On Involutive Yang–Baxter groups

Jan Okniński
based on a joint work with Ferran Cedó

Będlewo, June 2025

Plan of the talk

1. Set theoretic solutions of the Yang–Baxter equation, left braces, and Involutive Yang–Baxter (IYB) groups.

2. Relevant previous results and the statement of the Main Problem.

3. Solvable groups with nilpotent Sylow sybgroups of class at most 2.

4. The easy cases: A-groups and groups with the Sylow tower property.

5. Main result: most finite solvable groups with Sylow subgroups of nilpotency class at most 2 are IYB.

Let X be a non-empty set and let $r : X \times X \longrightarrow X \times X$ 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 the set 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 $x, y \in X$.

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

The **permutation group** of a solution (X, r) of the YBE is the following subgroup of the symmetric group S_X

$$\mathcal{G}(X, r) = \mathrm{gr}(\sigma_x \mid x \in X).$$

A group is an **IYB group** if it is isomorphic to the permutation group of a finite solution of the YBE.

Etingof, Schedler and Soloviev proved that for every solution (X, r) of the YBE there exists an abelian group A, an action of $\mathcal{G}(X, r)$ on A and a bijective 1-cocycle $\mathcal{G}(X, R) \to A$. Using this, they proved

Theorem 1 (Etingof, Schedler, Soloviev; 1999)

If (X, r) is a finite solution of the YBE, then the group $\mathcal{G}(X, r)$ is solvable.

A naive question followed: is every finite solvable group and IYB group?

Some known results

Theorem 2

Let G be a finite group. In any of the following cases G is an IYB group.

1. *G is nilpotent of nilpotency class 2 (Ault, Watters; 1973),*
2. *$G = A \rtimes H$ where A is abelian and H is an IYB group (Cedó, Jespers, del Rio; 2010),*

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

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

If we also have

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

then B is called a **two-sided brace**.

Theorem 3 (Rump; 2007)

1. *G is a finite IYB group if and only if G is the multiplicative group of a finite left brace B.*
2. *G is the multiplicative group of a finite two-sided brace $B = (B, +, \cdot)$ if and only if G is isomorphic to the circle group of a finite nilpotent ring $R = (R, +, *)$.*
   (If R is such a ring, then $a \cdot b = a * b + a + b$ leads to a two-sided brace $(R, +, \cdot)$.)

Theorem 4 (Bachiller, 2016)

For infinitely many primes p there exists a finite p-group G such that G is not the multiplicative group of a left brace; hence it is not an IYB group.

The constructed groups have orders p^{10} and have nilpotency class 9. Smaller examples are not known.

It is known that every Hall subgroup of an IYB group is an IYB group (Cedó, Jespers, del Rio; 2010).

(Recall that a subgroup H of G is a Hall subgroup of G if $|H|$ and $[G : H]$ are relatively prime. Clearly, Sylow subgroups are Hall subgroups.)

Thus, the following is a natural question.

Main Problem Let G be a finite solvable group. Suppose that all Sylow subgroups of G are IYB groups. Is G an IYB group?

Important group theoretical tools

Let G be a finite solvable group. It is known (Hall) that G has a **Sylow system** $\mathcal{S}$: a collection of Sylow subgoups $P_1, \ldots, P_n$ (one for each prime dividing $|G|$) such that $P_i P_j = P_j P_i$ for every i, j.

The **system normalizer of** G associated with $\mathcal{S}$ is

$$\mathrm{M}(G) = \bigcap_{i=1}^{n} \mathrm{N}_G(P_i).$$

If G is a normal subgroup of a finite group L, then the **system normalizer of** G **relative to** L (associated to $\mathcal{S}$) is

$$\mathrm{M}_L(G) = \bigcap_{i=1}^{n} \mathrm{N}_L(P_i).$$

First step: A-groups

A finite solvable group G is an A-**group** if all its Sylow subgroups are abelian.

It was known that already within this class of groups we get an abundance of left braces, whence also of solutions of the YBE.

Theorem 5 (Cedó, Jespers, JO; 2020)

Let $n > 1$ be an integer. Let $p_1, p_2, \dots, p_n$ be distinct primes. There exist positive integers $l_1, l_2, \dots, l_n$, only depending on $p_1, p_2, \dots, p_n$, such that for each n-tuple of integers $m_1 \geq l_1$, $m_2 \geq l_2, \dots, m_n \geq l_n$ there exists a **simple** *left brace of order $p_1^{m_1} p_2^{m_2} \cdots p_n^{m_n}$ that has a metabelian multiplicative group which is an A-group.*

Theorem 6 (P. Hall; 1937)

If H/N is a nilpotent factor of a finite group G and H is solvable then $G = N\,\mathrm{M}_G(H)$.

In particular, if G is solvable, with the **lower nilpotent series** $G = D_0 \supset D_1 \supset \cdots \supset D_n = 1$, then we may take $H = D_{i-1}, N = D_i$.
So $G = D_i\,\mathrm{M}_G(D_{i-1})$.
(By definition, D_i/D_{i+1} is the largest nilpotent quotient of the group D_i.)

Theorem 7 (Taunt; 1949)

Assume that an A-group H is a normal subgroup of a finite group G. If H' is the derived group of H, then H' is a complementary in G to any system normalizer $\mathrm{M}_G(H)$ of H relative to G; so $G = H' \rtimes \mathrm{M}_G(H)$.

In particular, if G is a solvable A-group, then $G = L_i \rtimes \mathrm{M}_G(L_{i-1})$, where $G = L_0 \supset L_1 \supset \cdots \supset L_n = 1$ is the derived series of G.

Ben David and Ginosar (2016) claimed that every finite solvable A-group is an IYB group.
However, their proof is only valid under certain additional hypothesis.
Though, the proof can be easily corrected, as follows.

Theorem 8

Every finite solvable A-group is an IYB group.

Proof.

Let G be a finite solvable A-group. Let $G = L_0 \supset L_1 \supset \cdots \supset L_n = 1$ be the derived series of G. We shall prove the result by induction on n.
Clearly, every finite abelian group is IYB.
Suppose that $n > 1$ and that every finite solvable A-group of derived length $n-1$ is an IYB group.
We know (Taunt) that $\mathrm{M}_G(L_{n-2})$ is a complement in G of L_{n-1}, i.e. $G \cong L_{n-1} \rtimes \mathrm{M}_G(L_{n-2})$. Clearly, the derived length of $\mathrm{M}_G(L_{n-2})$ is $n-1$ and thus, by the induction hypothesis, $\mathrm{M}_G(L_{n-2})$ is an IYB group.
By Theorem 2 (part 3), G is an IYB group. □

Next step - nilpotent groups of nilpotency class 2

The following observation is well known: if R is a nilpotent ring of index n, then the circle group of R is nilpotent of class at most $n-1$.

Theorem 9 (Ault, Watters; 1973)

The nilpotent group G of class 2 is the circle group of a nilpotent ring of index 3 if and only if there is a mapping $m : G \times G \longrightarrow \mathrm{Z}(G)$ such that for all g, h and k in G,
(i) $m(gh, k) = m(g, k)m(h, k)$,
(ii) $m(g, hk) = m(g, h)m(g, k)$,
(iii) $m(m(g, h), k) = m(g, m(h, k)) = e$, where e is the identity in G, and
(iv) $m(g, h)m(h, g)^{-1} = [g, h]$.

Assume that every element of $\mathrm{Z}(G)$ has a unique square root. (In particular, if $\mathrm{Z}(G)$ has odd order.) Then we set $m(g, h) = [g, h]^{1/2}$ and it is not difficult to verify that conditions (i) to (iv) are satisfied.

Actually, defining $+$ and $\cdot$ on G by: $g + h = hgm(g, h)$ and $g \cdot h = m(g, h)$, we get a nilpotent ring.

Easy case: solvable groups with Sylow tower property

If G is a finite group such that $G = A \rtimes H$, where A is an abelian normal subgroup and H is an IYB subgroup, then G is also an IYB group (by Theorem 2).

This is essentially due to the fact that if we consider the trivial structure of brace on the abelian group A, then every automorphism of the group A is also an automorphism of the trivial brace A. This motivates our first observation.

Lemma 10

Let G be a nilpotent group of class 2 and with derived subgroup G' of odd order. Then there exists a structure of left brace on G such that $\mathrm{Aut}(G) = \mathrm{Aut}(G, +, \cdot)$.

Proof.

Since G' has odd order, every element of G' has a unique square root. We define a sum $+$ in G by the rule

$$h_1 + h_2 = h_1 h_2 [h_2, h_1]^{\frac{1}{2}}$$

for $h_1, h_2 \in G$.
By Theorem 9, $(G, +, \cdot)$ is a two-sided brace. Let $f \in \mathrm{Aut}(G)$.
Then

$$\begin{aligned} f(h_1 + h_2) =& f(h_1 h_2 [h_2, h_1]^{\frac{1}{2}}) \\ =& (f(h_1) f(h_2)) [f(h_2), f(h_1)]^{\frac{1}{2}} \\ =& f(h_1) + f(h_2), \end{aligned}$$

for all $h_1, h_2 \in G$. Hence $f \in \mathrm{Aut}(G, +, \cdot)$ and thus $\mathrm{Aut}(G) = \mathrm{Aut}(G, +, \cdot)$. □

Consequently, we get the following generalization of Theorem 2 part 3).

Lemma 11

Let G be a finite group with a normal nilpotent subgroup N of nilpotency class at most 2 and with derived subgroup N' of odd order and a subgroup H such that $G = N \rtimes H$. If H is an IYB group, then G is also an IYB group.

Proof.

If N is abelian, then G is an IYB group by Theorem 2.

Let $(H, +, \cdot)$ be a structure of left brace on the group H. Suppose that N is nilpotent of nilpotency class 2. By Lemma 10, there exists a structure of left brace $(N, +, \cdot)$ on the group N such that $\mathrm{Aut}(N) = \mathrm{Aut}(N, +, \cdot)$. We define the sum $+$ on G by

$$ah_1 + bh_2 = (a + b)(h_1 + h_2)$$

for all $a, b \in N$ and $h_1, h_2 \in H$. Since $\mathrm{Aut}(N) = \mathrm{Aut}(N, +, \cdot)$, we have that $(G, +, \cdot)$ is a left brace; as it is the inner semidirect product of the left brace $(N, +, \cdot)$ by the left brace $(H, +, \cdot)$.
Hence, the result follows. □

Recall that a finite group G has the **Sylow tower property** if there exists a normal series

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

such that G_{i+1}/G_i is isomorphic to a Sylow subgroup of G, for every $i = 0, \ldots, n-1$.

In this case G is solvable and G_1 is a normal Sylow subgroup of G.

The proof of the following result uses Lemma 11 and is an easy generalization of the inductive argument used in the proof of Theorem 8 (Ben David and Ginosar).

Theorem 12

Let G be a finite group such that all Sylow 2-subgroups of G are abelian. If G has the Sylow tower property and all the Sylow subgroups of G have nilpotency class at most 2, then G is an IYB group.

Proof.

Since G has the Sylow tower property, there exists a normal series

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

such that G_{i+1}/G_i is isomorphic to a Sylow subgroup of G, for every $i = 0, \ldots, n-1$. Note that n is the number of distinct prime divisors of the order of G. We shall prove the result by induction on n.

For $n = 1$, $G = G_1$ is a p-group for some prime p and by the hypothesis it has nilpotency class at most 2. Hence G is an IYB group in this case.

Suppose $n > 1$ and that the result holds for $n-1$. Let $p_1, \ldots, p_n$ be the distinct prime divisors of the order of G, such that G_{i+1}/G_i is a p_{i+1}-group for all $i = 0, \ldots, n-1$.

By Schur-Zassenhaus theorem, G_1 has a complement H in G. Thus G is the semidirect product $G_1 \rtimes H$. Clearly, $H \cong G/G_1$ has the Sylow tower property and the number of prime divisors of $|H|$ is $n-1$. Since the Sylow subgroups of H are also Sylow subgroups of G, by the induction hypothesis H is an IYB group. Since G_1 has nilpotency class at most 2, by Lemma 11, G is an IYB group. So, the result follows by induction. □

Groups with Sylow subgroups of nilpotency class 2

Recall that the **Fitting subgroup** $F(G)$ of a finite group G is the maximal normal nilpotent subgroup of G.

The following group theory result plays the key role in our approach.

Theorem 13

Let G be a finite solvable group such that all Sylow subgroups have nilpotency class at most 2. Then there exist nilpotent subgroups $N_1, \ldots, N_k$ and subgroups $G = M_0 \supset M_1 \supset \cdots \supset M_{k-1} \supset M_k = \{1\}$ such that

(i) $G = N_1 \cdots N_i M_i$, *for all* $1 \leq i \leq k$,

(ii) $M_{i-1} = N_i M_i$, *for all* $1 \leq i \leq k$,

(iii) N_i *is normal in* M_{i-1}, *for all* $1 \leq i \leq k$,

(iv) $((\ldots((N_1 \cap M_1)N_2) \cap \cdots \cap M_{i-1})N_i) \cap M_i$ *is normal in* M_i *and a central subgroup of* $F(M_{i-1})F(M_i)$, *for all* $1 \leq i \leq k$.

About the proof

If G is nilpotent, then we may put $k = 1$, $N_1 = G$ and $M_1 = \{1\}$ and the result follows in this case.

Suppose that G is not nilpotent. Let $\pi_1 \colon G \longrightarrow G/F(G)$ be the natural map. Let $H = \pi_1^{-1}(\mathrm{Z}(F(G/F(G))))$. Note that H is a non-nilpotent normal subgroup of G, and $F(G)$ is a proper subgroup of H such that $H/F(G)$ is abelian.

Let $N_1 = H'$ be the derived subgroup of H. Then $N_1 \subseteq F(G)$.
Let $P_1, \dots, P_m$ be a Sylow system of H, that is $H = P_1 \cdots P_m$, P_r is a Sylow p_r-subgroup of H and $P_j P_r = P_r P_j$, for all j, r.

Then $M_1 = \mathrm{M}_G(H) = \mathrm{N}_G(P_1) \cap \cdots \cap \mathrm{N}_G(P_m)$ is a system normalizer of H relative to G. Thus, by the result of Hall, $G = M_1 N_1$.
Since H is non-nilpotent, $M_1 \neq G$.

One shows that $N_1 \cap M_1 \subseteq \mathrm{Z}(F(G)F(M_1))$, as desired (condition (iv)).

Next, suppose that $1 \leq i$ and we have constructed subgroups $N_1, \ldots, N_i$ and a strictly decreasing chain $M_1 \supset \cdots \supset M_i$, with $M_i \neq 1$ and with the claimed properties.

The inductive step, leading to the desired decomposition $M_i = N_{i+1}M_{i+1}$, is a slight modification of the above construction of the decomposition $M = M_1N_1$.

Since $M_i \subset M_{i+1}$, this procedure has to stop, proving the assertion.

Main result

Theorem 14
Let G be a finite group of even order such that all Sylow subgroups have nilpotency class at most 2 and Sylow 2-subgroups are abelian. (In particular, this happens if $|G|$ is odd.) Then G is an IYB group.

Remark. It can be verified that the left braces constructed in the proof in general are not two-sided braces, in contrast to the motivating case of groups of nilpotency class 2 (Ault and Watters).

About the proof

We use assertion of Theorem 13. In particular $G = N_1 \cdots N_k$ and $M_i = N_{i+1} \cdots N_k$ for $i < k - 1$. We define a sum on each N_i by the rule

$$x + y = xy[y, x]^{\frac{1}{2}},$$

for all $x, y \in N_i$. Note that $(N_i, +, \cdot)$ is a left brace by Theorem 9.

Thus, we may assume that $k > 1$. We define a sum on G by the rule

$$(x_1 \cdots x_k) + (y_1 \cdots y_k) = (x_1 + y_1) \cdots (x_k + y_k),$$

for all $x_1, y_1 \in N_1, \ldots, x_k, y_k \in N_k$.

First, the technical conditions of Theorem 13 are used to prove that this sum is well-defined.

Next, note that the restriction of the sum in G to N_i is exactly the sum on N_i defined previously. Since each $(N_i, +, \cdot)$ is a left brace, it is easy to see that $(G, +)$ is an abelian group.

Finally, one verifies that $(G, +, \cdot)$ is a left brace and the result follows.

A potential approach towards a counterexample

Remark Assume that B is an IYB group of order p^n, for a prime p. If there exists some $\sigma \in \mathrm{Aut}(B, \cdot)$ of prime order $q \neq p$ such that $\sigma \notin \mathrm{Aut}(B, +, \cdot)$ for every left brace structure $(B, +, \cdot)$ on B, then the answer to Main Problem is negative.

Indeed, assume that P is a finite p-group, for a prime p, such that $\mathrm{Aut}(P)$ is not a p-group. Let q be a prime divisor of $|\mathrm{Aut}(P)|$, $q \neq p$. Let $\alpha \in \mathrm{Aut}(P)$ be of order q. Suppose that P is an IYB group. Consider the semidirect product $P \rtimes \mathbb{Z}/(q)$, where

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \alpha^{b_1}(a_2), b_1 + b_2).$$

If the answer to Main Problem is affirmative, then since the abelian group $\mathbb{Z}/(q)$ is an IYB group, then $P \rtimes \mathbb{Z}/(q)$ is also an IYB group.

Let $P_1 = P \times \{0\}$ and $P_2 = \{1\} \times \mathbb{Z}/(q)$. Since P_1 is normal in the multiplicative group of B, one can show that there exists a structure of left brace B on $P \rtimes \mathbb{Z}/(q)$ such that P_1 is the Sylow p-subgroup of the additive group of B.

Furthermore, there exists $(a, b) \in P \rtimes \mathbb{Z}/(q)$ such that $(a, b)P_2(a, b)^{-1}$ is the Sylow q-subgroup of the additive group of B. Let $f\colon B \longrightarrow P \rtimes \mathbb{Z}/(q)$ be the map defined by

$$f(a_1, b_1) = (a, b)^{-1}(a_1, b_1)(a, b).$$

Then f is an isomorphism from the multiplicative group of B to the group $P \rtimes \mathbb{Z}/(q)$. We define a structure of left brace B_1 on the group $P \rtimes \mathbb{Z}/(q)$ defining a sum $+_1$ on the group $P \rtimes \mathbb{Z}/(q)$ as follows:

$$(a_1, b_1) +_1 (a_2, b_2) = f(f^{-1}(a_1, b_1) + f^{-1}(a_2, b_2)),$$

for $(a_1, b_1), (a_2, b_2) \in P \rtimes \mathbb{Z}/(q)$, where $+$ is the sum of the left brace B.

Note that f is an isomorphism of left braces from the left brace B to the left brace B_1. In particular, $f(P_1) = P_1$ is the Sylow p-subgroup of $(B_1, +_1)$ and $P_2 = f((a,b)P_2(a,b)^{-1})$ is the Sylow q-subgroup of $(B_1, +_1)$.

It is easy to see that $\lambda_y(x) = yxy^{-1}$ for $x \in P_1, y \in P_2$, in the left brace B_1 (because P_1 is normal in B_1), so that we obtain

$$\begin{aligned} \lambda_{(1,1)}(a_1, 0) &= (1,1)(a_1,0)(1,-1) \\ &= (\alpha(a_1),1)(1,-1) = (\alpha(a_1),0). \end{aligned}$$

Let $\beta \in \mathrm{Aut}(P_1)$ be the automorphism defined by $\beta(x,0) = (\alpha(x),0)$. Then $\beta \in \mathrm{Aut}(P_1, +, \cdot)$ because $\lambda_{(1,1)} \in \mathrm{Aut}(B_1, +)$.

In particular, this proves that there exists a structure of left brace on the group P such that α is an automorphism of this left brace.

The statement of the remark follows.

SELECTED BIBLIOGRAPHY

[AW] J.C. Ault and J. F. Watters, Circle groups of nilpotent rings, Amer. Math. Monthly 80 (1973), 48–52.

[B] D. Bachiller, Counterexample to a conjecture about braces, J. Algebra 453 (2016), 160–176.

[BDG] N. Ben David and Y. Ginosar, On groups of I-type and involutive Yang–Baxter groups, J. Algebra 458 (2016), 197–206.

[CJO] F. Cedó, E. Jespers and J. Okniński, An abundance of simple left braces with abelian multiplicative Sylow subgroups, Rev. Mat. Iberoam. 36 (2020), 1309–1332.

[CJdR] F. Cedó, E. Jespers and Á. del Río, Involutive Yang–Baxter groups, Trans. Amer. Math. Soc. 362 (2010), 2541–2558.

[R] W. Rump, Construction of finite braces, Ann. Comb. 23 (2019), 391–416

[T] D. R. Taunt, On *A*-groups, Proc. Cambridge Philos. Soc. 45 (1949), 24–42.