Indecomposable solutions with permutation brace of size p^3

Joint work with Magdalena Wiertel

Braiding New Ground, Maynooth University

Andrew Darlington

Friday 18th September 2026

VRIJE UNIVERSITEIT BRUSSEL

Ingredients

- (finite, non-degenerate involutive set-theoretic) **solution**, (X, r), to the Yang–Baxter Equation (YBE)

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

- Brace $(B, +, \cdot)$: $(B, +)$, $(B, \cdot)$ groups with

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

  for all $a, b, c \in B$.

- Braces $\leftrightsquigarrow$ solutions to the YBE

Permutation groups

To every solution, (X, r), we can associate a group

$$\mathcal{G}(X, r) = \langle \sigma_x \mid x \in X \rangle$$

where $r(x, y) = (\sigma_x(y), \cdots)$ and the operation, $\circ$ is composition. This is called the *permutation group* of the solution (finite quotient of $G(X, r)$).

Fact
We can define an operation + on $\mathcal{G}(X, r)$ such that $(\mathcal{G}(X, r), +, \circ)$ is a brace.

Indecomposable solutions

It is often helpful to look for ‘building blocks’ of solutions. A solution (X, r) is called *indecomposable* if whenever $X = Y \cup Z$, if $(Y, r|_{Y\times Y})$ and $(Z, r|_{Z\times Z})$ are both solutions, then $Y, Z \in \{\varnothing, X\}$.

$\lvert X\rvert$	2	3	4	5	6	7	8	9	10
# sols	2	5	23	88	595	3456	34530	321931	4895272
# ind. sols	1	1	5	1	10	1	100	16	36

Fact

(X, r) is indecomposable $\iff \mathcal{G}(X, r)$ acts transitively on X.

The problem

Can we construct indecomposable solutions in a systematic way?

The BCJ construction

Let $(B, +, \cdot)$ be a brace and for all $a \in B$, let $\lambda_a \in \mathrm{Aut}(B, +)$ be given by

$$\lambda_a(b) = -a + a \cdot b \quad \forall b \in B.$$

This gives an action of $(B, \cdot)$ on $(B, +)$.

Theorem (Bachiller – Cedó – Jespers)
Suppose $\exists x \in B$ *where* $B = \langle \mathrm{Orb}(x) \rangle_+$. *Take* $K \leq \mathrm{Stab}(x)$ *corefree in* $(B, \cdot)$.

Then the map $r : (B/K) \times (B/K) \to (B/K) \times (B/K)$:

$$r(b \cdot K, c \cdot K) = \left(\lambda_b(x) \cdot c \cdot K, \lambda_{\lambda_b(x) \cdot c}(x)^{-1} \cdot b \cdot K\right)$$

gives an indecomposable solution on B/K *such that* $\mathcal{G}(X, r) \cong B$ *as braces.*

Moreover every indecomposable solution (Y, r) *with* $\mathcal{G}(Y, r) \cong B$ *arises in this way.*

Braces of order p^3

For p an odd prime, there are 3 groups of order p^3, but $6p + 19$ braces of order p^3:

- 3 with $(B, +) \cong \mathbb{Z}/p^3$
- $4p + 10$ with $(B, +) \cong \mathbb{Z}/p \times \mathbb{Z}/p^2$
- $2p + 6$ with $(B, +) \cong (\mathbb{Z}/p)^3$

These were classified by Bachiller, and he gives us the explicit λ-map for each one.

Example

The majority of braces don't satisfy the conditions of BCJ (they are not one-generator braces). But let's fix an $\varepsilon \in \{1\} \cup \mathbb{F}_p \setminus \mathbb{F}_p^2$, and consider the λ map on $(B, +) \cong \mathbb{Z}/p \times \mathbb{Z}/p^2$ given by

$$\lambda_{(b_1,b_2)}((x_1, x_2)) = \left(x_1 + x_2 b_2, x_2 + p\varepsilon\left(x_1 b_2 + \binom{b_2}{2} x_2\right)\right).$$

We can show that $(x_1, x_2) \in B$ 'one generates' B iff $\mathrm{Ord}_+(x_2) = p^2$.

The core-free subgroups of $\mathrm{Stab}((x_1, x_2))$ are

$$\{1\} \cup \langle (1, 0) \rangle \cup \{\langle (i, p) \rangle \mid 1 \leq i \leq p - 1\}.$$

Example

Let $1 \leqslant x \leqslant (p-1)/2$, and λ (determining a brace B) and K a core-free subgroup as before.

Then, up to isomorphism, there are $(p^2-1)/2$ indecomposable solutions associated B, which are given by $(B/K, r)$, where

$$r(b \cdot K, c \cdot K) =$$

$$\left(\begin{pmatrix} c_1 + x(b_2 + c_2) \\ c_2 + x + p\varepsilon\left(\binom{x}{2}c_2 + x\binom{b_2}{2} + xc_1\right) \end{pmatrix} \cdot K, \right.$$

$$\left. \begin{pmatrix} b_1 - x(b_2 + c_2) \\ b_2 - x + p\varepsilon\left(x^2 c_2 + x^3 - \binom{c_2+x}{2}x + \binom{x+1}{2}(b_2 - x) - b_1 x\right) \end{pmatrix} \cdot K \right)$$

Some results

Theorem (AD, M. Wiertel)
Let p be an odd prime. Up to isomorphism, there are $(p^3+3p)/4$ and $(p^3+p^2+11p+3)/4$ solutions of size p^2 and p^3, respectively, with permutation brace of size p^3.

Some results

Theorem (AD, M. Wiertel)
Moreover, denote by $n_2(p,B)$ and $n_3(p,B)$ the number of indecomposable solutions of size p^2 and p^3, respectively, with the permutation brace $(B,+,\cdot)$. Then

$$n_2(p,B) = \begin{cases} p & \text{if } (B,+) \cong \mathbb{Z}_p^3, \\ p(p^2-1)/4 & \text{if } (B,+) \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_p \end{cases}$$

and

$$n_3(p,B) = \begin{cases} p+1 & \text{if } (B,+) \cong \mathbb{Z}_p^3, \\ 1+(p+1)(p^2-1)/4 & \text{if } (B,+) \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_p, \\ 2p-1 & \text{if } (B,+) \cong \mathbb{Z}_{p^3}. \end{cases}$$

Computational results

$\lvert\mathcal{G}\rvert$	#IndSols	$\lvert\mathcal{G}\rvert$	#IndSols	$\lvert\mathcal{G}\rvert$	#IndSols
2	1	16	86	30	4
3	1	17	1	31	1
4	3	18	9	32	?
5	1	19	1	33	1
6	2	20	10	34	2
7	1	21	3	35	1
8	13	22	2	36	67
9	4	23	1	37	1
10	2	24	62	38	2
11	1	25	6	39	3
12	11	26	2	40	52
13	1	27	27	41	1
14	2	28	7	42	8
15	1	29	1	43	1

Computational results

$\lvert\mathcal{G}\rvert$	#IndSols	$\lvert\mathcal{G}\rvert$	#IndSols	$\lvert\mathcal{G}\rvert$	#IndSols
44	7	58	2	72	488
45	4	59	1	73	1
46	2	60	28	74	2
47	1	61	1	75	13
48	434	62	2	76	7
49	8	63	14	77	1
50	13	64	?	78	8
51	1	65	1	79	1
52	10	66	4	80	?
53	1	67	1	81	?
54	98	68	10	82	2
55	5	69	1	83	1
56	69	70	4	84	44
57	3	71	1	85	1

Computational results

$\|\mathcal{G}\|$	#IndSols
86	2
87	1
88	39
89	1
90	18
91	1
92	7
93	3

$\|\mathcal{G}\|$	#IndSols
94	2
95	1
96	?
97	1
98	17
99	4
100	100
101	1

$\|\mathcal{G}\|$	#IndSols
102	4
103	1
104	52
105	3
106	2
107	1

Future plans

- Other classes of braces
- Skew braces?
- Bypass braces?

Thank You!

Questions?