Logic, l-groups, and the QYBE

Wolfgang Rump

The

Quantum-Yang-Baxter-Equation (QYBE)

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

is an equation in $\mathrm{End}(V^{\otimes 3})$, where V is a vector space and $R \in \mathrm{End}(V^{\otimes 2})$ a linear operator. R^{ij} is the action of R on the ith and jth factor of $V^{\otimes 3}$.

The QYBE arose first in statistical mechanics (Yang 1967) and is fundamental for the theory of quantum groups (quasi-triangular Hopf algebras).

Most of the known solutions are deformations of the trivial solution $R = 1_{V \otimes V}$.

ICM 1990: V. G. Drinfeld (On Some unsolved problems in quantum group theory) initiated the study of *combinatorial solutions*, i. e. solutions induced by a map

$$R : X \times X \to X \times X$$

for a fixed basis X of V.

The unitarity condition

$$\boxed{R^{21}R = 1}$$

implies that R is bijective.

The components of such a map

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

are binary operations $(x, y) \mapsto x^y$ resp. $(x, y) \mapsto {}^x y$ on X. A solution R is called

left non-degenerate	if $x \mapsto x^y$ is bijective,
right non-degenerate	if $y \mapsto {}^x y$ is bijective,
square-free	if $R(x, x) = (x, x)$.

Explicitly, `QYBE` is equivalent to three equations:

$$\boxed{x^{({}^y z)(y^z)} = x^{yz}; \quad {}^{(x^{({}^y z)})}(y^z) = ({}^x y)^{({}^{(x^y)} z)}; \quad {}^{xy} z = {}^{({}^x y)({}^{x^y})} z.}$$

The `unitarity condition` gives two equations

$$\boxed{{}^{({}^x y)}(x^y) = x; \quad ({}^x y)^{(x^y)} = y}$$

which imply, in particular, that the two operations x^y and ${}^x y$ determine each other.

Therefore, let R be left non-degenerate and let $y \mapsto x \cdot y$ be inverse to $y \mapsto y^x$. Then the five equations are equivalent to a single equation:

$$\boxed{(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z)}$$

Definition. We call a set X together with a binary operation $X \times X \xrightarrow{\cdot} X$ a **cycloid** if the equation

$$\text{(L)} \qquad \boxed{(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z)}$$

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

Thus if $y \mapsto x \cdot y$ is invertible, X yields a solution of the QYBE. (Then we call X a **cycle set**.)

Combinatorial solutions of the QYBE (hence cycle sets) arise in various mathematical contexts, e. g.:

- Quantum algebras (Gateva-Ivanova 1994)
- Semigroups of I-type (Tate, Van den Bergh 1996)
- Bieberbach groups (G.-I., Van den Bergh 1998)
- Semi-simple Hopf algebras (Etingof, Gelaki 1998)
- Geometric crystals (Etingof 2001)
- Dynamical systems (Goncharenko, Veselov 2004)

Quantum binomial algebras have a basis $\{x_1, \ldots, x_n\}$ of *skew-polynomial type*, i. e. with $\binom{n}{2}$ relations

$$x_j x_i = x_{i'} x_{j'}, \quad i < j > i' < j'$$

forming a *Gröbner basis*: They allow a unique reduction of monomials to ordered monomials. They have nice properties (Noetherian, Auslander-regular, Macaulay, global dimension n, Koszul, ...).

Every quantum binomial algebra gives rise to a square-free unitary solution

$$R(x_j, x_i) := (x_{j'}, x_{i'})$$

of the QYBE.

Conversely, Gateva-Ivanova verified for $n \leqslant 31$, or $n = pq$ (with p, q prime), the following

Conjecture (1996). *Every square-free unitary solution of the QYBE arises in this way.*

Etingof, Schedler, and Soloviev (Duke 1998) verified it for $n \leqslant 8$ and proved its equivalence to a formally simpler statement:

Decomposibility Conjecture. *For a finite set X with more than one element, every square-free unitary solution R: $X^2 \to X^2$ of the QYBE is decomposable.*

Here R is said to be **decomposable** if there is a non-trivial partition $X = Y \amalg Z$ with $R(Y^2) \subset Y^2$ and $R(Z^2) \subset Z^2$.

Note that a decomposition $X = Y \amalg Z$ tells us nothing about $R(Y, Z)$ or $R(Z, Y)$.

The conjecture can be translated into the language of cycle sets (Adv. Math. 2005):

Proposition 1. *There is a category equivalence between cycle sets X and left non-degenerate unitary solutions R of the QYBE. Moreover,*

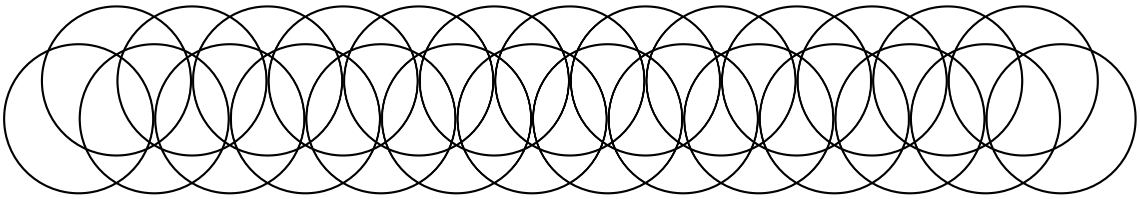
$$\begin{aligned} R \textit{ non-degenerate} &\Leftrightarrow x \mapsto x \cdot x \textit{ bijective} \\ R \textit{ square-free} &\Leftrightarrow \forall x \in X \colon x \cdot x = x \\ R \textit{ indecomposable} &\Leftrightarrow y \mapsto x \cdot y \textit{ transitive} \end{aligned}$$

Theorem 1. *Every finite cycle sets X is non-degenerate.*

So the decomposibility conjecture turns into the

Conjecture. *Every finite square-free cycle set with more than one element is decomposable.*

Cycles ...



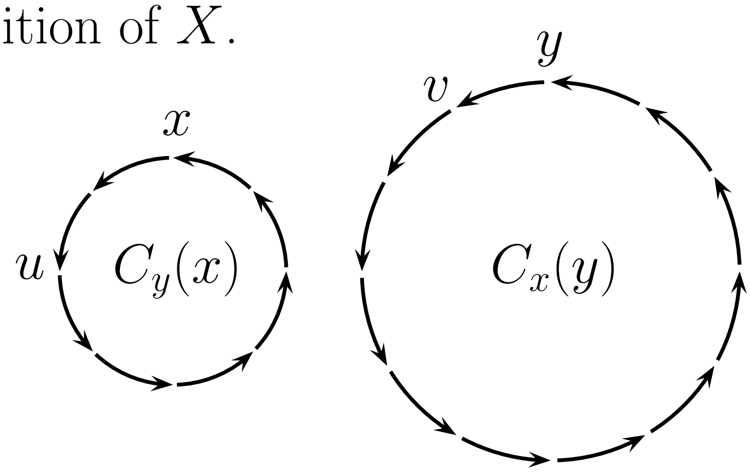
Let X be a *square-free* cycle set, i. e. $x \cdot x = x$ for all $x \in X$. (Then X is non-degenerate.) For any $x \in X$, the powers of the left multiplication $y \mapsto x \cdot y$ decompose X into (finite or infinite) orbits which we call *cycles* $C_x(y)$ (represented by y). Thus $C_x(x) = \{x\}$.

Proposition 2. *Let X be a square-free cycle set, with different elements $x, y \in X$. Then*

$$C_x(y) \cap C_y(x) = \varnothing.$$

For $u \in C_y(x)$ and $v \in C_x(y)$, $x \cdot v = u \cdot v$.

Thus if $X = C_x(y) \cup C_y(x)$, the two cycles yield a decomposition of X.



Gateva-Ivanova's conjecture is equivalent to the following

Bi-Cycle Conjecture. *Every finite square-free cycle set admits a linear ordering such that*

$$x < y \Rightarrow C_y(x) < C_x(y).$$

To prove the preceding conjectures, we established the following

Theorem 2. *Every finite square-free cycle set X with $|X| > 1$ is decomposable, i. e. there exists a non-trivial partition $X = Y \amalg Z$ with $X \cdot Y \subset Y$ and $X \cdot Z \subset Z$.*

Note: The Theorem 2 implies the bi-cycle conjecture: If $X = Y \amalg Z$, we can put $Y < Z$ and then proceed by induction.

A counterexample for $|X| = \infty$

Let $C_0 = \langle z \rangle$ be the infinite cyclic group. Every element of the group ring $\mathbb{F}_2 C_0$ is of the form

$$a = \sum_{n \in N} z^n$$

with $N \subset \mathbb{Z}$ finite. Define $v \colon \mathbb{F}_2 C_0 \to \mathbb{F}_2 C_0$ by

$$v(a) := \begin{cases} z^{\max N} & \text{for } a \neq 0 \\ 0 & \text{for } a = 0. \end{cases}$$

Then we have a binary operation

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

on $\mathbb{F}_2 C_0$ which satisfies

$$a \cdot a = a$$
$$a \cdot (a \cdot b) = b.$$

Theorem 3. *With the above defined product, the infinite set $\mathbb{F}_2 C_0$ is an indecomposable square-free cycle set. The corresponding solution of the QYBE is given by*

$$R(a, b) = (b \cdot a, a \cdot b).$$

The cycloid equation

$$\text{(L)} \qquad \boxed{(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z)}$$

occurs in a quite different context: (L) means "logic"! We interpret $x, y, z \in X$ as propositions and

$$x \to y := x \cdot y$$

as "x implies y". Then (L) becomes a true statement in classical logic:

$$\boxed{(x \to y) \to (x \to z) = (y \to x) \to (y \to z)}$$

which also holds in Brouwer's intuitionistic logic as well as in Łukasiewicz' infinite-valued logic, and in many other types of logical systems.

We call $1 \in X$ a **logical unit** (="true") if

$$\boxed{1 \to x = x\,; \quad x \to x = x \to 1 = 1}$$

holds for all $x \in X$. A logical unit is always unique.

In a unital cycloid X, equivalence of propositions can be factored out so that X becomes a poset with

$$x \leqslant y \;\Leftrightarrow\; x \to y = 1.$$

We call such X (equivalent propositions are equal) ***L*-algebras**. They provide the semantics for a very general type of logic. Their affinity to the QYBE leads to a rather interesting structure theory.

In the sequel, we write again $\cdot$ instead of $\to$. We call an L-algebra $(X, \cdot)$ **self-similar** if each of its left multiplications $y \mapsto x \cdot y$ induces an isotone bijection from the predecessor poset

$$\downarrow x := \{y \in X \mid y \leqslant x\}$$

onto all of X.

Every self-similar L-algebra X is a **left hoop**, i. e. it admits a second multiplication $X \times X \to X$ (written as juxtaposition), uniquely determined by the equations

$$\text{(A)} \qquad xy \cdot z = x \cdot (y \cdot z)$$

$$\text{(H)} \qquad (x \cdot y)x = (y \cdot x)y.$$

Furthermore, any pair of elements $x, y \in X$ admits an infimum ("x and y")

$$x \wedge y := (x \cdot y)x.$$

Example (The "logic" of l-groups): For any lattice-ordered group G, the negative cone G_- is a self-similar L-algebra such that

$$x \cdot y := yx^{-1} \wedge 1$$

for $x, y \in G$. So (L) also refers to "lattice-ordered"!

Theorem 4. *Every L-algebra X has a natural embedding into a smallest self-similar L-algebra $S(X)$ which respects existing meets $x \wedge y$ in X.*

We have seen: Every l-group G has its "logic", that is, the L-algebra G_-. Conversely,

Every "logic" defines a group:

The hoop equation (H) implies that the self-similar closure $S(X)$ of an L-algebra X satisfies the left Ore condition. Hence it has a left quotient group $G(X)$, and there is a natural map

$$q\colon X \longrightarrow G(X).$$

We call $G(X)$ the **structure group** of X.

If X has a smallest element 0 (="false"), we can define the **negation**:

$$\neg x := x \cdot 0.$$

Then

$$q(x) = q(y) \;\Leftrightarrow\; \neg x = \neg y.$$

So q is an embedding if and only if double negation does not change anything!

We call an L-algebra X **semiregular** if

$$x(y \wedge z) = xy \wedge xz$$

holds for $x, y, z \in S(X)$.

Theorem 5. *The structure group $G(X)$ of a semiregular L-algebra X is an l-group.*

Example 2. Every partially ordered set Ω defines an L-algebra $\widehat{\Omega} := \Omega \cup \{1\}$ by adjoining a greatest element 1 to Ω. For $x, y \in \widehat{\Omega}$, we set $x \cdot y := 1$ if $x \leqslant y$ and $x \cdot y := y$ otherwise. Such an L-algebra $\widehat{\Omega}$ is never self-similar unless $\Omega = \varnothing$.

Proposition 3. *A partially ordered set Ω is a tree if and only if $\widehat{\Omega}$ is semiregular.*

The "logic" of a topological space

The set $\mathcal{O}(X)$ of open sets of a topological space X is an L-algebra with

$$U \cdot V := X \smallsetminus \overline{U \smallsetminus V}$$

for $U, V \in \mathcal{O}(X)$. With respect to intersection,

$$UV := U \cap V,$$

$\mathcal{O}(X)$ is a (left and right) hoop, a so-called Heyting-algebra. A space X is **extremally disconnected** if the closure of every open set is open. Compact extremally disconnected spaces form the projective objects in the category of compact spaces. Every irreducible algebraic variety is extremally disconnected in the Zariski topology.

Theorem 6. *Let X be a topological space. The L-algebra $\mathcal{O}(X)$ is semiregular if and only if X is extremally disconnected.*

Corollary. *The L-algebra $\mathcal{O}(X)$ of an extremally disconnected space X is embedded into its structure group if and only if X is almost discrete (i. e. every open set is closed).*

If X is discrete, it generates an l-group cone. The corollary provides a new type of generation.

What about "common sense" logic?

Every Boolean algebra B is of course an L-algebra. Its structure group $G(B)$ is an Archimedean l-group.

Definition. Let G be an l-group.

(a) An element $s \in G_-$ is **singular** if $s = gh$ with $g, h \in G_-$ implies that $g \vee h = 1$.

(b) An element $s \in G_-$ is a **strong unit** if for each $g \in G$, there exists an $n \in \mathbb{N}$ such that $s^n \leqslant g$.

Theorem 7. *A singular strong unit $0 \in G_-$ of an l-group G is unique, and then the interval $B := [0, 1]$ is a Boolean algebra with structure group G. Conversely, every Boolean algebra B arises in this way.*

Corollary. *The category of Boolean algebras is equivalent to the full subcategory of l-groups with a singular strong unit.*