COLLOQUIUM MATHEMATICUM

VOL. 109 2007 NO. 1

GENERALIZED RADICAL RINGS, UNKNOTTED BIQUANDLES, AND QUANTUM GROUPS

BY

WOLFGANG RUMP (Stuttgart)

Abstract. Generalized radical rings (braces) were introduced for the study of set-theoretical solutions of the quantum Yang–Baxter equation. We discuss their relationship to groups of I-type, virtual knot theory, and quantum groups.

Introduction. Some problems and conjectures arose from the study of set-theoretical solutions [1] of the Yang–Baxter equation. A theory of non-degenerate solutions was developed by Etingof, Schedler, and Soloviev [3] for the involutive case, and by Lu, Yan and Zhu [19] and Soloviev [27] for the general case. In [3, 19, 27], a *structure group* is associated to a non-degenerate solution, which amounts to a universal linear extension of the solution. In an equivalent context, this construction was anticipated by Gateva-Ivanova and Van den Bergh [8]. Moreover, the structure group G gives rise to a matched pair (G, G) of groups [30, 31].

Using the structure group, a non-degenerate unitary solution $S\colon X^2 \to X^2$ defines a surjection $X \twoheadrightarrow \overline{X}$ such that S induces a non-degenerate unitary solution $\overline{S}$ on $\overline{X}$, the *retraction* [3] of S. So it may happen that after finitely many steps, X is mapped into a singleton. In this case, X is called a *multipermutation solution*.

In [6, 7], Gateva-Ivanova investigated a class of Artin–Schelter regular semigroup rings, and it was shown [8] that they lead to involutive solutions $S\colon X^2 \to X^2$ which are *square-free*, i.e. $S(x, x) = (x, x)$ for all $x \in X$. She conjectured that every finite square-free involutive solution is obtained in this way. As observed in [3], the conjecture is equivalent to the statement that every such solution is *decomposable*, i.e. there are at least two orbits of the structure group on X, unless $|X| = 1$. After its proof [25], the conjecture was strengthened [5] to the assertion that every finite square-free involutive

2000 *Mathematics Subject Classification*: Primary 81R50, 16N20, 16W30; Secondary 16S40.

Key words and phrases: Yang–Baxter equation, radical ring, cycle set, brace, group of I-type, virtual knot, quantum group.

solution is a multipermutation solution. In [5], this enhanced statement is called the "strong conjecture".

In [25], we introduced *cycle sets*, i.e. sets with a binary operation and a single relation (see Definition 2). Cycle sets X are equivalent to left non-degenerate unitary solutions $S\colon X \times X \to X \times X$ of the Yang–Baxter equation. We showed [25] that finite cycle sets are also right non-degenerate. The linear extension of a non-degenerate cycle set is an abelian group A with a left distributive multiplication such that the circle operation

$$a \circ b := ab + a + b$$

makes A into a group. Thus A consists of two groups, the additive group $(A, +)$ and the *adjoint group* $G = (A, \circ)$, such that A is a right G-module, and the connection between $(A, +)$ and G is given by a bijective 1-cocycle $G \to A$. We call such a structure A a *brace* [26]. In particular, every radical ring is a brace, and every brace has an underlying cycle set.

Although braces are non-associative and only one-sided distributive, some concepts of ring theory do apply to braces. For example, the kernel of a morphism is an ideal in the usual sense, and every ideal I of a brace A leads to a factor brace A/I. On the other hand, the product of two ideals need not be an ideal. Nevertheless, braces have a radical series

$$A \supset AA \supset A(AA) \supset A(A(AA)) \supset \cdots$$

consisting of ideals, while $(AA)A$ need not be an ideal, in general. Dually, there is a socle series [26] which also consists of ideals, where the *socle* $\mathrm{Soc}(A)$ is defined as in ring theory, i.e. $\mathrm{Soc}(A) := \{x \in A \mid \forall a \in A\colon ax = 0\}$. The retraction of A is just the factor brace $A/\mathrm{Soc}(A)$, and for a cycle set X, the retraction can be obtained from the retraction of the brace $A = \mathbb{Z}^{(X)}$ generated by X. In this terminology, the strong conjecture simply states that certain finite braces are nilpotent. Another interesting fact is that the additive group of the retraction $A/\mathrm{Soc}(A)$ is determined by the cycle set structure of A. (Thus irretractable braces are completely determined by their underlying cycle sets!)

In the present paper, we start with a brief review of braces and cycle sets, and then exhibit their relationship to groups of I-type, virtual knots, and quantum groups. Monoids of I-type (see [8, 11, 12]) arose in the theory of Sklyanin algebras [32]. They consist of a finitely generated free abelian monoid $\mathbb{N}^{(X)}$ with an additional (not necessarily commutative) monoid structure, such that the multiplication of a fixed element $a \in \mathbb{N}^{(X)}$ by the generators $x \in X$ just gives a permutation of the elements $x + a$ (see Definition 1). By [12, Corollary 2.3] (or [25, Theorem 2]), it makes no difference if we replace $\mathbb{N}^{(X)}$ by the free abelian group $\mathbb{Z}^{(X)}$. Theorem 1.3 of [8] states that monoids of I-type are equivalent to finite involutive non-degenerate so-

lutions of the Yang–Baxter equation. We will give a simple proof in terms of cycle sets. Precisely, we show that every group $\mathbb{Z}^{(X)}$ of I-type defines a cycle set structure on X, and vice versa (Theorem 1).

Section 4 exhibits a relationship between cycle sets and *biquandles*, which are invariants of virtual knots in the sense of Kauffman [15]. We prove that non-degenerate cycle sets are in one-to-one correspondence with "unknotted" biquandles (Theorem 2).

Bijective 1-cocycles have been used by Etingof and Gelaki [2] for the construction of minimal semisimple triangular Hopf algebras over $\mathbb{C}$. More generally, Lu, Yan and Zhu [21] obtained a classification of quasi-triangular Hopf algebras with positive structure constants and proved [20] that Hopf algebras with "positive bases" arise from matched pairs of groups. In Section 5, we associate a minimal triangular Hopf algebra $H_K(A)$ over a given field K to any finite brace A, and show that $H_K(A)$ is semisimple if and only if the characteristic of K does not divide $|A|$. Furthermore, we show that braces admit a dual. For cycle sets, a dual was defined in [25], and it was shown that duals are necessarily unique. Moreover, a cycle set X has a dual if and only if it is non-degenerate. Since braces A are non-degenerate, their underlying cycle sets can be dualized. We show that the dual cycle set comes again from a brace which is naturally associated to A.

1. Generalized radical rings. For any associative ring R, the *circle operation*

$$a \circ b := ab + a + b \tag{1}$$

makes R into a semigroup with unity 0. Jacobson has shown [10] that R is a *radical ring* (i.e. $\operatorname{Rad} R = R$) if and only if $(R, \circ)$ is a group. With respect to this *adjoint* group R°, a radical ring can be regarded as a right module, with right operation

$$x^a := xa + x, \quad x \in R,\ a \in R^\circ. \tag{2}$$

In fact, we have

$$x(ab + a + b) + x = (xa + x)b + (xa + x) \quad \text{for } x, a, b \in R. \tag{3}$$

The identical map $\pi\colon R^\circ \to R$ then satisfies the 1-cocycle condition

$$\pi(a \circ b) = \pi(a)^b + \pi(b). \tag{4}$$

Thus every radical ring gives rise to a bijective 1-cocycle. So we are led to the following structure, introduced in [26].

DEFINITION 1. A *brace* is an abelian group A with a multiplication (juxtaposition) so that

(I) $(a + b)c = ac + bc$,

(II) A is a group with respect to the circle operation (1).

The group $(A,\circ)$ will be called the *adjoint group* A° of A.

Condition (II) can be replaced by two conditions:

(II_1) $a(bc+b+c)=(ab)c+ab+ac$,

(II_2) for all $a\in A$, the map $x\mapsto x^a := xa+x$ is bijective.

In fact, (II_1) is equivalent to the associativity of the circle operation, and (I) implies that $0c=0$ for all $c\in A$, whence $0\circ c=c$. Furthermore, (II_2) states that every equation $x\circ a=b$ in A has a unique solution. As is well-known, this implies that $(A,\circ)$ is a group. In particular, the equation $c\circ 0=c$ yields

$$0c=c0=0 \tag{5}$$

for all $c\in A$.

Note that condition (II_1) is closely related to (3). If A is (left and right) distributive, (II_1) turns into associativity. This shows that distributive braces are tantamount to radical rings.

If we use the exponential notation of (II_2), the conditions (I) and (II_1) turn into

$$(a+b)^c=a^c+b^c, \tag{6}$$

$$a^{b\circ c}=(a^b)^c. \tag{7}$$

Therefore, a brace can be regarded as an abelian group A with an additional group structure $(A,\circ)$, such that $(A,\circ)$ operates from the right on $(A,+)$. To make this more transparent, let us consider the groups $A=(A,+)$ and $G=(A,\circ)$ separately, such that G and A are connected by a bijection $\pi\colon G\to A$ (the identical map). Equations (6) and (7) then imply that A is a right G-module. Thus, if we write (1) as

$$a\circ b=a^b+b,$$

the connection between the two groups A and G can be expressed by the fact that π is a bijective 1-cocycle, i.e. (4) holds for all $a,b\in G$. In other words, braces are equivalent to bijective 1-cocycles.

2. Braces and cycle sets. In [25], we introduced *cycle sets* which are in one-to-one correspondence with left non-degenerate involutive set-theoretical solutions of the quantum Yang–Baxter equation. In the terminology of [3], such a solution is given by a set X with a bijection $S\colon X\times X\to X\times X$ which makes X into a left non-degenerate symmetric set. If $S(x,y)=(x^y,{}^xy)$, this means, in particular, that the three equations

$$x^{yz}=x^{({}^yz)(y^z)};\qquad {}^{xy}z={}^{({}^xy)({}^{x^y})}z\,;\qquad {}^{(x^{({}^yz)})}(y^z)={}^{({}^xy)}({}^{(x^y)}z) \tag{8}$$

(see Definition 7 below) are satisfied in X. By contrast, the definition of a cycle set is rather simple.

DEFINITION 2. A *cycle set* [25] is a set $(X, \cdot)$ with a binary operation such that the left multiplications $y \mapsto x \cdot y$ are bijective, and

$$(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z) \tag{9}$$

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

By linear extension, the left multiplication defines a map

$$X \times \mathbb{N}^{(X)} \xrightarrow{\cdot} \mathbb{N}^{(X)}. \tag{10}$$

What is less obvious, a unique extension of the first variable to $\mathbb{N}^{(X)}$ is also possible if we impose the condition

$$(a + b) \cdot c = (a \cdot b) \cdot (a \cdot c), \tag{11}$$

which is symmetric in a and b. So we get a commutative diagram

$$\begin{array}{ccc} X \times \mathbb{N}^{(X)} & \longrightarrow & \mathbb{N}^{(X)} \\ \cap\downarrow & \nearrow_{\exists!} & \\ \mathbb{N}^{(X)} \times \mathbb{N}^{(X)} & & \end{array}$$

which makes $\mathbb{N}^{(X)}$ into a cycle set ([25, Proposition 6]).

DEFINITION 3. A cycle set A with abelian group structure is *linear* [25, 26] if

(a) $a \cdot (b + c) = a \cdot b + a \cdot c$,
(b) $(a + b) \cdot c = (a \cdot b) \cdot (a \cdot c)$

for $a, b, c \in A$.

Note that $\mathbb{N}^{(X)}$ is not linear since $(\mathbb{N}^{(X)}, +)$ is not a group. By [25, Proposition 9], every linear cycle set is *non-degenerate*, i.e. the map $a \mapsto a \cdot a$ is bijective. Moreover, Proposition 6 of [25] implies that a cycle set X extends to a linear cycle set $\mathbb{Z}^{(X)}$ if and only if X is non-degenerate. If we replace the left multiplication $b \mapsto a \cdot b$ of a linear cycle set A by its inverse $b \mapsto b^a$, the two equations of Definition 3 turn into the exponential rules (6) and (7), with $b \circ c = b^c + c$. Therefore, linear cycle sets are equivalent to braces. So we get

PROPOSITION 1. *For an abelian group A, the following structures on A are equivalent*:

(a) *a multiplication $A \times A \to A$ which makes A into a brace*;
(b) *an exponential map $(a, b) \mapsto a^b$ which satisfies* (6) *and* (7) *with $b \circ c := b^c + c$*;
(c) *a multiplication $A \times A \xrightarrow{\cdot} A$ which makes A into a linear cycle set*;
(d) *a group G and a right G-module structure on A, together with a bijective 1-cocycle $\pi \colon G \to A$.*

Furthermore, the above discussion exhibits an intimate relationship between braces and cycle sets, in that every non-degenerate cycle set X generates a brace $\mathbb{Z}^{(X)}$, while every brace can be regarded as a linear cycle set. By [25, Theorem 2], every finite cycle set is non-degenerate. So it is natural to ask the following

QUESTION. Does the implication

$$\mathbb{Z}^{(X)} \cong \mathbb{Z}^{(Y)} \;\Rightarrow\; X \cong Y$$

hold for finite cycle sets X and Y?

There is a formal analogy to the isomorphism problem for integral group rings which, although a counter-example is known in the general case [9], has found a positive solution for nilpotent groups [24, 34, 35]. If the answer to the above question would be positive, a unique brace could be associated to any square-free involutive solution of the quantum Yang–Baxter equation.

3. Non-commutative group deformation. The close relationship between braces and cycle sets can be used to relate cycle sets to groups of I-type, which arose in the theory of Sklyanin algebras [32].

DEFINITION 4. Let X be a finite set. The free abelian group $\mathbb{Z}^{(X)}$, together with a second group structure $(\mathbb{Z}^{(X)}, \circ)$ with the same neutral element 0, is said to be of *I-type* if

$$\{x \circ a \mid x \in X\} = \{x + a \mid x \in X\} \tag{12}$$

for all $a \in \mathbb{Z}^{(X)}$. If $\mathbb{Z}^{(X)}$ is replaced by the free abelian monoid $\mathbb{N}^{(X)}$, then $\mathbb{N}^{(X)}$ is called a *monoid of I-type*.

Groups and monoids of I-type were investigated recently by Jespers and Okniński [12]. It is shown there that every monoid of I-type admits a natural extension to a group of I-type, so that both concepts are in fact equivalent. By the following result, this can be viewed as a reformulation of [25, Theorem 2].

THEOREM 1. *Every group $(\mathbb{Z}^{(X)}, \circ)$ of I-type defines a finite cycle set, and vice versa.*

Proof. Every element $a \in \mathbb{Z}^{(X)}$ gives rise to a permutation $\sigma(a)$ of X with

$$x + a = \sigma(a)(x) \circ a \tag{13}$$

for all $x \in X$. We define a binary operation on X by

$$x \cdot y := \sigma(x)(y) \tag{14}$$

for $x, y \in X$. Thus by definition, the left multiplication of $x \in X$ coincides with $\sigma(x)$, which is bijective. To show that $(X, \cdot)$ is a cycle set, we have to verify (9) for $x, y, z \in X$.

From (13) and (14), we infer that

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

for $x, y \in X$. So we get

$$\begin{aligned}((x\cdot y)\cdot(x\cdot z))\circ(x+y) &= ((x \cdot y) \cdot (x \cdot z)) \circ (x \cdot y) \circ x \\ &= ((x \cdot y) + (x \cdot z)) \circ x = (x \cdot (y + z)) \circ x = x + y + z\end{aligned}$$

for all $z \in X$. This proves that $(x\cdot y)\cdot(x\cdot z)$ is symmetric in x and y, whence (9) is satisfied.

Conversely, let X be a finite cycle set. By [25, Theorem 2], X is non-degenerate. Hence X extends to a linear cycle set $\mathbb{Z}^{(X)}$ by [25, Proposition 6]. So $\mathbb{Z}^{(X)}$ is a brace, and the circle operation

$$a \circ b := a^b + b$$

makes $\mathbb{Z}^{(X)}$ into a group. Hence $x + a = (a \cdot x)^a + a = (a \cdot x) \circ a$ for all $a \in \mathbb{Z}^{(X)}$ and $x \in X$. This shows that $(\mathbb{Z}^{(X)}, \circ)$ is a group of I-type, and X is the corresponding cycle set.

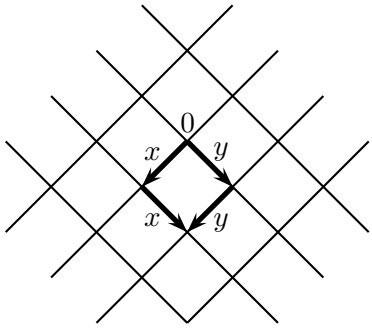
Finally, if $\mathbb{Z}^{(X)}$ is a group of I-type, the corresponding cycle set X extends to a linear cycle set $\mathbb{Z}^{(X)}$ such that

$$x \circ a = x^a + a \tag{16}$$

for $a \in \mathbb{Z}^{(X)}$ and $x \in X$. By induction, this implies that any group $(\mathbb{Z}^{(X)}, \circ)$ of I-type comes from the cycle set X. ∎

Thus every group $G = (\mathbb{Z}^{(X)}, \circ)$ of I-type can be regarded as a brace. Therefore, the right group action of G on the lattice $\mathbb{Z}^{(X)}$ extends to the real vector space $\mathbb{R}^{(X)}$, so that G becomes a Bieberbach group with fundamental domain $[0,1]^X$, the unit cube (cf. [8, Theorem 1.6]). For $|X| = 2$, the non-trivial group G of I-type (Example 1.2 of [8]) corresponds to the following linear cycle set.

Example. For the linear cycle set



$$X = \{x, y\}$$
$$G = \langle X \mid x \circ x = y \circ y \rangle$$

$$(nx + my) \cdot x = \begin{cases} x & \text{for } n + m \text{ even}, \\ y & \text{for } n + m \text{ odd}, \end{cases}$$

the quotient $\mathbb{R}^2/G$ is a Klein bottle.

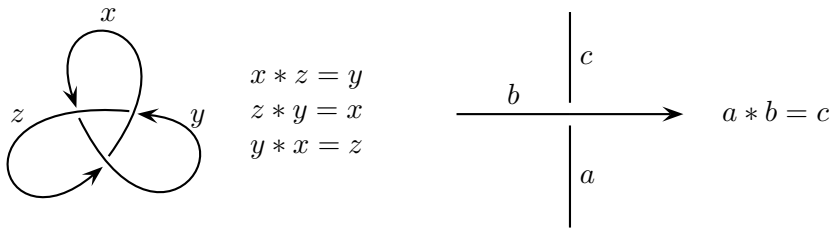
4. Quandles and biquandles. Binary operations with bijective left or right multiplication are well-known from knot theory. For a brief history, see [14].

DEFINITION 5. A set X with a binary operation $*$ is said to be a *quandle* [13, 22] if the right multiplication $y \mapsto y * x$ is bijective and such that

$$x * x = x, \qquad (x * y) * z = (x * z) * (y * z) \tag{17}$$

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

Every oriented knot $\mathcal{K}$ defines a quandle $Q(\mathcal{K})$ in the following way. Denote the arcs of $\mathcal{K}$ between successive crossings by variables. At each crossing, a relation is added as in the following example.



(The orientation of the vertical line is immaterial.)

In 1982, Joyce [13] and Matveev [22] showed independently that up to weak equivalence, two knots $\mathcal{K}$ and $\mathcal{K}'$ in $\mathbb{R}^3$ are distinguished by their quandle:

$$Q(\mathcal{K}) \cong Q(\mathcal{K}') \;\Rightarrow\; (\mathbb{R}^3, \mathcal{K}) \cong (\mathbb{R}^3, \mathcal{K}'). \tag{18}$$

If $-\mathcal{K}$ denotes the knot $\mathcal{K}$ with inverse orientation, and $\mathcal{K}^*$ stands for the mirror image of $\mathcal{K}$, the quandle $Q(-\mathcal{K}^*)$ is always isomorphic to $Q(\mathcal{K})$. Therefore, the quandle does not distinguish the trefoil $\mathcal{K}_3$ from its mirror image. Since

$$-\mathcal{K}_3 \cong \mathcal{K}_3,$$

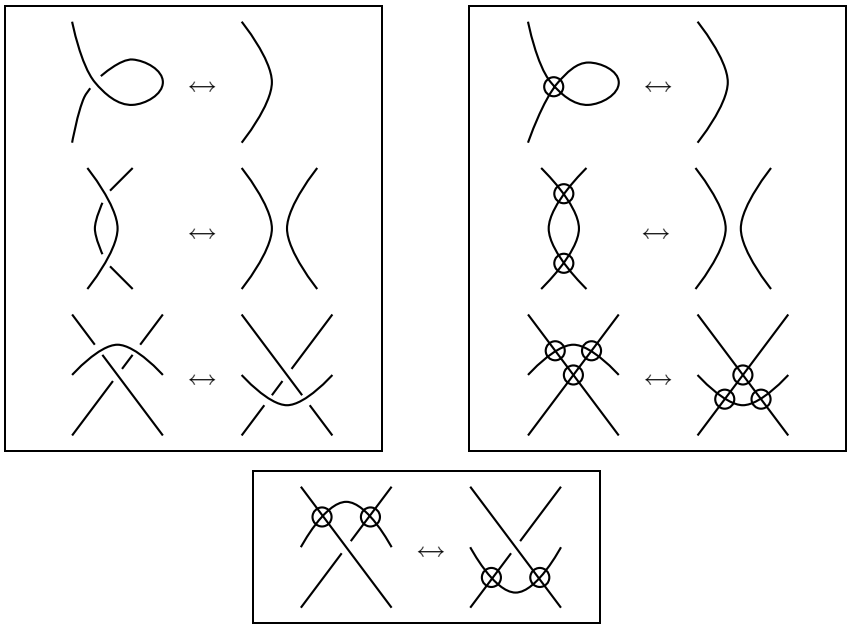
we have

$$Q(\mathcal{K}^*) \cong Q(\mathcal{K}).$$

Later on, the concept of quandle was generalized to that of a *biquandle*, which removes the lack of symmetry and also applies to virtual knots and links [15].

While real knots can be represented by their projection into a thickened sphere, *virtual knots* [15] arise when the genus of that sphere is increased. This can be achieved by attaching infinitesimal handles so that *virtual crossings* become possible, so called as they do not represent a singulatity. Algebraically, a virtual knot diagram is defined as follows.

Definition 6 (Kauffman). A *virtual* knot is given by a knot diagram with additional *virtual crossings* (at infinitesimal handles attached to the sphere), modulo generalized Reidemeister moves:



The virtual crossings are marked by a small circle.

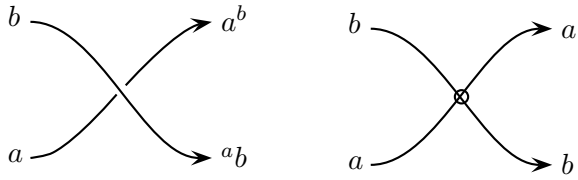
As virtual crossings do not represent a singularity, but merely arise from a global invariant (the genus) of the ambient surface, they can be moved over virtual and real crossings. This means that locally, virtual crossings can be treated as if they were not there.

Definition 7. A set X with two operations ${}^{x}y$ and x^{y} is called a *biquandle* if:

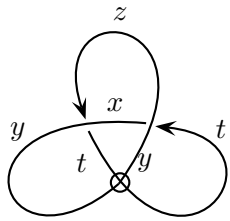
(a) $x^{yz} = x^{(yz)(y^z)}$, ${}^{xy}z = {}^{(xy)(x^y)}z$, ${}^{(x^{(yz)})}(y^z) = ({}^{x}y)^{({}^{(xy)}z)}$ for $x, y, z \in X$.
(b) The map $(x, y) \mapsto ({}^{x}y, x^{y})$ is bijective.
(c) The maps $x \mapsto x^{y}$ and $x \mapsto {}^{y}x$ are bijective with inverse operations $x \mapsto y \cdot x$ and $x \mapsto y \times x$, respectively.
(d) $(x \cdot x) \times (x \cdot x) = (x \times x) \cdot (x \times x) = x$.

To avoid parentheses, we write x^{yz} instead of $(x^{y})^{z}$, etc. The simplified version of condition (d) (cf. [16, 17]) is due to Stanovský [28].

In a similar way as quandles are invariants of real knots, biquandles can be associated to virtual knots [17, 4]. Every virtual knot $\mathcal{K}$ defines a biquandle $\mathrm{BQ}(\mathcal{K})$. Here the generators of $\mathrm{BQ}(\mathcal{K})$ are *semi-arcs* [4], i.e. the arcs between consecutive real crossings, ignoring any virtual crossing. The relations are given by the following diagrams:



For example,



$$\begin{aligned} x &= t^y \\ y &= {}^z x \\ z &= {}^t y \\ t &= z^x \end{aligned}$$

The following theorem shows that non-degenerate cycle sets can be regarded as biquandles.

THEOREM 2. *A non-degenerate cycle set defines a biquandle via*

$$ {}^x y = x^y \cdot y. \tag{19}$$

Conversely, every biquandle with this property is a non-degenerate cycle set.

Proof. Let X be a non-degenerate cycle set. Using (19), we can form a map $R\colon X \times X \to X \times X$ with

$$R(x,y) := (x^y, {}^x y).$$

By [25], this implies that R satisfies the set-theoretical quantum Yang–Baxter equation, which is equivalent to equations (a) of Definition 7. Furthermore, R is involutive, i.e. $R^{21}R = 1$, where $R^{21}(x,y) := ({}^y x, y^x)$, which implies condition (b) of Definition 7. Condition (c) just says that X is non-degenerate, and (d) follows by [25, Proposition 2].

Conversely, let X be a biquandle which satisfies (19). Then the first equation of condition (a) in Definition 7 can be rewritten as $x = {}^y z \cdot (y^z \cdot x^{yz})$. With the substitution $x \mapsto y \cdot (z \cdot x)$, this gives $y \cdot (z \cdot x) = ({}^y z) \cdot (y^z \cdot x) = (y^z \cdot z) \cdot (y^z \cdot x)$. Thus if we replace y by $z \cdot y$, we get $(z \cdot y) \cdot (z \cdot x) = (y \cdot z) \cdot (y \cdot x)$, i.e. X is a cycle set. Furthermore, condition (d) of Definition 7 implies that X is non-degenerate. ∎

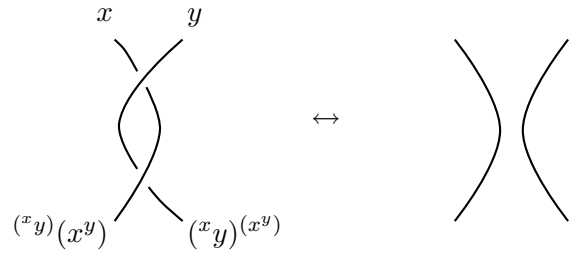
In view of Theorem 2, the question arises which virtual knots $\mathcal{K}$ correspond to finite cycle sets. By (19), we have $({}^x y)^{(x^y)} = y$, and thus

$${}^{({}^x y)}(x^y) = ({}^x y)^{(x^y)} \cdot (x^y) = y \cdot (x^y) = x.$$

Therefore, (19) is equivalent to

$$ {}^{({}^x y)}(x^y) = x, \qquad ({}^x y)^{(x^y)} = y. \tag{20}$$

In addition to the Reidemeister moves, this gives



Therefore, the real crossings of such a knot $\mathcal{K}$ can be removed, whence $\mathcal{K}$ has to be the unknot corresponding to the one-element cycle set:

$$\{\text{finite cycle sets}\} \cap \{\text{virtual knots}\} = \{\mathbf{O}\}.$$

5. Minimal quantum groups. Now we return to braces, i.e. linear cycle sets. Recall that a *quantum group* is a quasi-triangular Hopf algebra. For the general theory of Hopf algebras, see [29].

DEFINITION 8. Let K be a field. A Hopf algebra H over K with an element $R \in (H \otimes H)^{\times}$ is said to be *quasi-triangular* if

- $\Delta^{\mathrm{op}}(a) = R\Delta(a)R^{-1}$, $\forall a \in H$,
- $(\Delta \otimes 1)(R) = R^{13}R^{23}$, $(1 \otimes \Delta)(R) = R^{13}R^{12}$,
- $(\varepsilon \otimes 1)(R) = (1 \otimes \varepsilon)(R) = 1$.

The second line contains relations in $H^{\otimes 3}$ (braid relations). As usual, R^{ij} means R applied to the ith and jth coordinate, e.g., if $R = \sum a_i \otimes b_i$, then $R^{13} = \sum a_i \otimes 1 \otimes b_i$. The Hopf algebra H is said to be *triangular* if, in addition, $R^{21}R = 1$.

Assume that H is quasi-triangular with

$$R = \sum_{i=1}^{n} a_i \otimes b_i, \tag{21}$$

such that n is minimal. Consider the subspaces $A := Ka_1 + \cdots + Ka_n$ and $B := Kb_1 + \cdots + Kb_n$. Then A and B are sub-Hopf algebras of H, and $B \cong A^{*\mathrm{cop}}$, where A^* denotes the dual of A, and A^{cop} denotes the same algebra as A with switched comultiplication. Radford [23] has shown that

$$H_{\mathrm{R}} := AB = BA \tag{22}$$

is a quasi-triangular sub-Hopf algebra. If $H = H_{\mathrm{R}}$, the Hopf algebra H is called *minimal* [23]. (This implies that H is finite-dimensional!)

THEOREM 3 (Radford [23]). *Let H be a finite-dimensional Hopf algebra.*

(a) *The Drinfel'd double $D(H)$ is a minimal quasi-triangular Hopf algebra.*

(b) *Every minimal quasi-triangular Hopf algebra is a quotient of a Drinfel'd double.*

The first example of a minimal triangular semisimple Hopf algebra was found by Etingof and Gelaki [2] in 1998. Before we give a description in terms of braces, we show that braces arise in pairs. In [25], we defined the *dual* of a cycle set X to be a cycle set $(X, \times)$ which satisfies

$$(x \cdot y) \times (y \cdot x) = (x \times y) \cdot (y \times x) = x \tag{23}$$

for all $x, y \in X$. By [25, Proposition 2], the dual is unique, and X admits a dual if and only if it is non-degenerate. This concept admits an extension to braces.

PROPOSITION 2. *Let A be a brace. The dual cycle set of A is a brace A^{op} with respect to the addition and multiplication*

$$a \boxplus b := (a' + b')', \qquad a \boxdot b := (a'b')', \tag{24}$$

where a' denotes the inverse of a with respect to the circle operation (1)*. The adjoint groups of A and A^{op} are opposite to each other.*

Proof. We show first that the operations (24) define a brace A^{op}. Obviously, $(A, \boxplus)$ is an abelian group with the same zero element $0' = 0$. Moreover, A^{op} is right distributive, since

$$\begin{aligned}(a \boxplus b) \boxdot c &= ((a \boxplus b)'c')' = ((a' + b')c')' = (a'c' + b'c')' \\ &= ((a \boxdot c)' + (b \boxdot c)')' = (a \boxdot c) \boxplus (b \boxdot c).\end{aligned}$$

Furthermore, $(a \boxdot b) \boxplus a \boxplus b = ((a \boxdot b)' + a' + b')' = (a'b' + a' + b')' = (a' \circ b')' = b \circ a$, which shows that the circle operation for A is opposite to the circle operation of A^{op}. Thus A^{op} is a brace.

By [25, Proposition 2], the map $b \mapsto a \times b$ is inverse to $b \mapsto {}^a b = a^b \cdot b$. Thus it remains to prove that

$$a^b \cdot b = (b \boxdot a) \boxplus b \tag{25}$$

for all $a, b \in A$. Now $(b \boxdot a) \boxplus b = ((b \boxdot a)' + b')' = (b'a' + b')'$. Since $0 = a \circ a' = a^{a'} + a' = (a \cdot a) + a'$, we have

$$a' = -(a \cdot a) \tag{26}$$

for all $a \in A$. Therefore, (25) is equivalent to

$$-((a^b \cdot b) \cdot (a^b \cdot b)) = b'a' + b'. \tag{27}$$

Now $(a^b \cdot b) \cdot (a^b \cdot b) = (b \cdot a^b) \cdot (b \cdot b) = a \cdot (b \cdot b)$. Hence (27) reduces to $a \cdot b' = b'a' + b'$, i.e.

$$a \cdot b = ba' + b \tag{28}$$

for all $a, b \in A$. Replacing a by a', this means that $b^a = ba + b$, which is trivial. ∎

PROPOSITION 3. *Let A be a brace. With the abbreviation* (19), *the following equations hold for all $a, b, c \in A$:*

$$ {}^{a\circ b}c = {}^{a}({}^{b}c), \qquad a^{b\circ c} = (a^b)^c, \tag{29} $$

$$ {}^{a}(b \circ c) = {}^{a}b \circ {}^{(a^b)}c, \qquad (a \circ b)^c = a^{({}^b c)} \circ b^c. \tag{30} $$

Proof. The right-hand equation of (29) coincides with (7). By (1), we have

$$ a \circ b = a^b + b \tag{31} $$

for all $a, b \in A$. Therefore, the right-hand equation of (29) states that

$$ (a^b + b)^c = a^{({}^b c)(b^c)} + b^c. $$

By (6), this is equivalent to the first equation of (8). If we pass to the dual brace A^{op}, and use (19) and (25), the remaining equations follow by duality. ∎

Equations (29) and (30) show that every brace A gives rise to a *matched pair* (A°, A°) of groups in the sense of [30]. So we can form the matched product $G := A^\circ \bowtie A^\circ$ [30]. (Note that every group G with subgroups A and B such that every element of G is a unique product ab with $a \in A$ and $b \in B$ gives rise to a matched product $G = A \bowtie B$. Namely, every product ba can be written uniquely as ${}^b a \cdot b^a$ with ${}^b a \in A$ and $b^a \in B$, so that relations similar to (29) and (30) are satisfied. Conversely, equations (29) and (30) make $A \times B$ into a formal product $A \bowtie B = AB$ via $(a, b)(c, d) := (a \cdot {}^b c, b^c \cdot d)$ with $a, c \in A$ and $b, d \in B$.) We write the elements of $G = A^\circ \bowtie A^\circ$ as pairs (a, b) with $a, b \in A^\circ$.

Now let A be finite, and let K be a field. Using [31], we define a Hopf algebra $H_K(A)$ with basis G as follows:

Multiplication: $$ (a, b)(c, d) = \begin{cases} (a, b \circ d) & \text{for } a^b = c, \\ 0 & \text{otherwise.} \end{cases} $$

Comultiplication: $$ \Delta(a, b) = \sum_{a = c \circ d} (c, {}^d b) \otimes (d, b), $$

Unit element: $$ 1 = \sum_{a \in A} (a, 0), $$

Augmentation: $$ \varepsilon(a, b) = \delta_{a,0}, $$

Antipode: $$ S(a, b) = ((a \cdot b') \cdot a', a \cdot b') = ((a^b)', ({}^a b)'), $$

R-matrix: $$ R = \sum_{a,b \in A} (a, b') \otimes (a \cdot b, a). $$

Note that, alternatively, the group G can be represented as a semidirect product. In fact, the multiplication map

$$G = A^\circ \bowtie A^\circ \xrightarrow{m} A^\circ \tag{32}$$

has an abelian kernel

$$\operatorname{Ker} m = \{(a', a) \mid a \in A\} \tag{33}$$

isomorphic to the additive group of A. Therefore, G is a semidirect product

$$G = A^\circ \ltimes A \tag{34}$$

with abelian kernel $A = (A, +)$.

PROPOSITION 4. *Let K be a field of characteristic 0, and let A be a finite brace. Then $H_K(A)$ is a minimal triangular semisimple Hopf algebra.*

Proof. A straightforward calculation shows that $H(A)$ is a minimal triangular Hopf algebra. Furthermore, the restriction of the antipode S to G coincides with the map $g \mapsto g^{-1}$. Hence $S^2 = 1$. Now the Larson–Radford theorem [18] implies that $H_K(A)$ is semisimple. ∎

REMARK. If K is a field of characteristic $p > 0$, the Hopf algebra $H_K(A)$ is still minimal and triangular, but need not be semisimple. In this case, it is easily seen that

$$I := \sum_{a \in A} (0, a) \tag{35}$$

is a left and right integral, and $\varepsilon(I) = |A|$. Therefore, Maschke's theorem for Hopf algebras implies that $H_K(A)$ is semisimple if and only if p does not divide $|A|$. (Note that $\dim H_K(A) = |A|^2$.)

REFERENCES

[1] V. G. Drinfel'd, *On some unsolved problems in quantum group theory*, in: Quantum Groups (Leningrad, 1990), Lecture Notes in Math. 1510, Springer, Berlin, 1992, 1–8.

[2] P. Etingof and S. Gelaki, *A method of construction of finite-dimensional triangular semisimple Hopf algebras*, Math. Res. Lett. 5 (1998), 551–561.

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

[4] R. A. Fenn, M. Jordan and L. H. Kauffman, *Biquandles and virtual links*, Topology Appl. 145 (2004), 157–175.

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

[6] —, *Noetherian properties of skew polynomial rings with binomial relations*, Trans. Amer. Math. Soc. 343 (1994), 203–219.

[7] —, *Skew polynomial rings with binomial relations*, J. Algebra 185 (1996), 710–753.

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

[9] M. Hertweck, *A counterexample to the isomorphism problem for integral group rings*, Ann. of Math. 154 (2001), 115–138.
[10] N. Jacobson, *Structure of Rings*, Amer. Math. Soc. Colloq. Publ. 37, Amer. Math. Soc., Providence, RI, 1974.
[11] E. Jespers and J. Okniński, *Binomial semigroups*, J. Algebra 202 (1998), 250–275.
[12] —, —, *Monoids and groups of I-type*, Algebr. Represent. Theory 8 (2005), 709–729.
[13] D. Joyce, *A classifying invariant of knots, the knot quandle*, J. Pure Appl. Algebra 23 (1982), 37–65.
[14] S. Kamada, *Knot invariants derived from quandles and racks*, in: Invariants of Knots and 3-manifolds (Kyoto, 2001), Geom. Topol. Monogr. 4, Geom. Topol. Publ., Coventry, 2002, 103–117.
[15] L. Kauffman, *Virtual knot theory*, European J. Combin. 20 (1999), 663–690.
[16] L. H. Kauffman and V. O. Manturov, *Virtual biquandles*, Fund. Math. 188 (2005), 103–146.
[17] L. Kauffman and D. Radford, *Bi-oriented quantum algebras, and a generalized Alexander polynomial for virtual links*, in: Diagrammatic Morphisms and Applications (San Francisco, CA, 2000), Contemp. Math. 318, Amer. Math. Soc., Providence, RI, 2003, 113–140.
[18] R. G. Larson and D. E. Radford, *Semisimple cosemisimple Hopf algebras*, Amer. J. Math. 110 (1988), 187–195.
[19] J.-H. Lu, M. Yan and Y.-C. Zhu, *On the set-theoretical Yang–Baxter equation*, Duke Math. J. 104 (2000), 1–18.
[20] —, —, —, *On Hopf algebras with positive bases*, J. Algebra 237 (2001), 421–445.
[21] —, —, —, *Quasi-triangular structures on Hopf algebras with positive bases*, in: Contemp. Math. 267, Amer. Math. Soc., Providence, RI, 2000, 339–356.
[22] S. Matveev, *Distributive gruppoids in knot theory*, Mat. Sb. 119 (1982), 78–88 (in Russian); English transl.: Math. USSR-Sb. 47 (1984), 73–83.
[23] D. E. Radford, *Minimal quasitriangular Hopf algebras*, J. Algebra 157 (1993), 285–315.
[24] K. W. Roggenkamp and L. L. Scott, *Isomorphisms of p-adic group rings*, Ann. of Math. 126 (1987), 593–647.
[25] W. Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation*, Adv. Math. 193 (2005), 40–55.
[26] —, *Braces, radical rings, and the quantum Yang–Baxter equation*, J. Algebra, to appear.
[27] A. Soloviev, *Non-unitary set-theoretical solutions to the quantum Yang–Baxter equation*, Math. Res. Lett. 7 (2000), 577–596.
[28] D. Stanovský, *On axioms of biquandles*, preprint.
[29] M. E. Sweedler, *Hopf Algebras*, Benjamin, New York, 1969.
[30] M. Takeuchi, *Matched pairs of groups and bismash products of Hopf algebras*, Comm. Algebra 9 (1981), 841–882.
[31] —, *Survey on matched pairs of groups—an elementary approach to the ESS-LYZ theory*, in: Noncommutative Geometry and Quantum Groups (Warsaw, 2001), Banach Center Publ. 61, Inst. Math., Polish Acad. Sci., Warszawa, 2003, 305–331.
[32] J. Tate and M. Van den Bergh, *Homological properties of Sklyanin algebras*, Invent. Math. 124 (1996), 619–647.
[33] J. F. Watters, *On the adjoint group of a radical ring*, J. London Math. Soc. 43 (1968), 725–729.
[34] A. Weiss, *Rigidity of p-adic p-torsion*, Ann. of Math. 127 (1988), 317–332.

[35] A. Weiss, *Torsion units in integral group rings*, J. Reine Angew. Math. 415 (1991), 175–187.

Institut für Algebra und Zahlentheorie
Universität Stuttgart
Pfaffenwaldring 57
D-70550 Stuttgart, Germany
E-mail: rump@mathematik.uni-stuttgart.de

Received 31 October 2006;
revised 9 December 2006 (4812)