Braces and Hopf-Galois Structures

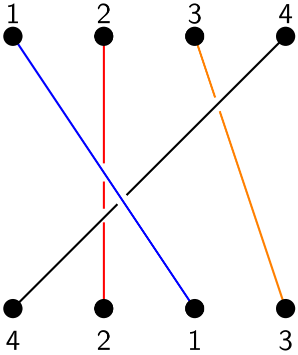
Nigel Byott

University of Exeter, UK

Omaha, 24 May 2017

Braids and the Yang-Baxter Equation

Consider a braid on n strings, e.g. $(n = 4)$



The final order of the strings is determined by an element of the **symmetric group** S_n.

If we also take account of whether one string goes over or under another, the configuration is described by the **braid group** B_n

Braids and the Yang-Baxter Equation

S_n is generated by the elementary transpositions $\sigma_{i.i+1} = (i, i+1)$ for $1 \leq i \leq n-1$, subject to relations

$$\sigma_{i,i+1}^2 = 1,$$

$$\sigma_{i,i+1}\sigma_{j,j+1} = \sigma_{j,j+1}\sigma_{i,i+1} \text{ if } |i-j| > 1,$$

$$\sigma_{i,i+1}\sigma_{j,j+1}\sigma_{i,i+1} = \sigma_{j,j+1}\sigma_{i,i+1}\sigma_{j,j+1} \text{ if } |i-j| = 1.$$

B_n has generators $\hat{\sigma}_{i,i+1}$ for $1 \leq i \leq n-1$ with the same relations, except that the generators have infinite order:

$$\hat{\sigma}_{i,i+1}\hat{\sigma}_{j,j+1} = \hat{\sigma}_{j,j+1}\hat{\sigma}_{i,i+1} \text{ if } |i-j| > 1,$$

$$\hat{\sigma}_{i,i+1}\hat{\sigma}_{j,j+1}\hat{\sigma}_{i,i+1} = \hat{\sigma}_{j,j+1}\hat{\sigma}_{i,i+1}\hat{\sigma}_{j,j+1} \text{ if } |i-j| = 1.$$

Braids and the Yang-Baxter Equation

Up to a shift of the subscripts, the interesting relation is

$$\hat{\sigma}_{12}\hat{\sigma}_{23}\hat{\sigma}_{12} = \hat{\sigma}_{23}\hat{\sigma}_{12}\hat{\sigma}_{23}$$

Many problems in mathematics and physics involve in some way actions/representation of S_n or B_n, so we should not be surprised if some form of the **braid relation**

$$s_{12}s_{23}s_{12} = s_{23}s_{12}s_{23}$$

arises in many different contexts.

Braids and the Yang-Baxter Equation

Here is a linear algebra version.

Let V be a vector space, and $R : V \otimes V \to V \otimes V$ a linear map. Consider the functions $V \otimes V \otimes V \to V \otimes V \otimes V$ given by

$$R_{12} = R \otimes \mathrm{id}_V, \quad R_{23} = \mathrm{id}_V \otimes R.$$

If R is invertible and satisfies the condition

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

in $\mathrm{GL}(V \otimes V \otimes V)$ then we get a representation of B_n on $V^{\otimes n}$ with

$$\hat{\sigma}_{i,i+1} \mapsto \underbrace{\mathrm{id} \otimes \cdots \mathrm{id}}_{i-1} \otimes R \otimes \underbrace{\mathrm{id} \otimes \cdots \mathrm{id}}_{n-i-1}.$$

This is a representation of S_n if also $R^2 = \mathrm{id}$.

Here is an alternative formulation.

Let $\tau : V \otimes V \to V \otimes V$ be the "twist" map: $\tau(a \otimes b) = b \otimes a$. Set

$$\overline{R} = \tau \circ R : V \otimes V \to V \otimes V$$

and let

$$\overline{R}^{12}, \overline{R}^{23}, \overline{R}^{13} : V \otimes V \otimes V \to V \otimes V \otimes V$$

be given by $\overline{R}$ acting in factors 1, 2 (resp. 2, 3, resp. 1, 3).

Then the braiding relation for R is equivalent to

$$\overline{R}^{12}\overline{R}^{13}\overline{R}^{23} = \overline{R}^{23}\overline{R}^{13}\overline{R}^{12}.$$

The equation

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

is called the **(classical) Yang-Baxter Equation** (YBE).
The equation

$$\overline{R}^{12}\overline{R}^{13}\overline{R}^{23} = \overline{R}^{23}\overline{R}^{13}\overline{R}^{12}.$$

is the called the **Quantum Yang-Baxter Equation** (QYBE).

The name comes from
C.N. Yang (1967) [wave function of n particles in 1 dimension];
R.J. Baxter (1971) [lattice models in statistical physics].

Two approaches to constructing solutions to (Q)YBE arise from the work of Drinfeld around 1990:
(1) quasitriangular structures on bialgebras (quantum groups): not the topic of this talk!
(2) set-theoretical solutions. These were studied in detail by
[ESS] P. Etingof, T. Schedler and A. Soloviev [Duke, 1999].

Braided Sets (after ESS)

A **braided set** is a pair (X, S) where X is a finite nonempty set and S is a bijection $S : X \times X \to X \times X$ such that

$$S_{12}S_{23}S_{12} = S_{23}S_{12}S_{23} : X \times X \times X \to X \times X \times X.$$

Then S gives a **set-theoretical solution** of YBE on the vector space V with basis X.

(X, S) is **involutive** if $S^2 = \mathrm{id}_{X\times X}$ (so it gives a repesentation of the symmetric group).

Write $S(x, y) = (g_x(y), f_y(x))$. Then (X, S) is **non-degenerate** if the functions g_x, $f_y : X \to X$ are bijections for all x, $y \in X$.

Trivial Example: If $S(x, y) = (y, x)$ $\forall x$, y then $g_x = f_y = \mathrm{id}_X$ for all x, y.

Let X be a non-degenerate involutive braided set (X, S).

Its **structure group** G_X has generators (labelled by) elements of X with the relations

$$xy = wz \text{ in } G_X \text{ if } S(x, y) = (w, z).$$

So in the trivial case $S(x, y) = (y, x)$ $\forall x$, y we get $G_X = \mathbb{Z}^X$, the free abelian group on X.

What is the relationship between G_X and $\mathbb{Z}^X$ in general?

Write $\mathbb{Z}^X$ additively, with generator t_X corresponding to $x \in X$.

Consider the semidirect product

$$\mathbb{Z}^X \rtimes \mathrm{Perm}(X) = \left\{ \left[\sum_{x \in X} c_x t_x, \alpha \right] : \sum_{x \in X} c_x t_x \in \mathbb{Z}^X, \alpha \in \mathrm{Perm}(X) \right\}$$

where

$$[t_x, \alpha][t_y, \beta] = [t_x + t_{\alpha(y)}, \alpha\beta].$$

ESS proved that G_X is soluble, and that there is an injective group homomorphism

$$\phi : G_X \to \mathbb{Z}^X \rtimes \mathrm{Perm}(X), \qquad x \mapsto [t_x, f_x^{-1}].$$

We can break ϕ into two parts: (i) a homomorphism

$$G_X \to \mathrm{Perm}(X), \qquad x \mapsto f_x^{-1},$$

(which gives an action of G_X on X and hence on $\mathbb{Z}^X$), and (ii) a function

$$\Pi : G_X \to \mathbb{Z}^X, \qquad x \mapsto t_x$$

which is not a homomorphism. (In fact, it is a cocycle for the above action.)

Now let $\Gamma = \phi(G_X) \cap \mathbb{Z}^X$ (an infinite abelian group) and set

$$A = \mathbb{Z}^X/\Gamma, \qquad G_X^0 = G_X/\phi^{-1}(\Gamma).$$

Then A is a finite abelian group, G_X^0 acts on A, and Π induces a bijective cocycle $\pi : G_X^0 \to A$ for this action.

Definition: A (finite) **bijective cocycle datum** (G, A, ρ, π) consists of a finite group G, an abelian group A, a homomorphism $\rho : G \to \mathrm{Aut}(A)$ (i.e. an action of G on A), and a bijection $\pi : G \to A$ which is a cocycle for this action: $\pi(gh) = \pi(g) + g \cdot \pi(h) = \pi(g) + \rho(g)(\pi(h))$.

So we have seen how to get a bijective cocycle datum (G_X^0, A, ρ, π) from a non-degenerate involutive braided set X. But we have lost sight of the set X: if $S(x, y) = (y, x)$ then $G_X^0 = \{1\}$ however large X is.

The problem of reconstructing all possible sets X from a bijective cocycle datum (there are infinitely many of them) is nontrivial, and has recently been solved by D. Bachiller, F. Cedó, E. Jespers (J. Algebra, 2016).

Braces

Braces were introduced by Wolfgang Rump [J. Algebra, 2007] to study set-theoretical solutions of YBE.

One of several equivalent definitions is the following:

A (left) brace is a set B with binary operations $+$, $\cdot$ such that

- $(B, +)$ is an abelian group;
- $(B, \cdot)$ is a group;
- $a \cdot (b + c) + a = a \cdot b + a \cdot c \ \forall a, b, c \in B$.

We will call $(B, +)$ the *additive group*, and $(B, \cdot)$ the *multiplicative group*, of B.

Homomorphisms of braces are maps preserving both operations.

Define a further binary operation $*$ by $a * b = a \cdot b - a$.

Proposition: If $(B, +, \cdot)$ is a brace then

- $(B, \cdot)$ acts on $(B, +)$ by $(a, b) \mapsto a * b$, giving a homomorphism $\rho : (B, \cdot) \to \mathrm{Aut}(B, +)$.
- The function $\mathrm{id}_B : (B, \cdot) \to (B, +)$ is a cocycle for this action.

In other words, a (finite) brace is just another way of describing a (finite) bijective cocycle datum.

So if we could classify (up to isomorphism) all braces with a given multiplicative group G, this would tell us something about braided sets and hence about set-theoretical solutions to YBE.

This has been done for G cyclic (Rump) and for $|G| = p^3$ (Bachiller).

Hopf-Galois Structures

Now let L/K be a finite Galois extension of fields and $G = \mathrm{Gal}(L/K)$. We are interested in finding actions of K-Hopf algebras on L which give a Hopf-Galois structure to L.

By Greither-Pariegis these correspond to regular subgroups N of $\mathrm{Perm}(G)$ which are normalised by left translations by G. We call the isomorphism class N the *type* of the corresponding Hopf-Galois structure.

If N is such a subgroup, we can use the bijection $N \to G$, $n \mapsto n(e_G)$ to identify the underlying sets of N and G. Then we can view G as a regular subgroup of $\mathrm{Hol}(N) = N \rtimes \mathrm{Aut}(N) \subset \mathrm{Perm}(N)$.

Thus we have a homomorphism $G \to \mathrm{Aut}(N)$ and a bijective (possibly nonabelian) cocycle $G \to N$.

The relationship between braces and Hopf-Galois structures

To summarise so far:

Theorem: Let G be a finite group and let A be an abelian group with $|A| = |G|$. Then the following are equivalent:

- finding a bijective cocycle datum (G, A, ρ, π);
- finding a brace $(B, \cdot, +)$ with $(B, \cdot) \cong G$ and $(B, +) \cong A$;
- finding a regular subgroup isomorphic to G in $\mathrm{Hol}(A)$.
- finding a Hopf-Galois structure of (abelian) type A on a Galois field extension with Galois group G;

However, the corresponding counting problems are **not** the same.
Two regular **subgroups** in $\mathrm{Hol}(A)$ give isomorphic braces if and only if they are conjugate under $\mathrm{Aut}(A)$: we need to count **orbits** of subgroups.

Two regular **embeddings** $G \to \mathrm{Hol}(A)$ give the same Hopf-Galois structure if and only if they are conjugate under $\mathrm{Aut}(A)$: we need to count the **number** of subgroups and multiply by $|\mathrm{Aut}(G)|/|\mathrm{Aut}(A)|$.

Which groups arise as the multiplicative group of a brace?

By [ESS], if G occurs as the multiplicative group of a brace, then G must be soluble.

Equivalently, if L/K has a Hopf-Galois structure of abelian type, then $G = \mathrm{Gal}(L/K)$ is soluble.
[In fact, we know that if L/K has a Hopf-Galois structure of nilpotent type then G is soluble.]

Question: Does every finite soluble group G occur as the multiplicative group of a brace?

i.e. If $\mathrm{Gal}(L/K)$ is soluble, must L/K admit a Hopf-Galois structure of abelian type?

David Bachiller (J. Algebra, 2016) gave a counterexample.

Bachiller's counterexample

Milnor conjectured that a nilpotent Lie group over $\mathbb{C}$ of dimension n admits a left-invariant affine structure. This means its Lie algebra has a faithful affine representation of dimension $n+1$. D. Burde (1997) found, with the aid of computer calculations, a family of nilpotent Lie algebras of dimension 10 over $\mathbb{C}$ which do not have a faithful affine representation of dimension 11. This gives a family of counterexamples to Milnor's conjecture.

Lazard showed that Lie algebras of nilpotency class $< p$ over $\mathbb{F}_p$ correspond to finite p-groups of nilpotency class $< p$. If we choose p large enough that $p > 10$ and the relations found by Burde still work in characteristic p (in principle this is a Gröbner basis calculation) then we get a group of order p^{10} which there is no brace/Hopf-Galois structure of *elementary* abelian type. A separate calculation shows $p = 23$ works.

Bachiller's counterexample

To rule out braces/Hopf-Galois structures whose type is abelian but not elementary abelian, Bachiller proves the following generalisation of a result of Featherstonhaugh, Caranti and Childs:

Theorem (Bachiller): Let p be prime and let B be a brace with

$$(B,+) \cong \mathbb{Z}/(p^{\alpha_1}) \times \cdots \times \mathbb{Z}/(p^{\alpha_m})$$

with $1 \leq \alpha_1 \leq \cdots \leq \alpha_m$. Assume that $m+2 \leq p$. Then, for each $x \in B$,

$$\text{Order of } x \text{ in } (B,\cdot) = \text{Order of } x \text{ in } (B,+).$$

In particular, if $(B,\cdot)$ is abelian then $(B,+) \cong (B,\cdot)$.

Conclusion: For all large enough primes p, there is a (solvable, nonabelian) group G of order p^{10} such that a Galois extension with group G admits no Hopf-Galois structures of abelian type.

Question: Is there an easier counterexample?

Quaternionic Braces

In the paper

> L. Guarnieri and L. Vendramin:
> *Skew Braces and the Yang-Baxter Equation,*
> (Mathematics of Computation, 2017)

the authors give results of computer calculations counting all braces of size n for $n \leq 120$ (excluding $n = 32$, 64, 81, 96).

On the basis of these, they formulate several conjectures and questions, mostly about quaternionic braces.

Quaternionic Braces

For $m \geq 2$, let Q_{4m} be the quaternion group of order $4m$:

$$Q_{4m} = \langle a, b, \ : \ a^m = b^2, a^{2m} = 1, bab^{-1} = a^{-1} \rangle.$$

Let $q(4m)$ be the number of isomorphism classes of braces with multiplicative group Q_{4m}.

Conjecture (Guarnieri and Vendramin)

$$q(4m) = \begin{cases} 2 & \text{if } m \text{ is odd,} \\ 6 & \text{if } m \equiv 2 \text{ or } 6 \pmod 8, \\ 9 & \text{if } m \equiv 4 \pmod 8, \\ 7 & \text{if } m \equiv 0 \pmod 8. \end{cases}$$

Work in progress:

Theorem 1 (NB):
Let $m = 2^s k$ with $s \geq 0$ and k odd, so $4m = 2^n k$ with $n = s + 2$.

Then every quaternionic brace of order $2^n k$ induces a quaternionic brace of order 2^n, and each quaternionic brace of order 2^n is induced from exactly one quaternionic brace of order $2^n k$ (up to isomorphism).

Thus $q(2^n k) = q(2^n)$. (If $s = 0$, interpret Q_4 as $C_2 \times C_2$.)

Theorem 2 (NB): If $n \geq 2$ and A is an abelian group of order 2^n whose holomorph contains an element of order 2^{n-1} then

$$A = C_{2^n}, \quad C_2 \times C_{2^{n-1}}, \quad C_4 \times C_{2^{n-2}}, \quad C_2 \times C_2 \times C_{2^{n-2}} \text{ or } C_2 \times C_2 \times C_2 \times C_{2^{n-3}}.$$

Examining these cases, we find

$$q(4) = 2, \qquad q(8) = 6, \qquad q(16) = 9, \qquad q(2^n) = 7 \text{ for } n \geq 5.$$

Conclusion: The Conjecture of Guarnieri and Vendramin is true.

Proof of Theorem 1 (sketch)

Let $Q \cong Q_{4m}$ be a regular subgroup in $\mathrm{Hol}(A)$ where $|A| = 4m = 2^n k$, A abelian.

Then $\mathrm{Hol}(A) = \mathrm{Hol}(B) \times \mathrm{Hol}(C)$ with B, C abelian, $|B| = 2^n$, $|C| = k$.

Via the projection $\mathrm{Hol}(A) \to \mathrm{Hol}(B)$, Q acts *transitively* on B.

The stabiliser of e_B in Q has order k, and the only subgroup of order k in Q is $T = \langle a^{2^{n-1}} \rangle$ which is **normal**. Hence Q/T is a regular subgroup of $\mathrm{Hol}(B)$ (and T is a regular subgroup of $\mathrm{Hol}(C)$).

This means that we have decomposed the quaternionic brace of order $2^n k$ into a quaternionic brace of order 2^n and a brace of (odd) order k (with multiplicative group $T \cong C_k$ and additive group C).

Equivalently, we have shown that a Hopf-Galois structure (of abelian type) with Galois group $Q_{2^n k}$ decomposes into one with Galois group Q_{2^n} and one with Galois group C_k. The last must be of cyclic type. (Split into prime-power pieces and use Tim Kohl's thesis!)

Proof of Theorem 1 (sketch - continued)

Conversely, how can we fit together regular subgroups

$$Q' \cong Q_{2^n} \subset \mathrm{Hol}(B), \qquad T \cong C_k \subset \mathrm{Hol}(C)$$

to get a regular quaternion subgroup

$$Q = Q_{2^n k} = T \rtimes Q' \subset \mathrm{Hol}(B \times C) = \mathrm{Hol}(B) \times \mathrm{Hol}(C) \ ?$$

We claim this can only be done if T is just translations by C_k, and then there is just one subgroup which works (up to conjugation by $\mathrm{Aut}(C)$).

We know how Q projects to $\mathrm{Hol}(B)$ (with kernel T). How does it project to $\mathrm{Hol}(C)$?

We need a homomorphism $\rho : Q \to \mathrm{Aut}(C)$ and a surjective cocycle $\pi : Q \to C$ for the corresponding action. As $\mathrm{Aut}(C)$ is abelian, ρ factors through $C_2 \times C_2$. In particular $\rho(T)$ is trivial, so T acts by translations. We check there is only one ρ for which a surjective π exists. All possible π are conjugate under $\mathrm{Aut}(C)$.

Final comments

(1) All this works for dihedral groups as well as quaternion ones.

(2) With some extra work (which I have not yet done) this would count all Hopf-Galois structures **of abelian type** on quaternion/dihedral Galois extensions of arbitrary degree.