Introduction

The original quantum Yang-Baxter equation

$$R^{12}R^{13}R^{23} = R^{23}R^{13}R^{12}$$

is an equation in $\mathrm{End}(V^{\otimes 3})$, where V is a vector space, and R^{ij} indicates the action of a linear operator $R \in \mathrm{End}(V \otimes V)$ on the ith and jth component of $V^{\otimes 3}$. Drinfeld [1] suggested to study solutions R induced by a map $X \times X \to X \times X$, where X is a basis of the vector space V. The problem to find and investigate such *set-theoretical solutions* has attracted several authors, e.g. [2,4,7,9,12,14,15]. Relationships to other mathematical structures, such as quantum binomial algebras [5,6,11], semigroups of I-type and Bieberbach groups [9,13], colourings of plane curves and bijective 1-cocycles [4], semisimple minimal triangular Hopf algebras [3], dynamical systems [14], and geometric crystals [2], have been discovered.

There is an obvious set-theoretical version of the *unitarity condition* $R^{21}R = 1$, which implies that $R : X^2 \to X^2$ is bijective. If $R(x, y) = (x^y, {}^x y)$, then R is said to be *non-degenerate* if the component maps $x \mapsto x^y$ and $y \mapsto {}^x y$ are bijective. A classification of non-degenerate unitary solutions R: $X^2 \to X^2$ in terms of an associated structure group was given by Etingof et al. [4]

If such a solution R fixes the diagonal of X^2, then R is called *square-free* [7]. This interesting concept has its origin in a class of semigroups of I-type [5,6,9], also called semigroups of *skew-polynomial type* [7] or *binomial semigroups* [11]. They were introduced and studied by Gateva-Ivanova [5,6] and naturally lead to square-free solutions of the quantum Yang-Baxter equation. A binomial semigroup S is defined by a set $X = \{x_1, \ldots, x_n\}$ of generators and $\binom{n}{2}$ relations $x_j x_i = x_{i'} x_{j'}$ with $i < j > i' < j'$ such that every pair (i', j') occurs exactly once on the right-hand side, and the overlaps $(x_k x_j)x_i = x_k(x_j x_i)$ do not give rise to new relations in S. The corresponding square-free solution R of the quantum Yang-Baxter equation is then given by $R(x_{i'}, x_{j'}) = (x_i, x_j)$. The semigroup algebra kS over a field k is a noetherian Cohen-Macaulay domain which is Artin-Schelter regular of global dimension n.

Gateva-Ivanova's main conjecture [8] states that every square-free non-degenerate unitary solution $R : X^2 \to X^2$ of the quantum Yang-Baxter equation with $|X| < \infty$ comes from a binomial semigroup. An equivalent *decomposability conjecture* [4] says that every such $R : X^2 \to X^2$ with $|X| > 1$ admits a non-trivial decomposition $X = Y \amalg Z$ such that the subsets Y^2 and Z^2 of X^2 are invariant under R. The latter conjecture has been verified for $|X|$ prime, and for $|X| \leqslant 8$ by Etingof et al. [4], using electronic computation. Gateva-Ivanova proved this also for $|X| = pq$ with p, q prime, and verified her main conjecture for $|X| \leqslant 31$ (see [7]).

In the present article, we prove Gateva-Ivanova's main conjecture in full generality, using previous work of [4]. Furthermore, we obtain some new results on non-degeneracy of unitary solutions $R : X^2 \to X^2$ of the quantum Yang-Baxter equation. To this end, we call R *left non-degenerate* if the left component map $x \mapsto x^y$ of R is bijective for all $y \in X$. We introduce a *cycle set* as a (not necessarily finite) set

X with a binary operation $X^2 \dot{\to} X$ such that the left multiplication $y \mapsto x \cdot y$ is bijective, and the equation

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

holds for all $x, y, z \in X$. Every cycle set X gives rise to a left non-degenerate unitary solution R of the quantum Yang-Baxter equation, and vice versa. Moreover, R is non-degenerate if and only if the map $x \mapsto x \cdot x$ is bijective, and R is square free if and only if $x \cdot x = x$ holds for all $x \in X$.

We shall provide several different characterizations for non-degeneracy in terms of cycle sets. For instance, a cycle set X is non-degenerate if and only if there exists a (necessarily unique) dual cycle set structure on X (see Definition 1). Every cycle set admits a natural extension to the free abelian monoid $\mathbb{N}^{(X)}$, and there is a further extension to $\mathbb{Z}^{(X)}$ if and only if X is non-degenerate (Proposition 6). In Theorem 2, we show that every finite cycle set is non-degenerate.

For a cycle set X, the left multiplications generate a permutation group $\mathrm{G}(X)$ which coincides with the reduced structure group G_X^0 of [4]. There is a certain reciprocity between $\mathrm{G}(X)$ (more generally: a *cycle group*, Section 5) and its underlying cycle set X, like the relationship between Lie groups and Lie algebras. The cycle group $\mathrm{G}(X)$ is connected with an abelian group $\mathrm{A}(X)$ via a bijective 1-cocycle $\bar{\tau}$: $\mathrm{G}(X) \sim \to \mathrm{A}(X)$ (see [4]), and there is a canonical cycle set morphism $X \to \mathrm{A}(X)$. A cycle set A which carries a $\mathrm{G}(A)$-module structure such that $0 \cdot a = a$ and $(a + b) \cdot c = (a \cdot b) \cdot (a \cdot c)$ holds for all $a, b, c \in A$, will be called *linear*. Apart from $\mathrm{A}(X)$, the Jacobson radical $\operatorname{Rad} R$ of any ring R can be regarded as a linear cycle set (Example 2).

To prove Gateva-Ivanova's conjecture, speaking in terms of cycle sets, we have to show that every square-free cycle set X with $1 < |X| < \infty$ admits a non-trivial decomposition $X = Y \amalg Z$ with $X \cdot Y \subset Y$ and $X \cdot Z \subset Z$. To verify this, we consider the image X_p of X in the p-component of the abelian group $\mathrm{A}(X)$ for any rational prime p. It turns out that X_p is again a square-free cycle set, but the natural map $X \to X_p$ need not be a cycle set morphism. Our proof makes use of the fact [4] that $\mathrm{G}(X)$ is solvable, and that $\mathrm{G}(X_p)$ is a Sylow p-subgroup of $\mathrm{G}(X)$, hence nilpotent.

Finally, we give an example of an indecomposable infinite square-free cycle set X, which shows that the decomposability conjecture [4] is false when X is infinite.

2. The quantum Yang-Baxter equation

For an arbitrary set X, let $\mathrm{S}(X)$ be the group of bijections $X \to X$. In this section, we study set-theoretical solutions $R \in \mathrm{S}(X \times X)$ of the quantum Yang-Baxter equation (QYBE)

$$R^{12} R^{13} R^{23} = R^{23} R^{13} R^{12}, \tag{1}$$

where for any $n \geqslant 2$, the induced map $R^{ij}: X^n \to X^n$ acts as R on the ith and jth component (in this order), and as the identity map on the other $n-2$ components. Thus (1) can be regarded as an equation in $\mathrm{S}(X^3)$. The map $R: X^2 \to X^2$ has two components

$$R(x,y) = (x^y, {}^x y) \tag{2}$$

which are binary operations on X. If R satisfies the *unitarity condition*

$$R^{21}R = 1, \tag{3}$$

these operations are related to each other by the equations

$$(x^y) = x, \quad ({}^x y)^{(x^y)} = y. \tag{4}$$

We call R *left non-degenerate* if the map $x \mapsto x^y$ is bijective for all $y \in X$. If, in addition, $y \mapsto {}^x y$ is bijective for all $x \in X$, then R is said to be *non-degenerate* [4].

Assume that R is left non-degenerate. Then there is a well-defined map

$$\sigma: X \to \mathrm{S}(X) \tag{5}$$

given by $\sigma(x)(y^x) = y$ for all $x, y \in X$. We call R *square free* if $R(x,x) = (x,x)$ holds for all $x \in X$. If R is unitary, this property is equivalent to $\sigma(x)(x) = x$.

For the rest of this section, let $R \in \mathrm{S}(X^2)$ be a square-free non-degenerate unitary solution of (1). The group G_X with generating set X and relations

$$x \cdot y = ({}^x y) \cdot (x^y) \tag{6}$$

for all $x, y \in X$ is called the *structure group* [4]. By Etingof et al. [4, Propositions 2.3 and 2.4] there is an embedding of G_X into a semidirect product

$$\phi: \ \mathrm{G}_X \hookrightarrow \mathrm{S}(X) \ltimes \mathbb{Z}^{(X)}, \tag{7}$$

where $\mathrm{S}(X)$ acts on the free abelian group $\mathbb{Z}^{(X)}$ by linear extension

$$\pi\Big(\sum n_x x\Big) := \sum n_x \pi(x), \tag{8}$$

and the elements of $\mathrm{S}(X) \ltimes \mathbb{Z}^{(X)}$ satisfy the commutation rule $\pi a = \pi(a)\pi$ for $\pi \in \mathrm{S}(X)$ and $a \in \mathbb{Z}^{(X)}$. The map ϕ is given by $\phi(x) := \sigma(x)x$, $\forall x \in X$.

By this definition, the first component of ϕ yields an extension $\sigma: \mathrm{G}_X \to \mathrm{S}(X)$ of the map (5) to a left action of G_X on X. Thus, $\mathbb{Z}^{(X)}$ becomes a left G_X-module. The second component of ϕ is a 1-cocycle $\tau: \mathrm{G}_X \to \mathbb{Z}^{(X)}$ with multiplication rule $\tau(gh) = h^{-1}\tau(g) + \tau(h)$, and τ is bijective by Etingof et al. [4, Proposition 2.5].

Regarding G_X as a subgroup of $\mathrm{S}(X) \ltimes \mathbb{Z}^{(X)}$, the left G_X-module structure $\mathrm{G}_X \to \mathrm{Aut}(\mathbb{Z}^{(X)})$ on $\mathbb{Z}^{(X)}$ turns into conjugation, i.e. $g \in \mathrm{G}_X$ is mapped to the automorphism $a \mapsto gag^{-1}$ of $\mathbb{Z}^{(X)}$. Moreover, the kernel of the group homomorphism

$\sigma\colon G_X \to S(X)$ is identified with $G_X \cap \mathbb{Z}^{(X)}$. Thus, if we define

$$G(X) := \sigma(G_X) \subset S(X), \quad A(X) := \mathbb{Z}^{(X)}/G_X \cap \mathbb{Z}^{(X)}, \tag{9}$$

we get a commutative diagram with exact rows

$$\begin{array}{ccccc} G_X \cap \mathbb{Z}^{(X)} & \hookrightarrow & G_X & \twoheadrightarrow & G(X) \\ || & & \downarrow\tau & & \downarrow\bar{\tau} \\ G_X \cap \mathbb{Z}^{(X)} & \hookrightarrow & \mathbb{Z}^{(X)} & \twoheadrightarrow & A(X), \end{array} \tag{10}$$

where $\bar{\tau}$ is a bijective 1-cocycle with respect to the induced action of $G(X)$ on $A(X)$.

3. Decomposability of square-free solutions

In [5,6], Gateva-Ivanova considers semigroups S of *skew-polynomial type*, given by a generating set $X = \{x_1, \dots, x_n\}$ and quadratic relations $x_j x_i = x_{i'} x_{j'}$. The corresponding semigroup rings kS over a field k are Artin-Schelter regular of global dimension n. Moreover, each such semigroup S is of I-type [9,13] and gives rise to a square-free non-degenerate unitary solution $R\colon X^2 \to X^2$ of the QYBE. Gateva-Ivanova's conjecture [8] states that conversely, every square-free non-degenerate unitary solution R over a finite set X is obtained in this way.

Following [4], we call a non-degenerate solution $R \in S(X^2)$ of the QYBE *decomposable* if there exists a non-trivial partition $X = Y \amalg Z$ with $R(Y^2) \subset Y^2$ and $R(Z^2) \subset Z^2$, such that the restrictions of R to Y^2 and Z^2 are again non-degenerate. If R is unitary, this condition simply means that Y and Z are invariant under $G(X)$. By an observation of [4], Gateva-Ivanova's conjecture is equivalent to the following statement, which will be proved in the remainder of this section.

Theorem 1. *Let X be a finite set with more than one element. Then every square-free non-degenerate unitary solution $R \in S(X^2)$ of the QYBE is decomposable.*

Proof. By Etingof et al. [4], 3.2, R induces a square-free non-degenerate unitary solution $\bar{R}$ on the image $\sigma(X)$ of the map (5). If $|\sigma(X)| = 1$, there is a single permutation $\pi \in S(X)$ with $\sigma(x) = \pi$ for all $x \in X$. Since R is square free, we get $\pi(x) = \sigma(x)(x) = x$ for all $x \in X$. Hence R is decomposable. If $|\sigma(X)| > 1$, a decomposition of $\bar{R}$ lifts to a decomposition of R. Thus by induction, we may assume that the map $\sigma\colon X \to S(X)$ is injective. By (10), this implies that the composition $X \hookrightarrow \mathbb{Z}^{(X)} \twoheadrightarrow A(X)$ is injective. So we can regard X as a subset of $A(X)$.

Suppose that X is indecomposable. Then $G(X)$ acts transitively on X. So there exists an intransitive normal subgroup N of $G(X)$, such that every strictly greater normal subgroup is transitive. Let $N' \supset N$ be a normal subgroup of $G(X)$ such that N'/N is a minimal normal subgroup of $G(X)/N$. By Etingof et al. [4, Theorem 2.15], the group $G(X)$ is solvable. Hence N'/N is an elementary abelian p-group. Since N is

normal, every element of $\mathrm{G}(X)$ induces a permutation of the set X/N of N-orbits on X. Thus N' acts transitively on X/N. Since the p-component $\mathrm{A}(X)_p$ of the abelian group $\mathrm{A}(X)$ is invariant under the action of $\mathrm{G}(X)$, the inverse image $S_p := \bar{\tau}^{-1}(\mathrm{A}(X)_p)$ is a subgroup of $\mathrm{G}(X)$. Therefore, $|S_p| = |\mathrm{A}(X)_p|$ shows that S_p is a Sylow p-subgroup of $\mathrm{G}(X)$. Hence S_pN/N is a Sylow p-subgroup of $\mathrm{G}(X)/N$. Since N'/N is a normal p-subgroup of $\mathrm{G}(X)/N$, this implies that $N' \subset S_pN$. Therefore, S_p acts transitively on X/N.

Similar to the above reasoning, we find a normal subgroup P of S_p acting intransitively on X/N, such that every strictly greater normal subgroup of S_p acts transitively on X/N. Thus, every element of S_p gives rise to a permutation of the set Y of P-orbits on X/N. Since S_p is nilpotent, there exists a normal subgroup $P' \supset P$ of S_p with $|P'/P| = p$. So, we get an induced transitive action of P'/P on Y, whence $|Y| = p$. Let X_p be the image of the map $X \hookrightarrow \mathrm{A}(X) \twoheadrightarrow \mathrm{A}(X)_p$. Then X_p generates $\mathrm{A}(X)_p$. Since $\bar{\tau}$ is a bijective 1-cocycle, $\bar{\tau}^{-1}(X_p)$ generates S_p. Hence, there is at least one element $\pi \in \bar{\tau}^{-1}(X_p)$ which permutes the elements of Y non-trivially. As the order of π is a power of p, this permutation must be a p-cycle. On the other hand, let $x \in X$ be an element which is mapped to $\bar{\tau}(\pi)$ under the canonical map $X \twoheadrightarrow X_p$. Then $\bar{\tau}(\pi) = mx$ for some $m \in \mathbb{N}$.

We show that the inverse image $\rho := \bar{\tau}^{-1}(x) \in \mathrm{G}(X)$ satisfies $\rho^m = \pi$. Assume, by induction, that $\rho^k = \bar{\tau}^{-1}(kx)$ has been proved for some $k \in \{1, \ldots, m\}$. Then $\bar{\tau}(\rho^k \cdot \rho) = \rho^{-1}\bar{\tau}(\rho^k) + \bar{\tau}(\rho) = \rho^{-1}kx + x = k\sigma(x)^{-1}(x) + x = (k+1)x$. This proves our claim. Hence we get $\pi(x) = \rho^m(x) = \sigma(x)^m(x) = x$. But this implies that π leaves the P-orbit of the N-orbit of x fixed, a contradiction. □

4. Cycle sets and non-degeneracy

Let X be a set with a binary operation $X \times X \to X$. If left multiplication $y \mapsto x \cdot y$ is invertible, the operation can be expressed by a map $\sigma: X \to \mathrm{S}(X)$ with

$$\sigma(x)(y) = x \cdot y. \tag{11}$$

We call X a *cycle set* if left multiplication is invertible, and the equation

$$(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z) \tag{12}$$

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

Proposition 1. *There is a bijective correspondence between cycle sets X and left non-degenerate unitary solutions R of the QYBE* (1).

In the sequel, we call R the *R-matrix* of X.

Proof. Assume first that $(X,\cdot)$ is a cycle set. Define $y^x := \sigma(x)^{-1}(y)$ and put

$$ {}^x y := x^y \cdot y. \tag{13}$$

Then we get a left non-degenerate bijection (2) which satisfies (4) by definition. Conversely, every left non-degenerate bijection (2) which satisfies the unitarity condition (3) yields a binary operation (11) via (5), such that (13) holds by virtue of (4). Therefore, it remains to be shown that under this correspondence, the QYBE (1) becomes equivalent to (12).

Explicitly, the QYBE (1) states that for all $x,y,z\in X$,

$$ x^{({}^y z)}(y^z) = x^{yz}, \quad {}^{(x^{(yz)})}(y^z) = ({}^x y)^{({}^{(x^y)}z)}, \quad {}^{xy}z = {}^{({}^x y)(x^y)}z. \tag{14}$$

The first of these equations can be written as $x = {}^y z \cdot (y^z \cdot x^{yz})$. By the substitution $x\mapsto y\cdot(z\cdot x)$, this is equivalent to $y\cdot(z\cdot x) = ({}^y z)\cdot(y^z\cdot x) = (y^z\cdot z)\cdot(y^z\cdot x)$. Replacing y by $z\cdot y$ gives $(z\cdot y)\cdot(z\cdot x) = (y\cdot z)\cdot(y\cdot x)$. Now an easy verification shows that (12) implies the other two equations in (14) (cf. [4, Proposition 2.2]). Hence (1) and (12) are equivalent. □

Next let us turn our attention to non-degeneracy. First, we prove

Lemma 1. *Let X be a cycle set. Then*

$$ ({}^x y)\cdot({}^x y) = x\cdot(y\cdot y) \tag{15}$$

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

Proof. By (13) and (12), we have $({}^x y)\cdot({}^x y) = (x^y\cdot y)\cdot(x^y\cdot y) = (y\cdot x^y)\cdot(y\cdot y) = x\cdot(y\cdot y)$. □

Definition 1. We call a cycle set X *non-degenerate* if every element admits a unique square root, i.e. if the map $x\mapsto x\cdot x$ is bijective. A binary operation $X\times X \overset{\circ}{\to} X$ will be called *dual* to the operation $X\times X \overset{\cdot}{\to} X$ on X if the equations

$$ (x\cdot y)\circ(y\cdot x) = x, \tag{16}$$

$$ (x\circ y)\cdot(y\circ x) = x \tag{17}$$

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

Proposition 2. *For a cycle set X, the following are equivalent*:

(a) *X is non-degenerate.*
(b) *The R-matrix of X is non-degenerate.*
(c) *The binary operation $X\times X\overset{\cdot}{\to}X$ admits a dual.*

If these equivalent conditions hold, then $(X,\circ)$ *is again a cycle set, and the map* $y\mapsto x\circ y$ *is inverse to* $y\mapsto {}^{x}y$ *for all* $x\in X$.

Proof. (a) $\Rightarrow$ (b): To show that $y\mapsto {}^{x}y$ is surjective, let $x,z\in X$ be given. Then there exists an element $y\in X$ with $y\cdot y=(z\cdot z)^{x}$. Hence (15) gives $z\cdot z=x\cdot(y\cdot y)=({}^{x}y)\cdot({}^{x}y)$, which yields $z={}^{x}y$. Moreover, (15) shows that y is uniquely determined by z.

(b) $\Rightarrow$ (c): Let $x\mapsto y\circ x$ denote the inverse of $x\mapsto {}^{y}x$. Then (13) implies $y\circ(y^{x}\cdot x)=y\circ {}^{y}x=x$, whence (16) holds. The first equation of (4) gives ${}^{x}y\circ x=x^{y}$. Therefore, $y\circ x=x^{x\circ y}$, and thus (17) holds.

(c) $\Rightarrow$ (a): The injectivity and surjectivity of $x\mapsto x\cdot x$ follows immediately by the substitution $y:=x$ in (16) and (17), respectively.

Thus if X is non-degenerate, then (13) and (16) give $x\circ {}^{x}y=(y\cdot x^{y})\circ(x^{y}\cdot y)=y$, which shows that $y\mapsto x\circ y$ is inverse to $y\mapsto {}^{x}y$. That $(X,\circ)$ is a cycle set follows by dualizing the corresponding argument in the proof of Proposition 1. □

For a non-degenerate cycle set X, let us call $X^{\circ}:=(X,\circ)$ the *dual* of X. Thus $X^{\circ\circ}=X$. Accordingly, every non-degenerate unitary solution (2) of the QYBE has a *dual* solution R°, namely,

$$R^{\circ}(x,y)=({}^{y}x,y^{x}). \tag{18}$$

Definition 2. A cycle set X will be called *square free* (*balanced*) if the first (second) of the following equations holds for all $x,y\in X$:

$$x\cdot x=x, \tag{19}$$

$$x\cdot y={}^{x}y. \tag{20}$$

Thus, X is square free if and only if its R-matrix satisfies $R(x,x)=(x,x)$ for all $x\in X$. Note that every balanced cycle set is non-degenerate, with dual operation $x\circ y=y^{x}$. We will show that every square-free cycle set is balanced.

For any element x of a cycle set X, the permutation $\sigma(x)$ leads to a partition of X into (possibly infinite) cycles. Let $\mathrm{C}_x(y)$ denote the cycle containing y. Thus, X is square-free if and only if $\mathrm{C}_x(x)=\{x\}$ for all $x\in X$. The following result generalizes Gateva-Ivanova's cyclic conditions [5,7] to balanced cycle sets.

Proposition 3. *Let* X *be a balanced cycle set. Then every pair of elements* $x,y\in X$ *gives rise to a pair of disjoint or equal cycles* $\mathrm{C}_y(x)$ *and* $\mathrm{C}_x(y)$. *Moreover,* $u\cdot w=v\cdot w$ *holds for each* $u,v\in\mathrm{C}_x(y)$ *and* $w\in\mathrm{C}_y(x)$. *Every square-free cycle set is balanced.*

Proof. By (13), Eq. (20) can be written as $x\cdot y=x^{y}\cdot y$, and if we replace x by $y\cdot x$, we get $(y\cdot x)\cdot y=x\cdot y$. By induction, this yields $w\cdot y=x\cdot y$ for all $w\in\mathrm{C}_y(x)$, and

thus $(x \cdot y) \cdot w = (w \cdot y) \cdot w = y \cdot w$. Again by induction, this implies that $u \cdot w = y \cdot w$ for all $u \in \mathrm{C}_x(y)$. Hence, if $w \in \mathrm{C}_x(y) \cap \mathrm{C}_y(x)$, then $\mathrm{C}_x(y) = \mathrm{C}_w(w) = \mathrm{C}_y(x)$. If X is square-free, then $x \cdot y = (y \cdot x^y) \cdot (y \cdot y) = (x^y \cdot y) \cdot (x^y \cdot y) = x^y \cdot y = {}^x y$. □

Remark. (1) For a square-free cycle set, Proposition 3 implies that the cycles $\mathrm{C}_x(y)$ and $\mathrm{C}_y(x)$ are disjoint when $x \neq y$.

(2) By Theorem 1, a square-free cycle set admits an ordering which respects the cycles (cf. [7, Theorem 6.5]), i.e. we have the following corollary. (For subsets Y, Z of a linearly ordered set X, write $Y < Z$ if $y < z$ holds for all $y \in Y$ and $z \in Z$.)

Corollary. *Every finite square-free cycle set X admits a linear ordering such that $x < y$ implies $\mathrm{C}_y(x) < \mathrm{C}_x(y)$ for all $x, y \in X$.*

Proof. By Theorem 1, X has a non-trivial decomposition $X = Y \amalg Z$ such that Y and Z are cycle sets with respect to the induced binary operation. We put $Y < Z$ and proceed by induction. Since X is finite, we end up with a linear ordering having the desired property. □

5. Cycle groups

For a cycle set X with R-matrix R, the subgroup of $\mathrm{S}(X)$ generated by the image of the map $\sigma: X \to \mathrm{S}(X)$ coincides with $\mathrm{G}(X)$. We define a map $\mathrm{G}(X) \times X \xrightarrow{+} \mathrm{G}(X)$ by

$$(\pi + x)(y) := \pi(x) \cdot \pi(y). \tag{21}$$

Then $(\pi\rho + x)(y) = \pi(\rho(x)) \cdot \pi(\rho(y)) = (\pi + \rho(x))(\rho(y))$ and $((\pi + x) + y)(z) = (\pi + x)(y) \cdot (\pi + x)(z) = (\pi(x) \cdot \pi(y)) \cdot (\pi(x) \cdot \pi(z))$. Hence (12) implies that

$$\pi\rho + x = (\pi + \rho(x))\rho, \tag{22}$$

$$(\pi + x) + y = (\pi + y) + x \tag{23}$$

holds for all $x, y \in X$ and $\pi, \rho \in \mathrm{G}(X)$.

Definition 3. Let (G, X) be a pair consisting of a group G acting on a set X together with a map $G \times X \xrightarrow{+} G$. We call (G, X) a *cycle group* if the equations (22) and (23) hold for $x, y \in X$ and $\pi, \rho \in G$. We abbreviate (G, X) by G when the underlying set X is clear from the context.

The above calculation shows that every cycle set X naturally defines a cycle group $G(X)$. Conversely, we have

Proposition 4. *For any cycle group (G, X), the operation*

$$x \cdot y := (1 + x)(y) \tag{24}$$

on X, where $1 \in G$ denotes the unit element, makes X into a cycle set.

Proof. Eq. (22) implies that $(x \cdot y) \cdot (x \cdot z) = (1 + x)(y) \cdot (1 + x)(z) = (1 + (1 + x)(y))((1 + x)(z)) = (1 \cdot (1 + x) + y)(z) = ((1 + x) + y)(z)$. So the assertion follows by (23). □

For a cycle group (G, X), let $\mathbb{N}^{(X)}$ denote the free commutative monoid generated by X. So the elements of $\mathbb{N}^{(X)}$ are finite linear combinations $\sum n_x x$ with coefficients n_x in $\mathbb{N} := \{0, 1, 2, \ldots\}$. The G-action on X admits a natural extension to $\mathbb{N}^{(X)}$ via (8). On the other hand, Eq. (23) shows that the map $G \times X \xrightarrow{+} G$ extends to an action of $\mathbb{N}^{(X)}$ on G, i.e.

$$\pi + 0 = \pi, \quad \pi + (a + b) = (\pi + a) + b \tag{25}$$

holds for all $\pi \in G$ and $a, b \in \mathbb{N}^{(X)}$.

Proposition 5. *Every cycle group (G, X) admits a natural extension to a cycle group $(G, \mathbb{N}^{(X)})$.*

Proof. It remains to prove (22) for all $x \in \mathbb{N}^{(X)}$. For $x = 0$, this is trivial. Inductively, assume that $\pi\rho + a = (\pi + \rho(a))\rho$ holds for some $a \in \mathbb{N}^{(X)}$. Then for any $x \in X$, we have $\pi\rho + (a + x) = (\pi + \rho(a))\rho + x = ((\pi + \rho(a)) + \rho(x))\rho = (\pi + (\rho(a) + \rho(x)))\rho = (\pi + \rho(a + x))\rho$. □

In particular, Proposition 5 shows that every cycle set X admits a natural extension to $\mathbb{N}^{(X)}$ such that

$$\mathrm{G}(\mathbb{N}^{(X)}) = \mathrm{G}(X).$$

Note, however, that the extended map $\sigma : \mathbb{N}^{(X)} \to \mathrm{G}(X)$ need not be surjective. (For example, consider the infinite cycle set $X = \mathbb{Z}$ with $n \cdot m := m + 1$ for all $n, m \in \mathbb{Z}$.) So the question arises whether X admits a further extension to the free abelian group $\mathbb{Z}^{(X)}$. For a cycle group (G, X), the G-action on X extends to $\mathbb{Z}^{(X)}$ via (8). If the map $G \times X \xrightarrow{+} G$ extends to a $\mathbb{Z}^{(X)}$-action on G, then the argument in the proof of Proposition 5 shows that (22) is automatically satisfied. Then the extended cycle group $(G, \mathbb{Z}^{(X)})$ will be called the *linear extension* of (G, X) to $\mathbb{Z}^{(X)}$.

Proposition 6. *A cycle group G admits a linear extension to $\mathbb{Z}^{(X)}$ if and only if the underlying cycle set X is non-degenerate.*

Proof. Suppose that the linear extension to $\mathbb{Z}^{(X)}$ exists. Then for each $x\in X$, we have $x=(1\cdot(1-x)+x)(x)=(1-x)(x)\cdot(1-x)(x)$ by virtue of (22) and (24). Hence X is non-degenerate. Conversely, let X be non-degenerate. It suffices to verify that

$$(\pi-x)(y):=\pi(y)^{\pi(x)\circ\pi(x)} \tag{26}$$

with $\pi\in G$ and $x,y\in X$ provides an inverse to the map $\pi\mapsto\pi+x$. In fact, Eq. (16) gives $((\pi+x)-x)(y)=(\pi+x)(y)^{(\pi+x)(x)\circ(\pi+x)(x)}=(\pi(x)\cdot\pi(y))^{\pi(x)}=\pi(y)$. By (17), we have $\pi(x)\circ\pi(x)=\pi(x)^{\pi(x)\circ\pi(x)}=(\pi-x)(x)$. Hence $((\pi-x)+x)(y)=(\pi-x)(x)\cdot(\pi-x)(y)=(\pi(x)\circ\pi(x))\cdot\pi(y)^{\pi(x)\circ\pi(x)}=\pi(y)$. □

Similar to the relationship between Lie groups and Lie algebras, the correspondence between cycle groups and cycle sets is not one-to-one. Let us call a cycle group *G faithful* if G acts faithfully on its underlying cycle set X. If G is faithful, we always identify G with a subgroup of $\mathrm{S}(X)$, so that $\mathrm{G}(X)$ becomes a subgroup of G via (24). For two elements π,ρ of G, let us write $\pi\approx\rho$ if $\pi+a=\rho+b$ for some $a,b\in\mathbb{N}^{(X)}$. We call π and ρ *connected* if there exists a sequence $\pi\approx\pi_1\approx\cdots\approx\pi_n=\rho$ in G.

Proposition 7. *For a faithful cycle group $G\subset\mathrm{S}(X)$, the connected component of* 1 *coincides with* $\mathrm{G}(X)$. *There is a bijective correspondence $X\mapsto\mathrm{G}(X)$ between cycle sets and faithful connected cycle groups.*

Proof. By (22), we have $1\cdot\pi+x=(1+\pi(x))\pi$, i.e.

$$\pi+x=(1+\pi(x))\pi \tag{27}$$

for all $\pi\in G$ and $x\in X$. By (24) and induction, this implies that $\mathrm{G}(X)$ is the connected component of 1. The remaining assertion is an immediate consequence of Proposition 4, and Eqs. (21) and (27). □

6. Reducedness and linearity

Recall that an equivalence $\sim$ on a set X with a binary operation $X\times X\dot{\to}X$ is said to be a *congruence relation* if for all $x,x',y,y'\in X$,

$$x\sim x',\ y\sim y'\Rightarrow x\cdot y\sim x'\cdot y'. \tag{28}$$

Lemma 2. *For any cycle set X, the map* (5) *defines a congruence relation*

$$x \sim y \ :\Leftrightarrow \sigma(x) = \sigma(y). \tag{29}$$

Proof. Assume that $\sigma(x) = \sigma(x')$ and $\sigma(y) = \sigma(y')$. For any $z \in X$, this gives $(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z) = (y' \cdot x) \cdot (y' \cdot z) = (x \cdot y') \cdot (x \cdot z) = (x' \cdot y') \cdot (x \cdot z)$. Hence $\sigma(x \cdot y) = \sigma(x' \cdot y')$. □

Thus for any cycle set X, the image $\sigma(X) \subset \mathrm{S}(X)$ can be endowed with an induced binary operation

$$\sigma(x) \cdot \sigma(y) := \sigma(x \cdot y) \tag{30}$$

which satisfies (12). We call $\sigma(X)$ the (*first*) *reduction* of X, and X will be called *reduced* if σ is injective. We shall see below that the reduction of a non-degenerate cycle set is again a (non-degenerate) cycle set.

Remark. In general, the first reduction $\sigma(X)$ of a non-degenerate cycle set X need not be reduced. Therefore, the first reduction of $\sigma(X)$ can be viewed as a second reduction of X, and so on (cf. [4, 3.2]). On the other hand, the reduction of a degenerate cycle set need not even be a cycle set.

Example 1. It is easy to verify that the binary operation

$$m \cdot n := n - \min\{m, 0\}$$

makes $\mathbb{Z}$ into a (degenerate) cycle set. However, left multiplication in the reduction $\sigma(\mathbb{Z})$ of $(\mathbb{Z}, \cdot)$ is no longer surjective. Thus $\sigma(\mathbb{Z})$ is not a cycle set.

Definition 4. A cycle group (G, A) will be called *linear* if A is a left G-module with respect to its G-action, and $G \times A \xrightarrow{+} G$ is a group action. Accordingly, we call a cycle set A *linear* if its cycle group $\mathrm{G}(A)$ is linear.

Proposition 8. *A cycle set A is linear if and only if it is an abelian group with*

$$a \cdot (b + c) = a \cdot b + a \cdot c, \tag{31}$$

$$0 \cdot a = a, \tag{32}$$

$$(a + b) \cdot c = (a \cdot b) \cdot (a \cdot c) \tag{33}$$

for all $a, b, c \in A$. If A is reduced, there is at most one linear structure on A.

Proof. Eq. (31) states that $\mathrm{G}(A)$ acts by automorphisms on A, whereas (32) and (33) are equivalent to (25) by virtue of (21). □

Example 2. Let R be any ring, associative with 1, and let A be a right ideal contained in the Jacobson radical of R. The operation

$$a \cdot b := b(1+a)^{-1}$$

on A satisfies (31)–(33), and thus A becomes a linear cycle set. If we take $A = \operatorname{Rad} R$, then A is square-free if and only if $a^2 = 0$ for all $a \in \operatorname{Rad} R$. Thus in the square-free case, we simply have $a \cdot b = b(1-a)$, and A decomposes into $|\operatorname{Rad} R/\operatorname{Rad}^2 R|$ non-trivial $\mathrm{G}(A)$-invariant subsets. The question arises whether every square-free cycle set X can be embedded in a compatible way into the radical of a ring. The following example shows that this is not always possible.

Example 3. For $X = \{0,1,2,3,4,5\}$, define $\sigma(0) = (12)(45)$, $\sigma(1) = (345)$, $\sigma(2) = (354)$, and $\sigma(3) = \sigma(4) = \sigma(5) = 1_X$. Then X is a square-free cycle set. (X corresponds to number 1240 in Laffaille's list [11] of quantum binomial algebras with six generators.) An easy calculation shows that every cycle set morphism $f\colon X \to \operatorname{Rad} R$ into the radical of a ring R satisfies $f(3) = f(4) = f(5)$.

The R-matrix of a linear cycle set is always non-degenerate by the following:

Proposition 9. *Let A be a linear cycle set. Then A is non-degenerate, and the map $a \mapsto \sigma(a) = 1 + a$ defines a surjection*

$$A \twoheadrightarrow \mathrm{G}(A), \tag{34}$$

such that $A_0 := \{a \in A \mid \sigma(a) = 1\}$ is a $\mathrm{G}(A)$-submodule of A, and the fibers of the map (34) *coincide with the residue classes of A_0.*

Proof. By (32) and (33), we have $a = 0 \cdot a = (-a+a) \cdot a = ((-a) \cdot a) \cdot ((-a) \cdot a)$, hence

$$a = ((-a) \cdot a) \cdot ((-a) \cdot a) \tag{35}$$

for every $a \in A$, which shows that A is non-degenerate. By (22), we get $1 \cdot (1+a) + b = (1 + (1+a)(b))(1+a)$, and thus

$$1 + a + b = (1 + (1+a)(b))(1+a) \tag{36}$$

for all $a, b \in A$. Hence $(1+a)^{-1} = 1 - a \cdot a$, which proves that the map (34) is surjective. Moreover, $a \in A_0$ implies that $1 + a + b = 1 + b$. This shows that A_0 is a subgroup of A with residue classes contained in the fibers of (34). Therefore, $b \in A_0$ implies that $1 + a + b = 1 + a$. So (36) gives $1 + (1+a)(b) = 1$, that is, $(1+a)(b) \in A_0$. Hence A_0 is a $\mathrm{G}(A)$-submodule. Now the implication $1 + a + b = 1 + a \Rightarrow (1+a)(b) \in A_0 \Rightarrow b \in A_0$ shows that the fibers of the map (34) coincide with the residue classes of A_0. $\square$

Remark. By Propositions 8 and 9, a reduced linear cycle set can be regarded as a G-module A, where G is a group, together with a bijection $\sigma: A \to G$ which satisfies (33) with $a \cdot b := \sigma(a)(b)$. Then (33) simply states that σ^{-1} is a bijective cocycle in the sense of [4, Proposition 2.5].

For a non-degenerate cycle set X, Proposition 9 shows that the $\mathbb{Z}^{(X)}$-action on $\mathrm{G}(X)$ induces an action of the $\mathrm{G}(X)$-module $\mathrm{A}(X) = \mathbb{Z}^{(X)}/\sigma^{-1}(1)$ on $\mathrm{G}(X)$. Hence $(\mathrm{G}(X), \mathrm{A}(X))$ is a reduced linear cycle group, and the composition $X \hookrightarrow \mathbb{Z}^{(X)} \twoheadrightarrow \mathrm{A}(X)$ yields a canonical morphism

$$X \to \mathrm{A}(X) \tag{37}$$

of cycle sets which is injective if and only if X is reduced. Moreover, we have the

Corollary. *Let X be a non-degenerate cycle set. Then the map* (37) *is surjective if X is linear. Thus* (37) *is bijective if and only if X is reduced and linear.*

Proof. If X is linear, then the surjection (34) factors through (37). Hence (37) is surjective. □

Proposition 10. *A cycle set X is non-degenerate if and only if its reduction is a non-degenerate cycle set.*

Proof. Suppose that X is non-degenerate. Then the reduction $\sigma(X)$ is a $\mathrm{G}(X)$-invariant subset of $\mathrm{A}(X)$, hence a cycle set. For any $a \in \sigma(X)$, Eq. (35) in $\mathrm{A}(X)$ shows that $\sigma(X)$ is non-degenerate. Conversely, let the reduction $\sigma(X)$ be a non-degenerate cycle set. For a given $x \in X$, this implies that there exists an element $y \in X$ with $\sigma(x) = \sigma(y) \cdot \sigma(y) = \sigma(y \cdot y)$. Therefore, $\sigma(y \cdot x^y) = \sigma(x) = \sigma(y \cdot y)$ gives $\sigma(x^y) = \sigma(y)$, since $\sigma(y)$ is left cancellative in $\sigma(X)$. Hence $x = \sigma(y)(x^y) = \sigma(x^y)(x^y) = x^y \cdot x^y$, and thus X is non-degenerate. □

As a consequence of the preceding results on non-degeneracy, we get

Theorem 2. *Every finite cycle set is non-degenerate.*

Proof. Let X be a finite cycle set. By Proposition 5, the corresponding cycle group $\mathrm{G}(X)$ extends to $\mathbb{N}^{(X)}$. We show first that the reduction of $\mathbb{N}^{(X)}$ is again a cycle set, i.e. that

$$\sigma(a \cdot b) = \sigma(a \cdot c) \Rightarrow \sigma(b) = \sigma(c) \tag{38}$$

holds for all $a, b, c \in \mathbb{N}^{(X)}$. This follows immediately since $\sigma(a)$ has finite order in $\mathrm{G}(X)$. By (36), the implication (38) yields

$$1 + a + b = 1 + a + c \Rightarrow 1 + b = 1 + c \tag{39}$$

for all $a,b,c\in\mathbb{N}^{(X)}$. Now let $x\in X$ be given. Since $\mathrm{G}(X)$ is finite, there are positive integers $m<n$ such that $1+mx=1+nx$. Hence $a:=(n-m-1)x\in\mathbb{N}^{(X)}$ satisfies $1=1+a+x$ by virtue of (39). Therefore, Eq. (22) with $\pi=1$ and $\rho=1+a$ gives $x=(1+a+x)(x)=(1+a\cdot x)((1+a)(x))=(a\cdot x)\cdot(a\cdot x)$. □

7. An indecomposable square-free cycle set

For a non-degenerate cycle set X, let X_{tors} be the inverse image of the torsion subgroup of $\mathrm{A}(X)$ under the map (37). As the torsion subgroup of $\mathrm{A}(X)$ is a $\mathrm{G}(X)$-submodule, we infer that X_{tors} is a $\mathrm{G}(X)$-invariant subset of X. Hence, we get a decomposition

$$X=X_{\mathrm{tors}}\ \amalg\ X_0 \tag{40}$$

of X into cycle sets X_{tors} and X_0. Accordingly, we call X *torsion*(*-free*) if $X=X_{\mathrm{tors}}$ (resp. $X=X_0$). Thus an indecomposable non-degenerate cycle set X is either torsion or torsion free. If X is square free, then X_{tors} consists of the elements $x\in X$ with $\mathrm{C}_x(y)$ finite for all $y\in X$.

Example 4. Consider the cycle set $X=\mathbb{Z}\cup\{\infty\}$ with $n\cdot x=x$, $\infty\cdot n=n+1$, and $\infty\cdot\infty=\infty$ for $n\in\mathbb{Z}$ and $x\in X$. Then X is square free with $X_{\mathrm{tors}}=\mathbb{Z}$ and $X_0=\{\infty\}$.

We conclude with an example which shows that Theorem 1 does not hold for square-free non-degenerate unitary solutions $R\in\mathrm{S}(X^2)$ of the QYBE with X infinite.

Example 5. Let $\mathbb{F}_2C_0$ be the group ring of the infinite cyclic group $C_0=\langle z\rangle$ over the field $\mathbb{F}_2$ with two elements. Thus every $a\in\mathbb{F}_2C_0$ can be written uniquely as a sum $a=\sum_{n\in N}z^n$ with a finite subset N of $\mathbb{Z}$. Define a map $v\colon\mathbb{F}_2C_0\to\mathbb{F}_2C_0$ as follows. For $a\neq0$ we set $v(a):=z^m$, where $m:=\max N$, and $v(0):=0$. Then

$$a\cdot b:=v(z^{-1}(a+b))+b \tag{41}$$

gives a binary operation on $\mathbb{F}_2C_0$ which satisfies $a\cdot a=a$ for all $a\in\mathbb{F}_2C_0$. Since $a\cdot(a\cdot b)=v(z^{-1}(a+v(z^{-1}(a+b))+b))+v(z^{-1}(a+b))+b=v(z^{-1}(a+b))+v(z^{-1}(a+b))+b=b$, we have

$$a\cdot(a\cdot b)=b \tag{42}$$

for all $a,b\in\mathbb{F}_2C_0$. To show that the operation (41) satisfies (12), it suffices, by symmetry, to prove $v(z^{-1}(v(z^{-1}(a+b))+b+v(z^{-1}(a+c))+c))=v(z^{-1}(b+c))$ for all $a,b,c\in\mathbb{F}_2C_0$. Substituting $d:=a+b$ and $e:=a+c$, this equation turns into

$$v(z^{-1}(v(z^{-1}d)+v(z^{-1}e)+d+e))=v(z^{-1}(d+e)). \tag{43}$$

For $v(d) = v(e)$ or $d = 0$ or $e = 0$, this is trivial. Thus we may assume that $v(d) = z^m$ and $v(e) = z^n$ with $m < n$. Then both sides of (43) are equal to $v(z^{-1}e)$.

So we have shown that $\mathbb{F}_2 C_0$ is a square-free cycle set. By (41), we have $v(zb) \cdot b = b + v(b)$ for all $b \in \mathbb{F}_2 C_0$. Hence, by induction, it follows that $\mathbb{F}_2 C_0$ is indecomposable. Eq. (42) shows that $\mathbb{F}_2 C_0$ is a torsion cycle set. The corresponding R-matrix is given by

$$R(a, b) = (b \cdot a, a \cdot b). \tag{44}$$

Acknowledgment

The author thanks Tatiana Gateva-Ivanova for providing him with her preprint [7] which served as a quick introduction to the subject.

References

[1] V.G. Drinfeld, On some unsolved problems in quantum group theory, in: P.P. Kulish (Ed.), Quantum Groups (Leningrad, 1990), Lecture Notes in Mathematics, Vol. 1510, Springer, Berlin, 1992, pp. 1–8.
[2] P. Etingof, Geometric crystals and set-theoretical solutions to the quantum Yang-Baxter equation, math. QA/0112278 (2001).
[3] P. Etingof, S. Gelaki, A method of construction of finite-dimensional triangular semisimple Hopf algebras, Math. Res. Lett. 5 (1998) 551–561.
[4] P. Etingof, T. Schedler, A. Soloviev, Set-theoretical solutions to the quantum Yang-Baxter equation, Duke Math. J. 100 (1999) 169–209.
[5] T. Gateva-Ivanova, Noetherian properties of skew-polynomial rings with binomial relations, Trans. Amer. Math. Soc. 343 (1994) 203–219.
[6] T. Gateva-Ivanova, Skew polynomial rings with binomial relations, J. Algebra 185 (1996) 710–753.
[7] T. Gateva-Ivanova, A combinatorial approach to the set-theoretic solutions of the Yang-Baxter equation, Preprint.
[8] T. Gateva-Ivanova, Regularity of skew-polynomial rings with binomial relations, Talk at the International Algebra Conference, Miskolc, Hungary, 1996.
[9] T. Gateva-Ivanova, M. Van den Bergh, Semigroups of I-type, J. Algebra 206 (1998) 97–112.
[10] E. Jespers, J. Okniński, Binomial semigroups, J. Algebra 202 (1998) 250–275.
[11] G. Laffaille, Quantum binomial algebras, preprint.
[12] J.-H. Lu, M. Yan, Y.-C. Zhu, On the set-theoretical Yang-Baxter equation, Duke Math. J. 104 (2000) 1–18.
[13] J. Tate, M. Van den Bergh, Homological properties of Sklyanin algebras, Invent. Math. 124 (1996) 619–647.
[14] A.P. Veselov, Yang-Baxter maps and integral dynamics, Preprint.
[15] A. Weinstein, P. Xu, Classical solutions of the quantum Yang-Baxter equation, Comm. Math. Phys. 148 (1992) 309–343.