UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Invariante diagonal y cableado de soluciones a la Ecuación de Yang–Baxter

Tesis presentada para optar al título de Doctor de la Universidad de Buenos Aires en el área Ciencias Matemáticas

Santiago Ramírez

Director de tesis: Leandro Vendramin
Consejero de estudios: Jonathan Ariel Barmak

Buenos Aires, 23 de octubre de 2025

Invariante diagonal y cableado de soluciones a la Ecuación de Yang–Baxter

Resumen. El problema general de clasificación o construcción de las soluciones conjuntistas a la ecuación de Yang–Baxter es en cierto sentido inaccesible debido a la cantidad de soluciones de la misma. Por esta razón resulta natural restringirse al estudio de ciertas clases de soluciones e intentar reducir el caso general al de estas clases de alguna manera. Una posibilidad es considerar las soluciones denominadas indescomponibles, aquellas que no se pueden escribir como una unión de dos soluciones más pequeñas. En esta tesis vamos a concentrarnos entonces en el estudio de las soluciones indescomponibles a la ecuación conjuntista de Yang–Baxter.

En una primera parte de esta tesis vamos a obtener resultados que garanticen la descomponibilidad o indescomponiblidad de una solución en términos de su invariante diagonal. Este invariante ya había sido definidio previamente en la literatura pero su relación con la descomponibilidad de las soluciones no había sido estudiada anteriormente. Luego de obtener resultados en esta dirección mediante métodos elementales introducimos la construcción del cableado de soluciones, que permite obtener a partir de una solución conjuntista nuevas soluciones del mismo tamaño. Luego de entender como se vinculan la descomponibilidad y el invariante diagonal de la solución original con los de las soluciones cableadas usamos esta nueva herramienta para extender los resultados anteriores obtenidos. La introducción de esta nueva herramienta nos permite también plantear nuevas preguntas respecto a la misma, como es el problema de decidir cuándo dos soluciones pueden obtenerse una de la otra via cableado.

En una segunda parte estudiamos el problema de construcción de todas las

soluciones indescomponibles que tengan un grupo de estructura dado. Usando una construcción de Bachiller, Cedó y Jespers, junto con la clasificación de braces de tamaño pq y p^2q de Acri y Bonatto, podemos dar una descripción de todas las soluciones indescomponibles con ciertos grupos de permutaciones. Para poder aplicar estos resultados debemos previamente calcular todos los grupos de automorfismo y entender las órbitas de la acción λ de todos los braces involucrados. Además de la descripción de las soluciones indescomponibles podemos entender como son los cableados de las soluciones construídas mediante el método de Bachiller, Cedó y Jespers, lo que nos permite entender cuales de las soluciones que construímos son equivalentes via cableado entre ellas.

Palabras clave: ecuación de Yang–Baxter, soluciones conjuntistas, braces, indescomponibilidad, cableado.

Diagonal invariant and cabling of solutions to the Yang–Baxter Equation

Abstract. The general problem of classification or construction of all set-theoretical solutions to the Yang–Baxter equation is in a way intractable due to the number of solutions that exist. For this reason it is natural to restrict oneself to the study of certain clases of solutions and attempt to reduce in some way the general case to understanding these classes. One of these posibilities is to consider the so-called indecomposable solutions, those that cannot be written as the disjoint union of two smaller solutions. In this thesis we are going to focus on the study of these indecomposable solutions to the Yang–Baxter equation.

In the first part of the thesis we will obtain results guaranteeing the decomposability or indecomposability of a solution in terms of its diagonal invariant. Although this invariant had been previously defined in the literature its connection to the indecomposability of the solutions had not been previously studied. After obtaining results in this direction by elementary means we will introduce the cabling of solutions, a novel construction allowing to obtain from a solution to the set-theoretical Yang–Baxter equation new solutions of the same size. After understanding how the indecomposability and diagonal invariant of the original solution relate to those of its cabled solutions we are able to use this new tool to extend the results obtained previously. We also pose some questions about this new construction, like the problem of deciding when two solutions can be obtained from one another via cabling.

In the second part of the thesis we study the problem of constructing all indecomposable solution with a given structure group. Using a construction of Bachiller, Cedó and Jespers, and the classification of braces of sizes pq and p^2q

of Acri and Bonatto, we are able to describe all indecomposable solutions with certain permutation groups. In order to be able to use this results we must previously compute all automorphism groups and the orbits of the λ action of all the braces involved. Besides obtaining a description of the indecomposable solutions through the method of Bachiller, Cedó and Jespers, we are also able to understand the cabling of these solutions in terms of this description, allowing us to determine precisely when two of these solutions are equivalnt via cabling.
Keywords: Yang–Baxter equation, set-theoretical solutions, braces, indecomposability, cabling.

Agradecimientos

Hay mucha gente a la cual quisiera y debería agredecer, y sería imposible mencionarlas a todas sin excederme en la longitud de estos agradacemientos ni que cometer omisiones que desearía no cometer. Voy a optar entonces por descartar cualquier intento de exhaustividad y nombrar solamente a aquellas personas que más directamente tuvieron que ver con el trabajo de esta tesis. Espero que el resto de las personas sepan de cualquier forma lo mucho que las aprecio y agradezco su compañía, y espero también tener la oprtunidad de expresárselo personalmente.

Primero a Leandro por haberme guiado en mi proceso de aprender a hacer investigación en matemática y haberme introducido en un área de la misma que de otra forma no se si hubiera tenido la posiblidad de explorar.

A Victoria y Marco que, junto con Leandro, fueron coautores de trabajos conmigo, algunos de los cuales forman parte de esta tesis.

A Andrea, Ángel y Eric por haber aceptado el trabajo de leer y evaluar este tesis.

A Jonathan por haber sido el consejero de estudios durante mi doctorado.

A Darío, Martín y Pablo, con quienes atravesamos juntos todo el doctorado y siempre nos ayudamos a lidiar con los problemas del mismo.

A mi familia que siempre me apoyó, y me sigue apoyando, en todos mis proyectos de vida.

A Marian que de una u otra forma me acompañó a lo largo de todo este proceso, 非常感谢.

Introducción

El origen de la ecuación de Yang–Baxter son los trabajos de Yang [41, 42] y Baxter [9, 10] en física estadística. En estos contextos la ecuación de Yang–Baxter suele aparecer de la forma

$$Y_{12}Y_{13}Y_{23} = Y_{23}Y_{13}Y_{12}, \tag{1}$$

donde $Y : V \otimes V \to V \otimes V$ es un operador lineal.

La ecuación 1 no es la forma usual de presentar la ecuación de Yang–Baxter en la literatura matemática sin embargo. Definiendo $R = Y\tau$, con τ el *twist* definido por $\tau(v \otimes w) = w \otimes v$, podemos expandir el lado izquierdo de la ecuación 1 para obtener

$$\begin{aligned} Y_{12}Y_{13}Y_{23} &= Y_{12}\tau_{12}T_{23}\tau_{12}Y_{23} \\ &= R_{12}T_{23}\tau_{23}\tau_{23}\tau_{12}Y_{23} \\ &= R_{12}R_{23}Y_{12}\tau_{23}\tau_{12} \\ &= R_{12}R_{23}R_{12}\tau_{12}\tau_{23}\tau_{12}, \end{aligned}$$

donde estamos usando que $\tau_{12}\tau_{23}Y_{23} = Y_{23}\tau_{12}\tau_{23}$ para cualquier morfismo $Y : V \otimes V \to V \otimes V$. Simétricamente obtenemos

$$Y_{23}Y_{13}Y_{12} = R_{23}R_{12}R_{23}\tau_{23}\tau_{12}\tau_{23},$$

y como el morfismo de twist satisface $\tau_{12}\tau_{23}\tau_{12} = \tau_{23}\tau_{12}\tau_{23}$, entonces vemos que la función Y satisface la ecuación (1) si y sólo si la función R satisface la misma ecuación que el twist, es decir

$$R_{12}R_{23}R_{12} = R_{23}R_{12}R_{23}. \tag{2}$$

Esta última ecuación, que también recibe el nombre de ecuación de trenzas, es la que denominaremos en lo que sigue como la ecuación de Yang–Baxter.

Fuera de su contexto original en la física el estudio de las soluciones a la ecuación de Yang–Baxter resulta interesante por su conexión con otras áreas de la matemática. En particular podemos resaltar su importancia en el estudio de grupos cuánticos [30], álgebras de Nichols [5], e invariantes de nudos y links [38].

En 1990 Drinfeld [24] propuso estudiar una clase particular de las soluciones a la ecuación de Yang–Baxter, las denominadas soluciones conjuntistas. Estas son las que resultan de tomar una base $X \subseteq V$ y extender linealmente a $V \otimes V$ una función $R : X \times X \to X \times X$ que satisface el análogo a la ecuación (2) en conjuntos, es decir que cumplen

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

El estudio sistemático de las mismas comienza con los trabajos de Etingof, Schedler y Soloviev en [25], y Gateva-Ivanova y Van den Bergh en [26]. En ambos casos se restringen al estudio de soluciones que sean *no-degeneradas* e *involutivas*, ver la definición 1.3. La primera de estas condiciones es particularmente importante ya que garantiza la posibilidad de estudiar las soluciones utilizando herramientas algebraicas como describiremos en el capítulo 1. Aunque no será el caso en este trabajo, muchas de estas herramientas algebraicas pueden generalizarse al caso no involutivo, [27], y el estudio de estas soluciones es también importante en la actualidad.

Resulta natural intentar clasificar y construir todas las soluciones conjuntistas de tamaños pequeños. En [25] ya se presenta una tabla con las cantidades de soluciones de tamaño menor o igual a 8, y también de soluciones que satisfacen propiedades adicionales, aunque esta tabla presentaba algunas errores para las soluciones de tamaño 8, y desde ese momento hasta la actualidad sólo se han podido construir exhaustivamente las soluciones de tamaño menor o igual a 11. Concretemente en [3] se construyeron todas las soluciones hasta tamaño 10, y en [39] se construyeron todas las soluciones de tamaño menor o igual a 11. Las cantidades totales de soluciones (involutivas) que se obtienen se pueden ver en el cuadro 1.

Como se puede apreciar no solo es computacionalmente díficil construir todas las soluciones, sino que la cantidad total de soluciones que se obtienen

Tamaño	2	3	4	5	6
Soluciones	2	5	23	88	595
Tamaño	7	8	9	10	11
Soluciones	3456	34530	321931	4895272	77182093

Cuadro 1: Cantidades de soluciones de tamaños menores o iguales a 11.

Tamaño	2	3	4	5	6
Soluciones	1	1	5	1	10
Tamaño	7	8	9	10	11
Soluciones	1	100	16	36	1

Cuadro 2: Cantidades de soluciones indescomponibles de tamaños menores o iguales a 11.

aumenta extremadamente rápido con el tamaño de las mismas. En particular esto hace que una clasificación general de todas las soluciones resulte impracticable. Para tratar de sortear este obstáculo se puede intentar definir alguna clase de soluciones "sencillas" y luego intentar describir una solución general en término de soluciones de esta clase. Hay varias posibles clases que se pueden intentar utilizar para esto, por ejemplo las denominadas soluciones *simples* [40], que son aquellas sin cocientes no-triviales, o las soluciones *irretractables* [25, 18], que son aquellas que no se retraen a una solución más pequeña.

La noción en la que vamos a concentrarnos en este trabajo es la de *indescomponibilidad*, una solución es indescomponible si no es una unión disjunta de dos subsoluciones. Si uno analiza cuáles de las soluciones construidas son indescomponibles se obtienen los valores que se observan en el cuadro 2. Como se puede apreciar la cantidad de soluciones indescomponibles resulta mucho más manejable por lo que parece más alcanzable una posible clasificación o la obtención de algún mecanismo general de construcción de soluciones indescomponibles que sea aplicable para tamaños más grandes.

Esta tesis se centra entonces en el estudio de la indescomponibilidad de soluciones conjuntistas no-degeneradas e involutivas a la ecuación de Yang–Baxter. En el primer capítulo se exponen las nociones y resultados básicos de la teoría de las soluciones conjuntistas a la ecuación de Yang–Baxter, pre-

sentando las herramientas algebraicas necesarias para el desarrollo de la tesis. Todos los resultados de este primer capítulo son resultados conocidos del área.

En el segundo capítulo se introduce el invariante diagonal de una solución y se exponen los resultados obtenidos en [34]. En este trabajo pudimos obtener mediante métodos elementales criterios indescomponibilidad de soluciones en términos del invariante diagonal. Este invariante ya aparece en [25] de manera explícita, sin embargo no se había hecho hasta el trabajo aquí expuesto un estudio de su relación con la indescomponibilidad de las soluciones.

En el tercer capítulo de la tesis se introduce la construcción del cableado de soluciones y se exponen los resultados obtenidos en [32] que extienden considerablemente los resultados del capítulo anterior a partir del estudio de esta nueva construcción. La presentación de los resultados en este capítulo es distinta de la presentación original, ya que se utilizan argumentos diagramáticos que permiten simplificar algunos argumentos y vincular esta construcción con una construcción anterior de Bachiller y Cedó.

Por último en el cuarto capítulo se exponen los resultados obtenidos [34]. En estos utilizamos una construcción de Bachiller, Cedó y Jespers, junto con la clasificación de brazas de tamaños pq y p^2q de Acri y Bonatto para dar una descripción explícita de todas las soluciones indescomponibles cuyos grupos de permutaciones son de tamaño pq, o son grupos abelianos o diedrales de tamaño p^2q. Además utilizamos esta descripción para calcular los cableados de las soluciones obtenidas, cosa que no se encuentra en el trabajo original ya que la noción de cableado de soluciones es posterior a la publicación del mismo.

Índice general

Capítulo 1

Brazas y la Ecuación de Yang–Baxter

En este capítulo introducimos los conceptos fundamentales sobre las soluciones a la ecuación de Yang–Baxter necesarios para desarrollar los resultados obtenidos. Todos los resultados de este capítulo son resultados ya establecidos en la literatura.

1.1. La Ecuación de Yang–Baxter

En esta sección vamos a dar las definiciones y resultados más elementales del del estudio de las soluciones de la ecuación de Yang–Baxter. Los mismos fueron originalmente desarrollados por Etingof, Schedler y Soloviev en [25].

Definición 1.1. Una *solución conjuntista a la ecuación de Yang–Baxter* es un par (X, r) donde X es un conjunto y $r : X \times X \to X \times X$ es una función biyectiva tal que

$$(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id}) = (\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r). \tag{1.1}$$

Definimos un *morfismo* de soluciones como una función $f : X \to Y$ entre dos soluciones (X, r) e (Y, r'), que satisface que si $r(w, x) = (y, z)$, entonces

$r'(f(w), f(x)) = (f(y), f(z))$, i.e. tal que el siguiente diagrama connmuta,

$$\begin{array}{ccc} X \times X & \xrightarrow{f \times f} & Y \times Y \\ \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle r'} \\ X \times X & \xrightarrow{f \times f} & Y \times Y \end{array}$$

Las funciones componentes de r se suelen notar σ y τ, con uno de sus argumentos como subíndice, de forma que valga $r(x, y) = (\sigma_x(y), \tau_y(x))$. Con esta notación la condición de ser solución se puede interpretar en términos de estas funciones componentes.

Lema 1.2 (Etingof–Schedler–Soloviev)**.** *Una función $r : X \times X \to X \times X$ es solución de la ecuación de Yang–Baxter si y sólo si las funciones componentes satisfacen las siguientes identidades para todo $x, y, z \in X$*

- $\sigma_x \circ \sigma_y = \sigma_{\sigma_x(y)} \circ \sigma_{\tau_y x}$,
- $\sigma_{\tau_{\sigma_y(z)}(x)}(\tau_z(y)) = \tau_{\sigma_{\tau_y(x)}(z)}(\sigma_x(y))$,
- $\tau_z \circ \tau_y = \tau_{\tau_z(y)} \circ \tau_{\sigma_y(z)}$.

Demostración. Evaluando la Ecuación (1.1) en x, y, z obtenemos del lado izquierdo

$$\begin{aligned}(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id})(x, y, z) &= (r \times \mathrm{id})(\mathrm{id} \times r)(\sigma_x(y), \tau_y(x), z) \\ &= (r \times \mathrm{id})(\sigma_x(y), \sigma_{\tau_y(x)}(z), \tau_z(\tau_y(x))) \\ &= (\sigma_{\sigma_x(y)}(\sigma_{\tau_y(x)}(z)), \tau_{\sigma_{\tau_y(x)}(z)}(\sigma_x(y)), \tau_z(\tau_y(x))),\end{aligned}$$

y evaluando el lado derecho obtenemos

$$\begin{aligned}(\mathrm{id} \times r)(r \times \mathrm{id})(\mathrm{id} \times r)(x, y, z) &= (\mathrm{id} \times r)(r \times \mathrm{id})(x, \sigma_y(z), \tau_z(y)) \\ &= (\mathrm{id} \times r)(\sigma_x(\sigma_y(z)), \tau_{\sigma_y(z)}(x), \tau_z(y)) \\ &= (\sigma_x(\sigma_y(z)), \sigma_{\tau_{\sigma_y(z)}(x)}(\tau_z(y)), \tau_{\tau_z(y)}(\tau_{\sigma_y(z)}(x))).\end{aligned}$$

Notemos que en ambos casos en la primera coordenada la variable z no aparece en los subíndices. Como esto vale para todo z podemos eliminarla a igualar ambas coordenadas, obteniendo la primera de las identidades que buscabamos. Análogamente al igualar las terceras coordenadas obtenemos la tercera

identidad luego de eliminar la variable x por razones análogas. Por último al igualar las segundas coordenadas obtenemos exactamente la segunda identidad. □

Definición 1.3. Una solución (X, r) se dice *no-degenerada* si todas las funciones $\sigma_x, \tau_y : X \to X$ son biyectivas, y se dice *involutiva* si r es una involución, i.e. $r^2 = \mathrm{id}$.

En lo que sigue *solución* siempre va a querer decir solución conjuntista, no-degenerada e involutiva de la ecuación de Yang–Baxter.

Ejemplo 1.4. En cualquier conjunto X podemos considerar la *solución trivial* en X, dada por $r(x, y) = (y, x)$. Observemos que esta solución satisface $\sigma_x = \mathrm{id} = \tau_y$ para todos los elementos $x, y \in X$.

En el caso de las soluciones involutivas además de satisfacer las identidades del Lema 1.2, las funciones componentes quedan determinada cada una por la otra de acuerdo la siguiente identidad adicional:

Proposición 1.5 (Etingof–Schedler–Soloviev)**.** *Sea (X, r) una solución involutiva, entonces las funciones componentes de r satisfacen*

$$\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(x).$$

Demostración. Por la involutividad tenemos que para todo par $x, y \in X$ vale $R^2(x, y) = (x, y)$, e inspeccionando la primer componente en esta ecuación obtenemos

$$\sigma_{\sigma_x(y)}(\tau_y(x)) = x,$$

de donde se sigue lo que queremos aplicando la función $\sigma^{-1}_{\sigma_x(y)}$ a ambos lados. □

Ejemplo 1.6. Si las funciones σ y τ no dependen del subíndice, la solución (no necesariamente involutiva en este caso) pertenece a la familia de soluciones llamadas *de Lyubashenko*. Es decir que (X, r) es una solución de Lyubashenko si existen permutaciones σ y τ tales que $r(x, y) = (\sigma(y), \tau(x))$.

En este caso de las identidades del Lema 1.2, la única que resulta no trivial es la segunda, que se simplifica a $\sigma \circ \tau = \tau \circ \sigma$. Es decir que dos permutaciones σ, τ determinan una solución de Lyubashenko, si y sólo si conmutan.

Más aún en el caso de soluciones de Lyubashenko involutivas, de la Proposición 1.5 obtenemos que se debe tener $\tau = \sigma^{-1}$.

Ejemplo 1.7. Un caso particular de soluciones de Lyubashenko involutivas son las *soluciones cíclicas*, que se obtienen al tomar σ igual a un ciclo de longitud máxima. Es fácil ver que todas estas son equivalentes a la solución definida en $\mathbb{Z}/n\mathbb{Z}$ por $r(x, y) = (y - 1, x + 1)$.

Esta familia de soluciones es importante porque cuando n es un primo p dan la única solución *indescomponible*, de tamaño p. Este es un resultado de Etingof, Schedler y Soloviev, ver Teorema 2.12 de [25].

Definición 1.8. Dada una solución (X, r) y un subconjunto $Y \subseteq X$ decimos que Y es una *subsolución* si la función r se restringe a una función de $Y \times Y$ en $Y \times Y$.

Si existen dos subsoluciones $Y_1, Y_2 \subseteq X$ tales que X es la unión disjunta de Y_1 y Y_2, y ambas son no vacías decimos que X es una solución *descomponible*. En caso contrario, i.e. si no existe una tal descomposición, decimos que X es una solución *indescomponible*.

Uno de los principales invariantes algebraicos de una solución se obtiene al utilizar las aplicaciones de la función r como "relaciones de conmutación" en un grupo. Concretamente tenemos la siguiente definición:

Definición 1.9. Si (X, r) es una solución definimos su *grupo de estructura* como

$$G(X, r) = \langle x \in X | xy = \sigma_x(y)\tau_y(x) \rangle .$$

Las identidades del Lema 1.2 garantizan que este grupo actúa de manera natural en la solución X, por lo tanto obtenemos también como invariante la imagen de esta acción.

Definición 1.10. Si (X, r) es una solución definimos su *grupo de permutaciones* como

$$\mathcal{G}(X, r) = \langle \sigma_x \rangle_{x \in X} \subseteq \mathrm{Sym}(X).$$

Proposición 1.11 (Etingof–Schedler–Soloviev)**.** *Si (X, r) es una solución, el mapa natural $X \to \mathcal{G}(X, r)$ definido por $x \mapsto \sigma_x$ se extiende a un morfismo de grupos $G(X, r) \to \mathcal{G}(X, r)$.*

Demostración. La primera identidad del Lema 1.2 es

$$\sigma_{\sigma_x(y)}\sigma_{\tau_x(y)}(z) = \sigma_x\sigma_y(z).$$

Esto dice exactamente que los generadores del grupo de permutaciones satisfacen las relaciones que definen al grupo de estructura, y por lo tanto la función del enunciado define un morfismo de grupos. □

El siguiente resultado nos permite interpretar la (in)descomponibilidad de una solución en términos de estos invariantes.

Proposición 1.12 (Etingof–Schedler–Soloviev)**.** *Una solución (X, r) es indescomponible si y sólo si la acción de su grupo de estructura en X es transitiva, o, equivalentemente, si el grupo de permutaciones de la solución es un subgrupo transitivo de* $\mathrm{Sym}(X)$.

Demostración. Supongamos primero que la solución es descomponible, i.e. $X = X_1 \bigsqcup X_2$ con X_1 y X_2 subsoluciones. Como X_1 es una subsolución sabemos que para todo $x \in X_1$ se tiene que $X_1 \subset X$ es un subconjunto invariante de σ_x, y por lo tanto X_2 también es invariante al ser su complemento. Por el mismo razonamiento tenemos que X_2 y X_1 también son subconjuntos invariantes por la acción de σ_x para todo $x \in X_2$. Como los σ_x generan el grupo de permutaciones los subconjuntos X_1 y X_2 son invariantes por la acción de todo el grupo de permutaciones, i.e. la acción no es transitiva.

Asumamos ahora que la acción del grupo de permutaciones no es transitiva. Podemos escribir entonces $X = X_1 \bigsqcup X_2$, con X_1 y X_2 dos subconjuntos no vacíos e invariantes por la acción del grupo de permutaciones. En particular sabemos que para todo $x \in X_1$ vale que X_1 es un subconjunto invariante por la acción de σ_x. Más aún por la Proposición 1.5 tenemos que si además $y \in X_1$ entonces tenemos

$$\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(x),$$

como $\sigma_x(y) \in X_1$, entonces X_1 es invariante por la acción de $\sigma_{\sigma_x(y)}$ y por lo tanto el lado derecho de la ecuación pertenece a X_1. Podemos concluir entonces que X_1 es invariante por la acción de τ_x para todo $x \in X_1$. De esto deducimos que X_1 es efectivamente una subsolución de X. El mismo razonamiento nos permite concluir que X_2 también es una subsolución. □

Observemos que la definición que dimos del grupo de permutaciones utiliza únicamente las funciones σ. De la tercera identidad del Lema 1.2 se deduce que podríamos definir un grupo similar utilizando las funciones τ y obtendríamos

una acción a derecha del grupo de estructura. La demostración del resultado anterior se podría adaptar fácilmente a esta acción a derecha, y uno se puede preguntar si estas dos acciones contienen la misma información sobre la solución o no. El Corolario 2.8 responde afirmativamente a esta pregunta.

Más adelante vamos a necesitar del siguiente resultado de Cedó, Jespers y Okniński que determina todas las posibles soluciones cuyo grupo de estructura actúa de manera primitiva en la solución, a las que denominamos *soluciones primitivas*.

Teorema 1.13 (Cedó–Jespers–Okniński)**.** *Si (X, r) es una solución primitiva de la ecuación de Yang–Baxter, entonces $|X|$ es un número primo, y entonces X es una solución cíclica.*

Demostración. Ver [17, Teorema 3.1]. □

Recordemos que quiere decir que un grupo actúe de manera primitiva.

Definición 1.14. Dado un grupo G que actúa en un conjunto X, una familia de subconjuntos de X, $\{\Delta_1, \ldots, \Delta_N\}$, es un *sistema de bloques* para la acción de G si para todo $i, j \leq N$ y $g \in G$ se tiene que $g \cdot \Delta_i = \Delta_j$ ó $(g \cdot \Delta_i) \cap \Delta_j = \emptyset$.

Decimos que un grupo G actúa de manera *primitiva* en un conjunto X si actúa de manera transitiva y la acción no admite ningún sistema de bloques no trivial, es decir los únicos sistemas de bloques para la acción son $\{X\}$ y $\{\{x\} | x \in X\}$.

1.2. Diagramas de trenzas

Las soluciones a la ecuación de Yang–Baxter determinan representaciones de los grupos de trenzas, B_n. Recordemos que estos grupos están determinados por las presentaciones

$$B_n = \langle \sigma_1, \ldots, \sigma_{n-1} | \sigma_i \sigma_j = \sigma_j \sigma_i \, , \, \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1} \rangle,$$

donde las relaciones se están tomando con $i \leq n-1$ y $|i-j| \geq 2$. Notemos que el segundo grupo de relaciones de la presentación tiene la misma forma que la ecuación de Yang–Baxter. En efecto dada una solución de la ecuación de Yang–Baxter (X, r), obtenemos acciones de los grupos de trenzas, de B_n

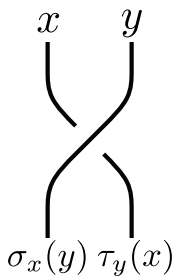


Figura 1.1: Representación diagramática de la acción de r.

en X^n, dada por la aplicación $\sigma_i \mapsto r_{i,i+1}$, donde $r_{i,i+1}$ es aplicar la función r de la solución en las coordenadas i e $i+1$.

Los elementos del grupo de trenzas están en correspondencia con clases de isotopía de *trenzas geométricas*, y se pueden presentar diagramáticamente mediante *diagramas de trenzas*. Una exposición formal sobre la correspondencia entre elementos del grupo de trenzas, trenzas geométricas y diagramas de trenzas se puede ver en los primeros capítulos de [22] o [31].

Usando la acción anterior de los grupos podemos interpretar los diagramas de trenzas como composiciones de las funciones $r_{i,i+1}$ y razonar diagramáticamente sobre las soluciones de la ecuación de Yang–Baxter. La aplicación de la función r en un par (x, y) queda representada por el diagrama de la figura 1.1.

De esta forma la ecuación de Yang–Baxter se corresponde con la equivalencia de los diagramas de trenza de la figura 1.2. La trenza opuesta a la de la figura 1.1, i.e. con la hebra izquierda pasando por detrás de la hebra derecha, representa la acción de la función r^{-1}. Como vamos a trabajar con soluciones involutivas tenemos que $r = r^{-1}$, y por lo tanto podríamos utilizar diagramas que no hagan la distinción entre ambos tipos de cruces. Para preservar la intuición topológica al momento de hacer razonamientos diagramáticos vamos a utilizar diagramas de trenzas estándar.

Notemos que siempre que tengamos un diagrama como el de la figura 1.1, en el que conozcamos el valor de sólo dos cualesquiera de los cuatro extremos del diagrama, entonces hay una única forma de completar el diagrama con los restantes dos valores para que el mismo corresponda con una aplicación correcta de la función r.

Lema 1.15. *Sea $r : X \times X \to X \times X$ una solución de la ecuación de Yang–*

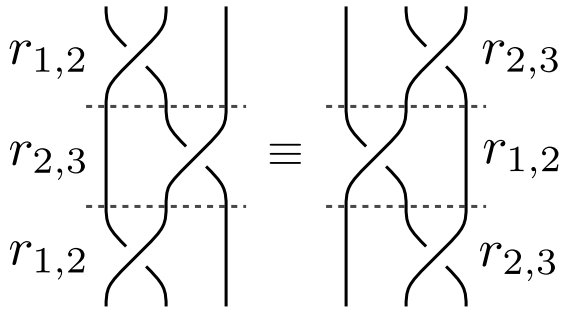


Figura 1.2: Ecuación de Yang–Baxter.

Baxter.

1. *Dados $a, c \in X$ existen únicos $b, d \in X$ tales que $r(a, b) = (c, d)$.*
2. *Dados $b, d \in X$ existen únicos $a, c \in X$ tales que $r(a, b) = (c, d)$.*
3. *Dados $a, d \in X$ existen únicos $b, c \in X$ tales que $r(a, b) = (c, d)$.*
4. *Dados $b, c \in X$ existen únicos $a, d \in X$ tales que $r(a, b) = (c, d)$.*

Demostración. Estas situaciones se corresponden con el diagrama de la figura 1.3. Los dos primeros casos se corresponden con el valor inicial de una hebra y el final de la otra. Los últimos dos casos se corresponden con conocer el valor inicial y final de una misma hebra.

Tenemos en general que $c = \sigma_a(b)$, y $d = \tau_b(a)$. Por la no-degeneración de la solución en el primer caso se tiene que cumplir que $b = \sigma_a^{-1}(c)$, y entonces $d = \tau_{\sigma_a^{-}1(c)}(a)$. Los restantes casos son completamente análogos. □

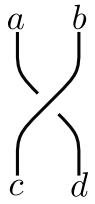


Figura 1.3: Diagrama Lema 1.15.

1.3. Brazas

Tanto el grupo de estructura como el grupo de permutaciones de una solución tienen una estructura adicional de grupo abeliano. Esta estructura satisface junto con la estructura original ciertas condiciones que le dan a este grupo una estructura de *braza*. En esta sección introducimos el concepto de braza y recopilamos los resultados básicos que necesitaremos en lo que sigue.

Definición 1.16. Una *braza* es una tripla $(B, +, \circ)$ tal que $(B, +)$ es un grupo abeliano, $(B, \circ)$ es un grupo y se satisface la siguiente ecuación para toda tripla de elementos $a, b, c \in B$:

$$a \circ (b + c) = a \circ b - a + a \circ c. \tag{1.2}$$

El grupo abeliano $(B, +)$ se denomina la *estructura aditiva* de la braza, y el grupo $(B, \circ)$ se denomina la *estructura multiplicativa* de la braza.

Definimos un *morfismo* de brazas como una función $f : B \to B'$ entre dos brazas $(B, +, \circ)$ y $(B, +', \circ')$ que respeta tanto la estructura aditiva como multiplicativa de la braza, i.e. que cumple

$$f(a + b) = f(a) +' f(b),$$
$$f(a \circ b) = f(a) \circ' f(b),$$

para todo $a, b \in B$.

La definición original de braza es de Rump en [36], sin embargo esta definición es distinta a la que estamos dando, aunque resulta equivalente. Esta versión de la definición es de Cedó, Jespers y Okniński en [16], donde también prueban la equivalencia entre ambas definiciones y desarrollan los resultados que exponemos en esta sección.

Ejemplo 1.17. Dado un grupo abeliano $(B, +)$ tomando como estructura multiplicativa $\circ$ la misma operación $+$ tenemos

$$a \circ (b + c) = a + b + c = a + b - a + c + a = a \circ b - a + a \circ c,$$

y por lo tanto $(B, +, +)$ resulta una braza. Una braza de esta forma, i.e. una en el cual las estructuras aditiva y multiplicativa coinciden, se dice una *braza trivial*.

Lema 1.18. *Las estructuras aditiva y multiplicativa de una braza tienen el mismo elemento neutro.*

Demostración. Sea $(B, +, \circ)$ una braza y notemos por 0 al elemento neutro de su estructura aditiva. Para cada $a \in B$ tenemos

$$a \circ 0 = a \circ (0 + 0) = a \circ 0 + a \circ 0 - a,$$

y por lo tanto $a \circ 0 = a$, es decir que 0 es también el elemento neutro de la estructura multiplicativa. □

Para simplificar algunos argumentos va a resultar útil reescribir la ecuación (1.2) en términos de la resta, en lugar de la suma, de elementos.

Lema 1.19. *Sea $(B, +, \circ)$ una braza, para todo $a, b, c \in B$ se tiene*

$$a \circ (b - c) = a \circ b - a \circ c + a. \tag{1.3}$$

Demostración. Por la ecuación (1.2) tenemos

$$a \circ (b - c) = a \circ b + a \circ (-c) - a,$$

y por el Lema 1.18

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

De esta última ecuación podemos despejar

$$a \circ (-c) = 2a - a \circ c. \tag{1.4}$$

Remplazando esta expresión en la primera ecuación tenemos

$$a \circ (b - c) = a \circ b + (2a - a \circ c) - a,$$

que simplificando resulta la ecuación (1.3). □

Definición 1.20. Sea $(B, +, \circ)$ una braza. Para cada $b \in B$ definimos la función $\lambda_b : B \to B$ por $\lambda_b(x) = (b \circ x) - b$.

Proposición 1.21 (Cedó–Jespers–Okniński)**.** *Sea $(B, +, \circ)$ una braza. La función $\lambda_{\cdot}$ define una acción por automorfismos del grupo multiplicativo $(B, \circ)$ en el grupo aditivo $(B, +)$.*

Demostración. Primero veamos que para todo $a \in B$ la función λ_a resulta aditiva. Dados $b, c \in B$ tenemos

$$\begin{aligned}\lambda_a(b+c) &= a \circ (b+c) - a = a \circ b + a \circ c - a - a \\ &= \lambda_a(b) + \lambda_a(c),\end{aligned}$$

como queríamos. Chequeamos ahora que esto define una acción del grupo multiplicativo. Dados $a, b, c \in B$ tenemos

$$\lambda_a(\lambda_b(c)) = a \circ (b \circ c - b) - a.$$

Aplicando el Lema 1.19 obtenemos

$$\lambda_a(\lambda_b(c)) = a \circ b \circ c - a \circ b + a - a,$$

lo que se simplifica a $\lambda_{a \circ b}(c)$.

Como además tenemos que

$$\lambda_e(a) = (e \circ a) - e = a - e = a,$$

es decir, que el elemento neutro actúa por la identidad, tenemos que la acción es por automorfismos. □

La acción del grupo multiplicativo de la braza en el grupo aditivo resulta particularmente útil para entender y trabajar con estas estructuras. Otra forma de presentar las brazas que pone esto de manifiesto es a través de 1-cociclos.

Definición 1.22. Dado un grupo $(G, \cdot)$, un *1-cociclo biyectivo* de G en un grupo abeliano $(A, +)$ es el siguiente dato:

1. Una acción de G en A por automorfismos de grupo,
2. una función biyectiva $\pi : G \to A$,

tales que para todo $x, y \in G$ se cumple que

$$\pi(x \cdot y) = \pi(x) + x \cdot \pi(y). \tag{1.5}$$

Si $(B, +, \circ)$ es una braza entonces podemos construir un 1-cociclo biyectivo del grupo $(B, \circ)$ en el grupo abeliano $(B, +)$ tomando como función biyectiva a la identidad y como acción λ. El siguiente resultado describe como reconstruir cualquiera de las dos estructuras de grupo de la braza a partir de la otra a partir de la acción λ, y en particular garantiza que la definición anterior es efectivamente un 1-cociclo.

Proposición 1.23 (Cedó–Jespers–Okniński)**.** *Sea $(B, +, \circ)$ una braza. Para todo $a, b \in B$ se cumplen las siguientes dos identidades:*

$$a \circ b = \lambda_a(b) + a,$$
$$a + b = a \circ \lambda_a^{-1}(b).$$

Demostración. Para la primera identidad simplemente desarrollamos la acción por definición en el lado derecho de la identidad,

$$\lambda_a(b) + a = (a \circ b - a) + a = a \circ b.$$

Para probar la segunda identidad desarrollamos nuevamente la acción en el lado derecho. Notando $\overline{a}$ al inverso multiplicativo de a tenemos como λ es una acción,

$$a \circ \lambda_a^{-1}(b) = a \circ \lambda_{\overline{a}}(b) = a \circ (\overline{a} \circ b - \overline{a}).$$

Usando el Lema 1.19 para distribuir la operación de $\circ$ sobre la diferencia que obtenemos,

$$a \circ \lambda_a^{-1}(b) = a \circ \overline{a} \circ b - a \circ \overline{a} + a = b - 0 + a = b + a,$$

donde estamos usando que ambas operaciones tienen el mismo elemento neutro por el Lema 1.18. □

Recíprocamente dado un 1-cociclo biyectivo podemos obtener una braza identificando ambos grupos via la biyección del cociclo.

Proposición 1.24 (Cedó–Jespers–Okniński)**.** *Dado un 1-cociclo biyectivo π de un grupo $(G, \cdot)$ en un grupo abeliano $(A, +)$, la operación $\circ : A \times A \to A$ definida por*

$$a \circ b = \pi(\pi^{-1}(a) \cdot \pi^{-1}(b)),$$

determina la estructura multiplicativa de una braza en A con estructura aditiva $(A, +)$.

Demostración. Dados $a, b, c \in A$ tenemos

$$\begin{aligned} a \circ (b+c) &= \pi(\pi^{-1}(a) \cdot \pi^{-1}(b+c)) \\ &= \pi(\pi^{-1}(a)) + \pi^{-1}(a) \cdot \pi(\pi^{-1}(b+c)) \\ &= \pi(\pi^{-1}(a)) + \pi^{-1}(a) \cdot (b+c) \\ &= \pi(\pi^{-1}(a)) + \pi^{-1}(a) \cdot b + \pi^{-1}(a) \cdot c. \end{aligned}$$

Reescribiendo b como $\pi(\pi^{-1}(b))$ podemos agrupar los primeros dos términos y usar la condición de cociclo para obtener la operación $\circ$,

$$\begin{aligned} a \circ (b+c) &= (\pi(\pi^{-1}(a)) + \pi^{-1}(a) \cdot \pi(\pi^{-1}(b))) + \pi^{-1}(a) \cdot c \\ &= \pi(\pi^{-1}(a) \cdot \pi^{-1}(b)) + \pi^{-1}(a) \cdot c \\ &= a \circ b + \pi^{-1}(a) \cdot c. \end{aligned}$$

Luego podemos sumar y restar a, reescribir uno de estos junto con c y procediendo de la misma forma de antes se obtiene el resultado que queremos. □

Observación 1.25. *Notemos al identificar la acción usada en el dato del* 1*-cociclo coincide con la acción* λ *de la braza al identificar ambos grupos via el* 1*-cociclo.*

Observación 1.26. *Con la definición apropiada de morfismos entre* 1*-cociclos biyectivos esta correspondencia entre* 1*-cociclos y brazas resulta funtorial, y entonces una equivalencia entre las categorías correspondientes.*

Los subconjuntos de una braza invariantes por la acción λ resultan interesantes de considerar. El siguiente resultado sobre conjuntos de generadores invariantes por la acción va a resultar útil más adelante.

Proposición 1.27. *Sea* $(B, +, \circ)$ *una braza y* $X \subseteq B$ *un subconjunto que es invariante por la acción* λ *y que genera el grupo aditivo de la braza. Entonces* X *genera también el grupo multiplicativo de la braza.*

Demostración. Usando la Proposición 1.23 vamos a probar que el grupo generado aditivamente está incluido en el grupo generado multiplicativamente por inducción en la longitud de una palabra (en el grupo aditivo). Si $b \in \langle X \rangle_+$ admite una representación de longitud 1 es porque es un elemento de X, y

por lo tanto pertenece a $\langle X\rangle_\circ$. Si ahora $b = x_1 + \cdots + x_n$, entonces por la Proposición 1.23 tenemos

$$\begin{aligned} b &= x_1 + \cdots + x_n \\ &= x_1 \circ \lambda_{x_1}^{-1}(x_2 + \cdots + x_n) \\ &= x_1 \circ (\lambda_{x_1}^{-1}(x_2) + \cdots + \lambda_{x_1}^{-1}(x_n)). \end{aligned}$$

Como X es invariante por la acción λ la expresión dentro del paréntesis en la última línea es una suma de $n-1$ términos de X, y por lo tanto lo que queremos demostrar se sigue por inducción. □

Dar una noción apropiada de *ideal* para brazas también requiere considerar subconjuntos invariantes por la acción λ.

Definición 1.28. Dada una braza $(B, +, \circ)$, decimos que un subconjunto $I \subseteq B$ es un *ideal* de B si

1. es un subgrupo normal de $(B, \circ)$,
2. para todo $x \in B$ se cumple que $\lambda_x(I) \subseteq I$.

Proposición 1.29 (Cedó–Jespers–Okniński)**.** *Sea $(B, +, \circ)$ una braza. Un subconjunto $I \subseteq B$ es un ideal si y sólo si es el núcleo de un morfismo de brazas.*

Demostración. Sea $f : B \to B'$ un morfismo de brazas en una braza B'. Como f es morfismo del grupo multiplicativo su núcleo es normal en $(B, \circ)$. Para verificar la segunda condición tomemos $a \in B$ y $x \in \mathrm{Ker}(f)$. Aplicando f a $\lambda_a(x)$, y como f es morfismo de ambas estructuras, tenemos

$$f(\lambda_a(x)) = f(a \circ x - a) = f(a) \circ f(x) - f(a) = f(a) - f(a) = 0,$$

de modo que el núcleo de f resulta invariante para la acción λ y por lo tanto un ideal.

Recíprocamente si I es un ideal de B por la Proposición 1.23 como I es un subgrupo mulitplicativo e invariante por la acción λ resulta un también subgrupo de la estructura aditiva, y como esta es abeliana es automáticamente normal. Necesitamos verificar que los cocientes por I para ambas estructuras

coinciden, i.e. que las coclases aditivas y multiplicativas de I coinciden. En tal caso el conjunto de coclases hereda ambas estructuras de grupo y estas satisfacen automáticamente la condición de braza.

Sean $a, b \in B$ elementos de la misma coclase multiplicativa, i.e. $a = b \circ j$ para algún $j \in I$. Tenemos entonces por la Proposición 1.23 que

$$a = b \circ j = b + \lambda_b(j).$$

Como I es invariante por la acción λ esto quiere decir que a y b también pertenecen a la misma coclase aditiva. Recíprocamente si a y b pertencen a la misma coclase aditiva usando la Proposición 1.23 tenemos

$$a = b + j = b \circ \lambda_b^{-1}(j)$$

y tenemos que a y b pertenecen también a la misma coclase multiplicativa. Tenemos entonces que una braza cociente bien definido, y la función cociente es un morfismo de brazas con núcleo I. □

El siguiente ideal definido para toda braza resulta particularmente importante.

Definición 1.30. Dado una braza $(B, +, \circ)$, definimos su *zócalo* como el núcleo del morfismo λ, i.e.

$$\mathrm{Soc}(B) = \{b \in B | \forall x \in B \, \lambda_b(x) = x\}.$$

Observación 1.31. *La condición de que b esté en el sócalo es las funciones de multiplicación y suma por b coincidan, i.e. para todo $a \in B$ se tiene $b \circ a = b + a$.*

Proposición 1.32 (Cedó–Jespers–Okniński)**.** *Sea $(B, +, \circ)$ una braza, su sócalo,* $\mathrm{Soc}(B)$*, resulta un ideal.*

Demostración. Como el sócalo es el núcleo de la acción por λ es un subgrupo normal de la estructura multiplicativa. Para ver que el sócalo es un ideal sólo hay que probar que es invariante por la acción λ.

Dados elementos $a \in B$ y $b \in \mathrm{Soc}(B)$ tenemos

$$\lambda_a(b) = a \circ b - a = 0 + a \circ b - a = a \circ (b + a^{-1}).$$

Por la observación 1.31 esta última expresión puede reescribirse como

$$\lambda_a(b) = a \circ (b \circ a^{-1}),$$

y como el sócalo es normal en $(B, \circ)$ este elemento pertenece nuevamente al sócalo. □

1.4. Brazas y la Ecuación de Yang–Baxter

La primera relación que se puede obtener entre soluciones a la ecuación de Yang–Baxter y brazas es que toda braza resulta ser también una solución.

Proposición 1.33 (Cedó–Jespers–Okniński)**.** *Dada una braza* $(B, +, \circ)$ *definimos* $r : B \times B \to B \times B$ *por*

$$r(a, b) = (\lambda_a(b), \rho_b(a)), \tag{1.6}$$

donde $\rho_b(a) = \lambda_{\lambda_a^{-1}(b)}(a)$*. Con esta definición* (B, r) *es una solución de la ecuación de Yang–Baxter.*

Demostración. Ver [16, Lemma 4.1]. □

El resultado anterior se puede ver también en [36, Sección 2], en ese caso utilizando el lenguaje de *cycle-sets*, que resultan equivalentes a nuestras soluciones.

Observemos que el grupo de permutaciones de la solución definida en la Proposición 1.33 es precisamente la imagen de la acción λ. El núcleo de este morfismo es por definición precisamente el sócalo de la braza B, de modo que podemos transportar la estructura aditiva de B al grupo de permutaciones. Resulta entonces que en este caso tenemos una estructura natural de braza en el grupo de permutaciones.

Esto resulta ser cierto en general, y se debe a que el grupo de estructura de cualquier solución tiene una estructura natural de braza, y la inclusión de la solución en su grupo de estructura resulta ser de hecho universal. Para describir esta estructura de braza lo más cómodo resulta darla en términos de 1-cociclos biyectivos.

Dada una solución (X, r), consideramos la braza que tiene como estructura multiplicativa $(G, \circ) = G(X, r)$ y la estructura aditiva dada por el grupo abeliano libre generado por X, i.e. $\mathbb{Z}^X$. Como el grupo de estructura actúa en X por la Proposición 1.11, podemos considerar como acción por automorfismos la extensión lineal a $\mathbb{Z}^X$ de esta acción.

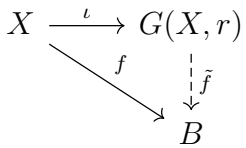
Lo único que resta por definir es al biyección entre los dos grupos. La definición de este morfismo es bastante complicada, aunque podemos describirlo de manera bastante sencilla. Como ambos grupos están generados por los elementos de X podemos definir $\pi : X \to \mathbb{Z}^X$ simplemente como la función identidad. Luego usando la condición de cociclo, ecuación (1.5), podemos extender esto a palabras de longitud arbitraria garantizando obtener un cociclo. Observamos que esto no es una buena definición, ya que a priori no es claro que la "inclusión" de X en $G(X, r)$ sea inyectiva, que la extensión que queremos hacer de una función bien definida, y también habría que chequear la biyectividad de la misma. Está construcción puede verse con detalle en la segunda sección de [25].

Teorema 1.34 (Etingof–Schedler–Soloviev)**.** *Sean (X, r) una solución de la ecuación de Yang–Baxter y $\cdot : G(X, r) \times \mathbb{Z}^X \to \mathbb{Z}^X$ la extensión lineal de la acción del $G(X, r)$ en X. Existe una biyección $\pi : G(X, r) \to \mathbb{Z}^X$, que es la identidad al restringirlo a X, que es un 1-cociclo biyectivo.*

Demostración. Ver [25, Sección 2]. □

La estructura de braza obtenida de este modo, junto con la función de inclusión de la solución en el grupo de estructura, resulta además universal entre todas los morfismos de soluciones que salen de X y llegan a brazas.

Teorema 1.35 (Rump)**.** *Sean (X, r) una solución y $\iota : X \to G(X, r)$ la inclusión natural de X en el grupo de estructura. Para todo morfismo de soluciones $f : X \to B$ con $(B, +, \circ)$ una braza, usando la estructura de solución definida en la Proposición 1.33, existe un único morfismo de brazas $\tilde{f} : G(X, r) \to B$, tal que $\tilde{f} \circ \iota = f$, i.e. tal que el siguiente diagrama conmuta*



Demostración. Ver [36, Proposition 1]. □

A partir de esta estructura de braza en el grupo de estructura podemos entonces obtener una estructura de braza en el grupo de permutaciones de una solución general de la misma forma que se obtiene en el caso de las brazas.

Corolario 1.36. *Sea (X, r) una solución de la ecuación de Yang–Baxter. El grupo de permutaciones $\mathcal{G}(X, r)$ de la solución hereda una estructura de braza de $G(X, r)$ a través del morfismo definido en la Proposición 1.11.*

Demostración. El mapa definido en la Proposición 1.11 es un morfismo de grupos para la estructura multiplicativa de la braza. Para ver que le da a $\mathcal{G}(X, r)$ una estructura de braza alcanza con ver que su núcleo es ideal.

Por definición, el núcleo del morfismo que estamos mirando es el núcleo de la acción del grupo de estructura en el conjunto subyacente de la solución. Como la acción λ dada por el Teorema 1.34 es la extensión lineal de la acción en X, tenemos que el núcleo del morfismo al grupo de permutaciones es exactamente el sócalo de la estructura de braza del grupo de estructura. Como el sócalo es un ideal esto prueba lo que queríamos. □

En particular tenemos que la función $X \to \mathcal{G}(X, r)$, $x \mapsto \sigma_x$ es un morfismo de soluciones, y por lo tanto el conjunto de las permutaciones σ_x es una subsolución de $\mathcal{G}(X, r)$. Esto lleva a la siguiente definición.

Definición 1.37. Dada (X, r) una solución de la ecuación de Yang–Baxter, su *retracción* es la solución $\mathrm{Ret}(X, r) = \{\sigma_x\}_{x \in X}$. Decimos que la solución es irretractable si $\mathrm{Ret}(X, r)$ es isomorfa a X, es decir si la función natural $X \to \mathrm{Ret}(X, r)$ es inyectiva, y decimos que es retractable en caso contrario.

Una solución se dice multipermutación si existe $k \in \mathbb{N}$ tal que $\mathrm{Ret}^k(X, r)$ es una solución de tamaño 1, donde Ret^k está definido recursivamente por

$$\mathrm{Ret}^0(X, r) = (X, r)$$

$$\mathrm{Ret}^{k+1}(X, r) = \mathrm{Ret}(\mathrm{Ret}^k(X, r)).$$

En tal caso el menor valor de k para el que esto sucede se llama el nivel de multipermutación de la solución.

1.4.1. Construcción de Bachiller-Cedó-Jespers

En esta sección vamos a describir los resultados de [8] que necesitaremos en el Capítulo 4. Dada una braza B fija, en este paper se da una descripción de todas las soluciones X que tienen a B como braza de permutaciones. El primero de los resultados describe como construir las soluciones que se buscan a partir de un dato de órbitas y subgrupos de la braza.

Teorema 1.38 (Bachiller-Cedó-Jespers)**.** *Sea $(B, +, \circ)$ una braza y λ la acción del grupo multiplicativo en el grupo aditivo. Notemos $\mathcal{O}$ al conjunto de órbitas de la acción λ, y para cada $O \in \mathcal{O}$ fijemos $a_O \in O$. Para cada tripla $(I, \mathcal{J}, \mathcal{K})$ que satisfaga*

1. *$I \subseteq \mathcal{O}$ es un subconjunto de órbitas tal que su unión genera el grupo aditivo de B,*
2. *$\mathcal{J} = \{J_i\}_{i\in I}$ es una familia de conjuntos no vacíos indexados por las órbitas de I,*
3. *$\mathcal{K} = \{K_{i,j}\}_{i\in I, j\in J_i}$ es una familia indexada de subgrupos de $(B, \circ)$,*
4. *para todo $i \in I$ y $j \in J_i$ se tiene que $K_{i,j} \subseteq st(a_i)$, el estabilizador de a_i por la acción λ,*
5. *la intersección de todos los interiores normales de los subgrupos que pertenecen a $\mathcal{K}$ es trivial, i.e. $\bigcap_{i\in I}\bigcap_{j\in J_i} \mathrm{core}(K_{i,j}) = 1$,*

se tiene en el conjunto

$$X = \bigsqcup_{i\in I}\bigsqcup_{j\in J_i} B/K_{i,j},$$

una estructura de solución de la ecuación de Yang–Baxter, cuya función r queda definida por las funciones σ siguientes,

$$\sigma_{bK_{i,j}}(b'K_{i',j'}) = (\lambda_b(a_i) \circ b')K_{i',j'}.$$

Más aún cualquier solución de la ecuación de Yang–Baxter que tenga braza de permutaciones isomorfa a $(B, +, \circ)$ es isomorfa a una solución de las anteriores.

Definición 1.39. Dados un grupo G y un subgrupo $H < G$, llamamos *interior normal* de H , y lo notamos $\mathrm{core}(H)$, al núcleo del morfismo dado por la multiplicación a izquierda de G en G/H. Concretamente tenemos

$$\mathrm{core}(H) = \bigcap_{g \in G} gHg^{-1}.$$

Uno puede presentar este mismo resultado usando para la construcción un dato más compacto de la siguiente manera

Teorema 1.40 (Bachiller–Cedó–Jespers)**.** *Sean $(B, +, \circ)$ una braza e I un conjunto. Para cada $i \in I$ sea x_i un elemento de B tal que la unión de todas las órbitas $\{\lambda_b(x_i) | b \in B\}$ generan el grupo aditivo de la braza. Por último para cada i sea K_i un subgrupo del estabilizador de x_i tales que la intersección de todos sus interiores normales es trivial, i.e.*

$$\bigcap_{i \in I} \bigcap_{b \in B} b \circ K_i \circ b^{-1} = \{1\}.$$

Se tiene entonces que el conjunto $X = \bigsqcup_{i \in I} B/K_i$ es una solución de la ecuación de Yang–Baxter con las funciones σ dadas por

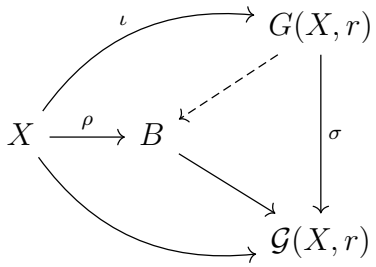
$$\sigma_{aK_i}(bK_j) = (\lambda_a(x_i) \circ b)K_j.$$

Más aún, toda solución de la ecuación de Yang–Baxter con braza de permutaciones isomorfo a $(B, +, \circ)$ es isomorfa a una de esta forma.

La siguiente observación sobre el resultado anterior va a resultar importante para poder analizar algunas propiedades de las soluciones en terminos de los datos de construcción.

Observación 1.41. *Siguiendo las demostraciones de [8] y [6] se puede ver que en el teorema anterior las condiciones de que las órbitas consideradas generen el grupo aditivo de la braza y que la intersección de los interiores normales de los subgrupos sean triviales son importantes sólo para poder garantizar que la braza que se obtiene sea exactamente el original. En particular si tomamos un dato como el anterior pero que no satisface estas condiciones obtenemos una*

solución (X, r), para la cual el morfismo natural de la braza de estructura en la braza de permutaciones factoriza por B como en el siguiente diagrama



donde la función ρ está dada por

$$\rho(bK_i) = \lambda_b(a_i),$$

y la función $B \to \mathcal{G}(X, r)$ es la dada por la acción natural de multiplicación a izquierda en el cociente.

De esta forma la imagen del morfismo $G(X, r) \to B$ está dada por el subgrupo aditivo generado por lás órbitas del dato, y la intersección de los interiores normales caracteriza el núcleo del morfismo $B \to \mathcal{G}(X, r)$. Por lo tanto las condiciones del teorema son las que garantizan que este último morfismo sea un isomorfismo. En general sin embargo la braza de permutaciones de la solución obtenida resulta un subcociente de la braza original B.

Las soluciones determinadas por datos distintos pueden en principio ser isomorfas. El segundo resultado de Bachiller, Cedó y Jespers caracteriza cuando sucede esto en términos de los automorfismos de la braza B.

Teorema 1.42 (Bachiller–Cedó–Jespers)**.** *Sean $(B, +, \circ)$ una braza y $(a_i, K_i)_{i\in I}$ y $(b_j, K'_j)_{j\in J}$ dos datos como los del Teorema 1.38. Las soluciones asociadas a estos dos datos son isomorfas si y sólo si existe una biyección $\phi : I \to J$, un automorfismo de brazas $\psi : B \to B$ y elementos $(z_i)_{i\in I}$ tales que $\psi(a_i) = \lambda_{z_i}(b_{\phi(i)})$ y $\psi(K_i) = z_i \circ K'_{\phi(i)} \circ z_i^{-1}$.*

Capítulo 2

El invariante diagonal

En este capítulo vamos a presentar los resultados de [34]. El punto de partida de los mismos es la demostración en [35] de una conjetura de Gateva-Ivanova, que afirma que toda solución *libre de cuadrados*, y de tamaño mayor que 1, es descomponible.

Definición 2.1. Una solución de la ecuación de Yang–Baxter, (X, r) se dice *libre de cuadrados* si satisface $r(x, x) = (x, x)$ para todo $x \in X$.

En los resultados de este capítulo interpretamos la condición de ser libre de cuadrados en términos del *invariante diagonal* de las soluciones y damos demostraciones de resultados similares de descomponibilidad para otros valores del invariante.

Los resultados preliminares de la Sección 2.1 son resultados conocidos previamente. Las secciones siguientes contienen los resultados y observaciones originales que se encuentran publicados en [34].

2.1. El invariante diagonal

Definición 2.2. Dada una solución (X, r) definimos las funciones $T, U : X \to X$ como $T(y) = \tau_y^{-1}(y)$ y $U(x) = \sigma_x^{-1}(x)$.

Ejemplo 2.3. En el caso de las soluciones de Lyubashenko, Ejemplo 1.6, tenemos que la funciones T y U son respectivamente las funciones σ y τ que definen la solución.

Estas definiciones pueden interpretarse en términos de los elementos fijos por la función r, lo que permite deducir rápidamente varias propiedades de estas funciones.

Proposición 2.4. *Dada (X, r) una solución de la ecuación de Yang–Baxter, $x, y \in X$ tenemos que $y = U(x)$ $(x = T(y))$, si y sólo si y (resp. x) es el único elemento tal que $r(x, y) = (x, *)$, i.e. $r(x, y)$ tiene al elemento x en la primer componente y cualquier otro elemento en la segunda, (resp. $r(x, y) = (*, y)$). Más aún ambas condiciones se cumplen si y sólo si $r(x, y) = (x, y)$.*

Demostración. Observemos que pedir que $r(x, y) = (x, z)$ para algún $z \in X$, es equivalente a pedir $\sigma_x(y) = x$, es decir $y = U(x)$. Por otro lado como $r^2 = \mathrm{id}$ tenemos que $(x, y) = r^2(x, y) = r(x, z)$, y por lo tanto tenemos que $z = U(x) = y$.

El caso de la función T es completamente análogo. □

En particular esta caracterización nos permite ver que estas funciones son invertibles.

Corolario 2.5. *Las funciones T y U son inversas mutuas.*

Como estás dos funciones resultan inversas una de la otra tienen descomposiciones en ciclos disjuntos con la misma cantidad de ciclos de cada longitud. En particular esto nos provee de un invariante numérico asociado a la solución.

Definición 2.6. Dada una solución de la ecuación de Yang–Baxter (X, r) definimos su *invariante diagonal* como la partición asociada a la descomposición en ciclos disjuntos de su función T, o equivalentemente U.

Proposición 2.7. *Sea (X, r) una solución de la ecuación de Yang–Baxter. Para cada $x \in X$ tenemos que*

$$\mathrm{T} \circ \sigma_x \circ \mathrm{T}^{-1} = \tau_x^{-1}$$

Demostración. Necesitamos probar que $T \circ \sigma_x = \tau_x^{-1} \circ T$. Evaluando en y el lado derecho de esta identidad tenemos

$$\begin{aligned} \tau_x^{-1}(T(y)) &= \tau_x^{-1} \circ \tau_y^{-1}(y) \\ &= (\tau_y \circ \tau_x)^{-1}(y). \end{aligned}$$

Utilizando la tercera identidad del Lema 1.2 podemos reescribir la última línea

$$\begin{aligned}\tau_x^{-1}(T(y)) &= (\tau_{\tau_y(x)} \circ \tau_{\sigma_x(y)})^{-1}(y) \\ &= \tau_{\sigma_x(y)}^{-1}(\tau_{\tau_y(x)}^{-1}(y)).\end{aligned}$$

Para calcular $\tau_{\tau_y(x)}^{-1}(y)$, observemos que estamos en una situación como la de la figura 2.1. En este caso el diagrama se puede completar poniendo $\sigma_x(y)$ y x en los extremos superior e inferior izquierdos respectivamente. Por el Lema 1.15, esta es la única forma de completar el diagrama de modo que tenemos

$$\begin{aligned}\tau_x^{-1}(T(y)) &= \tau_{\sigma_x(y)}^{-1}(\sigma_x(y)) \\ &= T(\sigma_x(y)).\end{aligned}$$

□

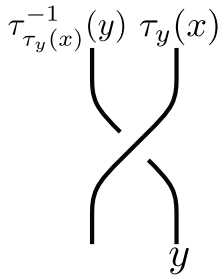


Figura 2.1: Diagrama Proposición 2.7.

Corolario 2.8. *Sea (X, r) una solución y definamos*

$$\tilde{\mathcal{G}}(X, r) = \langle \tau_x |\ x \in X \rangle \subseteq \mathrm{Sym}(X).$$

Entonces $\tilde{\mathcal{G}}(X, r)$ y $\mathcal{G}(X, r)$ son isomorfos como grupos de permutaciones.

2.2. Resultados sobre descomponibilidad

En esta sección veremos como el analisis combinatorio del invariante diagonal de una solución permite obtener resultados sobre la descomponibilidad de la misma. La primera observación importante es que una descomposición de la solución no puede "partir" los ciclos del invariante diagonal.

Lema 2.9. *Sea (X, r) una solución de la ecuación de Yang–Baxter. Cada órbita de la acción de $\mathcal{G}(X, r)$ en X es una unión disjunta de órbitas de la función T.*

Demostración. Basta ver que x y $T(x)$ pertenecen a la misma órbita de la acción de $\mathcal{G}(X, r)$, para todo $x \in X$, de donde se sigue lo que queremos por inducción. Por el Corolario 2.5 sabemos que las funciones T y U son inversas mutuas, por lo tanto basta ver que x y $U(x)$ están en la misma órbita. Ahora, tenemos que $U(x) = \sigma_x^{-1}(x)$, y por lo tanto estos dos elementos pertenecen a una misma órbita. □

En particular obtenemos el primer resultado de indescomponiblidad

Corolario 2.10. *Sea (X, r) una solución de la ecuación de Yang–Baxter. Si su invariante diagonal es un ciclo de longitud máxima, i.e. $|X|$, entonces la solución es indescomponible.*

Ejemplo 2.11. Dado $n \in \mathbb{N}$ siempre podemos obtener una solución de tamaño n cuyo invariante diagonal es un ciclo de longitud n tomando la solución cíclica de tamaño n.

Los siguientes resultados que podemos obtener de manera elemental cubren casos en los que el invariante diagonal tiene algún punto fijo. El siguiente resultado nos permite en tales casos obtener una relación más directa entre el invariante diagonal y el grupo de permutaciones.

Lema 2.12. *Sean (X, r) una solución de la ecuación de Yang–Baxter, y $x \in X$ tal que $T(x) = x$. Entonces para todo $y \in Y$ se tiene*

$$T(\tau_y(x)) = \tau_{\sigma_x(y)}(x).$$

Demostración. Evaluando ambos lados de la ecuación de Yang–Baxter en la tripla (x, x, y), y recordando que por la Proposición 2.4 $r(x, x) = (x, x)$, obtenemos del lado izquierdo

$$\begin{aligned}(r \times \mathrm{id})(\mathrm{id} \times r)(r \times \mathrm{id})(x, x, y) &= (r \times \mathrm{id})(\mathrm{id} \times r)(x, x, y) \\ &= (r \times \mathrm{id})(x, \sigma_x(y), \tau_y(x)) \\ &= (\sigma_x(\sigma_x(y)), \tau_{\sigma_x(y)}(x), \tau_y(x)).\end{aligned}$$

Y evaluando del lado derecho obtenemos

$$\begin{aligned}(\mathrm{id}\times r)(r\times\mathrm{id})(\mathrm{id}\times r)(x,x,y) &= (\mathrm{id}\times r)(r\times\mathrm{id})(x,\sigma_x(y),\tau_y(x))\\ &= (\mathrm{id}\times r)(\sigma_x(\sigma_x(y)),\tau_{\sigma_x(y)}(x),\tau_y(x)).\end{aligned}$$

En particular tenemos que $r(\tau_{\sigma_x(y)}(x),\tau_y(x)) = \tau_{\sigma_x(y)}(x),\tau_y(x)$, y por lo tanto, por la Proposición 2.4, tenemos que $T(\tau_y(x)) = \tau_{\sigma_x(y)}(x)$. □

Este resultado nos permite obtener resultados de descomponibilidad en casos en que el invariante diagonal tenga algún punto fijo y algún ciclo de longitud "suficientemente larga".

Teorema 2.13. *Sea (X,r) una solución de la ecuación de Yang–Baxter de tamaño $n>1$. Si el invariante diagonal es un ciclo de longitud $n-1$, entonces X es descomponible.*

Demostración. Sea $x_0\in X$ tal que $T(x_0)=x_0$, e $Y = X\setminus\{x_0\}$. Supongamos que la solución es indescomponible, y sea $f: Y\to X$ la función dada por $y\mapsto\tau_y(x_0)$. Como X es indescomponible tiene que existir algún $y\in X$, y como $T(x_0)=x_0$ necesariamente en Y, tal que $f(y)\neq x_0$. Fijemos un tal y, i.e. $y\in Y$ tal que $f(y)\in Y$.

Como T es un ciclo de longitud $n-1$ que deja fijo a x_0, debe mover cíclicamente todos los elementos de Y. Tenemos entonces que podemos obtener todos los elementos de Y aplicando iteradamente la función T a $f(y)$, es decir que

$$Y = \{f(y), T(f(y)), T^2(f(y)),\ldots,T^{n-2}(f(y))\}.$$

Dado $z\in Y$, aplicando el Lema 2.12 obtenemos

$$T(f(z)) = T(\tau_z(x_0)) = \tau_{\sigma_{x_0}(z)(x_0)} = f(\sigma_{x_0}(z).$$

Por lo tanto podemos escribir a Y como

$$Y = \{f(y), f(\sigma_{x_0}(y)),\ldots,f(\sigma_{x_0}^{n-2}(y))\}.$$

En particular todos los elementos anteriores deben ser distintos, y por lo tanto todos los elementos $y,\sigma_{x_0}(y),\ldots,\sigma_{x_0}^{n-2}(y)$, deben ser todos elementos distintos. Esto quiere decir que la permutación σ_{x_0} debe permutar cíclicamente todos los elementos de Y.

Afirmamos que esto implica que la acción del grupo de permutaciones es primitiva. En efecto supongamos que no y sea B un bloque no trivial que contenga a x_0. Como $\sigma_{x_0}(x_0) = x_0$, ya que $T(x_0) = x_0$, entonces $\sigma_{x_0}(B) = B$. Por otro lado si B es no trivial debe contener algún $z \in Y$, y por inducción usando lo anterior tenemos que $\sigma_{x_0}^k(z) \in B$ para todo $k \in \mathbb{N}$. Ahora por lo visto antes esto quiere decir que $Y \subseteq B$, y por lo tanto $B = X$, contradiciendo la no trivialidad del bloque.

Finalmente por 1.13 esto implica que X es una solución cíclica, lo que contradice el hecho de que su invariante T sea un ciclo de longitud $n-1$. □

Este resultado se puede generalizar con argumentos elementales similares al caso en que el invariante diagonal sea un ciclo de longitud $n-2$ o $n-3$, restringiendo los posibles valores de n. Para esto necesitamos el siguiente lema previo

Lema 2.14. *Sea (X, r) una solución de la ecuación de Yang–Baxter. Si existe $x \in X$ tal que σ_x es un ciclo de longitud por lo menos $|X|/2$ y coprima con $|X|$, entonces la solución es descomponible.*

Demostración. Observemos primero que una solución con estas características no puede ser una solución cíclica, y por lo tanto, por el Teorema 1.13, su grupo de permutaciones no actúa de forma primitiva en la solución. Supongamos que la solución es indescomponible y tomemos $x \in X$ como en el enunciado, $y \in X$ algún punto fijo de σ_x y B algún bloque no trivial que contenga a y.

Como $\sigma_x(y) = y$ tenemos que $\sigma_x(B) = B$. Si B contuviera algún elemento que pertence al ciclo de σ_x debe entonces contenerlos a todos. Pero entonces el bloque sería de tamaño mayor a $|X|/2$, lo que no es posible. Tenemos entonces que B sólo puede contener puntos fijos de σ_x. Como y era arbitrario, esto vale para cualquier bloque que contenga algún punto fijo de σ_x. En particular, como estamos suponiendo que la acción es transitiva, el tamaño de este bloque va a tener que dividir a la cantidad de puntos fijos de σ_x. Como también tiene que dividir a $|X|$ y estos dos números son coprimos el bloque debe ser trivial. □

Teorema 2.15. *Sea (X, r) una solución de tamaño n, entonces*

1. *Si la función T es un ciclo de longitud $n-2$ y n es impar, entonces la solución es descomponible.*

2. *Si la función T es un ciclo de longitud $n-3$ y n es coprimo con 3 entonces la solución es descomponible.*

Demostración. Notamos por m la longitud del ciclo de T, y

$$Y = \{y \in X | T(y) \neq y\}, \quad Z = \{z \in X | T(z) = z\}.$$

Si $X = Y \bigsqcup Z$ es una descomposición de la solución entonces no hay nada que hacer. Si no existen $z \in Z$ y $x \in X$ tales que $\tau_x(z) \in Y$. Como T permuta cíclicamente los elementos de Y, y como z es un punto fijo de T, tenemos al igual que en la demostración anterior que

$$Y = \{\tau_x(z), T(\tau_x(z)), \ldots, T^{m-1}(\tau_x(z))\} = \{\tau_x(z), \tau_{\sigma_z(x)}(z), \ldots, \tau_{\sigma_z^{m-1}(x)}(z)\}.$$

De esto podemos deducir que la descomposición de σ_z en ciclos disjuntos debe contener un ciclo de longitud por lo menos m. Por otro lado como $T^m = \mathrm{id}$ tenemos que para cualquier $x' \in X$ y $k \in \mathbb{N}$ se tiene que

$$T^{k+m}(\tau_{x'}(z)) = T^k(\tau_{x'}(z)),$$

y por lo tanto $\tau_{\sigma_z^{k+m}(x')}(z) = \tau_{\sigma_z^k(x')}(z)$, y m es el mínimo período para esta relación. Por lo tanto el ciclo de σ_z debe tener longitud divisble por m.

Supongamos primero que $2m > n$, en este caso necesariamente se tiene que cumplir que el ciclo tiene longitud exactamente m. Como $z \in Z$ sabemos que $\sigma_z(z) = z$. En el primer caso de los que nos interesan esto implica que σ_z es un ciclo de longitud m, y por el Lema 2.14 esto garantiza que la solución es descomponible. En el segundo caso podría suceder que σ_z sea un producto de un ciclo de longitud m y uno de longitud 2. Analizemos ahora este caso.

Igual que en los otros casos sabemos que el grupo de permutaciones no actúa de forma primitiva por el Teorema 1.13. Tomemos entonces un bloque no trivial que contenga a z. Si este bloque contiene algún elemento de uno de los ciclos de σ_z debe contener también los demas elementos del mismo ciclo, en particular no puede contener elementos del ciclo de longitud m. Por ser un bloque no trivial debe contener entonces a los elementos del ciclo de longitud 2, y entonces el bloque es de tamaño 3. Como $|X|$ es coprimo con 3 esto no puede suceder.

Por último queda analizar los casos en que $2m \leq n$. En el primer caso esto es $n \leq 4$, y en el segundo caso $n \leq 6$. Revisando todas las soluciones de

tamaño menor o igual a 6 en la base de datos de GAP se puede verificar que todas satisfacen el resultado. □

También podemos obtener un resultado similar al Lema 2.14 que garantiza la descomponibilidad de una solución dependiendo de la existencia de alguna función τ con propiedades particulares. Este resultado nos permite obtener como corolario que cuando el grupo de permutaciones actúa regularmente en X la solución resulta necesariamente retractable.

Teorema 2.16. *Sea (X, r) una solución de la ecuación de Yang–Baxter, tal que $|X| > 1$. Si existe $x \in X$ tal que $\tau_x = \mathrm{id}$ entonces X es descomponible.*

Demostración. Dado $x \in X$ tal que $\tau_x = id$, y $y, z \in X$ arbitrarios consideramos la ecuación de Yang–Baxter aplicada a la terna (z, y, x). Mirando sólo la última coordenada obtenemos,

$$\tau_y(\tau_{\sigma_y(x)}(z)) = \tau_y(z).$$

Como las funciones τ son biyectivas esto implica $\tau_{\sigma_y(x)}(z) = z$. Como y y z son arbitrarios, esto quiere decir que si $\tau(x) = \mathrm{id}$ entonces para todo $y \in X$ se tiene que $\sigma_y(x)$ también cumple esto. En particular toda la órbita de x por la acción del grupo de permutaciones debe tener $\tau = \mathrm{id}$, por lo tanto la solución solo puede ser indescomponible si $|X| = 1$. □

Corolario 2.17. *Sea (X, r) una solución de la ecuación de Yang–Baxter con $|X| > 1$. Si $\mathcal{G}(X, r)$ actúa regularmente en X, entonces la solución es retractable.*

Demostración. Recordemos primero que la acción de un grupo G en un conjunto X se dice regular si y sólo si para todo par $x, y \in X$ existe un único $g \in G$ tal que $g \cdot x = y$. En particular sabemos que si $\mathcal{G}(X, r)$ actúa regularmente en X entonces $|\mathcal{G}(X, r)| = |X|$.

Por otro lado si la acción es regular, entonces también es transitiva, y por lo tanto sabemos que la solución es indescomponible. Luego por el Teorema 2.16 ninguno de los τ_x puede ser la identidad, y como $|\mathcal{G}(X, r)| = |X|$ tiene que haber dos elementos $x, y \in X$ tal que $\tau_x = \tau_y$, es decir que la solución es retractable. □

2.3. Resultados computacionales

En esta sección recolectamos algunas observaciones relacionadas con los resultados de este capítulo obtenidas al analizar la base de datos de soluciones de tamaño menor o igual a 10 de [3] en GAP.

En el Ejemplo 2.11 observamos que para todo n se puede obtener una solución que satisface las hipótesis del Corolario 2.10 tomando la solución cíclica de ese tamaño. Cuando n es un número primo esta solución es la única solución indescomponible de este tamaño, [25]. Sin embargo cuando n no es primo hay en general más soluciones con este invariante diagonal.

Ejemplo 2.18. Consideremos la solución con ID $[4, 19]$ en la base de datos del paquete de Yang–Baxter de GAP. Esta está es la solución en el conjunto $\{1, 2, 3, 4\}$ dada por tomar

$$\begin{aligned} &\sigma_1 = (14), && \sigma_2 = (1243), && \sigma_3 = (23), && \sigma_4 = (1342), \\ &\tau_1 = (12), && \tau_2 = (1324), && \tau_3 = (34), && \tau_4 = (1423). \end{aligned}$$

Esta solución tiene invariante T igual a la permutación (1234), pero no es una solución cíclica.

Analizando la base de datos completa se puede encontrar la cantidad total de soluciones de este tipo para cada n menor o igual 10. En el cuadro 2.1 se puede ver la cantidad de soluciones indescomponibles con cada invariante diagonal de tamaño menor o igual a 10, cuando n es un número primo sabemos que hay una única solución indescomponible y por lo tanto estos casos no aparecen en la tabla. En particular vemos que en todos los casos tenemos más de una solución con invariante diagonal un ciclo de longitud máxima.

Resulta natural preguntarse si los resultados de los Teoremas 2.13 y 2.15 pueden generalizarse a resultados que sólo miren la cantidad de puntos fijos del invariante T. Analizando las soluciones de tamaño menor o igual a 10 vemos que es cierto que todas las soluciones que tienen un único punto fijo resultan descomponibles, hay soluciones de tamaño 4, 8 y 9 cuyo invariante diagonal tiene más de un punto fijo.

Ejemplo 2.19. Consideremos la solución con ID $[4, 13]$. Esta es la solución (X, r) con $X = \{1, 2, 3, 4\}$ y r dada por las siguientes funciones σ:

$$\sigma_1 = (34), \quad \sigma_2 = (1324), \quad \sigma_3 = (1423), \quad \sigma_4 = (12). \tag{2.1}$$

Tamaño	# Soluciones	Invariante Diagonal
4	3	4
	1	2
	1	2,2
6	6	6
	3	3,3
	1	2,2,2
8	7	2,2
	25	2,2,2,2
	2	2,2,4
	1	2,6
	14	8
	51	4,4
9	1	3,3
	6	3,3,3
	9	9
10	1	2,2,2,2,2
	15	5,5
	20	10

Cuadro 2.1: Cantidad de soluciones indescomponibles con invariante diagonal dado.

Esta solución resulta indescomponible y su función U es la permutación (23), que tiene dos puntos fijos. Como se puede ver en el cuadro 2.1 esta es la única solución con estas propiedades de tamaño 4.

Ejemplo 2.20. Consideremos la solución con ID $[8, 13881]$. Esta es la solución (X, r) con $X = \{1, 2, \ldots, 8\}$ y r dada por las siguientes funciones σ:

$$\sigma_1 = (45) \qquad \sigma_2 = (36), \qquad \sigma_3 = (27),$$
$$\sigma_4 = (18), \qquad \sigma_5 = (13428657), \qquad \sigma_6 = (17568243),$$
$$\sigma_7 = (12468753), \qquad \sigma_8 = (13578642).$$

Esta solución resulta indescomponible y su función U es la permutación (56)(78), que tiene cuatro puntos fijos. Como se puede ver en el cuadro 2.1

hay otras seis soluciones con estas propiedades. Estas son las soluciones con ID $[8, 15578]$, $[8, 15579]$, $[8, 15580]$, $[8, 15584]$, $[8, 15585]$ y $[8, 15586]$.

El único otro tamaño en el que se encuentran soluciones cuya función U tiene algún punto fijo es en tamaño 9, que es al igual que en los ejemplos anteriores, una potencia de un primo. En este caso, al igual que en el primero hay una única solución con estas características. Estas observaciones sugieren las siguientes conjeturas.

Conjetura 2.21. *Si (X, r) es una solución cuya función U tiene un único punto fijo, entonces la solución es descomponible.*

Conjetura 2.22. *Si (X, r) es una solución indescomponible y $|X|$ es libre de cuadrados, entonces su función U no tiene ningún punto fijo.*

Conjetura 2.23. *Para cada primo p se tiene una única solución indescomponible de tamaño p^2 cuya función U tiene puntos fijos, más aún esta solución tiene exactamente p puntos fijos.*

Conjetura 2.24. *Para cada primo p hay una única solución indescomponible de tamaño $2p$ cuya función U es un producto de p transposiciones.*

Un resultado en una dirección similar a estas fue obtenido recientemente por Castelli y Kanrar en [13], donde estudian el caso de que el invariante diagonal sea un p-ciclo con p primo. En este paper demuestran que, con la hipótesis adicional de que el tamaño de la solución sea una potencia de p o que el grupo de permutaciones sea nilpotente, las únicas soluciones indescomponibles de este tipo tienen tamaño 2 ó 4 si $p = 2$, o tamaño p si este es un primo impar.

Es también natural preguntarse si se pueden obtener criterios de descomponibilidad similares al Lema 2.14 y al Teorema 2.16 que miren el valor de alguna permutación τ. Analizando la base de datos por ejemplo se puede observar lo siguiente

Observación 2.25. *Todas las soluciones, (X, r), con $|X| \leq 10$ cumplen que si existe algún $x \in X$ tal que alguno de los ciclos de τ_x tiene longitud coprima con $|X|$, entonces la solución es descomponible.*

Esta observación sin embargo no puede extenderse a un resultado general. En [28] Kanrar y Rump construyen una familia de soluciones cuyos tamaños son potencias de 2, pero que contienen un elemento cuya permutación asociada tienen un ciclo de longitud impar. Sin embargo si se ha podido demostrar que esta condición sobre las permutaciones garantiza la descomponibilidad de las mismas si satisfacen algunas condiciones adicionales. Castelli lo probó para soluciones que sean multipermutación en [12], y Cedó y Okniński lo probaron para soluciones cuyo tamaño es libre de cuadrados en [19].

Observación 2.26. *Analizando con más detalle la base de datos se puede observar que en todas las soluciones indescomponibles de tamaño menor o igual a 10 se cumple que el orden de la función T divide al orden del grupo de permutaciones de la solución. Esto resulta cierto en general aunque no lo podemos demostrar todavía. Con las herramientas de cableado que vamos a desarrollar en el Capítulo 3 lo vamos a poder demostrar, ver Teorema 3.14.*

Capítulo 3

Cableado de soluciones

En este capítulo vamos a exponer los resultados de [32]. El principal resultado de este trabajo fue la introducción del *cableado* de soluciones, que construye a partir de una solución de la ecuación de Yang–Baxter, otras soluciones del mismo tamaño. Utilizando como herramienta esta construcción es posible extender los resultados de indescomponibilidad del Capítulo 2.

3.1. Construcción de Bachiller y Cedó

Como paso intermedio para la construcción del cableado vamos a ver la construcción de Bachiller y Cedó. En [15], Cedó, Jespers y del Río definen, dada una solución X, una estructura de solución en X^2. Esta construcción fue generalizada por Bachiller y Cedó en [7] a la construcción de, para cada $n \in \mathbb{N}$, una estructura de solución en X^n. La descripción de esta solución está dada por el siguiente resultado.

Teorema 3.1 (Bachiller–Cedó)**.** *Sea (X, r) una solución de la ecuación de Yang–Baxter, con $r(x, y) = (\sigma_x(y), \tau_y(x))$. Sea n un entero mayor a 1. Dado $\overline{x} = (x_1, \ldots, x_n) \in X^n$ consideramos la función $f_{\overline{x}} : X^n \to X^n$ definida por*

$$f_{\overline{x}}(\overline{y}) = (h_1(\overline{x}, \overline{y}), \ldots, h_n(\overline{x}, \overline{y})),$$

con las funciones h_j definidas recursivamente por

$$h_1(\overline{x}, \overline{y}) = \sigma_{x_1} \cdots \sigma_{x_n}(y_1)$$

y

$$h_j(\overline{x},\overline{y}) = \sigma^{-1}_{h_{j-1}(\overline{x},\overline{y})} \cdots \sigma^{-1}_{h_1(\overline{x},\overline{y})} \sigma_{x_1} \cdots \sigma_{x_n} \sigma_{y_1} \cdots \sigma_{y_{j-1}}(y_j), \tag{3.1}$$

para $2 \leq j \leq n$. *Entonces* $f_{\overline{x}}$ *es biyectiva y* (X^n, r^n), *con* $r^n : X^n \times X^n \to X^n \times X^n$ *definida por*

$$r^n(\overline{x},\overline{y}) = (f_{\overline{x}}(\overline{y}), f^{-1}_{f_{\overline{x}}(\overline{y})}(\overline{x})),$$

es una solución de la ecuación de Yang–Baxter.

La solución de Bachiller y Cedó puede representarse diagramáticamente como la acción de pasar las hebras en bloques de a n, como se ve en la Figura 3.1. Es claro que la trenza del diagrama define una estructura de solución en X^n.

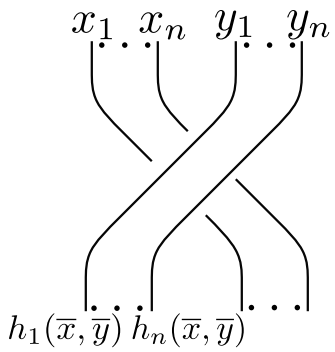


Figura 3.1: Solución de Bachiller-Cedó.

Para ver que esta solución coincide con la definida en el Teorema 3.1 procedemos por inducción. Es claro que h_1 definido de acuerdo al diagrama coincide con la definición del Teorema 3.1. Para h_i con $i > 1$, notamos que el resultado de pasar la i-ésima hebra de $\overline{y}$ como en el diagrama de la Figura 3.1, es equivalente a primero pasar la hebra por delante de las $i-1$ hebras anteriores de $\overline{y}$ y las n hebras de $\overline{x}$, luego pasar las $i-1$ hebras de $\overline{y}$ por delante de las hebras de $\overline{x}$, y finalmente pasar la i-ésima hebra de $\overline{y}$, ahora en el primer lugar, por delante de las $i-1$ hebras de $\overline{y}$. El resultado de este proceso es que en la i-ésima hebra de $\overline{y}$ queda precisamente la definición dada en la ecuación (3.1)

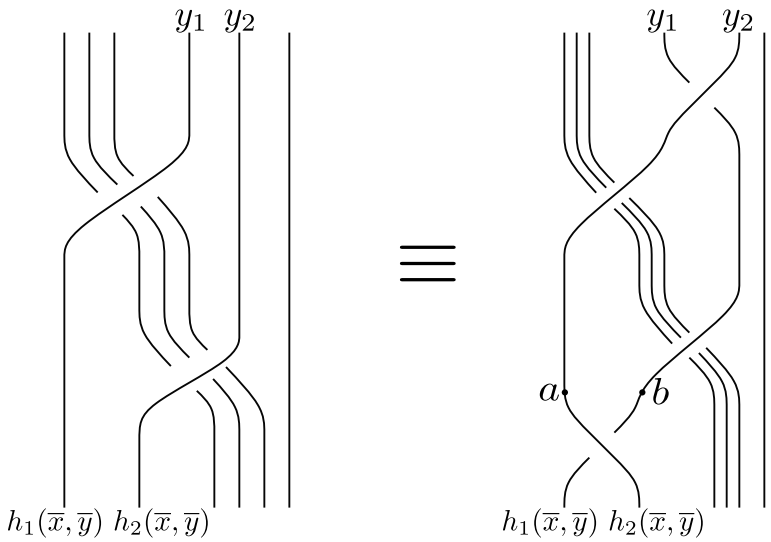


Figura 3.2: Equivalencia para las definiciones de h_2.

Ilustramos este argumento mostrando la equivalencia para h_2 en X^3. Los diagramas equivalentes pueden verse en la Figura 3.2. Tenemos en este caso

$$a = \sigma_{x_1}\sigma_{x_2}\sigma_{x_3}\sigma_{y_1}(y_2),$$

y

$$h_2(\overline{x},\overline{y}) = \tau_b(a).$$

Como X es una solución involutiva tenemos

$$\tau_b(a) = \sigma^{-1}_{\sigma_a(b)}(a) = \sigma^{-1}_{h_1(\overline{x},\overline{y})}(a),$$

que es precisamente la definición del Teorema 3.1.

3.2. Elementos congelados y cableado

Dentro de las soluciones de Bachiller y Cedó podemos identificar a las soluciones cableadas. Consideremos $\overline{x},\overline{y} \in X^n$, y supongamos adicionalmente que $\overline{y}$ es invariante por la acción del grupo de trenzas B_n en X^n. Afirmamos que en esta situación el resultado actuar con $\sigma_{\overline{x}}$ en $\overline{y}$ también resulta invariante por la acción del grupo de trenzas.

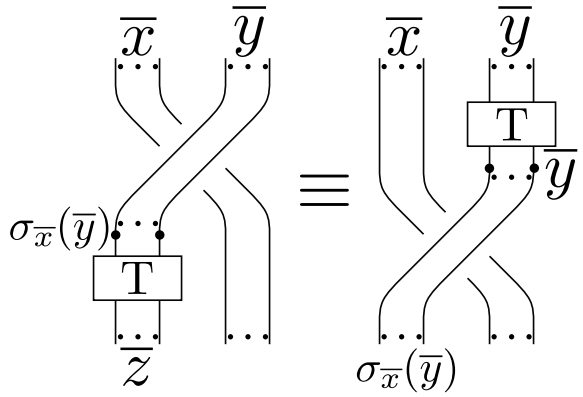


Figura 3.3: Acción de T en $\sigma_{\overline{x}}(\overline{y})$.

Para ver que es efectivamente llamemos $\overline{z} = \sigma_x(\overline{y})$, y tomemos $T \in B_n$ una trenza arbitraria. La acción de T sobre $\overline{z}$ se puede representar diagramáticamente concatenando un diagrama de la trenza T a las primeras n hebras del diagrama que define la estructura de la solución de Bachiller y Cedó. Ahora este diagrama resulta equivalente al que tiene a esa misma trenza del otro lado del cruce, como se ve en la Figura 3.3. Ahora en este segundo diagrama la trenza T está actuando sobre $\overline{y}$, que es invariante por la acción del grupo de trenzas, y por lo tanto los primeros n lugares del final de este diagrama leen los elementos de $\sigma_{\overline{x}}(\overline{y})$.

Esto nos dice que los invariantes por la acción del grupo de trenzas van a formar una subsolución de la solución de Bachiller y Cedó. Más aún, como no tuvimos que hacer ninguna suposición sobre el elemento $\overline{x}$, podemos afirmar no sólo que es una subsolución, sino que nos da una descomposición de la solución original.

Lo único que restaría ver que efectivamente hay elementos invariantes por la acción de todo el grupo de trenzas. Para esto basta con ver que la caracterización de la Proposición 2.4 se puede extender para caracterizar los elementos invariantes para todas las acciones grupos de trenzas B_n en X^n.

Proposición 3.2. *Sea (X, r) una solución de la ecuación de Yang–Baxter. Un elemento $\overline{x} = (x_0, x_1, \ldots, x_{n-1}) \in X^n$ es invariante por la acción de todo el grupo de trenzas B_n si y sólo si $x_i = U^i(x_0)$.*

Demostración. Como los elementos σ_i generan el grupo de trenzas, basta che-

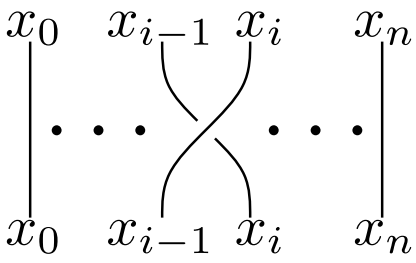


Figura 3.4: Acción de σ_i en un elemento invariante.

quear la invariancia respecto a estos elementos. Ahora el elemento σ_i actúa como se ve en la Figura 3.4, y por la Proposición 2.4 que esto se invariante es equivalente a $x_i = U(x_{i-1})$. De donde se sigue inmediatemente el resultado que queremos. □

Definición 3.3. Llamamos el *elemento congelado comenzando en* x a la tupla $(x, U(x), \dots, U^{n-1}(x))$ que aparece en la Proposición 3.2. Notamos $x^{[n]}$, al elemento congelado de longitud n comenzando en x.

Los elementos congelados de la definición anterior aparecen como *frozen words* en [20] o como *twisted powers* en [21]. En estos papers se estudian las estructuras de Garside que surgen a partir de soluciones a la ecuación de Yang–Baxter. De estos mismos trabajos también surge la siguiente definición, que vamos a poder reinterpretar usando las soluciones cableadas.

Definición 3.4. Dada (X, r) una solución de la ecuación de Yang–Baxter, llamamos su *clase de Dehornoy* al mínimo $d \in \mathbb{N}$ tal que en el grupo de permutaciones se tiene

$$xU(x) \cdots U^{d-1}(x) = \mathrm{id}\,.$$

Observación 3.5. *En principio no queda claro que la clase de Dehornoy esté bien definida sólo de la definición anterior. Una demostración de este hecho se puede ver [21], pero también va a deducirse de lo que veamos en las próximas secciones.*

Definición 3.6. Dada una solución (X, r) a la ecuación de Yang–Baxter y $n \in \mathbb{N}$ definimos la solución cableada $(X^{(n)}, r^{(n)})$, por

$$X^{(n)} = \{(x, U(x), \dots, U^{n-1}(x)\} \subseteq X^n,$$

y $r^{(n)} = r^n$, la misma función que en la solución de Bachiller y Cedó.

De la discusión anterior sabemos que todos los cableados de una solución tienen el mismo tamaño que la solución original, y podemos identificar el conjunto subyacente de todas ellas mirando la primer coordenada de la tupla. Más aún sabemos que vale el siguiente resultado.

Teorema 3.7. *La solución de Bachiller-Cedó es descomponible para todo $n > 1$, independientemente de la solución inicial (X, r), y el cableado da una descomposición $X^n = X^{(n)} \bigsqcup \left(X^n \setminus X^{(n)}\right)$.*

3.3. Propiedades del cableado

En [15], Bachiller y Cedó prueban que el grupo de permutaciones de la solución (X^n, r^n) es un subgrupo del grupo de permutaciones de la solución original, y dan condiciones que garantizan que estos dos coinciden. Para poder caracterizar el grupo de permutaciones de las soluciones cableadas y estudiar sus propiedades vamos a ver primero que podemos realizarlas dentro de la braza de estructura de la solución original.

Teorema 3.8. *Sean (X, r) una solución de la ecuación de Yang–Baxter y $n \in \mathbb{N}$. Tenemos que el conjunto $\{n \cdot x | x \in X\} \subseteq G(X, r)$, es una subsolución de la estructura de solución en $G(X, r)$. Más aún esta solución es isomorfa a la solución cableada $X^{(n)}$.*

Demostración. Primero recordemos que en cualquier braza tenemos que la estructura aditiva satisface $x + y = x \circ \lambda_x^{-1}(y)$, y la estructura de braza en el grupo de estructura cumple que $\lambda_x(y) = \sigma_x(y)$. En particular tenemos $x + x = x \circ \sigma_x^{-1}(x) = x \circ U(x)$. De esto podemos ver que la multiplicación por $n \in \mathbb{N}$ está dada por

$$n \cdot x = x \circ U(x) \circ U^2(x) \circ \cdots \circ U^{n-1}(x).$$

Si notamos entonces $r(n \cdot x, n \cdot y) = (z, w)$, tenemos

$$\begin{aligned} z &= \lambda_{n \cdot x}(n \cdot y) \\ &= n \cdot \lambda_{x \circ U(x) \circ \cdots \circ U^{n-1}(x)}(y) \\ &= n \cdot (\sigma_x \sigma_{U(x)} \cdots \sigma_{U^{n-1}(x)}(y)) \end{aligned}$$

Es claro que este elemento pertenece al conjunto que queremos. Más aún es precisamente el mismo elemento que obtenemos de la identificación del cableado con los elemntos de X, lo que demuestra lo que queríamos. □

Esta realización de la solución cableada ya aparece implícitamente en [11] en su demostración del Teorema 3.17, aunque no estudian propiedades de la misma. En la siguiente sección vamos a presentar una demostración simplificada de este resultado.

A partir de esta realización del cableado de soluciones podemos reinterpretar la clase de Dehornoy. Notemos que la condición de que $xU(x)\dots U^d(x)$ sea la identidad en el grupo de permutaciones de la solución resulta entonces equivalente a que $n \cdot x$ sea la identidad. En particular tenemos que la clase de Dehornoy está bien definida y se tiene el siguiente resultado.

Teorema 3.9. *Dada una solución (X, r) de la ecuación de Yang–Baxter su clase de Dehornoy es el exponente de la estructura aditiva de su braza de permutaciones.*

Demostración. De la discusión anterior es claro que la clase de Dehornoy es el mínimo común múltiplo del orden aditivo de los elementos de X en la braza de permutaciones. Como los elementos de X generan aditivamente la braza de permutaciones esto es lo mismo que el exponente del grupo. □

Por otro lado de la definición original del cableado de una solución se puede ver fácilmente como cambia la función U al cablear una solución.

Teorema 3.10. *Sea (X, r) una solución de la ecuación de Yang–Baxter, y notemos U_X a su función U, y U_n a la función U de la solución cableada $X^{(n)}$. Tenemos entonces que $U_n = U_X^n$.*

Demostración. Veamos al cableado dentro de X^n. Para calcular la función U tenemos que caracterizar los elementos invariantes de $X^n \times X^n$. Concretamente $U_n(x^{[n]})$ va a ser el elemento dado por las últimas n coordenadas del elemento congelado $x^{[2n]} = (x, U_X(x), \dots, U_X^{n-1}(x), U_X^n(x), \dots, U_X^{2n-1}(x))$. Es decir que tenemos $U_n(x^{[n]}) = (U_X^n(x))^{[n]}$. □

Teorema 3.11. *Sea (X, r) una solución de la ecuación de Yang–Baxter. Tenemos entonces que $(X^{(n)})^{(m)} = X^{(nm)}$.*

Demostración. Los elementos de $(X^{(n)})^{(m)}$ son de la forma

$$(x^{[n]}, U^n(x)^{[n]}, \ldots, (U^{n(m-1)}(x)^{[n]}),$$

pero estos elementos son exactamente los de la forma

$$(x, U(x), \ldots, U^{n-1}(x), U^n(x), \ldots, U^{nm-1}(x)),$$

i.e. los elementos de $X^{(nm)}$. □

A partir de los resultados anteriores podemos caracterizar los grupos de permutaciones de las soluciones cableadas.

Teorema 3.12. *Sea (X, r) una solución de la ecuación de Yang–Baxter. El grupo de permutaciones $\mathcal{G}(X^{(n)}, r)$ es la imagen de $\mathcal{G}(X, r)$ por el morfismo de multiplicación por n, de la estructura aditiva de la braza.*

Demostración. Consideremos al cableado dentro de la braza de estructura de solución. Tenemos entonces que la primera coordenada de $r(n \cdot x, n \cdot y)$ está dada por $n \cdot \lambda_{n \cdot x}(y)$. Como el morfismo del grupo de estructura al grupo de permutaciones es de brazas tenemos que este elemento es $n \cdot ((n \cdot \sigma_x)(y))$. Via la identificación de los elementos del cableado con los de la solución original esto nos dice que $r^{(n)}(x, y) = ((n\sigma_x)(y), *)$, que es exactamente lo que queríamos. □

Similarmente podemos ver que la retractabilidad de una solución implica lo mismo para todos sus cableados.

Teorema 3.13. *Sea (X, r) una solución retractable de la ecuación de Yang–Baxter. Tenemos entonces que todos los cableados de solución son retractables.*

Demostración. Como vimos en la demostración del Teorema 3.12, la permutación σ de un elemento x del cableado está dado por $n \cdot \sigma_x$, la multiplicación por n de la permutación en la solución original. En particular vemos que dos elementos que definían la misma permutación en la solución original también definen la misma permutación en la solución cableada. □

Y finalmente podemos demostrar el hecho que mencionamos en la Observación 2.26.

Teorema 3.14. *Sea X una solución indescomponible. Entonces el orden de la función U divide a la clase de Dehornoy, y por lo tanto al orden del grupo de permutaciones.*

Demostración. Sea d la clase de Dehornoy de la solución, y consideremos la solución cableada $X^{(d)}$. Por el Teorema 3.8 tenemos que para todo $x \in X$, $\sigma_x^{(d)} = d \cdot \sigma_x$, y por el Teorema 3.9 este elemento es la permutación id. Por lo tanto la solución $X^{(d)}$ es la solución trivial en X y por lo tanto su función U es la permutación id. Luego por el Teorema 3.10 tenemos $U^d = \mathrm{id}$. □

3.4. Resultados sobre descomponibilidad

Vamos ahora a aplicar los resultados obtenidos sobre el cableado para obtener resultados de descomponibilidad de soluciones. El resultado básico del cual vamos a desprender los resultados de descomponibilidad es el siguiente.

Teorema 3.15. *Sean (X, r) una solución de la ecuación de Yang–Baxter, y $n \in \mathbb{N}$. Sean también $x \in X$, y m y m' los tamaños de las órbitas de x por las acciones de $\mathcal{G}(X, r)$ y $\mathcal{G}(X^{(n)}, r)$ respectivamente. Entonces m' es un múltiplo de m_n, el divisor maximal de m que es coprimo con n.*

Demostración. Sean $\mathcal{G}(X, r)_x$ y $\mathcal{G}(X^{(n)}, r)_x$ los estabilizadores de x por las acciones de los correspondientes grupos de permutaciones. Tenemos entonces que

$$|\mathcal{G}(X, r)| = m|\mathcal{G}(X, r)_x|, \qquad |\mathcal{G}(X^{(n)}, r)| = m'|\mathcal{G}(X^{(n)}, r)|.$$

Como $\mathcal{G}(X^{(n)}, r)$ se obtiene como la imagen de la multiplicación por n en $\mathcal{G}(X, r)$, tenemos que

$$|\mathcal{G}(X^{(n)}, r)| = \frac{|\mathcal{G}(X, r)|}{p_1^{d_1} \cdots p_l^{d_l}},$$

para algunos $d_i > 0$ y donde los p_i son los primos que dividen tanto a $|\mathcal{G}(X, r)|$ como a n.

Por otro lado como $\mathcal{G}(X^{(n)}, r)$ es un subgrupo de $\mathcal{G}(X, r)$ tenemos que $\mathcal{G}(X^{(n)}, r)_x$ es un subgrupo de $\mathcal{G}(X, r)_x$. En particular tenemos que

$$|\mathcal{G}(X^{(n)}, r)_x| = \frac{|\mathcal{G}(X, r)_x|}{t},$$

para algún $t \in \mathbb{N}$. Tenemos entonces

$$m' = \frac{|\mathcal{G}(X^{(n)}, r)|}{|\mathcal{G}(X^{(n)}, r)_x|} = \frac{|\mathcal{G}(X, r)|t}{(p_1^{d_1} \cdots p_l^{d_l})|\mathcal{G}(X, r)_x|} = \frac{mt}{p_1^{d_1} \cdots p_l^{d_l}}.$$

Como esto es un número entero tiene que ser divisible m_n, definido como en el enunciado, ya que los primos p_i son justamente los primos que dividen al máximo común divisor $(m : n)$. □

Teorema 3.16. *Sea (X, r) una solución indescomponible de la ecuación de Yang–Baxter, y $k \in \mathbb{N}$ coprimo con $|X|$. Tenemos entonces que la solución cableada $X^{(k)}$ es también indescomponible.*

Demostración. Dado $x \in X$ arbitrario sabemos que el tamaño de la órbita de x por la acción de $\mathcal{G}(X, r)$, m, es exactamente $|X|$, ya que la solución es indescomponible. Ahora por el Teorema 3.15 sabemos que el tamaño de la órbita de x por el grupo $\mathcal{G}(X^{(n)}, r)$ es un múltiplo del divisor maximal de m coprimo con k. Pero como k es coprimo con m por hipótesis este divisor es m, y por lo tanto la órbita de x debe ser todo X, de modo que la solución cableada es también indescomponible. □

De este resultado podemos deducir fácilmente el siguiente Teorema que ya había sido demostrado por Camp-Mora y Sastriques en [11].

Teorema 3.17 (Camp-Mora–Sastriques)**.** *Sea (X, r) una solución de la ecuación de Yang–Baxter. Si $|X|$ y el orden de la permutación T de la solución son coprimos, entonces la solución es descomponible, o de tamaño 1.*

Demostración. Sea k el orden de la permutación T. Considerando la solución cableada $X^{(k)}$ tenemos que su invariante diagonal es la partición asociada a $T^k = \mathrm{id}$, y por lo tanto $X^{(k)}$ es libre de cuadrados. Se sigue del resultado de Rump que este cableado es descomponible, si no es de tamaño 1. Pero entonces del Teorema 3.16 deducimos que la solución original también tiene que ser descomponible. □

Para las siguientes aplicaciones la idea es utilizar el Teorema 3.15 junto con el Teorema 3.10 y el Lema 2.9 para obtener restricciones sobre los tamaños de las órbitas de una solución.

Teorema 3.18. *Sea (X, r) una solución indescomponible de la ecuación de Yang–Baxter de tamaño pq, con p y q primos distintos. El invariante diagonal de X no puede tener ninguna parte de tamaño s, donde s satisfaga*

$$(p-1)q < s < pq,$$

y s no sea divisible por p.

Demostración. Supongamos que T tiene una parte de tamaño s con $(p-1)q < s < pq$ y que además p no divide a s. Como p no divide a s tenemos que para todo $t \in \mathbb{N}$ el p^t-cableado de la solución X tiene una parte de tamaño s.

Como p no divide a s, el invariante diagonal de la solución cableada $X^{(p^k)}$ tiene también una parte de tamaño s para todo $k \in \mathbb{N}$. Ahora, por el Lema 2.9 esta parte debe estar contenida enteramente en una órbita, y por el Teorema 3.15 el tamaño de esta órbita es un múltiplo del divisor maximal de pq que es coprimo con p, i.e. q. Como además tenemos que $(p-1)q < s < pq$, esta órbita tiene que tener tamaño pq, es decir que la solución cableada también debe ser indescomponible.

Por otro lado para k suficientemente grande el grupo de permutaciones de $X^{(p^k)}$ no es divisible por p, por el Teorema 3.8. En particular no puede actuar transitivamente en un conjunto de tamaño pq, y entonces para p suficientemente grande la solución cableada no puede ser indescomponible, contradiciendo lo obtenido en el párrafo anterior. Por lo tanto la solución original no podía tener una parte de tamaño s. □

Teorema 3.19. *Sea (X, r) una solución indescomponible de la ecuación de Yang–Baxter de tamaño ab, y con invariante diagonal (a, c, c'), donde los números a, b, c, c' son coprimos dos a dos, salvo posiblemente c y c'. Entonces no se puede cumplir que $b > a + c$.*

Demostración. Supongamos que (X, r) es una solución como en el enunciado. La solución cableada $X^{(a)}$ tiene invariante diagonal $(c, c', 1, \ldots, 1)$, con a unos. Tenemos entonces que el orden del invariante diagonal es el mínimo común múltiplo de c y c', que es coprimo con $ab = |X|$. Por lo tanto por el Teorema 3.17 la solución es descomponible, es decir que la acción del grupo de permutaciones tiene por lo menos dos órbitas.

Por el Lema 2.9 cada una de las partes está contenida enteramente en una órbita. Por lo tanto las óribtas que no contienen a la parte de tamaño c' tienen tamaño menor o igual que $|X| - c' = a + c$. Por otro lado por el Teorema 3.15 el tamaño de todas las órbitas de la solución cableada debe ser un múltiplo del divisor maximal de ab que es coprimo con a, es decir a. Por lo tanto se tiene que cumplir que $b \leq a + c$. □

Teorema 3.20. *Sea (X, r) una solución indescomponible de la ecuación de Yang–Baxter de tamaño $2d$, con d impar, e invariante diagonal $(2a, b, c)$ donde a, b y c son impares, y $b \geq c$. Entonces se cumple que $2a + c = d = b$.*

Demostración. Sea (X, r) una solución de tamaño $2d$ e invariante diagonal $(2a, b, c)$ como en el enunciado. La solución cableada $X^{(2)}$ tiene entonces invariante diagonal (a, a, b, c), y por el Teorema 3.17 esta solución es descomponible. Por el Teorema 3.15 las órbitas de esta solución son divisibles por d, ya que d es impar, y como la solución es descomponible debe haber exactamente dos órbitas de tamaño d.

Como a, b y c son impares solo podemos sumar d usando una cantidad de impar de partes. Es decir que debe haber una órbita con sólo una parte y otra órbita con tres partes. Como ambas órbitas suman lo mismo no puede ser que las dos órbitas de tamaño a estén en órbitas distintas, y como $b \geq c$ la única opción posible es que las dos partes de tamaño a formen junto con la de tamaño c la órbita de tres partes y b forme la otra órbita, de dónde se deduce lo que queríamos. □

De estos resultados se deducen restricciones para el invariante diagonal que no se desprenden sólo del Teorema 3.17. Por ejemplo, del Teorema 3.18 se deduce que el invariante diagonal de una solución indescomponible de tamaño 14 no puede tener una parte de tamaño 9 u 11, descartando, por ejemplo, los invariantes $(9, 4, 1)$ y $(11, 2, 1)$ que no tienen orden coprimo con 14.

Además de estos resultados generales, podemos aplicar los mismos razonamientos para obtener resultados particulares como los siguientes.

Proposición 3.21. *Si (X, r) es una solución indescomponible de tamaño 30 el invariante diagonal no puede tener una parte de tamaño 21 y una de tamaño 7, i.e. no puede ser $(21, 7, 1, 1)$ ó $(21, 7, 2)$.*

Demostración. Si la (X, r) es una solución de tamaño 30 con invariante diagonal como en el enunciado entonces las soluciones cableadas $X^{(3^k)}$ tienen invariante diagonal con cuatro partes de tamaño de 7. Para k suficientemente grande esta solución no puede ser indescomponible, por el Teorema 3.12.

Si la solución original fuera indescomponible, entonces por el Teorema 3.15, las órbitas de la misma deben tener tamaño divisible por 10. Pero con cuatro partes de tamaño 7 la única forma de obtener esto es que estén todas las partes en una misma órbita de tamaño 30. Es decir que todos estos cableados resultan indescomponibles, contradiciendo el último párrafo. □

Proposición 3.22. *Si (X, r) es una solución indescomponible de tamaño 50, su invariante diagonal no puede tener tres partes de tamaño 13.*

Demostración. Consideremos las soluciones cableadas $X^{(\cdot 2^k)}$. Por el Teorema 3.10 estas soluciones tienen todas invariante diagonal con tres partes de tamaño 13. Nuevamente para k suficientemente alto esta solución no puede ser indescomponible, por el Teorema 3.12.

Por el Teorema 3.15 si la solución original fuera indescomponible las órbitas de las soluciones cableades tienen que tener tamaño divisible por 25. Pero con tres partes de tamaño 13 la única forma de que esto sea posible es que pertenezcan todas a una órbita de tamaño 50, por lo que la solución debería ser indescomponible, contradiciendo lo obtenido en el párrafo anterior. □

Corolario 3.23. *Si (X, r) es una solución indescomponible de tamaño* 50 *su invariante diagonal no puede tener una parte de tamaño 39.*

Demostración. Si tuvieramos una solución de esta forma la solución cableada $X^{(3)}$ sería una solución indescomponible de tamaño 50 cuyo invariante diagonal tendría tres partes de tamaño 13, contradiciendo la proposición anterior. □

3.5. Resultados computacionales

A partir de la base de datos de soluciones de tamaño menor o igual a 10 de [3] podemos ver que sucede al calcular los cableados de las soluciones indescomponibles de tamaño pequeño. En particular nos interesa el caso en el que luego de realizar el cableado se vuelva a obtener una solución indescomponible.

Por el Teorema 3.16 el cableado de una solución indescomponible por un número coprimo con el tamaño de la solución vuelve a ser indescomponible. De esta forma uno puede conseguir nuevas soluciones indescomponibles como en el siguiente ejemplo

Ejemplo 3.24. Consideremos la solución con ID $[8, 34200]$ en la base de datos del paquete de Yang–Baxter de GAP. Esta es la solución (X, r) con $X = \{1, \ldots, 8\}$ y función r dada por las siguientes funciones σ:

$$\begin{aligned}
&\sigma_1 = (12)(34)(56)(78), && \sigma_2 = (12)(36)(47)(58), && \sigma_3 = (1543)(2678),\\
&\sigma_4 = (1367)(2854), && \sigma_5 = (17)(24)(38)(56), && \sigma_6 = (1763)(2458),\\
&\sigma_7 = (1345)(2876), && \sigma_8 = (15)(26)(38)(47).
\end{aligned}$$

Esta solución resulta indescomponible, y a partir de las funciones σ podemos ver fácilmente que su función U es la permutación $(12)(345678)$. Si consideremaos la solución cableada $X^{(3)}$ como 3 es coprimo con 8 obtenemos una nueva solución indescomponible pero cuya función U debe ser $(12)(36)(47)(58)$, y por lo tanto no puede ser isomorfa a la original. Se puede verificar que la nueva solución obtenida es la solución con ID $[8, 32424]$.

En el ejemplo anterior el proceso de cableado resulta "destructivo", en el sentido de que no podemos volver a obtener la solución original como un cableado de la nueva solución. Esto se debe a que la nueva solución se obtiene al cablear por un número que es coprimo con el orden de la solución pero no con el orden del invariante diagonal, o más en general el orden del grupo de permutaciones. Cabe destacar que entre todas las soluciones de tamaño menor o igual a 10 la solución anterior es la única en la que el orden del grupo de permutaciones es divisble por un primo que no divide al tamaño de la solución. Esto motiva la siguiente definición.

Definición 3.25. Decimos que dos soluciones (X_1, r_1) y (X_2, r_2) son *equivalentes por cableado* si existen $k, k' \in \mathbb{N}$ tales que $X_1^{(k)} \equiv X_2$ y $X_2^{(k')} \equiv X_1$.

Del Teorema 3.8 sabemos que el k-cableado de una solución, y su correspondiente braza de permutaciones, se pueden identificar con la imagen de la multiplicación por k en la braza de la solución original. De esto se desprende que si dos soluciones son equivalentes por cableado el k que pasa de una a otra

Tamaño	# Sols. Indescomponibles	# Sols. Inequivalentes
4	5	5
6	10	8
8	100	94
9	16	12
10	36	16

Cuadro 3.1: Cantidad de soluciones indescomponibles, y cantidad de clases de equivalencia por cableado de soluciones indescomponibles de tamaño compuesto y a lo sumo 10.

debe ser coprimo con el orden del grupo de permutaciones. Más aún, cuando k es coprimo por el orden del grupo de permutaciones, N, la acción de multiplicación por k factoriza por las unidades de $\mathbb{Z}_N$. Por lo tanto si $X_1^{(k)} \equiv X_2$ y k es coprimo con el orden de grupo de permutaciones entonces X_1 y X_2 son equivalentes por cableado.

Proposición 3.26. *Dos soluciones (X_1, r_1), (X_2, r_2) son equivalentes por cableado si y sólo si tienen la misma braza de permutaciones y existe k coprimo con $\mathcal{G}(X_1, r_1)$ tal que $X_1^{(k)} \equiv X_2$.*

Esto nos permite encontrar todas las soluciones indescomponibles que son equivalentes por cableado en la base de datos de soluciones de GAP, ya que sólo hay que verificar el resultado de cablear cada solución indescomponible por un conjunto de generadores de $\mathcal{U}(\mathbb{Z}_N)$, con N el tamaño del grupo de permutaciones de la solución. Si contamos la cantidad de soluciones indescomponibles de cada tamaño disponible en la base de datos obtenemos el cuadro 3.1.

Observación 3.27. *Si (X, r) es una solución indescomponible en principio podría ser posible que la solución cableada $X^{(k)}$ también sea indescomponible aún cuando k no sea coprimo con $|X|$. Sin embargo al verificar lo que sucede con las soluciones indescomponibles de tamaño menor o igual 10 tenemos que en todos los casos la solución cableada $X^{(k)}$ resulta descomponible si k no es coprimo con el tamaño de la solución.*

Capítulo 4

Construcciones explícitas

En este capítulo vamos a exponer los resultados de [33]. En el mismo usamos el esquema de clasificación Bachiller, Cedó y Jespers, Teorema 1.40, para describir explícitamente todas las soluciones indescomponibles que tienen grupo de permutaciones isomorfo a alguno de ciertas familias. Concretamente los grupos cuyas soluciones vamos a clasificar son todos los grupos de tamaño pq, y todos los grupos abelianos o diedrales de tamaño p^2q, donde p y q son primos cualesquiera (uno debe ser 2 en el caso diedral).

Para esto vamos a necesitar conocer todas las posibles estructuras de braza de estos grupos. Esta clasifcación fue realizada por Acri y Bonatto en [1] y [2]. A partir de esta clasificación vamos a necesitar en cada caso calcular los grupos de automorfismos de braza y la acción λ para poder encontrar todas las soluciones asociadas a menos de isomorfismo.

4.1. Resultados preliminares

4.1.1. Esquema de clasificación

Para clasificar las soluciones vamos a utilizar la construcción explícita de las soluciones de [8] como la formulamos en el Teorema 1.38. Notemos que Rump en [37] da una construcción, relacionada a esta, para soluciones indescomponibles en términos de cycle-sets. Para nuestros resultados necesitamos la descripción explícita de [8] de modo que antes de estudiar las brazas asociadas a cada grupo necesitamos ver como leer la indescomponibilidad en

términos del dato del Teorema 1.40. A partir de este dato también podemos ver como leer la retractabilidad de la solución, y encontrar el dato asociado a su retracción, y sus cableados.

Proposición 4.1. *Sean $(B, +, \circ)$ una braza y $(a_i, K_i)_{i\in I}$ el dato de una solución como en el Teorema 1.40, y notemos (X, r) a la solución asociada. Entonces vale lo siguiente*

1. *La solución X es indescomponible si y sólo si $|I| = 1$.*

2. *La solución X es irretractable si y sólo si K_i es el estabilizador completo de a_i para todo $i \in I$ y todos los a_i pertenecen a órbitas distintas de la acción λ.*

   Más aún, si la solución no es irretractable su retracción está dada por el dato que tiene los mismos a_i, pero tomando uno sólo por cada órbita, y tomando como subgrupos el estabilizador completo de cada elemento.

3. *Para cada número natural k la solución cableada $X^{(k)}$ se puede describir como las del Teorema 1.40 con el dato $(ka_i, K_i))_{i\in I}$.*

Observemos que en el segundo punto los subgrupos elegidos para el dato de la retracción pueden no cumplir que sus interiores normales tengan intersección trivial y en el último punto las órbitas de los elementos ka_i pueden no generar el grupo aditivo de la braza. Como notamos en la Observación 1.41 estos siguen definiendo soluciones, a pesar de que su braza de permutaciones no es en general isomorfa a B.

Demostración. 1. Observemos que por la definición de la solución, cada subconjunto B/K_i es invariante por la acción de todo el grupo de permutaciones, y por la tanto para que la solución sea indescomponible debe valer $|I| = 1$.

Por otro lado supongamos $|I| = 1$, y sean a y K los únicos elementos del dato de la solución. Como (a, K) satisface las hipótesis del dato de solución sabemos que la órbita de a por la acción λ genera el grupo aditivo de la braza, y entonces por la Proposición 1.27 tenemos que esta órbita genera también el grupo multiplicativo. De la fórmula explícita para las funciones σ de la solución del Teorema 1.40 se puede ver que entonces la

órbita de un elemento bK por la acción de las permutaciones σ coincide con la órbita de la acción de todo el grupo $(B, \circ)$ por multiplicación a izquierda en el cociente. En particular esta acción es transitiva.

2. Como notamos en la Observación 1.41 la acción por las funciones σ factoriza por la braza B, de modo que la acción de σ_{bK_i} es la acción por multiplicación a izquierda de $\lambda_b(a_i)$. Esto quiere decir que $\sigma_{bK_i} = \sigma_{b'K_j}$ si y sólo si $\lambda_b(a_i)$ y $\lambda_{b'}(a_j)$ actúan de igual forma en X por multiplicación a izquierda. Como los subgrupos elegidos cumplen que sus interiores normales tienen intersección trivial esto se cumple si y sólo si $\lambda_b(a_i) = \lambda_{b'}(a_j)$.

   En particular a_i y a_j deben pertenecer a la misma órbita. Esto nos garantiza que es condición necesaria que no halla ninguna órbita repetida en el dato. Más aún si este es el caso, tenemos que $\lambda_b(a_i) = \lambda_{b'}(a_i)$ si y sólo si b y b' pertenecen a la misma coclase del estabilizador de a_i, de donde se deduce el resto de lo que queríamos.

3. Por la Observación 1.41 sabemos que la función $\sigma_- : X \to \mathcal{G}(X, r)$ factoriza por la braza B, via el morfismo $xK_i \mapsto \lambda_x(a_i)$, con la acción en X dada por la multiplicación a izquierda. Pero siguiendo este morfismo para el dato (na_i, K_i), tenemos $xK_i \mapsto \lambda_x(na_i) = n\lambda_x(a_i)$. Por lo tanto tenemos que la función σ asociada en este solución es precisamente la multiplicación por n de la función σ en la solución original, es decir que nos da el cableado por n.

□

Con este resultado en mente vemos que si nuestro interés es únicamente construir soluciones indescomponibles entonces los datos a considerar consisten de únicamente un elemento de la braza y un subgrupo. Esto simplifica también las condiciones a verificar para que el dato defina una solución y si dos datos definen soluciones isomorfas. Podemos resumir el resultado para soluciones indescomponibles de la siguiente manera.

Teorema 4.2. *Sean $(B, +, \circ)$ una braza, $a \in B$ un elemento tal que su órbita por la acción λ genera el grupo aditivo de la braza, y K un subgrupo del estabilizador de a con interior normal trivial. Entonces B/K es una solución*

indescomponible con las funciones σ dadas por

$$\sigma_{xK}(yK) = (\lambda_x(a) \circ y)K.$$

Más aún, cualquier solución indescomponible con grupo de permutaciones isomorfo a $(B, +, \circ)$ es isomorfa a una de estas, y dos de estos datos, (a, K) y (a', K'), definen soluciones isomorfas si y sólo existe un automorfismo de brazas $\psi : B \to B$ y un elemento $z \in B$ tales que $\psi(a) = a'$ y

$$\psi(K) = z \circ K' \circ z^{-1}.$$

Observación 4.3. *En el caso en que estemos analizando un grupo abeliano el único subgrupo K que hay considerar en el resultado anterior es el subgrupo trivial, ya que es el único subgrupo con interior normal trivial.*

Por otro lado, si estamos analizando si dos soluciones definidas (a, K) y (a, K') son isomorfas y tenemos que K y K' son subgrupos triviales, entonces la condición de conjugación se satisface trivialmente y sólo tenemos que decidir si existe o no un automorfismo ψ tal $\psi(a) = a'$.

4.1.2. Clasificación de brazas

Nuestro objetivo es encontrar todas las soluciones cuyo grupo de permutaciones tiene tamaño pq, o los abelianos o diedrales de tamaño p^2q, donde p y q son primos distintos. Para poder usar el resultado anterior necesitamos entender todas las estructuras de braza que admiten estos grupos. Las brazas de tamaño pq fueron clasificadas por Acri y Bonatto en [1] y también por Alabdali y Byott en [4]. Las brazas de tamaño p^2q fueron clasificados por Dietzel en [23] y por Acri y Bonatto en [2]. Para la construcción de las soluciones vamos a referirnos a la clasificación de brazas de Acri y Bonatto, ya que la presentación explícita de las brazas dada en [1] y [2] simplifica el cálculo de los grupos de automorfismos y la acción λ.

Para los grupos de tamaño pq el resultado que nos interesa es la primera parte del teorema principal de [1]. Este resultado lo podemos enunciar de la siguiente manera

Teorema 4.4 (Acri–Bonatto)**.** *Sean $p > q$ números primos. Si $p \not\equiv 1 \pmod{q}$ entonces la única braza de tamaño pq es la braza trivial. Si $p \equiv 1 \pmod{q}$*

entonces hay una única braza no trivial de tamaño pq, e identificando el grupo aditivo con $\mathbb{Z}_p \times \mathbb{Z}_q$ la estructura multiplicativa está dada por

$$\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a + g^b c \\ b + d \end{pmatrix}, \tag{4.1}$$

donde g es cualquier elemento de $\mathbb{Z}_p$ de orden q.

Para las brazas de tamaño p^2q la situación es más complicada, aunque los casos a considerar se simplifican en parte para los grupos en los que estamos interesados. Para el caso en el que el grupo es cíclico los resultados se reducen a lo siguiente

Teorema 4.5 (Acri–Bonatto)**.** *Sean p y q números primos.*

1. *Si $p = 2$ entonces hay una única braza no trivial con estructura multiplicativa $\mathbb{Z}_{4q}$. Identificando la estructura aditiva de este grupo con $\mathbb{Z}_2^2 \times \mathbb{Z}_q$ la estructura multiplicativa está definida por*

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \circ \begin{pmatrix} d \\ e \\ f \end{pmatrix} = \begin{pmatrix} a + d + be \\ b + e \\ c + f \end{pmatrix}.$$

2. *Si $p \neq 2$ también hay una única braza no trivial con estructura multiplicativa $\mathbb{Z}_{p^2q}$. En esta caso la estructura aditiva se identifica con $\mathbb{Z}_{p^2q}$ y la multiplicación está dada por*

$$\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a + c + pac \\ b + d \end{pmatrix}.$$

En el caso en el que la estructura multiplicativa es el único grupo abeliano no cíclico de orden p^2q el resultado es similar. Hay siempre una única estructura de braza no trivial y la descripción explícita depende de si p es dos o no.

Teorema 4.6 (Acri–Bonatto)**.** *Sean p y q números primos.*

1. *Si $p = 2$ hay una única braza no trivial con estructura multiplicativa $\mathbb{Z}_2^2 \times \mathbb{Z}_q$. Identificando la estructura aditiva con $\mathbb{Z}_q \times \mathbb{Z}_4$ la estructura multiplicativa está definida por*

$$\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a + c \\ b + (-1)^b d \end{pmatrix}.$$

2. *Si $p \neq 2$ hay una única braza no trivial con estructura multiplicativa $\mathbb{Z}_p^2 \times \mathbb{Z}_q$. Identificando la esturctura aditiva con $\mathbb{Z}_p^2 \times \mathbb{Z}_q$ la estrucutra multiplicativa está definida por*

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \circ \begin{pmatrix} d \\ e \\ f \end{pmatrix} = \begin{pmatrix} a + d + be \\ b + e \\ c + f \end{pmatrix}.$$

La última clase de grupos que nos interesa son los grupos diedrales de tamaños $2p^2$ y $4q$. El primer caso es más sencillo y de hecho podemos describir lo que sucede en la clase, un poco más general, de los siguientes productos semidirectos.

Teorema 4.7 (Acri–Bonatto)**.** *Sean p y q primos con $p \equiv 1 \pmod{q}$. Hay una única braza con estructura multiplicativa el (único posible) producto semidirecto $\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_q$. Identificando la estructura aditiva con $\mathbb{Z}_{p^2} \times \mathbb{Z}_q$ su estructura multiplicativa está dada por*

$$\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a + g^b c \\ b + d \end{pmatrix},$$

donde g es un elemento de orden q de $\mathcal{U}(Z_{p^2})$.

Notemos que tomando $q = 2$ en el resultado anterior se obtienen las estructuras de braza de los grupos diedrales D_{p^2}.

El caso de los grupos diedrales es el más complejo ya que hay varias estructuras a considerar. Sin embargo el análisis de las soluciones asociadas no resulta particularmente complicado. Las estructuras de braza posibles están dadas por el siguiente resultado.

Teorema 4.8 (Acri–Bonatto)**.** *Sea p un número primo. Hay tres estructuras de braza con grupo multiplicativo D_{2p}, el grupo diedral de $4p$ elementos.*

1. *Identificando la estructura aditiva con $\mathbb{Z}_p \times \mathbb{Z}_4$ el producto*

$$\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a + (-1)^b c \\ b + (-1)^b d \end{pmatrix},$$

   da una estructura de braza.

2. *Identificando la estructura aditiva con $\mathbb{Z}_p \times \mathbb{Z}_4$ el producto*

$$\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a + (-1)^{b(b-1)/2} c \\ b + (-1)^b d \end{pmatrix},$$

   da una estructura de braza.

3. *Identificando la estructura aditiva con $\mathbb{Z}_2^2 \times \mathbb{Z}_p$ el producto*

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \circ \begin{pmatrix} d \\ e \\ f \end{pmatrix} = \begin{pmatrix} a + d \\ b + e \\ c + (-1)^a f \end{pmatrix},$$

   da una estructura de braza.

En particular hay dos brazas con grupo aditivo cíclico y uno con grupo aditivo no cíclico.

En las siguientes secciones vamos a analizar cada uno estos casos calculando la acción λ, para encontrar los elementos cuya órbita generen el grupo aditivo. También tenemos que calcular en cada caso el grupo de automorfismos para poder caracterizar cuando dos de las soluciones calculadas son isomorfas.

4.2. Resultados generales

En esta sección vamos a recopilar algunos resultados que resultan útiles en varios de los casos que vamos a analizar. El primer resultado general independiente del tamaño que vamos a considerar es la caracterización de las soluciones indescomponibles asociadas a las brazas triviales.

Observación 4.9. *De la definición de la acción λ es inmediato que para todo braza trivial la acción resulta trivial, i.e. $\lambda_a(b) = b$ para todo $a, b \in B$.*

Proposición 4.10. *Sea $(B, +, \circ)$ una braza trivial, i.e. $\circ = +$. Si el grupo subyacente $(B, +)$ es cíclico entonces hay una única solución indescomponible con braza de permutaciones $(B, +, \circ)$. Si el grupo subyacente no es cíclico entonces no hay ninguna solución indescomponible con braza de permutaciones $(B, +, \circ)$.*

Demostración. Por el Teorema 4.2 tenemos que encontrar todas las órbitas de la acción λ que generen el grupo aditivo. Pero por la Observación 4.9 todas las órbitas tienen único elemento. Es decir que necesitamos un generador del grupo subyacente. En particular si el grupo subyacente no es cíclico entonces no hay soluciones indescomponibles.

Como el grupo subyacente es abeliano su único subgrupo con interior normal trivial es el subgrupo trivial. En particular cada generador del grupo produce una única solución. Por último como la braza es trivial cualquier cualquier automorfismo del grupo subyacente resulta naturalmente un automorfismo de braza. Por lo tanto siempre podemos encontrar un automorfismo que envía cualquier generador en cualquier otro, y estos claramente aplican el subgrupo trivial en el mismo. Esto quiere decir que todas las soluciones anteriores son isomorfas. □

Lema 4.11. *Sea $(B, +, \circ)$ una braza y $X \subseteq B$ una órbita por la acción λ que genera el grupo aditivo entonces todos los elementos de X tienen el mismo orden aditivo, y este es divisible por todos los primos que dividen a $|B|$.*

Demostración. Como X es una órbita de la acción por λ, y esta es por automorfismos del grupo aditivo, todos los elementos tienen el mismo orden. Notemos n el orden de los elementos de X.

Por otro lado como $(B, +)$ es abeliano el orden de la suma de dos elementos divide al mínimo común múltiplo del orden de los elementos. En particular como todos los elementos de X tienen orden n, el orden de cualquier elemento del subgrupo generado por X divide a n. Como X genera al grupo entero estero quiere decir que n debe ser el exponente del grupo, de donde se deduce el enunciado. □

4.3. Brazas de tamaño pq

Por el Teorema 4.4 hay a lo sumo dos posibles brazas de tamaño pq, si $p > q$ son primos distintos. Como el único grupo abeliano de tamaño pq es el cíclico, siempre hay una única braza trivial de este tamaño. Para esta braza la Proposición 4.10 asegura que hay una única solución indescomponible.

Cuando $p \equiv 1 \pmod{q}$ tenemos además una braza no trivial. El grupo aditivo tiene que ser el grupo cíclico, y escribiéndolo como el producto $\mathbb{Z}_p \times \mathbb{Z}_q$ su estructura multiplicativa está descripta por la ecuación (4.1). Observemos que tomando la acción de $\mathbb{Z}_q$ en $\mathbb{Z}_p$ dada por la multiplicación por g, este producto es precisamente el producto semidirecto $\mathbb{Z}_p \rtimes \mathbb{Z}_q$.

Dados dos elementos $(a, b), (a', b') \in B$ la acción por lambda resulta

$$\lambda_{\binom{a}{b}} \binom{a'}{b'} = \binom{a + g^b a'}{b + b'} - \binom{a}{b} = \binom{g^b a'}{b'}.$$

Del Lema 4.11 se deduce que cualquier órbita que genere al grupo aditivo debe tener un generador, ya que este es cíclico, y los generadores de este grupo son los pares (a, b) con tanto a como b generadores del grupo respectivo. El estabilizador de cualquiera de estos puntos por la acción λ es el subgrupo $\mathbb{Z}_p \times \{0\}$ por la tanto cada órbita tiene tamaño $[\mathbb{Z}_p \rtimes \mathbb{Z}_q : \mathbb{Z}_p \times \{0\}] = q$ y la cantidad de órbitas es $\frac{(p-1)(q-1)}{q}$, ya que hay $(p-1)(q-1)$ generadores. Más aún, como los estabilizadores son normales, la única posible elección de K en el Teorema 1.38 es el subgrupo trivial.

Para ver cuáles de estas órbitas dan soluciones isomorfas necesitamos entender cuál es el grupo de automorfismos de la braza.

Lema 4.12. *Sean p y q primos tales que $p \equiv 1 \pmod{q}$, el grupo de automorfismos de la braza no trivial de tamaño pq es isomorfo a $\mathcal{U}(\mathbb{Z}_p)$.*

Demostración. Sabemos que el grupo aditivo es $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$, y por lo tanto su grupo de automorfismos es $\mathcal{U}(\mathbb{Z}_{pq}) = \mathcal{U}(\mathbb{Z}_p) \times \mathcal{U}(\mathbb{Z}_q)$, más aún la acción en la identificación que tenemos nosotros es via la multiplicación coordenada a coordenada. Si tomamos un elemento (α, β) de este grupo, la condición de que sea morfismo de brazas es que cumple lo siguiente

$$\binom{\alpha(a + g^b c)}{\beta(b + d)} = \binom{\alpha(a + g^{\beta b} c)}{\beta(b + d)}, \qquad \forall a, c \in \mathbb{Z}_p, b, d \in \mathbb{Z}_q.$$

Inspeccionando las primeras coordenadas vemos que es necesario que $g^b = g^{\beta b}$, y como la segundas coordenadas son siempre iguales esta condición es suficiente. Como g es un elemento de orden q, la condición anterior se cumple si y sólo si $\beta = 1$, de donde se deduce lo que queríamos demostrar. □

De esta descripción vemos que dos órbitas son conjugadas por un automorfismos si y sólo si tienen la misma segunda coordenada, notemos que todos los elementos de una órbita tienen la misma segunda coordenada. En particular hay exactamente $q - 1$ soluciones no isomorfas que lo tienen como braza de permutaciones, más aún podemos parametrizarlas por $\mathcal{U}(\mathbb{Z}_q)$.

Observación 4.13. *Dado $n \in \mathbb{N}$ coprimo con pq, sabemos que el cableado de cualquiera de las soluciones anteriores por n nos da una solución con la misma braza de permutaciones. Usando la Proposición 4.1 podemos ver que cualquiera de las soluciones obtenidas se puede obtener de cualquiera de las otras cableando por un n apropiado.*

Podemos resumir los resultados de esta sección en el siguiente resultado:

Teorema 4.14. *Sea G un grupo de orden pq, con p y q primos distintos,*

1. *Si G es cíclico, hay una única solución indescomponible con grupo de permutaciones G.*

2. *Si G es un producto semidirecto $\mathbb{Z}_p \rtimes \mathbb{Z}_q$, hay exactamente $q - 1$ soluciones indescomponibles con grupo de permutaciones G, y son todas equivalentes por cableado.*

Además, todas las soluciones anteriores tienen tamaño pq.

Observemos que cuando $q = 2$ y p es un primo impar el producto semidirecto del teorema anterior es el grupo diedral D_p. Tenemos como caso particular del resultado anterior el siguiente corolario.

Corolario 4.15. *Dado p un primo impar hay una única solución indescomponible, a menos de isomorfismo, con grupo de permutaciones isomorfo a D_p. Más aún, esta solución es de tamaño $2p$.*

4.4. Brazas abelianas de tamaño p^2q

Veamos ahora el caso de las brazas de tamaño p^2q con grupo multiplicativo abeliano. Para esto vamos a usar el Teorema 4.5, que describe las brazas con estructura multiplicativa cíclica, y el teorema 4.6 que describe las brazas con estructura multiplicativa no cíclica, pero abeliana.

4.4.1. Brazas cíclicas

Empezemos analizando las soluciones que provienen de brazas cíclicas. En el caso en que $p = 2$ tenemos por el Teorema 4.5 tenemos una única braza no trivial. Como en este caso el grupo aditivo es cíclico por la Proposición 4.10 la braza trivial provee una solución indescomponible. Para la braza no trivial, podemos identificar su grupo aditivo con $\mathbb{Z}_2^2 \times \mathbb{Z}_q$ y su estructura multiplicativa queda dada por

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \circ \begin{pmatrix} d \\ e \\ f \end{pmatrix} = \begin{pmatrix} a + d + be \\ b + e \\ c + f \end{pmatrix}.$$

La acción por λ en este caso resulta

$$\lambda_{\begin{pmatrix} a \\ b \\ c \end{pmatrix}} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} \alpha + b\beta \\ \beta \\ \gamma \end{pmatrix}.$$

Es fácil ver entonces que las órbitas de la misma son, o bien de un único elemento $\mathcal{O}_{\alpha,\gamma} = \{(\alpha, 0, \gamma)\}$, con α y γ arbitrarios, o bien con dos elementos y de la forma $\mathcal{O}_\gamma = \{(a, 1, \gamma) : a \in \mathbb{Z}_2\}$ con γ arbitrario. De estas órbitas es claro que las que generan son exactamente las $\mathcal{O}_\gamma$ con γ un generador de $\mathbb{Z}_q$.

Como el grupo es abeliano cada una de esas órbitas provee una solución indescomponible, y para decidir cuáles de ellas son isomorfas hay que calcular el grupo de automorfismos de la braza.

Lema 4.16. *Dado q un primo impar, el grupo de automorfismos de la única braza no trivial con grupo multiplicativo isomorfo a $\mathbb{Z}_{4q}$ es isomorfo al producto $\mathbb{Z}_2 \times \mathcal{U}(\mathbb{Z}_q)$.*

Demostración. El grupo de isomorfismos de la estructura aditiva está dado por $\mathrm{GL}_2(2) \times \mathcal{U}(\mathbb{Z}_q)$ actuando por multiplicación de $\mathrm{GL}_2(2)$ en las primeras dos coordenadas y de $\mathbb{Z}_q$ en la última. Consideremos (A, u) un elemento de este grupo con $A = \left(\begin{smallmatrix} x & y \\ w & z \end{smallmatrix}\right)$. Dados dos elementos (a, b, c) y (d, e, f) de la braza planteando la condición de que (A, u) sea morfismo del grupo aditivo y mirando la segunda coordenada obtenemos

$$w(a + d) + z(b + e) = w(a + d + be) + z(b + e).$$

Como esta identidad tiene que valer para toda elección de $a, b, d, e \in \mathbb{Z}_2$ tenemos que necesariamente $w = 0$. Como la matriz A debe ser invertible tenemos que entonces $x = z = 1$, y la condición en la primera coordenada se simplifica a

$$a + yb + d + ye + be = a + d + be + yb + yd,$$

que vale siempre. Por otro lado la condición en la última coordenada se cumple trivialmente. Es decir que el grupo de automorfismos es isomorfo al producto del grupo de matrices unitriangulares por $\mathcal{U}(\mathbb{Z}_q)$, que es isomorfo al del enunciado. □

En particular vemos que dadas dos órbitas que generan $\mathcal{O}_\gamma$ y $\mathcal{O}_{\gamma'}$ podemos considerar el automorfismo dado por tomar A la matriz identidad y $u = \gamma'\gamma^{-1}$, y este aplica la primer órbita en la segunda. Por lo tanto tenemos que en este caso todas las órbitas proveen soluciones isomorfas.

Consideremos ahora el caso p impar. Nuevamente por la Proposición 4.10 la braza trivial con grupo multiplicativo cíclico provee de una solución indescomponible, y por el Teorema 4.5 sabemos que hay una única braza no trivial a considerar. En este caso la braza adicional tiene estructura aditiva isomorfa a $\mathbb{Z}_{p^2q} \cong \mathbb{Z}_{p^2} \times \mathbb{Z}_q$ y la estructura multiplicativa está dada por

$$\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a + c + pac \\ b + d \end{pmatrix}.$$

La acción λ en este caso está dada por

$$\lambda_{\binom{a}{b}} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha + pa\alpha \\ \beta \end{pmatrix}.$$

Dado un elemento (α, β) de la braza vemos que si α no es coprimo con p entonces queda fijo por la acción de cualquier elemento. Por otro lado si α es coprimo con p, i.e. un generador de $\mathbb{Z}_{p^2}$, entonces su órbita va a consistir de todos los elementos que coinciden con él en la segunda coordenada, y en la primera coordenada módulo p. Las órbitas que generan el grupo aditivo son precisamente las segundas cuando β es no nulo. Podemos parametrizarlas entonces $\mathcal{U}(\mathbb{Z}_p) \times \mathcal{U}(\mathbb{Z}_q)$, con $\mathcal{O}_{\alpha,\beta} = \{(a, \beta) : a \equiv \alpha \pmod{p}\}$.

Para decidir cuáles de las órbitas anteriores proveen la misma solución calculamos el grupo de automorfismos de la braza.

Teorema 4.17. *Si p es un primo impar el grupo de automorfismos de braza de la única braza no trivial de tamaño p^2q con grupo multiplicativo cíclico es isomorfo a $\mathbb{Z}_p \times \mathcal{U}(\mathbb{Z}_q)$.*

Demostración. Los automorfismos del grupo aditivo son $\mathcal{U}(\mathbb{Z}_{p^2}) \times \mathcal{U}(\mathbb{Z}_q)$, actuando por multiplicación en ambas coordenadas. Dado un elemento (x, y) de este grupo de automorfismos, si miramos la condición para que sea automorfismo de la estructura aditiva en la primera coordenada obtenemos que para todo $a, c \in \mathbb{Z}_{p^2}$ se tiene que cumplir

$$xa + xc + x^2pac = xa + xc + xpac.$$

Tomando $a = c = 1$ tenemos que $xp(x - 1) = 0$, es decir que $x \equiv 1 \pmod{p}$. Como el núcleo de la reducción módulo p es isomorfo $\mathbb{Z}_p$ tenemos que el grupo de automorfismos es el que queríamos. □

En particular tenemos que actuar por un automorfismo en un elemento no cambia el resto módulo p de su primera coordenada y entonces dos órbitas que generan $\mathcal{O}_{\alpha,\beta}$ y $\mathcal{O}_{\alpha',\beta'}$ proveen soluciones isomorfas si y sólo si $\alpha = \alpha'$, y por lo tanto hay $p - 1$ soluciones no isomorfas.

Observación 4.18. *Las órbitas anteriores están generadas por generadores del grupo aditivo. En particular sabemos que dadas dos órbitas $\mathcal{O}$ y $\mathcal{O}'$ siempre podemos encontrar $n \in \mathbb{N}$ coprimo con pq tal que $n\mathcal{O} = \mathcal{O}'$. Por la Proposición 4.1 tenemos entonces que a partir de cualquiera de las soluciones no triviales podemos conseguir todas las demas realizando cableados.*

Podemos resumir los resultados obtenidos para los grupos cíclicos de la siguiente manera.

Teorema 4.19. *Dados p y q primos distintos hay exactamente p soluciones indescomponibles no isomorfas con grupo de permutaciones isomorfo a $\mathbb{Z}_{p^2q}$. Todas estas soluciones son equivalentes por cableado.*

4.4.2. Brazas no cíclicas

Las estructuras de las brazas con grupo multiplicativo abeliano y no cíclico están descriptas en el Teorema 4.6. Al igual que en el caso anterior hay siempre una única braza no trivial pero su descripción depende de si p es 2 o no. Observemos que como el grupo multiplicativo no es cíclico en estos casos por la Proposición 4.10 la braza trivial no provee soluciones indescomponibles.

Empezemos entonces por el caso $p = 2$. En este caso la estructura aditiva de la única braza no trivial se identifica con $\mathbb{Z}_{4q} \cong \mathbb{Z}_q \times \mathbb{Z}_4$ y la estructura aditiva queda dada por

$$\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a+c \\ b+(-1)^b d \end{pmatrix}.$$

La acción λ está dada entonces por

$$\lambda_{\begin{pmatrix} a \\ b \end{pmatrix}} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ (-1)^b \beta \end{pmatrix}.$$

Tenemos entonces $2q$ órbitas de un elemento de la forma $\{(\alpha, 0)\}$ o $\{(\alpha, 2)\}$, y otras q órbitas de dos elementos $\mathcal{O}_\alpha = \{(\alpha, \pm 1)\}$. De estas órbitas las que generan el grupo aditivo son las $\mathcal{O}_\alpha$ con α un generador de $\mathbb{Z}_q$. Es decir que estas órbtias están parametrizadas por $\mathcal{U}(\mathbb{Z}_q)$ y hay $q-1$ de ellas.

Para decidir cuáles de las órbitas anteriores proveen la misma solución calculamos el grupo de automorfismos.

Proposición 4.20. *Dado q un primo impar, el grupo de automorfismos la única braza no trivial con estructura multiplicativa ismorfa a $\mathbb{Z}_q \times \mathbb{Z}_2^2$ es isomorfo a $\mathcal{U}(\mathbb{Z}_{4q})$.*

Demostración. El grupo de automorfismos de la estructura aditiva de la braza está dado por $\mathcal{U}(\mathbb{Z}_q) \times \mathcal{U}(\mathbb{Z}_4)$ actuando por multiplicación coordenada a

coordenada. Si miramos la condición para que uno de estos sea un automorfismo también de la estructura multiplicativa tenemos que esta condición se satisface trivialmente en la primera coordenada y en la segunda tenemos

$$xb + (-1)^{xb}xd = xb + (-1)^b xd.$$

Como x es impar por se una unidad de $\mathbb{Z}_4$, tenemos que esta segunda condición también se satisface trivialmente y por lo tanto todos los automorfismos del grupo aditivo resultan automorfismos de braza. □

De este resultado deducimos que todas las órbitas que generan son conjugadas por un automorfismo de brazas, y por lo tanto hay una única solución indescomponible con este grupo de permutaciones.

Veamos ahora el caso p impar. Igual que en el caso de $p = 2$ hay una única braza no trivial con grupo multiplicativo abeliano y no cíclico. En este caso la braza está descripta en el segundo caso del Teorema 4.6, el grupo aditivo es isomorfo a $\mathbb{Z}_p^2 \times \mathbb{Z}_q$, y la estructura aditiva está dada por

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \circ \begin{pmatrix} d \\ e \\ f \end{pmatrix} = \begin{pmatrix} a + d + be \\ b + e \\ c + f \end{pmatrix}.$$

Observemos que esta estructura está definida por la misma ecuación que la braza de la primera parte del Teorema 4.5, i.e. la única braza no trivial con grupo multiplicativo el cíclico de orden $4q$. En particular las descripciones de la acción λ y de las órbitas de esta acción son análogas a las obtenidas en ese caso. Concretamente tenemos órbitas correspondientes a los puntos fijos de la forma $\mathcal{O}'_{\alpha,\gamma} = \{(\alpha, 0, \gamma)\}$ parametrizadas por $\mathbb{Z}_p \times \mathbb{Z}_q$ y otras de la forma $\mathcal{O}_{\alpha,\gamma} = \{(a, \alpha, \gamma) | a \in \mathbb{Z}_p\}$ parametrizadas por $\mathcal{U}(\mathbb{Z}_p) \times \mathbb{Z}_q$. Al igual que en el caso anterior es claro que las órbitas que generan son las de la segunda forma con γ un generador de $\mathbb{Z}_q$.

El cálculo del grupo de automorfismos es también análogo, aunque un poco más delicado.

Proposición 4.21. *Dados p y q primos con p impar, el grupo de automorfismos de la única braza de tamaño p^2q, no trivial con estructura aditiva no cíclica es isomorfa a $G \times \mathcal{U}(\mathbb{Z}_q)$, con*

$$G = \left\{ \begin{pmatrix} z^2 & y \\ 0 & z \end{pmatrix} : z \in \mathbb{Z}_p^\times, y \in \mathbb{Z}_p \right\} \subseteq \mathrm{GL}_2(p).$$

Demostración. El grupo de automorfismos de la estructura aditiva está dado por $\mathrm{GL}_2(p) \times \mathcal{U}(\mathbb{Z}_q)$. Tomando (A, u) un elemento de este grupo, y notando $A = \left(\begin{smallmatrix} x & y \\ w & z \end{smallmatrix}\right)$, al ver la condición de que actúe por automorfismos de la estructura multiplicativa en la segunda y notando obtenemos

$$w(a+d) + z(b+e) = w(a+d+be) + z(b+e).$$

Como esto vale para todo $a, b, d, e \in \mathbb{Z}_p$ tenemos que necesariamente vale $w = 0$. En particular para que A sea invertible debe valer que $x, z \in \mathcal{U}(\mathbb{Z}_p)$. Usando esta condición y mirando ahora la primera coordenada tenemos

$$x(a+d) + y(b+e) + z^2be = x(a+d+be) + y(b+e),$$

y esta ecuación se cumpla para todo $a, b, d, e \in \mathbb{Z}_p$ si y sólo si $x = z^2$. Por último como en la condición en la úlitma coordenada se cumple trivialmente no hay ninguna restricción adicional. □

Observación 4.22. *El grupo G del resultado anterior es el producto semidirecto $\mathbb{Z}_p \rtimes \mathcal{U}(\mathbb{Z}_p)$ con la acción dada por la multplicación por z^{-1}.*

Dadas $\mathcal{O}_{\alpha,\gamma}$ y $\mathcal{O}_{\alpha',\gamma'}$ dos órbitas que generen el grupo aditivo tenemos que la acción de $(A, \gamma^{-1}\gamma')$, con $A = \left(\begin{smallmatrix} \alpha^{-2}\alpha'^2 & 0 \\ 0 & \alpha^{-1}\alpha \end{smallmatrix}\right)$, aplica la primera órbita en la segunda. Tenemos entonces que todas las órbitas proveen soluciones indescomponibles isomorfas.

Podemos resumir lo que sucede con los grupos no cíclicos de tamaño p^2q en el siguiente resultado.

Teorema 4.23. *Dados p y q primos distintos hay una única solución indescomponible con grupo de permutaciones isomorfo a $\mathbb{Z}_p^2 \times \mathbb{Z}_q$.*

4.5. Brazas diedrales

En esta última sección vemos a considerar los grupos diedrales. Antes de empezar el análisis de los distintos casos a considerar podemos notar que a pesar de que los grupos diedrales no son abelianos, tampoco tienen muchos subgrupos con interior normal trivial, lo que simplifica la construcción de las soluciones asociadas.

Concretamente en un grupo diedral cualquier rotación genera un subgrupo normal, así que un grupo con interior normal trivial no puede tener ninguna rotación. Pero por otro lado cualquier par de reflexiones distintas genera una rotación, es decir que los únicos subgrupos no triviales con interior normal trivial son los generados por una única reflexión. En particular deducimos el siguiente resultado.

Teorema 4.24. *Si X es una solución indescomponible con grupo de permutaciones el grupo diedral D_n, entonces $|X| = n$ ó $|X| = 2n$.*

4.5.1. D_{p^2}

Dados p y q primos impares con $p \equiv 1$ (mód q) hay un único producto semidirecto no trivial $\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_q$, con la acción dada por la multiplicación por cualquier elemento de orden q de $\mathbb{Z}_{p^2}$. El grupo diedral D_{p^2} es el caso particular de tomar $q = 2$, y en este caso se puede tomar p cualquier primo impar. Para cualquiera de estos grupos el Teorema 4.7 garantiza que hay una única braza con este grupo multiplicativo. Su estructura aditiva se identifica con $\mathbb{Z}_{p^2} \times \mathbb{Z}_q$ y su estructura multiplicativa queda dada por

$$\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a + g^b c \\ b + d \end{pmatrix},$$

donde g es cualquier elemento de orden q de $\mathbb{Z}_{p^2}^{\times}$. Observemos que estas brazas están definidas por la misma ecuación que las brazas del Teorema 4.4, por lo que el análisis es similar al de esos casos.

La acción λ está dada por

$$\lambda_{\begin{pmatrix} a \\ b \end{pmatrix}} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} g^b \alpha \\ \beta \end{pmatrix}.$$

Del Lema 4.11 deducimos que cualquier órbita que genere el grupo aditivo debe contener un generador. Órbitas de estas hay entonces $\frac{p(p-1)(q-1)}{q}$, cada una con q elementos. El estabilizador de cualquiera de estos generadores es $\mathbb{Z}_{p^2} \times \{0\}$, y su único subgrupo con interior normal trivial es el trivial. En particular cada órbita provee una única solución indescomponible.

Para ver cuáles de estas soluciones son isomorfas calculamos el grupo de automorfismos de la solución.

Proposición 4.25. *Sean p y q primos distintos con $p \equiv 1 \pmod{q}$. El grupo de automorfismos de la única braza con estructura multiplicativa isomorfa a $\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_q$ es isomorfo a $\mathcal{U}(\mathbb{Z}_{p^2})$.*

Demostración. El grupo de isomorfismos de la estructura aditiva está dado por $\mathcal{U}(\mathbb{Z}_{p^2}) \times \mathcal{U}(\mathbb{Z}_q)$ actuando por la multiplicación coordenada a coordenada. La condición de que un elemento (x, y) actúe por automorfismos de la estructura multiplicativa es

$$\begin{pmatrix} xa + xg^b c \\ yb + yd \end{pmatrix} = \begin{pmatrix} xa + xg^{yb} c \\ yb + yd \end{pmatrix}.$$

Vemos entonces que esta condición se cumple para todo $a, d \in \mathbb{Z}_{p^2}$, $b, d \in \mathbb{Z}_q$ si y sólo si $y = 1$, de donde se deduce lo que queríamos. □

Como las órbitas que dan estas soluciones estan generadas por generadores del grupo aditivo, por la Proposición 4.1 tenemos entonces que podemos obtener cualquiera de estas soluciones a partir de cualquier otra de estas realizando cableados.

De este resultado vemos que las órbitas generadas por dos generadores producen la misma solución indescomponible si y sólo si tienen la misma segunda coordenada. Más aún como el grupo aditivo es cíclico podemos obtener cualquier generador de otro multiplicando por algún numero coprimo con p^2q. Es decir que todas las soluciones que obtenemos resultan equivalentes por cableado. Tenemos entonces el siguiente resultado:

Teorema 4.26. *Sean p y q primos tales que $p \equiv 1 \pmod{q}$. Hay $q - 1$ soluciones indescomponibles no isomorfas con grupo de permutaciones isomorfo a $\mathbb{Z}_{p^2} \rtimes \mathbb{Z}_q$, más aún todas estas tienen tamaño p^2q y son todas equivalentes por cableado.*

Tomando $q = 2$ tenemos entonces el siguiente resultado para el caso de los grupos diedrales

Corolario 4.27. *Dado p un primo impar, hay una única solución indescomponible con grupo de permutaciones isomorfo al grupo diedral D_{p^2}. Esta solución tiene tamaño $2p^2$.*

4.5.2. D_{2p}

La última clase de grupos a considerar son los grupos diedrales D_{2p} con p un primo impar. En este caso hay tres estructuras de braza a considerar, descriptas en el Teorema 4.8.

La primera braza que vamos a considerar tiene estructura aditiva isomorfa a $\mathbb{Z}_p \times \mathbb{Z}_4$ y su estructura multiplicativa está dada por

$$\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a + (-1)^b c \\ b + (-1)^b d \end{pmatrix}. \tag{4.2}$$

La acción λ está dada entonces por

$$\lambda_{\begin{pmatrix} a \\ b \end{pmatrix}} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} (-1)^b \alpha \\ (-1)^b \beta \end{pmatrix}.$$

Vemos de esto que salvo la órbita de $(0,0)$ y la de $(0,2)$ todas las órbitas tienen dos elementos, y todos los estabilizadores son iguales al subgrupo

$$\{(a,b) \in \mathbb{Z}_p \times \mathbb{Z}_4 : b \in \{0,2\}\}.$$

De la fórmula para la estructura aditiva vemos que estos elementos son precisamente las rotaciones del grupo diedral. En particular tenemos que el único subgrupo con interior normal que tienen es el subgrupo trivial.

Por el Lema 4.11, las órbitas que generan el grupo aditivo son precisamente las órbitas de algún generador. Para decidir cuales de estas proveen soluciones isomorfas calculamos el grupo de automorfismos de la solución.

Proposición 4.28. *Dado p un primo impar, el grupo de automorfismos de la braza con grupo aditivo cíclico y grupo multiplicativo dado por la ecuación* (4.2) *tiene grupo de automorfismos isomorfo a $\mathcal{U}(\mathbb{Z}_{4p})$.*

Demostración. El grupo de automorfismos del grupo aditivo está dado por $\mathcal{U}(\mathbb{Z}_{4p}) = \mathcal{U}(\mathbb{Z}_p) \times \mathcal{U}(\mathbb{Z}_4)$ actuando por multiplicación coordenada a coordenada. Dado un elemento (x,y) de este grupo la condición de que actúe por automorfismos de del grupo multiplicativo es

$$\begin{pmatrix} x(a + (-1)^b d) \\ y(b + (-1)^b e) \end{pmatrix} = \begin{pmatrix} x(a + (-1)^{yb} d) \\ y(b + (-1)^{yb} e) \end{pmatrix},$$

y como y es impar esta condición se cumple siempre. □

En particular como todos los generadores del grupo aditivo son conjugados por un isomorfismo, tenemos que todas las órbitas generan soluciones indescomponibles isomorfas.

La segunda estructura de braza que vamos a considerar también tiene grupo aditivo isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_4$, y en este caso la estructura multiplicativa es

$$\begin{pmatrix} a \\ b \end{pmatrix} \circ \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a + (-1)^{b(b-1)/2} c \\ b + (-1)^b d \end{pmatrix}. \tag{4.3}$$

En este caso va a haber órbitas de 1, 2 ó 4 elementos. Las órbitas de los generadores del grupo aditivo van a ser órbitas de 4 elementos con estabilizadores $\{(a, 0) : a \in \mathbb{Z}_p\}$, que nuevamente consiste únicamente de rotaciones. Tenemos entonces que cada una de estas órbitas da una única solución indescomponible y para ver cuáles de ellas son isomorfas calculamos el grupo de automorfismos de la braza.

Proposición 4.29. *Dado p un primo impar, el grupo de automorfismos de la braza con grupo aditivo cíclico y estructura multiplicativa dada por la ecuación* (4.3) *es isomorfo a $\mathcal{U}(\mathbb{Z}_p)$.*

Demostración. Como en el caso anterior los automorfismos del grupo aditivo están dados por multiplicar por un elemento $(x, y) \in \mathcal{U}(\mathbb{Z}_p) \times \mathcal{U}(\mathbb{Z}_4)$. Para que uno de estas sea morfismo del grupo aditivo se tiene que cumplir que

$$\begin{pmatrix} x(a + (-1)^{b(b-1)/2} d) \\ y(b + (-1)^b d) \end{pmatrix} = \begin{pmatrix} x(a + (-1)^{yb(yb-1)/2} d) \\ y(b + (-1)^{yb} d) \end{pmatrix},$$

y esto se cumple para todo $a, c \in \mathbb{Z}_p$, $b, d \in \mathbb{Z}_4$ si y sólo si $y = 1$. □

En particular tenemos que dos generadores son conjugados por un automorfismo si y sólo si coinciden en la primera coordenada. Como todas las órbitas de los generadores tienen un elemento que vale 1 en la primera coordenada, podemos concluir que hay una única solución indescomponible a menos de isomorfismo para esta braza.

Queda por analizar una última braza. En este caso la estructura aditiva

es isomorfa a $\mathbb{Z}_2^2 \times \mathbb{Z}_p$ y la multiplicativa queda dada por

$$\begin{pmatrix} a \\ b \\ c \end{pmatrix} \circ \begin{pmatrix} d \\ e \\ f \end{pmatrix} = \begin{pmatrix} a+d \\ b+e \\ c+(-1)^a f \end{pmatrix} \tag{4.4}$$

La acción λ está dada entonces por

$$\lambda_{\begin{pmatrix} a \\ b \\ c \end{pmatrix}} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ (-1)^a \gamma \end{pmatrix}.$$

Si tomamos entonces un elemento (α, β, γ), su órbita tiene uno o dos elementos, y ambos coinciden en las primeras dos coordenadas. Su proyección en las primeras dos coordenadas genera entonces un grupo de orden 2. Tenemos entonces que en este caso no hay ninguna órbita que genere el grupo aditivo y por lo tanto ninguna solución indescomponible tiene esta braza de permutaciones.

Simplemente por completitud calculamos en este caso también el grupo de automorfismos de la braza.

Proposición 4.30. *Sea p un primo impar. El grupo de automorfismos de la braza con grupo aditivo $\mathbb{Z}_2^2 \times \mathbb{Z}_p$ y estructura multiplicativa dada por la ecuación* (4.4) *es isomorfo a $\mathbb{Z}_2 \times \mathcal{U}(\mathbb{Z}_p)$.*

Demostración. El grupo de automorfismos del grupo aditivo está dado por $\mathrm{GL}_2(2) \times \mathcal{U}(\mathbb{Z}_p)$. Dado un elemento (A, u) de este grupo con, $A = \left(\begin{smallmatrix} x & y \\ w & x \end{smallmatrix}\right)$, la condición de que actúe por automorfismos del grupo multiplicativo en las primeras dos coordenadas es trivial. Mirando esta condición en la tercer coordenada tenemos

$$u(c + (-1)^a f) = uc + (-1)^{xa+yb} uf,$$

es decir que para todo $a, b \in \mathbb{Z}_2$ se cumple $a = xa+yb$. Tomando $a = 0$ tenemos $y = 0$. Como A es invertible se sigue de manera inmediata que $x = z = 1$, y por lo tanto (A, u) actúa por automorfismos del grupo aditivo si y sólo si A es unitriangular inferior. □

En conclusión tenemos el siguiente resultado de clasificación de las soluciones con grupo de permutaciones D_{2p}.

Teorema 4.31. *Dado p un primo impar hay dos soluciones indescomponibles no isomorfas con grupo de permutaciones isomorfo a D_{4p}. Ambas soluciones tienen tamaño $4p$.*

Observación 4.32. *En este caso las dos soluciones que se obtienen tienen brazas asociadas diferentes y por lo tanto no se puede conseguir una de otra a través de la operación de cableado. Más aún el ambas soluciones son fijas por la operación de cableado por un n coprimo con $2p$.*

El Teorema 4.24 nos garantiza que cualquier solución con grupo de permutaciones el diedral D_n tiene tamaño n ó $2n$. Sin embargo en los casos analizados sólo se obtienen soluciones de tamaño $2n$. Este no es siempre el caso ya que hay una solución de tamaño 4 con grupo de permutaciones D_4. Sin embargo, una búsqueda exhaustiva por las soluciones de tamaño menor o igual a 8 encuentra únicamente este contraejemplo. Esto nos lleva a proponer la siguiente conjetura.

Conjetura 4.33. *Si $n \neq 4$ todas las soluciones indescomponibles con grupo de permutaciones el diedral D_n tienen tamaño $2n$.*

Esta conjetura fue verificada para el caso de n impar de manera independiente por Kanrar y Rump en [29] y Castelli junto con el autor de esta tesis en [14]. Sigue sin embargo abierta la pregunta en el caso de n par.

Observación 4.34. *En todos los casos analizados en este capítulo, todas las soluciones halladas para una braza dada resultaron equivalentes por cableado, y en particular tienen el mismo invariante diagonal, aunque no lo hayamos calculado en ningún caso. Sin embargo estas observaciones no son resultados generales, como lo muestran los siguientes ejemplos encontrados usando GAP.*

Ejemplo 4.35. Sea (X, r_1) la solución con ID $[6, 589]$ en la base de datos del paquete de Yang–Baxter de GAP. Esta es la solución (X, r_1) con $X = \{1, \ldots, 8\}$ y la función r_1 dada por las siguientes funciones σ:

$$\sigma_1 = (123)(456), \qquad \sigma_2 = (163)(245), \qquad \sigma_3 = (164)(235),$$
$$\sigma_4 = (164)(235), \qquad \sigma_5 = (123)(456), \qquad \sigma_6 = (163)(245).$$

Esta solución tiene función U igual a (132546) y su braza de permutaciones es la braza con ID $[12, 7]$ en la base de datos del paquete de Yang–Baxter de GAP.

Por otro lado la solución (X, r_2) con ID $[6, 592]$, la función r_2 está dada por las funciones σ:

$$\begin{aligned} &\sigma_1 = (124)(356), && \sigma_2 = (163)(245), && \sigma_3 = (123)(456), \\ &\sigma_4 = (123)(456), && \sigma_5 = (124)(356), && \sigma_6 = (163)(245). \end{aligned}$$

Esta solución tiene función U igual a (146)(253) y su braza de permutaciones es nuevamente la braza con ID $[12, 7]$. En particular vemos que el invariante diagonal de estas dos soluciones es distinto y por lo tanto no pueden ser equivalentes por cableado a pesar de tener la misma braza de permutaciones.

Ejemplo 4.36. Consideremos (X, r_1) la solución con $X = \{1, \ldots, 10\}$ y cuya función r_2 está dada por las siguientes funciones σ:

$$\begin{aligned} \sigma_1 = \sigma_3 = \sigma_5 = \sigma_7 = \sigma_9 = (1, 4, 5, 8, 9, 2, 3, 6, 7, 10), \\ \sigma_2 = \sigma_4 = \sigma_6 = \sigma_8 = \sigma_{10} = (1, 2, 5, 6, 9, 10, 3, 4, 7, 8). \end{aligned}$$

Esta solución tiene función U igual a $(1, 10, 9, 8, 7, 6, 5, 4, 3, 2)$, y su braza de permutaciones tiene ID $[50, 7]$ en la base de datos de GAP.

Por otro lado se puede considerar la solución (X, r_2) donde la función r_2 está dada por las siguientes funciones σ:

$$\begin{aligned} \sigma_1 = \sigma_3 = \sigma_5 = \sigma_7 = \sigma_9 = (1, 6, 7, 2, 3, 8, 9, 4, 5, 10), \\ \sigma_2 = \sigma_4 = \sigma_6 = \sigma_8 = \sigma_{10} = (1, 2, 7, 8, 3, 4, 9, 10, 5, 6). \end{aligned}$$

Esta solución también tiene función U igual a $(1, 10, 9, 8, 7, 6, 5, 4, 3, 2)$ y braza de permutaciones la de ID $[50, 7]$. Sin embargo usando GAP se puede verificar que a pesar de tener la misma braza de permutaciones e invariante diagonal estas dos soluciones no sólo no son isomorfas sino que tampoco son equivalentes por cableado. Para verificar esto último sólo hay que chequear que el 3-cableado de estas soluciones es isomorfo a la solución original ya que 3 genera el grupo de unidades de $\mathbb{Z}_3$.

Bibliografía

[1] E. Acri and M. Bonatto. Skew braces of size pq. *Communications in Algebra*, 48(5):1872–1881, 2020.

[2] E. Acri and M. Bonatto. Skew braces of size p^2q I: Abelian type. *Algebra Colloquium*, 29(02):297–320, 2022.

[3] Ö. Akgün, M. Mereb, and L. Vendramin. Enumeration of set-theoretic solutions to the Yang–Baxter equation. *Mathematics of Computation*, 91(335):1469–1481, 2022.

[4] A. A. Alabdali and N. P. Byott. Skew braces of squarefree order. *Journal of Algebra and Its Applications*, 20(07):2150128, 2019.

[5] N. Andruskiewitsch and H.-J. Schneider. Pointed hopf algebras. *New directions in Hopf algebras*, 43:1–68, 2002.

[6] D. Bachiller. Classification of braces of order p^3. *Journal of Pure and Applied Algebra*, 219:3568–3603, 2014.

[7] D. Bachiller and F. Cedó. A family of solutions of the Yang–Baxter equation. *Journal of Algebra*, 412:218–229, 2014.

[8] D. Bachiller, F. Cedó, and E. Jespers. Solutions of the Yang–Baxter equation associated with a left brace. *Journal of Algebra*, 463:80–102, 2016.

[9] R. J. Baxter. Partition function of the eight-vertex lattice model. *Annals of Physics*, 70(1):193–228, 1972.

[10] R. J. Baxter. Solvable eight-vertex model on an arbitrary planar lattice. *Philosophical Transactions of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 289(1359):315–346, 1978.

[11] S. Camp-Mora and R. Sastriques. A criterion for decomposabilty in QYBE. *International Mathematics Research Notices*, 2023(5):3808–3813, 2021.

[12] M. Castelli. On the indecomposable involutive solutions of the Yang–Baxter equation of finite primitive level. *Publicacions Matemàtiques*, 69(2):429 – 444, 2025.

[13] M. Castelli and A. Kanrar. On indecomposable involutive solutions to the Yang-Baxter equation whose squaring map is a p-cycle. *arXiv preprint arXiv:2508.01613*, 2025.

[14] M. Castelli and S. Ramírez. On uniconnected solutions of the Yang-Baxter equation and Dehornoy's class. *Journal of Algebra*, 657:57–80, 2024.

[15] F. Cedó, E. Jespers, and A. Del Rio. Involutive Yang–Baxter groups. *Transactions of the American Mathematical Society*, 362(5):2541–2558, 2010.

[16] F. Cedó, E. Jespers, and J. Okniński. Braces and the Yang–Baxter equation. *Communications in Mathematical Physics*, 327:101–116, 2014.

[17] F. Cedó, E. Jespers, and J. Okniński. Primitive set-theoretic solutions of the Yang–Baxter equation. *Communications in Contemporary Mathematics*, 24(09):2150105, 2022.

[18] F. Cedó, E. Jespers, and J. Okniński. Retractability of set theoretic solutions of the Yang—Baxter equation. *Advances in Mathematics*, 224(6):2472–2484, 2010.

[19] F. Cedó and J. Okniński. Indecomposable solutions of the Yang–Baxter equation of square-free cardinality. *Advances in Mathematics*, 430:109221, 2023.

[20] F. Chouraqui and E. Godelle. Finite quotients of groups of I-type. *Advances in Mathematics*, 258:46–68, 2014.

[21] P. Dehornoy. Set-theoretic solutions of the Yang–Baxter equation, RC-calculus, and Garside germs. *Advances in Mathematics*, 282:93–127, 2014.

[22] P. Dehornoy. *Le calcul des tresses*. Calvage et Mounet, 2019.

[23] C. Dietzel. Braces of order p^2q. *Journal of Algebra and Its Applications*, 20(08):2150140, 2021.

[24] V. G. Drinfeld. On some unsolved problems in quantum group theory. In *Quantum Groups: Proceedings of Workshops held in the Euler International Mathematical Institute, Leningrad, Fall 1990*, pages 1–8. Springer, 2006.

[25] P. Etingof, T. Schedler, and A. Soloviev. Set-theoretical solutions to the quantum Yang–Baxter equation. *Duke Math. J.*, 100(2):169–209, 1999.

[26] T. Gateva-Ivanova and M. Van den Bergh. Semigroups of I-Type. *Journal of Algebra*, 206(1):97–112, 1998.

[27] L. Guarnieri and L. Vendramin. Skew braces and the yang–baxter equation. *Mathematics of Computation*, 86(307):2519–2534, 2017.

[28] A. Kanrar and W. Rump. A decomposition problem for involutive solutions to the Yang–Baxter equation. *Bulletin of the Belgian Mathematical Society - Simon Stevin*, 31(5):688 – 702, 2024.

[29] A. Kanrar and W. Rump. A note on braces and Frobenius action. *Communications in Algebra*, 53(7):2920–2925, 2025.

[30] C. Kassel. *Quantum groups*, volume 155. Springer Science & Business Media, 2012.

[31] C. Kassel and V. Turaev. *Braid groups*, volume 247. Springer Science & Business Media, 2008.

[32] V. Lebed, S. Ramírez, and L. Vendramin. Involutive Yang–Baxter: cabling, decomposability, and Dehornoy class. *Revista Matemática Iberoamericana*, 40(2):623–635, 2023.

[33] S. Ramírez. Indecomposable solutions of the Yang–Baxter equation with permutation group of sizes pq and p^2q. *Communications in Algebra*, 51(10):4185–4194, 2023.

[34] S. Ramírez and L. Vendramin. Decomposition theorems for involutive solutions to the Yang–Baxter equation. *International Mathematics Research Notices*, 2022(22):18078–18091, 2022.

[35] W. Rump. A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation. *Advances in Mathematics*, 193(1):40–55, 2005.

[36] W. Rump. Braces, radical rings, and the quantum Yang–Baxter equation. *Journal of Algebra*, 307(1):153–170, 2007.

[37] W. Rump. Classification of indecomposable involutive set-theoretic solutions to the Yang–Baxter equation. *Forum Mathematicum*, 32(4):891–903, 2020.

[38] V. Turaev. The Yang–Baxter equation and invariants of links. *New Developments in the Theory of Knots*, 11:175, 1990.

[39] D. Van Caudenberg, B. Bogaerts, and L. Vendramin. Incremental SAT-based enumeration of solutions to the Yang–Baxter Equation. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 3–22. Springer, 2025.

[40] L. Vendramin. Extensions of set-theoretic solutions of the Yang–Baxter equation and a conjecture of Gateva-Ivanova. *Journal of Pure and Applied Algebra*, 220(5):2064–2076, 2016.

[41] C.-N. Yang. Some exact results for the many-body problem in one dimension with repulsive delta-function interaction. *Physical Review Letters*, 19(23):1312, 1967.

[42] C. N. Yang. S matrix for the one-dimensional n-body problem with repulsive or attractive δ-function interaction. *Physical Review*, 168(5):1920, 1968.