An explicit construction of brace blocks

Lorenzo Stefanello

Joint work with Andrea Caranti

Braces in Bracelet Bay, 4 January 2022

Outline

- Introduction
- The main construction
- Examples and applications

Introduction

Definition ([Rump, 2007], [Guarnieri and Vendramin, 2017])

A *skew brace* is a triple $(G, \cdot, \circ)$, where $(G, \cdot)$ and $(G, \circ)$ are groups and for all $g, h, k \in G$,

$$g \circ (h \cdot k) = (g \circ h) \cdot g^{-1} \cdot (g \circ k).$$

(Here $^{-1}$ denotes the inverse with respect to $\cdot$.)

Definition ([Childs, 2019])

A *bi-skew brace* is a triple $(G, \cdot, \circ)$, where both $(G, \cdot, \circ)$ and $(G, \circ, \cdot)$ are skew braces.

Brace blocks

Definition ([Koch, 2021b], [Caranti and LS, 2021a])

Let G be a nonempty set. A *brace block* on G is a family $(\circ_i \mid i \in I)$ of group operations on G, where I is an index set, such that $(G, \circ_i, \circ_j)$ is a (bi-)skew brace for all $i, j \in I$.

Main goal: find an explicit way to construct brace blocks.

The main construction

Koch's first construction

In [Koch, 2021a], the following construction was introduced.

Let $(G, \cdot)$ be a finite group, and let ψ be an abelian endomorphism of G (meaning that the image $\psi(G)$ is abelian).

Then $(G, \cdot, \circ)$ is a bi-skew brace, where

$$g \circ h = g \cdot \psi(g)^{-1} \cdot h \cdot \psi(g).$$

Koch's second construction

In [Koch, 2021b], Koch observed that if ψ is an abelian endomorphism of G yielding the bi-skew brace $(G, \cdot, \circ)$, where

$$g \circ h = g \cdot \psi(g)^{-1} \cdot h \cdot \psi(g),$$

then ψ is also an abelian endomorphism of $(G, \circ)$.

Iterating his first construction, he found a brace block $(\circ_n \mid n \in \mathbb{N})$ on G, with $\circ_0 = \cdot$ and $\circ_1 = \circ$.

A first generalisation

Let $(G, \cdot)$ be a group.

In [Caranti and LS, 2021b], we characterised the endomorphisms ψ of G such that $(G, \cdot, \circ)$ is a bi-skew brace, where

$$g \circ h = g \cdot \psi(g)^{\varepsilon} \cdot h \cdot \psi(g)^{-\varepsilon}.$$

(Here $\varepsilon = \pm 1$.)

For example, the result holds if $\psi([G, G]) \leq Z(G)$.

The key observation

We can generalise Koch's second construction assuming that ψ satisfies the weaker condition $\psi([G, G]) \leq Z(G)$.

But we do not have to use that ψ is an endomorphism!

As it appears always inside a conjugation, what is really important is that ψ is an "endomorphism modulo the center", that is,

$$\psi(g \cdot h) \equiv \psi(g) \cdot \psi(h) \pmod{Z(G)}.$$

The setting

Let $(G, \cdot)$ be a group, let K be a subgroup of G contained in $Z(G)$, and let A be a subgroup of G such that A/K is abelian.

Consider the ring

$$\mathcal{A} = \{\psi \in \mathrm{End}(G/K) \mid \psi(G/K) \leq A/K\}.$$

For all $\psi \in \mathcal{A}$, define $\psi^{\uparrow}$ to be a lifting of ψ, that is, a set-theoretic map $\psi^{\uparrow} \colon G \to A$ such that

$$\psi^{\uparrow}(g)K = \psi(gK).$$

Finally, on the model of [Caranti, 2018], consider the set

$$\mathcal{B} = \{\alpha \colon G \times G \to K \mid \alpha \text{ is bilinear and } \alpha(K, G) = \alpha(G, K) = 1\}.$$

The main theorem

Recall: $K \leq Z(G)$, A/K abelian,

$\mathcal{A} = \{\psi \in \mathrm{End}(G/K) \mid \psi(G/K) \leq A/K\}$,
$\mathcal{B} = \{\alpha\colon G \times G \to K \mid \alpha \text{ is bilinear and } \alpha(K, G) = \alpha(G, K) = 1\}$.

For all $(\psi, \alpha) \in \mathcal{A} \times \mathcal{B}$, define

$$g \circ_{\psi,\alpha} h = g \cdot \psi^{\uparrow}(g) \cdot h \cdot (\psi^{\uparrow}(g))^{-1} \cdot \alpha(g, h).$$

Then $(G, \cdot, \circ_{\psi,\alpha})$ is a bi-skew brace.

Theorem ([Caranti and LS, 2021a])

The family $(\circ_{\psi,\alpha} \mid (\psi, \alpha) \in \mathcal{A} \times \mathcal{B})$ *is a brace block on* G.

The construction can be iterated!

Assume the previous setting, and set $\circ_0$ to be $\cdot$.

Theorem ([Caranti and LS, 2021a])

Let $((\psi_n, \alpha_n) \mid n \geq 1)$ *be a sequence of elements of* $\mathcal{A} \times \mathcal{B}$*, and for all* $n \geq 1$ *define*

$$g \circ_n h = g \circ_{n-1} \psi_n^{\uparrow}(g) \circ_{n-1} h \circ_{n-1} \overline{\psi_n^{\uparrow}(g)} \circ_{n-1} \alpha_n(g, h).$$

(Here an overline denotes the inverse with respect to $\circ_{n-1}$*.)*

Then for all $n \geq 1$*, there exists* $(q_n, \beta_n) \in \mathcal{A} \times \mathcal{B}$ *such that*

$$g \circ_n h = g \cdot q_n^{\uparrow}(g) \cdot h \cdot (q_n^{\uparrow}(g))^{-1} \cdot \beta_n(g, h).$$

In particular, $(\circ_n \mid n \in \mathbb{N})$ *is a brace block on* G*.*

Examples and applications

Koch's first construction revisited

We can recover Koch's constructions in the following way.

Let $(G, \cdot)$ be a group, let φ be an abelian endomorphism of G, let $K = 1$, and let A be an abelian subgroup of G with $\varphi(G) \le A$.

Consider

$$\psi = -\varphi \in \mathcal{A} = \{\phi \in \mathrm{End}(G) \mid \phi(G) \le A\}.$$

Then $(G, \cdot, \circ_\psi)$ is a bi-skew brace, where

$$g \circ_\psi h = g \cdot \psi(g) \cdot h \cdot \psi(g)^{-1} = g \cdot \varphi(g)^{-1} \cdot h \cdot \varphi(g).$$

Koch's second construction revisited

We can iterate the construction with $(\psi_n \mid n \geq 1)$, taking

$$\psi_n = \psi = -\varphi$$

for all $n \in \mathbb{N}$, to find that $(\circ_n \mid n \in \mathbb{N})$ is a brace block on G, where

$$g \circ_n h = g \cdot q_n(g) \cdot h \cdot q_n(g)^{-1}.$$

Here

$$q_n = \sum_{i=1}^{n} \binom{n}{i} \psi^i = \sum_{i=1}^{n} \binom{n}{i} (-\varphi)^i.$$

Let $(G, \cdot)$ be a group of nilpotence class two, let $K = [G, G]$, and let $A = G$. In this case $\mathcal{A} = \mathrm{End}(G/K)$.

For all $n \in \mathbb{N}$ and $g \in G$, write

$$\psi_n(gK) = (gK)^n.$$

Then $\psi_n \in \mathcal{A}$ and

$$\psi_n^{\uparrow} \colon g \to g^n$$

is a lifting of ψ_n.

We derive that $(\circ_{\psi_n} \mid n \in \mathbb{N})$ is a brace block on G, where

$$g \circ_{\psi_n} h = g \cdot g^n \cdot h \cdot g^{-n} = g \cdot h \cdot [g, h]^n.$$

A pleasant example

Let p be a prime number, and let $G = \{(a,b,c) \mid a,b,c \in \mathbb{Z}_p\}$ be the p-adic Heisenberg group, with group operation

$$(a,b,c)\cdot(a',b',c') = (a+a', b+b', c+c'+ab').$$

Then G is a topological group of class two, so $(\circ_{\psi_{p^n}} \mid n \in \mathbb{N})$ is a brace block for G, where for all $g=(a,b,c), h=(a',b',c') \in G$,

$$g \circ_{\psi_{p^n}} h = g\cdot h\cdot [g,h]^{p^n} = g\cdot h\cdot(0,0,p^n(ab'-a'b)).$$

In particular, the following facts hold:

- The brace block consists of infinitely many distinct operations.
- The skew braces of the kind $(G,\cdot,\circ_{\psi_{p^n}})$ are not isomorphic.
- The operations $\circ_{\psi_{p^n}}$ converge to the original operation:

$$\lim_{n\to\infty} g \circ_{\psi_{p^n}} h = g\cdot h.$$

Definition ([Drinfel'd, 1992])

A *(set-theoretic nondegenerate) solution* of the Yang–Baxter equation is a couple (X, r), where X is a nonempty set and

$$\begin{aligned} r\colon X \times X &\to X \times X \\ (x, y) &\mapsto (\sigma_x(y), \tau_y(x)) \end{aligned}$$

is a bijective map such that

$$(r \times \mathrm{id}_X)(\mathrm{id}_X \times r)(r \times \mathrm{id}_X) = (\mathrm{id}_X \times r)(r \times \mathrm{id}_X)(\mathrm{id}_X \times r)$$

and σ_x and τ_x are bijective for all $x \in X$.

By the work in [Rump, 2007], [Guarnieri and Vendramin, 2017], every skew brace yields a solution of the Yang–Baxter equation:

$$(G, \cdot, \circ) \rightsquigarrow r(g, h) = (g^{-1} \cdot (g \circ h), \overline{g^{-1} \cdot (g \circ h)} \circ g \circ h).$$

(Here $^{-1}$ denotes the inverse with respect to $\cdot$ and an overline denotes the inverse with respect to $\circ$.)

Let $(G, \cdot)$ be a group, and assume our main setting.

Theorem ([Caranti and LS, 2021a])

Let $(\psi, \alpha), (\varphi, \beta) \in \mathcal{A} \times \mathcal{B}$. Then the following is a solution for G:

$$\begin{aligned} r(g, h) = (&(\psi - \varphi)^{\uparrow}(g) \cdot h \cdot ((\psi - \varphi)^{\uparrow}(g))^{-1} \cdot \beta(g^{-1}, h) \cdot \alpha(g, h), \\ &(\psi^{\uparrow}(h))^{-1} \cdot (\psi - \varphi)^{\uparrow}(g) \cdot h^{-1} \cdot ((\psi - \varphi)^{\uparrow}(g))^{-1} \\ &\cdot g \cdot \psi^{\uparrow}(g) \cdot h \cdot (\psi^{\uparrow}(g))^{-1} \cdot \psi^{\uparrow}(h) \cdot \beta(g, h) \cdot \alpha(h^{-1}, g)). \end{aligned}$$

Regular subgroups

Let $(G, 1)$ be a pointed set, and let $\mathrm{Perm}(G)$ be the group of permutations on G.

Definition

A subgroup N of $\mathrm{Perm}(G)$ is *regular* if the map

$$\begin{aligned} N &\to G \\ \eta &\mapsto \eta[1] \end{aligned}$$

is a bijection.

We can write $N = \{\nu(g) \mid g \in G\}$, where $\nu(g)[1] = g$.

Bi-skew braces and regular subgroups

Fact

There is a bijective correspondence between operations $\circ$ on G such that $(G, \circ)$ is a group with identity 1 and regular subgroups $N = \{\nu(g) \mid g \in G\}$ of $\mathrm{Perm}(G)$, given by

$$g \circ h = \nu(g)[h].$$

Theorem ([Guarnieri and Vendramin, 2017], [Caranti, 2020])

Let $(G, \circ)$ and $(G, \diamond)$ be groups with identity 1, and let $N_\circ$ and $N_\diamond$ the corresponding regular subgroups. Then $(G, \circ, \diamond)$ is a bi-skew brace if and only if $N_\circ$ and $N_\diamond$ normalise each other.

Brace blocks and graphs

Definition

The *normalising graph* of G is the undirected graph whose vertices are the regular subgroups of $\mathrm{Perm}(G)$, and where two vertices are joined by an edge if and only if the corresponding subgroups normalise each other.

Fact

Brace blocks on G correspond to complete subgraphs in the normalising graph of G.

Can we explore this correspondence to find information in both settings?

Caranti, A. (2018).
Multiple holomorphs of finite p-groups of class two.
J. Algebra, 516:352–372.

Caranti, A. (2020).
Bi-skew braces and regular subgroups of the holomorph.
J. Algebra, 562:647–665.

Caranti, A. and LS (2021a).
Brace blocks from bilinear maps and liftings of endomorphisms.
arXiv:2110.11028.

Caranti, A. and LS (2021b).
From endomorphisms to bi-skew braces, regular subgroups, the Yang-Baxter equation, and Hopf-Galois structures.
J. Algebra, 587:462–487.

Bibliography II

Childs, L. N. (2019).
Bi-skew braces and Hopf Galois structures.
New York J. Math., 25:574–588.

Drinfel'd, V. G. (1992).
On some unsolved problems in quantum group theory.
In *Quantum groups (Leningrad, 1990)*, volume 1510 of *Lecture Notes in Math.*, pages 1–8. Springer, Berlin.

Guarnieri, L. and Vendramin, L. (2017).
Skew braces and the Yang-Baxter equation.
Math. Comp., 86(307):2519–2534.

Koch, A. (2021a).
Abelian maps, bi-skew braces, and opposite pairs of Hopf-Galois structures.
Proc. Amer. Math. Soc. Ser. B, 8:189–203.

Koch, A. (2021b).
Abelian maps, brace blocks, and solutions to the Yang-Baxter equation.
arXiv:2102.06104.

Rump, W. (2007).
Braces, radical rings, and the quantum Yang-Baxter equation.
J. Algebra, 307(1):153–170.