Publ. Mat. **70** (2026), 303–313
DOI: 10.5565/PUBLMAT7022601

SIMPLE SOLUTIONS OF THE YANG–BAXTER EQUATION OF CARDINALITY p^n

F. Cedó and J. Okniński

Abstract: For every prime number p and integer $n > 1$, a simple, involutive, non-degenerate, set-theoretic solution (X, r) of the Yang–Baxter equation of cardinality $|X| = p^n$ is constructed. Furthermore, for every positive integer m which is not square-free and is not a square of a prime number, a non-simple, indecomposable, irretractable, involutive, non-degenerate, set-theoretic solution (X, r) of the Yang–Baxter equation of cardinality $|X| = m$ is constructed. A recent question of Castelli on the existence of singular solutions of certain type is also answered affirmatively.

2020 Mathematics Subject Classification: Primary: 16T25, 20B15, 20F16.

Key words: Yang–Baxter equation, set-theoretic solution, indecomposable solution, simple solution, brace.

1. Introduction and preliminaries

An important open problem is to find all the solutions of the Yang–Baxter equation. Drinfeld in [**16**] suggested studying the set-theoretic solutions of the Yang–Baxter equation. Gateva-Ivanova and Van den Bergh ([**19**]) and Etingof, Schedler, and Soloviev ([**17**]) introduced the class of so-called involutive non-degenerate set-theoretic solutions of the Yang–Baxter equation. The study of this important class of solutions has attracted a lot of attention during the last twenty years; see for example [**8**] and the references therein.

Let X be a non-empty set and let $r\colon X \times X \longrightarrow X \times X$ be a map. For $x, y \in X$ we put $r(x, y) = (\sigma_x(y), \gamma_y(x))$. Recall that (X, r) is an involutive, non-degenerate set-theoretic solution of the Yang–Baxter equation if $r^2 = \mathrm{id}$, all the maps σ_x and γ_y are bijective maps from X to itself, and

$$r_{12}r_{23}r_{12} = r_{23}r_{12}r_{23},$$

where $r_{12} = r \times \mathrm{id}_X$ and $r_{23} = \mathrm{id}_X \times r$ are maps from X^3 to itself. Because $r^2 = \mathrm{id}$, one easily verifies that $\gamma_y(x) = \sigma^{-1}_{\sigma_x(y)}(x)$, for all $x, y \in X$ (see for example [**17**, Proposition 1.6]).

Convention. Throughout the paper a solution of the YBE will mean an involutive, non-degenerate, set-theoretic solution of the Yang–Baxter equation.

It is well known, see for example [**8**, Proposition 8.2], that a map $r(x, y) = (\sigma_x(y), \sigma^{-1}_{\sigma_x(y)}(x))$, defined for a collection of bijections $\sigma_x\colon X \longrightarrow X$, $x \in X$, is a solution of the YBE if and only if $\sigma_x\sigma_{\sigma_x^{-1}(y)} = \sigma_y\sigma_{\sigma_y^{-1}(x)}$ for all $x, y \in X$ and the maps $\gamma_y\colon X \longrightarrow X$ defined by $\gamma_y(x) = \sigma^{-1}_{\sigma_x(y)}(x)$, for all $x, y \in X$, are bijective. Furthermore, if X is finite, then (X, r) is a solution of the YBE if and only if $\sigma_x\sigma_{\sigma_x^{-1}(y)} = \sigma_y\sigma_{\sigma_y^{-1}(x)}$ for all $x, y \in X$.

To study solutions of the YBE, Rump introduced a new algebraic structure called left brace [**20**]. This made it possible to construct many new families of solutions of the YBE [**1, 2, 3, 9, 18, 22**].

A left brace is a set B with two binary operations, $+$ and $\circ$, such that $(B,+)$ is an abelian group (the additive group of B), $(B,\circ)$ is a group (the multiplicative group of B), and for every $a,b,c\in B$,

$$a\circ(b+c)+a=a\circ b+a\circ c.$$

In any left brace B the neutral elements 0, 1 for the operations $+$ and $\circ$ coincide. Moreover, there is an action $\lambda\colon (B,\circ)\longrightarrow \mathrm{Aut}(B,+)$, called the lambda map of B, defined by $\lambda(a)=\lambda_a$ and $\lambda_a(b)=-a+a\circ b$, for $a,b\in B$. We shall write $a\circ b=ab$ and a^{-1} will denote the inverse of a for the operation $\circ$, for all $a,b\in B$. A trivial brace is a left brace B such that $ab=a+b$, for all $a,b\in B$, i.e. all $\lambda_a=\mathrm{id}$. The socle of a left brace B is

$$\mathrm{Soc}(B)=\{a\in B\mid ab=a+b,\ \text{for all } b\in B\}.$$

Note that $\mathrm{Soc}(B)=\mathrm{Ker}(\lambda)$, and thus it is a normal subgroup of the multiplicative group of B. The solution of the YBE associated to a left brace B is (B,r_B), where $r_B(a,b)=(\lambda_a(b),\lambda^{-1}_{\lambda_a(b)}(a))$, for all $a,b\in B$ (see [**9**, Lemma 2]).

An ideal of a left brace B is a normal subgroup I of the multiplicative group of B such that $\lambda_a(b)\in I$, for all $b\in I$ and all $a\in B$. Note that

$$ab^{-1}=a-\lambda_{ab^{-1}}(b),$$

for all $a,b\in B$, and

$$a-b=a+\lambda_b(b^{-1})=a\lambda_{a^{-1}}(\lambda_b(b^{-1}))=a\lambda_{a^{-1}b}(b^{-1}),$$

for all $a,b\in B$. Hence, every ideal I of a left brace B is also a subgroup of the additive group of B. It is known that $\mathrm{Soc}(B)$ is an ideal of the left brace B (see [**20**, Proposition 7]). Note that, for every ideal I of B, B/I inherits a natural left brace structure.

A homomorphism of left braces is a map $f\colon B_1\longrightarrow B_2$, where B_1, B_2 are left braces, such that $f(ab)=f(a)f(b)$ and $f(a+b)=f(a)+f(b)$, for all $a,b\in B_1$. Note that the kernel $\mathrm{Ker}(f)$ of a homomorphism of left braces $f\colon B_1\longrightarrow B_2$ is an ideal of B_1.

Recall that if (X,r) is a solution of the YBE, with $r(x,y)=(\sigma_x(y),\gamma_y(x))$, then its structure group

$$G(X,r)=\mathrm{gr}(x\in X\mid xy=\sigma_x(y)\gamma_y(x)\ \text{for all } x,y\in X)$$

has a natural structure of a left brace such that $\lambda_x(y)=\sigma_x(y)$, for all $x,y\in X$. The additive group of $G(X,r)$ is the free abelian group with basis X. The permutation group $\mathcal{G}(X,r)=\mathrm{gr}(\sigma_x\mid x\in X)$ of (X,r) is a subgroup of the symmetric group Sym_X on X. The map $x\longmapsto\sigma_x$ from X to $\mathcal{G}(X,r)$ extends to a group homomorphism $\phi\colon G(X,r)\longrightarrow\mathcal{G}(X,r)$ and $\mathrm{Ker}(\phi)=\mathrm{Soc}(G(X,r))$. Hence there is a unique structure of a left brace on $\mathcal{G}(X,r)$ such that ϕ is a homomorphism of left braces; this is the natural structure of a left brace on $\mathcal{G}(X,r)$.

Let (X,r) and (Y,s) be solutions of the YBE. We write $r(x,y)=(\sigma_x(y),\gamma_y(x))$ and $s(t,z)=(\sigma'_t(z),\gamma'_z(t))$, for all $x,y\in X$ and $t,z\in Y$. A homomorphism of solutions $f\colon (X,r)\longrightarrow(Y,s)$ is a map $f\colon X\longrightarrow Y$ such that $f(\sigma_x(y))=\sigma'_{f(x)}(f(y))$ and $f(\gamma_y(x))=\gamma'_{f(y)}(f(x))$, for all $x,y\in X$. Since $\gamma_y(x)=\sigma^{-1}_{\sigma_x(y)}(x)$ and $\gamma'_z(t)=(\sigma')^{-1}_{\sigma'_t(z)}(t)$, it is clear that f is a homomorphism of solutions if and only if $f(\sigma_x(y))=\sigma'_{f(x)}(f(y))$, for all $x,y\in X$.

In [**17**], Etingof, Schedler, and Soloviev introduced the retract relation on solutions (X,r) of the YBE. This is the binary relation $\sim$ on X defined by $x \sim y$ if and only if $\sigma_x = \sigma_y$. Then, $\sim$ is an equivalence relation and r induces a solution $\overline{r}$ on the set $\overline{X} = X/{\sim}$. The retract of the solution (X,r) is $\mathrm{Ret}(X,r) = (\overline{X},\overline{r})$. Note that the natural map $f\colon X \longrightarrow \overline{X}\colon x \longmapsto \overline{x}$ is an epimorphism of solutions from (X,r) onto $\mathrm{Ret}(X,r)$.

Recall that a solution (X,r) is said to be irretractable if $\sigma_x \neq \sigma_y$ for all distinct elements $x,y \in X$, that is, $(X,r) = \mathrm{Ret}(X,r)$; otherwise the solution (X,r) is retractable.

Let (X,r) be a solution of the YBE. We say that (X,r) is indecomposable if $\mathcal{G}(X,r)$ acts transitively on X.

Definition 1.1. A solution (X,r) of the YBE is simple if $|X| > 1$ and for every epimorphism $f\colon (X,r) \longrightarrow (Y,s)$ of solutions either f is an isomorphism or $|Y| = 1$.

In this context, the following result (Proposition 4.1 in [**10**] and Lemma 3.4 in [**11**]) is crucial.

Lemma 1.2. *Assume that (X,r) is a simple solution of the YBE. Then it is indecomposable if $|X| > 2$ and it is irretractable if $|X|$ is not a prime number.*

Finite simple solutions of the YBE were introduced by Vendramin in [**23**]. His definition does not coincide with the above definition of simplicity, but for finite indecomposable solutions both definitions coincide by [**6**, Proposition 2]. It is not known whether there exists a simple solution of the YBE of cardinality m^2n for any integers $m,n > 1$. This was claimed in [**10**, Theorem 4.12], but the proof was incorrect, though an example of a simple solution of non-square cardinality was given; see [**13**]. On the other hand, all the simple solutions of the YBE of non-prime cardinality constructed in [**10, 11**] have square cardinality. In [**4**] Castelli gives an example of a simple solution of the YBE of cardinality 27, and two concrete simple solutions of the YBE of cardinality 12. In [**14**, Theorem 5.3] it is proved that if $n > 1$ is an integer and p is a prime divisor of $q-1$ for every prime divisor q of n, then there exists a simple solution of the YBE of cardinality p^2n. In this paper we construct, for every prime number p and every positive integer n, a simple solution of the YBE of cardinality p^n; see Theorem 3.2. Moreover, for every positive integer m which is not square-free and is not a square of a prime number, a non-simple, indecomposable, and irretractable solution (X,r) of the YBE of cardinality $|X| = m$ is constructed in Section 2. Finally, simple singular solutions (introduced by Rump in [**21**]) are constructed in Section 4. This answers a recent question of Castelli affirmatively [**5**].

2. Solutions of cardinality m^2n

By [**12**, Theorem 4.5] we know that if (X,r) is a finite indecomposable and irretractable solution, then $|X|$ is not square-free. On the other hand Dietzel, Properzi, and Trappeniers have proved in [**15**, p. 17] that if $|X| = p^2$ for a prime p, then (X,r) is indecomposable and irretractable if and only if (X,r) is simple. In this section we will show that if $|X|$ is not square-free and is not the square of a prime, then there exists an indecomposable and irretractable solution (X,r) of the YBE which is not simple.

Example 2.1. Let $m > 1$ be an integer which is not a prime number. Using the results of [**10**], we shall construct an indecomposable and irretractable solution of the YBE of cardinality m^2 which is not simple. This is in contrast to the case of solutions of cardinality p^2, for a prime p, as we mentioned above. Since m is not prime, there exist integers $m_1, m_2 > 1$ such that $m = m_1 m_2$. Let $X = (\mathbb{Z}/(m))^2$. Consider the family $(j_a)_{a\in\mathbb{Z}/(m)}$ of elements of $\mathbb{Z}/(m)$ such that $j_0 = 1$ and $j_a = m_1 + 1$, for all $a \in \mathbb{Z}/(m) \setminus \{0\}$. For every $(a_1, a_2) \in X$, let $\sigma_{(a_1,a_2)} \colon X \longrightarrow X$ be the map defined by

$$\sigma_{(a_1,a_2)}(x, y) = (x + a_2, y - j_{x+a_2-a_1}),$$

for all $(x, y) \in X$. Let $r \colon X \times X \longrightarrow X \times X$ be the map defined by

$$r((a_1, a_2), (c_1, c_2)) = (\sigma_{(a_1,a_2)}(c_1, c_2), \sigma^{-1}_{\sigma_{(a_1,a_2)}(c_1,c_2)}(a_1, a_2)),$$

for all $(a_1, a_2)(c_1, c_2) \in X$. By [**10**, Theorem 4.9], (X, r) is an indecomposable and irretractable solution of the YBE. Let $\pi \colon \mathbb{Z}/(m) \longrightarrow \mathbb{Z}/(m_1)$ be the natural homomorphism. Consider the solution $(\mathbb{Z}/(m_1), s)$ of the YBE, where

$$s(x, y) = (y - 1, x + 1),$$

for all $x, y \in \mathbb{Z}/(m_1)$. Let $f \colon X \longrightarrow \mathbb{Z}/(m_1)$ be the map defined by $f(a_1, a_2) = \pi(a_2)$. Note that

$$f(\sigma_{(a_1,a_2)}(c_1, c_2)) = f(c_1 + a_2, c_2 - j_{c_1+a_2-a_1}) = \pi(c_2 - j_{c_1+a_2-a_1}) = \pi(c_2) - 1$$

and $s(f(a_1, a_2), f(c_1, c_2)) = s(\pi(a_2), \pi(c_2)) = (\pi(c_2) - 1, \pi(a_2) + 1)$. Hence f is a homomorphism of solutions from (X, r) to $(\mathbb{Z}/(m_1), s)$. Clearly f is surjective. Hence the solution (X, r) is not simple. In the proof of [**10**, Proposition 6.2], one can see that $\mathcal{G}(X, r)$ is isomorphic to $B/\operatorname{Soc}(B)$, where B is some asymmetric product ([**7**]) of the trivial braces $(\mathbb{Z}/(m))^m$ and $\mathbb{Z}/(m)$.

Lemma 2.2. *Let $m, n > 1$ be integers. Let $\pi \colon \mathbb{Z}/(m) \longrightarrow \mathbb{Z}/(n)$ be a homomorphism and let $k \in \mathbb{Z}/(n)$. Let $X = \mathbb{Z}/(m)\times\mathbb{Z}/(n)\times\mathbb{Z}/(m)$. Consider $\sigma_{(a,b,c)} \in \operatorname{Sym}_X$ defined by*

$$\sigma_{(a,b,c)}(x, y, z) = (x - c, y - \pi(x - a) - k, z - \delta_{a,x-c}\delta_{b,y-\pi(x-a)-k}),$$

for all $a, c, x, z \in \mathbb{Z}/(m)$ and $b, y \in \mathbb{Z}/(n)$, where $\delta_{i,j}$ denotes the Kronecker delta.

Let $r \colon X \times X \longrightarrow X \times X$ be the map defined by

$$r((a, b, c), (x, y, z)) = (\sigma_{(a,b,c)}(x, y, z), \sigma^{-1}_{\sigma_{(a,b,c)}(x,y,z)}(a, b, c)),$$

for all $(a, b, c), (x, y, z) \in X$. Then (X, r) is a solution of the YBE.

Proof: Let $(a, b, c), (x, y, z) \in X$. Note that

$$\sigma^{-1}_{(a,b,c)}(x, y, z) = (x + c, y + \pi(x + c - a) + k, z + \delta_{a,x}\delta_{b,y}).$$

To prove that (X, r) is a solution of the YBE, since X is finite, it is enough to check that

$$\sigma^{-1}_{\sigma^{-1}_{(a,b,c)}(x,y,z)}\sigma^{-1}_{(a,b,c)} = \sigma^{-1}_{\sigma^{-1}_{(x,y,z)}(a,b,c)}\sigma^{-1}_{(x,y,z)}. \tag{1}$$

For all $u, w \in \mathbb{Z}/(m)$ and $v \in \mathbb{Z}/(n)$ we have that

$$\begin{aligned}
&\sigma^{-1}_{\sigma^{-1}_{(a,b,c)}(x,y,z)}\sigma^{-1}_{(a,b,c)}(u, v, w)\\
&\quad= \sigma^{-1}_{(x+c,y+\pi(x+c-a)+k,z+\delta_{a,x}\delta_{b,y})}(u + c, v + \pi(u + c - a) + k, w + \delta_{a,u}\delta_{b,v})\\
&\quad= (u + c + z + \delta_{a,x}\delta_{b,y}, v + \pi(u + c - a) + k + \pi(u + c + z + \delta_{a,x}\delta_{b,y} - x - c) + k,\\
&\qquad\qquad w + \delta_{a,u}\delta_{b,v} + \delta_{x+c,u+c}\delta_{y+\pi(x+c-a)+k,v+\pi(u+c-a)+k})\\
&\quad= (u + c + z + \delta_{a,x}\delta_{b,y}, v + \pi(2u + c + z - a - x + \delta_{a,x}\delta_{b,y}) + 2k,\\
&\qquad\qquad w + \delta_{a,u}\delta_{b,v} + \delta_{x,u}\delta_{y,v}),
\end{aligned}$$

which is symmetric in (a, b, c) and (x, y, z). Hence (1) follows and therefore (X, r) is a solution of the YBE. □

Theorem 2.3. *Let $m, n > 1$ be integers. Let $X = \mathbb{Z}/(m) \times \mathbb{Z}/(n) \times \mathbb{Z}/(m)$. Consider $\sigma_{(a,b,c)} \in \mathrm{Sym}_X$ defined by*

$$\sigma_{(a,b,c)}(x, y, z) = (x - c, y - 1, z - \delta_{a,x-c}\delta_{b,y-1})),$$

for all $a, c, x, z \in \mathbb{Z}/(m)$ and $b, y \in \mathbb{Z}/(n)$. Let $r\colon X \times X \longrightarrow X \times X$ be the map defined by

$$r((a, b, c), (x, y, z)) = (\sigma_{(a,b,c)}(x, y, z), \sigma^{-1}_{\sigma_{(a,b,c)}(x,y,z)}(a, b, c)),$$

for all $(a, b, c), (x, y, z) \in X$. Then (X, r) is an indecomposable and irretractable solution of the YBE. Furthermore, the map $f\colon X \longrightarrow \mathbb{Z}/(n)$ defined by $f(a, b, c) = b$ for all $(a, b, c) \in X$ is an epimorphism of solutions from (X, r) to $(\mathbb{Z}/(n), s)$, where $s(i, j) = (j - 1, i + 1)$ for all $i, j \in \mathbb{Z}/(n)$.

Proof: By Lemma 2.2, (X, r) is a solution of the YBE. Note that, for every positive integer i,

$$\sigma^{-i}_{(1,0,0)}(0, 0, 0) = (0, i, 0).$$

Hence $(0, i, 0)$ is in the orbit of $(0, 0, 0)$ by the action of $\mathcal{G}(X, r)$, for all $i \in \mathbb{Z}/(n)$. Note that

$$\sigma^{-1}_{(1,i,1)}(0, i - 1, 0) = (1, i, 0)$$

for all $i \in \mathbb{Z}/(n)$. Hence $(1, i, 0)$ is in the orbit of $(0, 0, 0)$ by the action of $\mathcal{G}(X, r)$, for all $i \in \mathbb{Z}/(n)$. Since

$$\sigma^{-1}_{(j+1,i,1)}(j, i - 1, 0) = (j + 1, i, 0)$$

for all $j \in \mathbb{Z}/(m)$ and $i \in \mathbb{Z}/(n)$, we have that $(j, i, 0)$ is in the orbit of $(0, 0, 0)$ by the action of $\mathcal{G}(X, r)$, for all $j \in \mathbb{Z}/(m)$ and $i \in \mathbb{Z}/(n)$. We also have that

$$\sigma^{-1}_{(j,i,0)}(j, i, k) = (j, i + 1, k + 1)$$

for all $j, k \in \mathbb{Z}/(m)$ and $i \in \mathbb{Z}/(n)$. Hence $\mathcal{G}(X, r)$ acts transitively on X. Therefore (X, r) is indecomposable.

Let $(a, b, c), (a', b', c') \in X$ be elements such that $\sigma_{(a,b,c)} = \sigma_{(a',b',c')}$. Hence

$$(x+c, y+1, z+\delta_{a,x}\delta_{b,y}) = \sigma^{-1}_{(a,b,c)}(x, y, z) = \sigma^{-1}_{(a',b',c')}(x, y, z) = (x+c', y+1, z+\delta_{a',x}\delta_{b',y})$$

for all $(x, y, z) \in X$. Thus $c = c'$ and

$$1 = \delta_{a,a}\delta_{b,b} = \delta_{a',a}\delta_{b',b},$$

and therefore $(a, b, c) = (a', b', c')$. Hence (X, r) is irretractable.

Finally, it is easy to check that the map $f\colon X \longrightarrow \mathbb{Z}/(n)$, defined by $f(a, b, c) = b$, is an epimorphism of solutions from (X, r) to $(\mathbb{Z}/(n), s)$. Therefore the result follows. □

3. Simple solutions of cardinality p^{2n+1}

The example constructed in [**10**, Theorem 4.12] is not correct. Hence, all the simple solutions of the YBE of non-prime cardinality constructed in [**10, 11**] have square cardinality. In [**14**, Theorem 5.3] it is proved that if $n > 1$ is an integer and p is a prime divisor of $q-1$ for every prime divisor q of n, then there exists a simple solution of the YBE of cardinality p^2n. In this section, for every prime number p and every integer $m > 1$, we shall construct simple solutions of the YBE of cardinality p^m.

Example 3.1. Let $m>1$ be an integer. Using the results from [**10**], we shall construct a simple solution of the YBE of cardinality m^2. Let $X=(\mathbb{Z}/(m))^2$. Consider the family $(j_a)_{a\in\mathbb{Z}/(m)}$ of elements of $\mathbb{Z}/(m)$ such that $j_0=1$ and $j_a=0$, for all $a\in\mathbb{Z}/(m)\setminus\{0\}$. For every $(a_1,a_2)\in X$, let $\sigma_{(a_1,a_2)}\colon X\longrightarrow X$ be the map defined by

$$\sigma_{(a_1,a_2)}(x,y)=(x+a_2,y-j_{x+a_2-a_1}),$$

for all $(x,y)\in X$. Let $r\colon X\times X\longrightarrow X\times X$ be the map defined by

$$r((a_1,a_2),(c_1,c_2))=(\sigma_{(a_1,a_2)}(c_1,c_2),\sigma^{-1}_{\sigma_{(a_1,a_2)}(c_1,c_2)}(a_1,a_2)),$$

for all $(a_1,a_2)(c_1,c_2)\in X$. By [**10**, Theorem 4.9], (X,r) is a simple solution of the YBE. In particular, for every prime number p and positive integer n, there exists a simple solution of the YBE of cardinality p^{2n}. By [**10**, Proposition 6.2], $\mathcal{G}(X,r)$ is isomorphic to some asymmetric product ([**7**]) of the trivial braces $(\mathbb{Z}/(m))^m$ and $\mathbb{Z}/(m)$. In particular for a prime number p and $m=p^n$, the permutation group $\mathcal{G}(X,r)$ is a p-group.

Let p be a prime number. Constructing a simple solution of cardinality p^k for any odd integer k is more difficult. In order to accomplish this goal, let n be a positive integer. Let $X=\mathbb{Z}/(p^n)\times\mathbb{Z}/(p)\times\mathbb{Z}/(p^n)$. Let $\pi\colon\mathbb{Z}/(p^n)\longrightarrow\mathbb{Z}/(p)$ be the canonical homomorphism. For $(a,b,c)\in X$, consider the map $\sigma_{(a,b,c)}\colon X\longrightarrow X$ defined by

$$\sigma_{(a,b,c)}(x,y,z)=(x-c,y+\pi(a-x),z-\delta_{a,x-c}\delta_{b,y+\pi(a-x)}),$$

for all $(x,y,z)\in X$. Note that $\sigma_{(a,b,c)}$ is bijective and

$$\sigma^{-1}_{(a,b,c)}(x,y,z)=(x+c,y+\pi(x+c-a),z+\delta_{a,x}\delta_{b,y}),$$

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

Theorem 3.2. *With the above notation, let $r\colon X^2\longrightarrow X^2$ be the map defined by*

$$r((a,b,c),(x,y,z))=(\sigma_{(a,b,c)}(x,y,z),\sigma^{-1}_{\sigma_{(a,b,c)}(x,y,z)}(a,b,c)),$$

for all $(a,b,c),(x,y,z)\in X$. Then (X,r) is a simple solution of the YBE.

Proof: By Lemma 2.2, (X,r) is a solution of the YBE.

We shall prove that (X,r) is indecomposable. Note that

$$\sigma^{-1}_{(a,b,c)}(0,0,0)=(c,\pi(c-a),\delta_{a,0}\delta_{b,0}).$$

In particular, for $b=1$, we get that $(c,\pi(c-a),0)$ is in the orbit of $(0,0,0)$ with respect to the action of $\mathcal{G}(X,r)$ for all $a,c\in\mathbb{Z}/(p^n)$. Note that

$$\sigma^{-1}_{(c,\pi(c-a),0)}(c,\pi(c-a),i)=(c,\pi(c-a),i+1),$$

for all $a,c,i\in\mathbb{Z}/(p^n)$. Since $(c,\pi(c-a),0)$ is in the orbit of $(0,0,0)$, we get that the orbit of $(0,0,0)$ is X. Hence (X,r) is indecomposable.

Let $f\colon(X,r)\longrightarrow(Y,s)$ be an epimorphism of solutions of the YBE. Suppose that f is not an isomorphism. Since (X,r) is indecomposable, by [**12**, Lemma 3.3], (Y,s) is indecomposable and $|f^{-1}(y)|=|f^{-1}(y')|$ for all $y,y'\in Y$. Hence $|Y|=p^k$ for some $k\in\{0,1,\dots,2n\}$. First we shall prove that $k<2$.

Let $f(0,0,0)=y_0$ and

$$f^{-1}(y_0)=\{(a_i,b_i,c_i)\mid 1\le i\le p^{2n+1-k}\}.$$

Assume that $(a_1,b_1,c_1)=(0,0,0)$. Note that

$$\begin{aligned}\sigma_{(a_i,b_i,c_i)}\sigma^{-1}_{(0,0,0)}(a_j,b_j,c_j) &= \sigma_{(a_i,b_i,c_i)}(a_j,b_j+\pi(a_j),c_j+\delta_{0,a_j}\delta_{0,b_j})\\ &= (a_j-c_i,b_j+\pi(a_i),c_j+\delta_{0,a_j}\delta_{0,b_j}-\delta_{a_i,a_j-c_i}\delta_{b_i,b_j+\pi(a_i)}),\end{aligned}$$

for all $i,j\in\{1,\dots,p^{2n+1-k}\}$. Note that, for every $1\leq i\leq p^{2n+1-k}$,

$$|\{\sigma_{(a_i,b_i,c_i)}\sigma^{-1}_{(0,0,0)}(a_j,b_j,c_j)\mid 1\leq j\leq p^{2n+1-k}\}|=p^{2n+1-k}.$$

Hence, for every $1\leq i\leq p^{2n+1-k}$, since f is a homomorphism of solutions,

$$f^{-1}(y_0)=\{(a_j-c_i,b_j+\pi(a_i),c_j+\delta_{0,a_j}\delta_{0,b_j}-\delta_{a_i,a_j-c_i}\delta_{b_i,b_j+\pi(a_i)})\mid 1\leq j\leq p^{2n+1-k}\}. \tag{2}$$

We shall prove that there exists $i\in\{1,\dots,p^{2n+1-k}\}$ such that c_i is invertible in $\mathbb{Z}/(p^n)$. Suppose that $c_i\in p(\mathbb{Z}/(p^n))$ for all $1\leq i\leq p^{2n+1-k}$. By (2), for $j=1$ we get that $(-c_i,\pi(a_i),\delta_{0,0}\delta_{0,0}-\delta_{a_i,-c_i}\delta_{b_i,\pi(a_i)})\in f^{-1}(y_0)$. Thus there exists $1\leq l\leq p^{2n+1-k}$ such that

$$c_l=\delta_{0,0}\delta_{0,0}-\delta_{a_i,-c_i}\delta_{b_i,\pi(a_i)}=1-\delta_{a_i,-c_i}\delta_{b_i,\pi(a_i)}.$$

Since $c_l\in p(\mathbb{Z}/(p^n))$, we have that $\delta_{a_i,-c_i}\delta_{b_i,\pi(a_i)}=1$. Hence $a_i=-c_i$ and $b_i=\pi(a_i)$, for all $1\leq i\leq p^{2n+1-k}$ and thus

$$(a_i,b_i,c_i)=(-c_i,\pi(-c_i),c_i)=(-c_i,0,c_i).$$

Hence

$$f^{-1}(y_0)=\{(-c_i,0,c_i)\mid 1\leq i\leq p^{2n+1-k}\}.$$

In particular, $c_i=c_j$ if and only if $i=j$. Now we have

$$y_0=f(-c_2,0,c_2)=f(\sigma_{(0,0,0)}\sigma^{-1}_{(-c_2,0,c_2)}(-c_2,0,c_2))=f(\sigma_{(0,0,0)}(0,0,c_2+1))=f(0,0,c_2).$$

Hence $-c_2=0=c_1$, and thus $c_2=c_1$, a contradiction, because $1<2\leq p^{2n+1-k}$. Thus, indeed, there exists $i\in\{1,\dots,p^{2n+1-k}\}$ such that c_i is invertible in $\mathbb{Z}/(p^n)$.

Since c_i is invertible in $\mathbb{Z}/(p^n)$, its additive order is p^n, and by (2), it follows that

$$a_1-c_i,a_1-2c_i,\dots,a_1-p^nc_i\in\{a_j\mid 1\leq j\leq p^{2n+1-k}\}\subseteq\mathbb{Z}/(p^n)$$

are p^n distinct elements, and this implies that

$$\{a_1,a_2,\dots,a_{p^{2n+1-k}}\}=\mathbb{Z}/(p^n). \tag{3}$$

Suppose that $n=1$. In this case, $\pi=\mathrm{id}$ and $k\leq 2$. Suppose that $k=2$. Thus $|f^{-1}(y_0)|=p$. Hence, there are p different first components of elements in (2). Moreover, for every $1\leq j\leq p$,

$$f^{-1}(y_0)=\{(a_j-c_i,b_j+a_i,c_j+\delta_{0,a_j}\delta_{0,b_j}-\delta_{a_i,a_j-c_i}\delta_{b_i,b_j+a_i})\mid 1\leq i\leq p\} \tag{4}$$

(since there are p different second components of elements in (4)) and thus (by looking at the second components of elements in (2) and at the first components in (4)), we get

$$\{b_1,b_2,\dots,b_p\}=\mathbb{Z}/(p)=\{c_1,c_2,\dots,c_p\}.$$

In particular, for $j=1$, we have that

$$f^{-1}(y_0)=\{(-c_i,a_i,\delta_{0,0}\delta_{0,0}-\delta_{a_i,-c_i}\delta_{b_i,a_i})\mid 1\leq i\leq p\}.$$

Since $\delta_{0,0}\delta_{0,0}-\delta_{a_i,-c_i}\delta_{b_i,a_i}\in\{0,1\}$, it follows that $p=2$ and

$$f^{-1}(y_0)=\{(0,0,0),(1,1,1)\}.$$

But, for $i=j=2$ in (4), we have that $(1-1,1+1,1+\delta_{0,1}\delta_{0,1}-\delta_{1,0}\delta_{1,0})=(0,0,1)\in f^{-1}(y_0)$, a contradiction. Hence $k<2$, in this case.

Suppose that $n>1$. Let $a\in p(\mathbb{Z}/(p^n))$ be a non-zero element. By (3), there exists $j\in\{1,\dots,p^{2n+1-k}\}$ such that $a_j=a$. We have

$$f(a_j,b_j,c_j+1)=f(\sigma^{-1}_{(a_j,b_j,0)}(a_j,b_j,c_j))=f(\sigma^{-1}_{(a_j,b_j,0)}(0,0,0))=f(0,0,0)=y_0.$$

By induction on l, one can see that

$$f(a_j,b_j,c_j+l)=y_0,$$

for all $1\le l\le p^n$. Hence, for every non-zero element $a\in p(\mathbb{Z}/(p^n))$ there exists $j_a\in\{1,\dots,p^{2n+1-k}\}$ such that

$$(a,b_{j_a},c)\in f^{-1}(y_0),$$

for all $c\in\mathbb{Z}/(p^n)$. In particular, $f(a,b_{j_a},0)=y_0$ and

$$\sigma_{(0,0,0)}\sigma^{-1}_{(a,b_{j_a},0)}(0,0,0)=\sigma_{(0,0,0)}(0,0,0)=(0,0,-1)\in f^{-1}(y_0).$$

Note that $\sigma_{(0,0,0)}\sigma^{-1}_{(a,b_{j_a},0)}(0,0,-1)=\sigma_{(0,0,0)}(0,0,-1)=(0,0,-2)\in f^{-1}(y_0)$, and one can see that $(0,0,-l)\in f^{-1}(y_0)$ by induction on l. Hence,

$$(0,0,c)\in f^{-1}(y_0),$$

for all $c\in\mathbb{Z}/(p^n)$. Therefore,

$$\{(a,b_{j_a},c)\mid a\in p(\mathbb{Z}/(p^n))\setminus\{0\},\ c\in\mathbb{Z}/(p^n)\}\cup\{(0,0,c)\mid c\in\mathbb{Z}/(p^n)\}\subseteq f^{-1}(y_0).$$

Thus $|f^{-1}(y_0)|\ge p^{n-1}p^n=p^{2n-1}$. By (3), there exists $(a_i,b_i,c_i)\in f^{-1}(y_0)$ such that $a_i=1$. Thus

$$|f^{-1}(y_0)|>p^{2n-1}.$$

Hence, for $n>1$, we also have that $k<2$.

Therefore, either $|Y|=p$ or $|Y|=1$.

Suppose that $|Y|=p$. Since (Y,s) is indecomposable, by [**17**, Theorem 2.13] (Y,s) is isomorphic to $(\mathbb{Z}/(p),s')$, where $s'(x,y)=(y-1,x+1)$ for all $x,y\in\mathbb{Z}/(p)$. Let $f(0,0,0)=y_0$. Let $g\colon(Y,s)\longrightarrow(\mathbb{Z}/(p),s')$ be an isomorphism of solutions. We have that $gf(\sigma_{(a,b,c)}(0,0,0))=g(y_0)-1$, for all $(a,b,c)\in X$. But we know that

$$\sigma_{(0,1,0)}(0,0,0)=(0,0,0),$$

and thus $gf(\sigma_{(0,1,0)}(0,0,0))=gf(0,0,0)=g(y_0)$, a contradiction. Hence $|Y|\ne p$.

Therefore $|Y|=1$ and (X,r) is simple. □

Proposition 3.3. *Let (X,r) be the simple solution described in Theorem 3.2. Then its permutation group $\mathcal{G}(X,r)$ is a p-group.*

Proof: Let $(a,b,c),(x,y,z)\in X=\mathbb{Z}/(p^n)\times\mathbb{Z}/(p)\times\mathbb{Z}/(p^n)$. The definition of the permutations $\sigma_{(a,b,c)}$ implies easily that every element σ of the group $\mathcal{G}(X,r)$ has the form

$$\sigma(x,y,z)=(x+\alpha,y+\beta_x,z+\gamma_{x,y})$$

for some $\alpha\in\mathbb{Z}/(p^n)$, $\beta_x\in\mathbb{Z}/(p)$, $\gamma_{x,y}\in\mathbb{Z}/(p^n)$, depending only on σ, on σ and x, and on σ and x, y, respectively. It follows that $\sigma^{p^n}(x,y,z)=(x,y+\beta'_x,z+\gamma'_{x,y})$ for some $\beta'_x\in\mathbb{Z}/(p)$, $\gamma'_{x,y}\in\mathbb{Z}/(p^n)$, depending only on σ and x, and on σ and x, y, respectively. Then, $\sigma^{p^{n+1}}(x,y,z)=(x,y,z+\gamma''_{x,y})$ for some $\gamma''_{x,y}\in\mathbb{Z}/(p^n)$, depending on σ and on x, y only. This implies that $\sigma^{p^{2n+1}}$ is the identity map. It follows that $\mathcal{G}(X,r)$ is a p-group. □

4. Singular simple solutions of cardinality p^{2n}

In [**21**] Rump introduced singular left braces.

Definition 4.1. Let B be a finite left brace. A prime divisor p of $|B|$ is called singular if there exists a finite indecomposable solution (X, r) of the YBE such that $B \cong \mathcal{G}(X, r)$ and p is not a divisor of $|X|$. We call B singular if B admits a singular prime. In this case, we say that the solution (X, r) is singular.

In [**21**] Rump proved that among the left braces of cardinality less than 36, there is a unique singular left brace, up to isomorphism, it has order 24, and it is the permutation group of an indecomposable and irretractable solution of cardinality 8. In [**5**, Example 21], it is proved that this singular solution has finite primitive level (see [**10**]); in particular it is not simple. Then Castelli in [**5**] constructs an infinite family of singular, indecomposable, and irretractable solutions of the YBE and all of them have finite primitive level. He asks whether there exist singular solutions which have no finite primitive level. We answer this question in the affirmative in the following result.

Theorem 4.2. *Let p be an odd prime number which is not a Fermat prime number. Let n be a positive integer and let q be an odd prime divisor of $p-1$. Then there exists a singular simple solution (X, r) of cardinality p^{2n}. Furthermore, $|\mathcal{G}(X, r)| = p^m q$ for some positive integer m.*

Proof: Note that since p is an odd prime and it is not a Fermat prime number, there exists an odd prime divisor q of $p-1$. Since q is a divisor of $p-1$, there exists $t \in \operatorname{Aut}(\mathbb{Z}/(p^n))$ of order q. Let $T = \operatorname{gr}(t)$. Note that the orbit of every non-zero element $a \in \mathbb{Z}/(p^n)$ by the action of T has cardinality q. Let $a \in \mathbb{Z}/(p^n)$ be a non-zero element. Since p is an odd prime, $a \neq -a$. Suppose that $-a$ is in the orbit of a by the action of T. Since the orbit of a has cardinality q, there exists an integer $1 < k < q$ such that $t^k(a) = -a$. Then $t^{2k}(a) = t^k(-a) = -t^k(a) = a$. Hence q is a divisor of $2k$. Since q is an odd prime, q is a divisor of k and we get a contradiction because $1 < k < q$. Thus, for every non-zero $a \in \mathbb{Z}/(p^n)$, $-a$ is not in the orbit of a by the action of T. Let I be the set of the orbits in $\mathbb{Z}/(p^n)$ by the action of T. We can choose an element a_i of each orbit $i \in I$ in such a way that $-a_i = a_l$ for some $l \in I$. We define a family $(j_a)_{a \in \mathbb{Z}/(p^n)}$ of elements of $\mathbb{Z}/(p^n)$ as follows: $j_0 = 1$ and

$$j_{t^k(a_i)} = t^k(-1) + 1,$$

for all $i \in I \setminus \{\{0\}\}$ and all $k \in \mathbb{Z}$. In particular, $j_{a_i} = 0$ for every $i \in I \setminus \{\{0\}\}$. Let $a \in \mathbb{Z}/(p^n) \setminus \{0\}$. There exist $i, l \in I$ and $k \in \mathbb{Z}$ such that $a = t^k(a_i)$ and $-a_i = a_l$. Now we have that

$$j_{-a} = j_{-t^k(a_i)} = j_{t^k(-a_i)} = j_{t^k(a_l)} = t^k(-1) + 1 = j_{t^k(a_i)} = j_a,$$

and for every $s \in \mathbb{Z}$, we also have that

$$j_{t^s(a)} - j_0 = j_{t^{s+k}(a_i)} - j_0 = t^{s+k}(-1) = t^s(j_{t^k(a_i)} - j_0) = t^s(j_a - j_0).$$

Let $X = \mathbb{Z}/(p^n) \times \mathbb{Z}/(p^n)$ and let $r \colon X \times X \longrightarrow X \times X$ be the map defined by

$$r((a_1, a_2), (c_1, c_2)) = (\sigma_{(a_1,a_2)}(c_1, c_2), \sigma^{-1}_{\sigma_{(a_1,a_2)}(c_1,c_2)}(a_1, a_2)),$$

where

$$\sigma_{(a_1,a_2)}(c_1, c_2) = (t(c_1) + a_2, t(c_2 - j_{t(c_1)+a_2-a_1}))$$

for all $a_1, a_2, c_1, c_2 \in \mathbb{Z}/(p^n)$. By [**14**, Theorem 3.1], (X, r) is a solution of the YBE. Let $a \in \mathbb{Z}/(p^n)$ be a non-zero element. Let $V_{a,1} = \operatorname{gr}(j_c - j_{c+t^z(a)} \mid c \in \mathbb{Z}/(p^n),\ z \in \mathbb{Z})$. For every $m > 1$, define $V_{a,m} = V_{a,m-1} + \mathrm{gr}(j_c - j_{c+v} \mid c \in \mathbb{Z}/(p^n),\ v \in V_{a,m-1})$. Then $V_a = \sum_{m=1}^{\infty} V_{a,m}$ is a subgroup of $\mathbb{Z}/(p^n)$. There exist $i \in I$ and $k \in \mathbb{Z}$ such that $a = t^k(a_i)$. Note that $1 = 1 - 0 = j_0 - j_{a_i} \in V_{a,1} \subseteq V_a$ because a_i is in the T-orbit of a. Hence $V_a = \mathbb{Z}/(p^n)$, for all non-zero $a \in \mathbb{Z}/(p^n)$. By [**14**, Theorem 3.5], the solution (X, r) is simple. Clearly $|X| = p^{2n}$. Note that for every positive integer m

$$\sigma^m_{(0,0)}(u, v) = (t^m(u), w),$$

for some $w \in \mathbb{Z}/(p^n)$. Let k be the order of $\sigma_{(0,0)}$. We have that

$$(u, v) = \sigma^k_{(0,0)}(u, v) = (t^k(u), v).$$

Hence $t^k(u) = u$, for all $u \in \mathbb{Z}/(p^n)$. Since t has order q, we get that q is a divisor of k. Therefore q is a divisor of $|\mathcal{G}(X, r)|$. Since $q \neq p$, the solution (X, r) is singular and $\mathcal{G}(X, r)$ is a singular left brace.

Note that the automorphism t is defined by the multiplication by the invertible element $t(1) \in \mathbb{Z}/(p^n)$ of multiplicative order q. Since the elements of the form $1 + pz \in \mathbb{Z}/(p^n)$ have multiplicative order a power of p, we have that $t(1) - 1 \notin p(\mathbb{Z}/(p^n))$. Hence $t(1) - 1$ is invertible in $\mathbb{Z}/(p^n)$. Therefore $t - \mathrm{id} \in \mathrm{Aut}(\mathbb{Z}/(p^n))$. By [**14**, Section 4], this allows us to describe the left brace structure of $\mathcal{G}(X, r)$. Namely, by [**14**, Proposition 4.1, the comments before Lemma 4.2 and Theorem 4.5], we have that $\mathcal{G}(X, r)$ is the asymmetric product $\overline{H} \rtimes_\circ A_1$ of a trivial brace $\overline{H}$ of order a power of p (see [**7**]) and the semidirect product $A_1 = \mathbb{Z}/(p^n) \rtimes T$ of the trivial braces $\mathbb{Z}/(p^n)$ and T (see [**8**]). In particular, $|\mathcal{G}(X, r)| = p^m q$, for some positive integer m. □

Acknowledgments. The first author was partially supported by the Spanish Research State Agency through grant PID2023-147110NB-I00.

The authors are grateful to the referees for helpful and constructive comments.

References

[1] D. Bachiller, F. Cedó, and E. Jespers, Solutions of the Yang–Baxter equation associated with a left brace, *J. Algebra* **463** (2016), 80–102. DOI: 10.1016/j.jalgebra.2016.05.024.

[2] D. Bachiller, F. Cedó, E. Jespers, and J. Okniński, Asymmetric product of left braces and simplicity; new solutions of the Yang–Baxter equation, *Commun. Contemp. Math.* **21(8)** (2019), 1850042, 30 pp. DOI: 10.1142/S0219199718500426.

[3] D. Bachiller, F. Cedó, and L. Vendramin, A characterization of finite multipermutation solutions of the Yang–Baxter equation, *Publ. Mat.* **62(2)** (2018), 641–649. DOI: 10.5565/PUBLMAT6221809.

[4] M. Castelli, A characterization of finite simple set-theoretic solutions of the Yang–Baxter equation, *Proc. Amer. Math. Soc.* **151(12)** (2023), 5047–5057. DOI: 10.1090/proc/16329.

[5] M. Castelli, On the indecomposable involutive solutions of the Yang–Baxter equation of finite primitive level, *Publ. Mat.* **69(2)** (2025), 429–444. DOI: 10.5565/publmat6922509.

[6] M. Castelli, F. Catino, and G. Pinto, Indecomposable involutive set-theoretic solutions of the Yang–Baxter equation, *J. Pure Appl. Algebra* **223(10)** (2019), 4477–4493. DOI: 10.1016/j.jpaa.2019.01.017.

[7] F. Catino, I. Colazzo, and P. Stefanelli, Regular subgroups of the affine group and asymmetric product of radical braces, *J. Algebra* **455** (2016), 164–182. DOI: 10.1016/j.jalgebra.2016.01.038.

[8] F. Cedó, Left braces: solutions of the Yang–Baxter equation, *Adv. Group Theory Appl.* **5** (2018), 33–90.

[9] F. Cedó, E. Jespers, and J. Okniński, Braces and the Yang–Baxter equation, *Comm. Math. Phys.* **327(1)** (2014), 101–116. DOI: 10.1007/s00220-014-1935-y.

[10] F. Cedó and J. Okniński, Constructing finite simple solutions of the Yang–Baxter equation, *Adv. Math.* **391** (2021), Paper no. 107968, 40 pp. DOI: 10.1016/j.aim.2021.107968.

[11] F. Cedó and J. Okniński, New simple solutions of the Yang–Baxter equation and solutions associated to simple left braces, *J. Algebra* **600** (2022), 125–151. DOI: 10.1016/j.jalgebra.2022.02.011.

[12] F. Cedó and J. Okniński, Indecomposable solutions of the Yang–Baxter equation of square-free cardinality, *Adv. Math.* **430** (2023), Paper no. 109221, 26 pp. DOI: 10.1016/j.aim.2023.109221.
[13] F. Cedó and J. Okniński, Corrigendum to "Constructing finite simple solutions of the Yang–Baxter equation" [Adv. Math. 391 (2021) 107968], *Adv. Math.* **451** (2024), Paper no. 109807, 3 pp. DOI: 10.1016/j.aim.2024.109807.
[14] F. Cedó and J. Okniński, New simple solutions of the Yang–Baxter equation and their permutation groups, *J. Pure Appl. Algebra* **229(9)** (2025), Paper no. 108025, 26 pp. DOI: 10.1016/j.jpaa.2025.108025.
[15] C. Dietzel, S. Properzi, and S. Trappeniers, Indecomposable involutive set-theoretical solutions to the Yang–Baxter equation of size p^2, *Comm. Algebra* **53(3)** (2025), 1238–1256. DOI: 10.1080/00927872.2024.2405024.
[16] V. G. Drinfeld, On some unsolved problems in quantum group theory, in: *Quantum Groups* (Leningrad, 1990), Lecture Notes in Math. **1510**, Springer-Verlag, Berlin, 1992, pp. 1–8. DOI: 10.1007/BFb0101175.
[17] P. Etingof, T. Schedler, and A. Soloviev, Set-theoretical solutions to the quantum Yang–Baxter equation, *Duke Math. J.* **100(2)** (1999), 169–209. DOI: 10.1215/S0012-7094-99-10007-X.
[18] T. Gateva-Ivanova, Set-theoretic solutions of the Yang–Baxter equation, braces and symmetric groups, *Adv. Math.* **338** (2018), 649–701. DOI: 10.1016/j.aim.2018.09.005.
[19] T. Gateva-Ivanova and M. Van den Bergh, Semigroups of I-type, *J. Algebra* **206(1)** (1998), 97–112. DOI: 10.1006/jabr.1997.7399.
[20] W. Rump, Braces, radical rings, and the quantum Yang–Baxter equation, *J. Algebra* **307(1)** (2007), 153–170. DOI: 10.1016/j.jalgebra.2006.03.040.
[21] W. Rump, Primes in coverings of indecomposable involutive set-theoretic solutions to the Yang–Baxter equation, *Bull. Belg. Math. Soc. Simon Stevin* **30(2)** (2023), 260–280. DOI: 10.36045/j.bbms.230429.
[22] A. Smoktunowicz, On Engel groups, nilpotent groups, rings, braces and the Yang–Baxter equation, *Trans. Amer. Math. Soc.* **370(9)** (2018), 6535–6564. DOI: 10.1090/tran/7179.
[23] L. Vendramin, Extensions of set-theoretic solutions of the Yang–Baxter equation and a conjecture of Gateva-Ivanova, *J. Pure Appl. Algebra* **220(5)** (2016), 2064–2076. DOI: 10.1016/j.jpaa.2015.10.018.

F. Cedó
Departament de Matemàtiques, Universitat Autònoma de Barcelona, 08193 Bellaterra (Barcelona), Spain
E-mail address: Ferran.Cedo@uab.cat
ORCID: 0000-0003-4703-2782

J. Okniński
Institute of Mathematics, University of Warsaw, Banacha 2, 02-097 Warsaw, Poland
E-mail address: okninski@mimuw.edu.pl
ORCID: 0000-0002-2434-3425

Received on July 1, 2024.
Accepted on May 5, 2025.