SKEW BRACES WITH PRIME MULTIPLE SIZE

Daniel Gil Muñoz

Charles University & Università di Pisa

AGTA 2025, Naples, Italy

Joint work with Teresa Crespo, Anna Rio and Montserrat Vela

TABLE OF CONTENTS

1.

AN INTRODUCTION TO SKEW BRACES

SKEW BRACES: A MOTIVATION

A skew brace is a structure that combines two group structures on a specific way.

Many notions from group theory are being translated to the setting of skew braces.

But also, skew braces play an important role in other topics of mathematics:

- The Yang-Baxter equation.
- Hopf-Galois theory.
- Ring theory.
- A very long etcetera.

Definition (Rump, 2007; Guarnieri-Vendramin, 2017)

A skew (left) brace is a triple $(B, \cdot, \circ)$, where B is a non-empty set and $\cdot, \circ$ are two group laws on B such that

$$a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c).$$

Additive group: $(B, \cdot)$.

Multiplicative group: $(B, \circ)$.

Brace $\equiv$ $(B, \cdot)$ abelian.

Size of $(B, \cdot, \circ)$: $|B|$.

A first example

If $(B, \cdot)$ is a group, then $(B, \cdot, \cdot)$ is a skew brace, referred to as the **trivial skew brace**.

Definition

The λ-function of a skew brace $(B, \cdot, \circ)$ is defined by

$$\begin{aligned} \lambda\colon \quad B &\longrightarrow \operatorname{Aut}(B, \cdot), \\ a &\longmapsto \lambda_a(b) = a^{-1} \cdot (a \circ b). \end{aligned}$$

- $a \circ b = a \cdot \lambda_a(b)$ for all $a, b \in B$.
- $\lambda_{a \circ b} = \lambda_a \lambda_b$ for all $a, b \in B$.

$\rightsquigarrow \lambda\colon (B, \circ) \longrightarrow \operatorname{Aut}(B, \cdot)$ is a group homomorphism.

Definition

A homomorphism between skew braces $(B, \cdot, \circ)$, $(B', \cdot', \circ')$ is a map $f\colon B \longrightarrow B'$ such that:

- $f(a \cdot b) = f(a) \cdot' f(b)$ for all $a, b \in B$.
- $f(a \circ b) = f(a) \circ' f(b)$ for all $a, b \in B$.

Isomorphism: bijective homomorphism.

$(B, \cdot, \circ)$ and $(B', \cdot', \circ')$ are isomorphic if
$\exists f\colon (B, \cdot, \circ) \longrightarrow (B', \cdot', \circ')$ isomorphism of skew braces.

2.

COUNTING ISOMORPHISM CLASSES OF SKEW BRACES

Since isomorphic skew braces provide similar information, we are interested in isomorphism classes of skew braces rather than skew braces themselves.

$b(m) \equiv$ number of isomorphism classes of braces with size m.

$s(m) \equiv$ number of isomorphism classes of skew braces with size m.

Problem

Given $m \in \mathbb{Z}$, determine $b(m)$ and $s(m)$.

REGULAR SUBGROUPS OF THE HOLOMORPH

Definition

The holomorph of a finite group N is

$$\mathrm{Hol}(N) = N \rtimes \mathrm{Aut(N)}, \quad (a,\eta)(b,\mu) = (a\eta(b), \eta\mu).$$

It can be seen as the normalizer of $\lambda(N)$ in $\mathrm{Perm}(N)$, where

$$\lambda\colon N \hookrightarrow \mathrm{Perm}(N), \quad \lambda(\eta)(\mu) = \eta\mu.$$

$$(\eta, f) \cdot \mu = \eta f(\mu), \quad (\eta, f) \in \mathrm{Hol}(N),\ \mu \in N.$$

$G \leq \mathrm{Hol}(N)$ is regular if it acts simply transitively on N.

Theorem (Guarnieri-Vendramin, 2017)

Let $N = (B, \cdot)$ be a finite group. There is a bijective correspondence between:

- The operations $\circ$ on B such that $(B, \cdot, \circ)$ is a skew brace.
- The regular subgroups of $\mathrm{Hol}(N)$.

Moreover, a regular subgroup corresponding to $\circ$ is isomorphic to $(B, \circ)$.

Skew braces with additive group N and multiplicative group G $\cong$ **Regular subgroups of Hol(N) isomorphic to G**

$$B_1 \cong B_2 \quad \longleftrightarrow \quad G_1 \sim G_2$$

$\sim$ means conjugation in $\mathrm{Hol}(N)$ by elements of $\mathrm{Aut}(N)$.

$$G_1 \sim G_2 \iff \exists \gamma \in \mathrm{Aut}(N) \text{ such that } G_2 = \gamma G_1 \gamma^{-1}$$

Isomorphism classes of skew braces with additive group N and multiplicative group G $\cong$ **Conjugacy classes by elements of Aut(N) of regular subgroups of Hol(N) isomorphic to G**

$$\sum_{[N]} \#\{\text{Regular subgroups of } \mathrm{Hol}(N) \text{ up to conjugation by } \mathrm{Aut}(N)\}$$

N running through:

- Representatives of abelian groups of order $m \rightsquigarrow b(m)$.
- Representatives of groups of order $m \rightsquigarrow s(m)$.

COMPUTING SKEW LEFT BRACES OF SMALL ORDERS

VALERIY G. BARDAKOV, MIKHAIL V. NESHCHADIM, AND MANOJ K. YADAV

ABSTRACT. We improve Algorithm 5.1 of [Math. Comp. **86** (2017), 2519-2534] for computing all non-isomorphic skew left braces, and enumerate left braces and skew left braces of orders up to 868 with some exceptions. Using the enumerated data, we state some conjectures for further research.

- Refinement of the previous method. ✓
- Determination of $b(m)$ and $s(m)$ for $m \leq 868$ with some gaps. ✓

$\rightsquigarrow$ Conjectures on the value of:

- $s(q^2p)$, p, q primes, $p > q + 1 \geq 3$. ✓
- $b(8p)$ and $s(8p)$, p prime, $p \geq 11$.
- $b(12p)$ and $s(12p)$, p prime, $p \geq 7$.

- E. Campedel, A. Caranti, I. Del Corso (2020)
- E. Acri, M. Bonatto (2022)

All these integers are of the form np, $n \in \mathbb{Z}$, p prime, $p \nmid n$.

3.

THE PRIME MULTIPLE CASE: PRODUCTS OF SKEW BRACES

THE SETTING

Let $n \in \mathbb{Z}$ and let p be an odd prime such that $p \nmid n$.

Assumption

Every group of order np has a normal subgroup of order p.

In particular, this is satisfied when:

- $n = 8$, $p \geq 11$.
- $n = 12$, $p \geq 7$.

THE RESULTS

- A description of the skew braces of size np.
- A framework to enumerate all such skew braces.
- The exact values of $b(8p)$, $b(12p)$ and $s(12p)$.

T. Crespo, D. Gil-Muñoz, A. Rio, M. Vela. **Left braces of size 8p**. J. Algebra 617 (2023), pages 317-339.

T. Crespo, D. Gil-Muñoz, A. Rio, M. Vela. **Inducing braces and Hopf Galois structures**. J. Pure Appl. Algebra 227 (2023), 107371.

→ T. Crespo, D. Gil-Muñoz, A. Rio, M. Vela. **Determining skew left braces of size np**. To appear in Communications in Algebra.

PRODUCTS OF SKEW BRACES

Every skew brace of size *np* can be described as a sort of product of a skew brace of size *n* and the trivial brace of size *p*.

Constructing products of skew braces

Let $(B_1, \cdot, \circ)$ and $(B_2, \cdot, \circ)$ be skew braces.
How can we define a skew brace structure on $B_1 \times B_2$?

- **Direct product**: Define $\cdot$ and $\circ$ on $B_1 \times B_2$ componentwise.
- **Semidirect product**: Define $\cdot$ componentwise and $\circ$ as a semidirect product by a morphism $\tau\colon (B_2, \circ) \longrightarrow \mathrm{Aut}(B_1, \circ)$.

Proposition

Let $\sigma\colon (B_2,\cdot) \longrightarrow \mathrm{Aut}(B_1,\cdot)$ be a group morphism. Suppose that for all $a, b \in B_2$, we have:

- $\sigma(a \circ b) = \sigma(b)^{\tau(a)} \cdot \sigma(a)$.
- $\sigma(b)^{\tau(a)}$ commutes with λ_c for all $c \in B_1$.

Then we can define $\cdot$ also as a semidirect product by σ to obtain a skew brace structure on $B_1 \times B_2$, called the **twofold semidirect product**.

If B_1 is the trivial brace of size p, this condition is just that

$$\sigma(a \circ b) = \sigma(a) \circ \sigma(b), \quad a, b \in B_1.$$

THE KEY IDEA

From a skew brace of size n and the trivial brace of size p, one can construct either one or two skew braces of size np.

Moreover, every skew brace of size np arise on this way.

- $(B_n, \cdot, \circ)$ skew brace of size n, $\mathbb{Z}_p$ trivial brace of size p.
- $\sigma\colon (B_n, \cdot, \circ) \longrightarrow \mathbb{Z}_p^\times$, $\tau\colon (B_n, \circ) \longrightarrow \mathbb{Z}_p^\times$.

$\rightsquigarrow$ $(\mathbb{Z}_p \times B_n, \cdot, \circ)$ and $(\mathbb{Z}_p \times B_n, \cdot, \circ')$ skew braces of size np, where:

$\rightsquigarrow (\mathbb{Z}_p \times B_n, \cdot, \circ)$ and $(\mathbb{Z}_p \times B_n, \cdot, \circ')$ skew braces of size np, where:

$$(m, a) \cdot (n, b) = (m + \sigma(a)n, a \cdot b),$$

$$(m, a) \circ (n, b) = (m + \tau(a)n, a \circ b),$$

$$(m, a) \circ' (n, b) = (\sigma(b)m + \tau(a)\sigma(a)n, a \circ b).$$

Remark

If $\sigma \equiv 1$, $\circ$ and $\circ'$ are the same, so we obtain a unique skew brace structure, which is the usual semidirect product.
If $E := (B_n, \cdot)$ is abelian, what we obtain is actually a brace.

Suppose that (σ, τ) and (σ', τ') provide $\mathbb{Z}_p \times B_n$ isomorphic skew brace structures.

- σ and σ' lie in the same orbit of

$$\begin{array}{ccc} \mathrm{Aut}(B_n) \times \mathrm{Hom}(B_n, \mathbb{Z}_p^*) & \longrightarrow & \mathrm{Hom}(B_n, \mathbb{Z}_p^*). \\ (g, \sigma) & \longrightarrow & \sigma g \end{array}$$

- τ and τ' lie in the same orbit of

$$\begin{array}{ccc} (\mathrm{Aut}(B_n) \cap \Sigma_\sigma) \times \mathrm{Hom}(F, \mathbb{Z}_p^*) & \longrightarrow & \mathrm{Hom}(F, \mathbb{Z}_p^*). \\ (g, \tau) & \longrightarrow & \tau \Phi_g \end{array}$$

Σ_σ: Stabilizer of σ. Φ_g: Conjugation by g.

THE ALGORITHM

- For each isomorphism class $[E]$ of groups of order n, determine the conjugacy classes of regular subgroups $F \leq \mathrm{Hol}(E)$.
- Determine $\mathrm{Hom}(B_n, \mathbb{Z}_p^\times) = \{\sigma \in \mathrm{Hom}(E, \mathbb{Z}_p^\times) \mid \pi_2(F) \subseteq \Sigma_\sigma\}$.
- Compute the orbits of the action $(g, \sigma) \mapsto \sigma g$, $g \in \mathrm{Aut}(B_n)$, $\sigma \in \mathrm{Hom}(B_n, \mathbb{Z}_p^\times)$.
- For each representative σ of an orbit, compute the orbits of the action $(g, \tau) \mapsto \tau\Phi_g$, $g \in \mathrm{Aut}(B_n) \cap \Sigma_\sigma$, $\tau \in \mathrm{Hom}(F, \mathbb{Z}_p^\times)$.

SKETCH OF PROOF

Let B_n be a skew brace of size n with additive group E and multiplicative group F.

For a pair (σ, τ), we find the conjugacy classes of regular subgroups of $\mathrm{Hol}(\mathbb{Z}_p \rtimes_\sigma E)$ isomorphic to $\mathbb{Z}_p \rtimes_\tau F$.

By Curran,

$$\mathrm{Aut}(\mathbb{Z}_p \rtimes_\sigma E) = \left\{ \begin{pmatrix} \alpha & \gamma_i \\ 0 & \lambda \end{pmatrix} : \alpha \in \mathbb{Z}_p^\times, i \in \mathbb{Z}_p, \lambda \in \Sigma_\sigma \right\}.$$

$\gamma_i : E \longrightarrow \mathbb{Z}_p$, $\gamma_i(a) = i - \sigma(a)i$ 1-coboundary.

FORMULA FOR THE NUMBER OF SKEW LEFT BRACES OF SIZE NP

$$s(np) = \sum_{B_n} \left(\frac{1}{|A_{B_n,1}|} \sum_{\tau \in \mathrm{Hom}((B_n,\circ),\mathbb{Z}_p^*)} |\mathrm{Stab}_{A_{B_n,1}}(\tau)| + 2 \sum_{\sigma \neq 1} \frac{1}{|A_{B_n,\sigma}|} \sum_{\tau \in \mathrm{Hom}((B_n,\circ),\mathbb{Z}_p^*)} |\mathrm{Stab}_{A_{B_n,\sigma}}(\tau)| \right)$$

There does not seem to be a general pattern for the numbers and sizes of orbits for σ and τ in terms of n and p.

4.

THE NUMBER OF SKEW BRACES OF SIZE 12P

Problem

Given a prime number p, find $b(12p)$ and $s(12p)$.

By computations, one shows $b(24) = 96$, $b(36) = 46$, $b(60) = 28$, $s(24) = 855$, $s(36) = 400$ and $s(60) = 418$.

If $p \geq 7$, then any group of order $12p$ has a unique normal subgroup of order p.

The isomorphism classes of groups of order 12 are

$$C_{12}, \quad C_6 \times C_2, \quad A_4, \quad D_6, \quad \mathrm{Dic}_{12}.$$

NUMBER OF SKEW LEFT BRACES WITH SIZE 12

E/F	C_{12}	$C_6 \times C_2$	A_4	D_6	Dic_{12}
C_{12}	1	1	0	2	1
$C_6 \times C_2$	1	1	1	1	1
A_4	0	2	4	0	2
D_6	2	2	0	4	2
Dic_{12}	2	2	0	4	2

SOLUTION FOR THE CASE E=C12, F=D6

- There are two conjugacy classes F_1, F_2 of regular subgroups of $\mathrm{Hol}(E)$.

One orbit for each

- $\sigma \in \mathrm{Hom}(B_{12}, \mathbb{Z}_p^*) \Longrightarrow \mathrm{Ker}(\sigma) = E$ or C_6.

$$\rightsquigarrow N \cong \mathbb{Z}_p \times C_{12} \text{ or } \mathbb{Z}_p \rtimes_6 C_{12}$$

- $\tau \in \mathrm{Hom}(F_i, \mathbb{Z}_p^*) \Longrightarrow \mathrm{Ker}(\tau) = F_i$, C_6 or D_3.

$$\rightsquigarrow G \cong \mathbb{Z}_p \times D_6 \text{ or } \mathbb{Z}_p \rtimes_c D_6 \text{ or } \mathbb{Z}_p \rtimes_d D_6$$

- Orbits of $\mathrm{Hom}(F_i, \mathbb{Z}_p^\times)$ under $\mathrm{Aut}(B_n) \cap \Sigma_\sigma$:

	$\mathrm{Ker}(\tau) = F_i$	$\mathrm{Ker}(\tau) = C_6$	$\mathrm{Ker}(\tau) = D_3$
F_1	1	1	1
F_2	1	1	2

Number of skew braces with $E = C_{12}$ and $F = D_6$:

N/G	$\mathbb{Z}_p \times D_6$	$\mathbb{Z}_p \rtimes_c D_6$	$\mathbb{Z}_p \rtimes_d D_6$
$\mathbb{Z}_p \times C_{12}$	2	2	3
$\mathbb{Z}_p \rtimes_6 C_{12}$	4	4	6

Doing this for all combinations of E's and F's we find:

Theorem (Crespo, G., Rio and Vela)

Let $p \geq 5$ be a prime number. Then

$$b(12p) = \begin{cases} 24 & \text{if } p \equiv 11 \pmod{12}, \\ 28 & \text{if } p \equiv 5 \pmod{12}, \\ 34 & \text{if } p \equiv 7 \pmod{12}, \\ 40 & \text{if } p \equiv 1 \pmod{12}. \end{cases}$$

$$s(12p) = \begin{cases} 324 & \text{if } p \equiv 11 \pmod{12}, \\ 410 & \text{if } p \equiv 5 \pmod{12}, \\ 606 & \text{if } p \equiv 7 \pmod{12}, \\ 782 & \text{if } p \equiv 1 \pmod{12}. \end{cases}$$

BIBLIOGRAPHY

E. Acri, M. Bonatto. **Skew Braces of Size p2q I: Abelian Type**. Alg. Colloquium 29 (2) (2022), pages 297-320.

E. Acri, M. Bonatto. **Skew Braces of Size p2q II: Non-abelian Type**. Journal of Algebra and its Applications 29 (3) (2022), pages 2250062.

V. G. Bardakov, M. V. Neshchadim, M. K. Yadav. **Computing skew left braces of small orders**. International Journal of Algebra and Computation 30.4 (2020), 839-851.

E. Campedel, A. Caranti, I. Del Corso. **Hopf-Galois extensions of degree p2q and skew braces of order p2q: the cyclic Sylow p-subgroup case**. J. Algebra 556 (2020), 1165-1210.

E. Campedel, A. Caranti, I. Del Corso. **Hopf-Galois extensions of degree p2q and skew braces of order p2q: the elementary abelian Sylow p-subgroup case**. New York J. Math. 30 (2024), 93-186.

F. Cedó. **Left Braces: Solutions of the Yang-Baxter Equation**. Advances in Group Theory and Applications 5 (2018), pages 33-90.

T. Crespo, D. Gil-Muñoz, A. Rio, M. Vela. **Inducing braces and Hopf Galois structures**. J. Pure Appl. Algebra 227 (2023), 107371.

T. Crespo, D. Gil-Muñoz, A. Rio, M. Vela. **Left braces of size 8p**. J. Algebra 617 (2023), pages 317-339.

T. Crespo, D. Gil-Muñoz, A. Rio, M. Vela. **Determining skew left braces of size np**. To appear in Communications in Algebra.

L. Guarnieri, L. Vendramin. **Skew braces and the Yang-Baxter equation**. Mathematics of Computation 86 (307) (2017), pages 2519-2534.

THANK YOU VERY MUCH!

This work was supported by:

GAČR

CZECH SCIENCE FOUNDATION