TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 372, Number 10, 15 November 2019, Pages 7191–7223
https://doi.org/10.1090/tran/7837
Article electronically published on June 17, 2019

THE STRUCTURE MONOID AND ALGEBRA OF A NON-DEGENERATE SET-THEORETIC SOLUTION OF THE YANG–BAXTER EQUATION

ERIC JESPERS, ŁUKASZ KUBAT, AND ARNE VAN ANTWERPEN

Abstract. For a finite involutive non-degenerate solution (X, r) of the Yang–Baxter equation it is known that the structure monoid $M(X, r)$ is a monoid of I-type, and the structure algebra $K[M(X, r)]$ over a field K shares many properties with commutative polynomial algebras; in particular, it is a Noetherian PI-domain that has finite Gelfand–Kirillov dimension. In this paper we deal with arbitrary finite (left) non-degenerate solutions. Although the structure of both the monoid $M(X, r)$ and the algebra $K[M(X, r)]$ is much more complicated than in the involutive case, we provide some deep insights.

In this general context, using a realization of Lebed and Vendramin of $M(X, r)$ as a regular submonoid in the semidirect product $A(X, r) \rtimes \mathrm{Sym}(X)$, where $A(X, r)$ is the structure monoid of the rack solution associated to (X, r), we prove that $K[M(X, r)]$ is a finite module over a central affine subalgebra. In particular, $K[M(X, r)]$ is a Noetherian PI-algebra of finite Gelfand–Kirillov dimension bounded by $|X|$. We also characterize, in ring-theoretical terms of $K[M(X, r)]$, when (X, r) is an involutive solution. This characterization provides, in particular, a positive answer to the Gateva-Ivanova conjecture concerning cancellativity of $M(X, r)$.

These results allow us to control the prime spectrum of the algebra $K[M(X, r)]$ and to describe the Jacobson radical and prime radical of $K[M(X, r)]$. Finally, we give a matrix-type representation of the algebra $K[M(X, r)]/P$ for each prime ideal P of $K[M(X, r)]$. As a consequence, we show that if $K[M(X, r)]$ is semiprime, then there exist finitely many finitely generated abelian-by-finite groups, $G_1, \dots, G_m$, each being the group of quotients of a cancellative subsemigroup of $M(X, r)$ such that the algebra $K[M(X, r)]$ embeds into $\mathrm{M}_{v_1}(K[G_1]) \times \cdots \times \mathrm{M}_{v_m}(K[G_m])$, a direct product of matrix algebras.

Received by the editors December 5, 2018.

2010 *Mathematics Subject Classification.* Primary 16N60, 16T25; Secondary 16R20, 16S36, 16S37.

Key words and phrases. Yang–Baxter equation, set-theoretic solution, prime ideal, (skew) brace.

The first author was supported in part by Onderzoeksraad of Vrije Universiteit Brussel and Fonds voor Wetenschappelijk Onderzoek (Belgium), grant G016117.

The second author was supported by Fonds voor Wetenschappelijk Onderzoek (Flanders), grant G016117.

The third author was supported by Fonds voor Wetenschappelijk Onderzoek (Flanders) via an FWO Aspirant-mandate.

©2019 American Mathematical Society

Introduction

Let V be a vector space over a field K. A linear map $R\colon V\otimes V\to V\otimes V$ is called a solution of the Yang–Baxter equation (or braided equation) if

$$(R\otimes \mathrm{id})\circ(\mathrm{id}\otimes R)\circ(R\otimes \mathrm{id})=(\mathrm{id}\otimes R)\circ(R\otimes \mathrm{id})\circ(\mathrm{id}\otimes R).$$

Recall that this equation originates from papers by Baxter [8] and Yang [47] on statistical physics, and the search for solutions has attracted numerous studies both in mathematical physics and pure mathematics.

As the study of arbitrary solutions is complex, Drinfeld, in 1992 [15], proposed to study the solutions which are induced by a linear extension of a map $r\colon X\times X\to X\times X$, where X is a basis of V. In this case r satisfies

$$(r\times \mathrm{id})\circ(\mathrm{id}\times r)\circ(r\times \mathrm{id})=(\mathrm{id}\times r)\circ(r\times \mathrm{id})\circ(\mathrm{id}\times r),$$

and one says that (X,r) is a set-theoretic solution of the Yang–Baxter equation. For any $x,y\in X$, we put $r(x,y)=(\lambda_x(y),\rho_y(x))$. Since the late 1990's several groundbreaking results have been discovered on this topic, including those by Gateva-Ivanova and Van den Bergh [21], Etingof, Schedler, and Soloviev [16], and Lu, Yan, and Zhu [34]. The investigations on the subject have intensified even more since the discovery of several algebraic structures associated to set-theoretic solutions. A particularly nice class of set-theoretic solutions (X,r) are the bijective (i.e., r is a bijection) solutions that are left and right non-degenerate (i.e., each λ_x, respectively each ρ_x, is a bijection). If furthermore $r^2=\mathrm{id}$, then the solution is said to be involutive. In order to deal with such involutive solutions Rump [41,43] introduced the new algebraic structure called "(left) brace", and Guarnieri and Vendramin [23] extended this algebraic structure to a "(left) skew brace" in order to also deal with arbitrary bijective non-degenerate solutions. Many fundamental results on these structures already have been obtained [4,5,7,12,13,18,30,33,42,45]. In particular, it has been shown that determining all finite (i.e., X is a finite set) bijective involutive non-degenerate solutions is equivalent to describing all finite (left) braces. In [6] a concrete realization of this description has been given. Moreover, braces have lent themselves as a novel method to solve questions in group and ring theory. For instance, Amberg, Dickenschied, and Sysak in [1] posed the question whether the adjoint group of a nil ring is an Engel group, and Zelmanov asked a similar question in the context of nil algebras over an uncountable field. Smoktunowicz, using tools related to braces, gave negative answers to both of these questions in [44]. Also non-bijective set-theoretic solutions are of importance and receive attention. For example Lebed in [31] shows that idempotent solutions provide a unified treatment of factorizable monoids, free and free commutative monoids, distributive lattices and Young tableaux, and Catino, Colazzo, and Stefanelli [10] and Jespers and Van Antwerpen [27] introduced the algebraic structure called "(left) semi-brace" to deal with solutions that are not necessarily non-degenerate or that are idempotent.

Etingof, Schedler, and Soloviev in [16] and Gateva-Ivanova and Van den Bergh in [21] introduced the following associated algebraic structures to a set-theoretic solution (X,r): the structure group $G(X,r)=\mathrm{gr}(X\mid xy=uv \text{ if } r(x,y)=(u,v))$ and the structure monoid $M(X,r)=\langle X\mid xy=uv \text{ if } r(x,y)=(u,v)\rangle$. In case (X,r) is finite involutive and non-degenerate it is shown that the group $G(X,r)$ is solvable and it is naturally embedded into the semidirect product $\mathbb{Z}^{(X)}\rtimes \mathrm{Sym}(X)$, where $\mathrm{Sym}(X)$ acts naturally on the free abelian group $\mathbb{Z}^{(X)}$ of rank $|X|$. It turns out that $G(X,r) = \mathrm{gr}((x,\lambda_x) \mid x \in X)$ and, in particular, these groups are (free abelian)-by-finite. Furthermore, in [25] it is shown that $M(X,r)$ is embedded in $G(X,r)$ and the latter is the group of fractions of $M(X,r)$. Furthermore, $G(X,r)$ and $\mathcal{G}(X,r) = \mathrm{gr}(\lambda_x \mid x \in X)$ are left braces, and, for finite X, groups of the type $\mathcal{G}(X,r)$ correspond to all finite (left) braces (for details we refer to [11]). In [21] Gateva-Ivanova and Van den Bergh showed that these structure groups are groups of I-type and, in particular, they are finitely generated and torsion-free, i.e., Bieberbach groups. These groups and monoids are of combinatorial interest, and their associated monoid algebra $K[M(X,r)]$, simply called the structure algebra of (X,r) (as it is the algebra generated by the set X and with defining relations $xy = uv$ if $r(x,y) = (u,v)$), provide non-trivial examples of quadratic algebras. That is, they are positively graded algebras generated by the homogeneous part of degree 1 and with defining homogeneous degree 2 relations. The structure algebras have similar homological properties to polynomial algebras in finitely many commuting variables; in particular they are Noetherian domains that satisfy a polynomial identity (PI-algebras) and have finite Gelfand–Kirillov dimension.

Recently, Lebed and Vendramin [32] studied the structure group $G(X,r)$ for arbitrary finite bijective non-degenerate solutions (i.e., not necessarily involutive). In [32, 34, 46] they associate, via a bijective 1-cocycle, to the structure group $G(X,r)$ the structure group $G(X,\triangleleft_r)$ of the structure rack $(X,\triangleleft_r)$ of (X,r). As a consequence, it follows that again the groups $G(X,r)$ are abelian-by-finite. Recall that a set X with a self-distributive operation $\triangleleft$ is called a rack if the map $y \mapsto y \triangleleft x$ is bijective for any $x \in X$ (cf. [29]). In contrast to the involutive case, the set X is not necessarily canonically embedded into $G(X,r)$, the reason being that $M(X,r)$ need not be cancellative in general (i.e., it is not necessarily embedded in a group). Hence, for an arbitrary solution (X,r) the structure monoid $M(X,r)$ contains more information on the original solution. However, it is in general not true that two set-theoretic solutions (X,r) and (Y,s) are isomorphic if and only if the monoids $M(X,r)$ and $M(Y,s)$ are isomorphic. This does hold if one of the solutions (and thus both) is assumed to be an involutive non-degenerate set-theoretic solution.

In this paper we give a structural approach to the study of the structure monoid $M(X,r)$ and the structure algebra $K[M(X,r)]$ for an arbitrary bijective left non-degenerate solution (X,r). In the same spirit as in [32], in Section 1 we associate a structure monoid, called the derived structure monoid and denoted $A(X,r)$, to such a solution and we show that the monoid $M(X,r)$ is a regular submonoid of $A(X,r) \rtimes \mathrm{Sym}(X)$; i.e., there is a bijective 1-cocycle $M(X,r) \to A(X,r)$. Again $A(X,r)$ turns out to be the structure monoid of a rack. This description allows us to study, in Sections 2 and 4, the algebraic structure of the monoids $A(X,r)$ and $M(X,r)$ and the structure algebras $K[A(X,r)]$ and $K[M(X,r)]$. It is shown that for a finite bijective left non-degenerate solution both monoids $A(X,r)$ and $M(X,r)$ are central-by-finite; i.e., they are finite "modules" over a finitely generated central submonoid. Hence, both structure algebras are Noetherian and PI. Furthermore, these algebras are closely related to polynomial algebras in finitely many commuting variables. For instance we show that the classical Krull dimensions and Gelfand–Kirillov dimensions of both algebras $K[A(X,r)]$ and $K[M(X,r)]$ coincide and are equal to $\mathrm{rk}\, A(X,r) = \mathrm{rk}\, M(X,r)$, i.e., the rank of the respective monoids (that is, the largest possible rank of a free abelian submonoid). Moreover, this dimension is bounded by $|X|$, and it also is shown that these dimensions are determined by the orbits of subsolutions of the rack solution (X,s) associated to (X,r). Gateva-Ivanova in [19] conjectured that the structure monoid of a finite square-free (i.e., $r(x,x)=(x,x)$ for all $x\in X$) non-degenerate solution (X,r) is cancellative if and only if the solution (X,r) is involutive. Using the structural results we prove that this conjecture is true, even without assuming that the solution (X,r) is square-free. Moreover, we show that the involutiveness of a solution is characterized by many properties of the structure algebra $K[M(X,r)]$. Among others, this coincides with the maximality of the Gelfand–Kirillov dimension, i.e., $\operatorname{GKdim} K[M(X,r)]=|X|$, and it is equivalent to $K[M(X,r)]$ being a prime algebra or a domain.

In Section 3 we study the prime ideals of the monoid $A(X,r)$ and the prime ideals of the related algebra. It is shown that prime ideals of $A(X,r)$ are in correspondence with specific subsolutions of the rack solution (X,s) associated to (X,r). Furthermore, we provide a description of the prime ideals of $K[A(X,r)]$.

In Section 5 we study the prime ideals of the monoid $M(X,r)$ and the prime ideals of $K[M(X,r)]$. In [22] prime ideals of monoids of IG-type were studied by Goffa and Jespers. It is shown that for a finite square-free left non-degenerate solution (X,r) the prime ideals of $A(X,r)$ determine the prime ideals of $M(X,r)$; these results are similar to those obtained for monoids of IG-type, i.e., regular submonoids of the holomorph of a finitely generated cancellative abelian monoid. Furthermore, prime ideals of the algebra $K[M(X,r)]$, where (X,r) is a finite bijective left non-degenerate solution, which intersect the monoid trivially correspond to prime ideals of the group algebra $K[G(X,r)]$. As $G(X,r)$ is a finitely generated finite-conjugacy group (FC-group for short) the prime ideals of $K[G(X,r)]$ are easy to describe. For more fundamental results of prime ideals of finitely generated abelian-by-finite groups or, more generally, polycyclic-by-finite groups, we refer the reader to the fundamental work of Roseblade [40].

In [20] Gateva-Ivanova, Jespers, and Okniński and in [26, 28] Jespers, Okniński, and Van Campenhout studied the prime ideals of quadratic algebras coming from monoids of quadratic type. These are monoids defined on a finite set X of cardinality n and defined by $\binom{n}{2}$ monomial relations of degree two so that the associated map $r\colon X\times X\to X\times X$ is non-degenerate, but it does not have to be a set-theoretic solution of the Yang–Baxter equation. They showed that the intersection of such prime ideals with the monoid is highly dependent on the divisibility structure of the monoid. In Section 6 the divisibility structure of $M(X,r)$ is studied. It is shown that the intersection of a prime ideal of $K[M(X,r)]$ with $M(X,r)$ is determined by divisibility properties. These results allow us to give a description of the Jacobson radical $\mathcal{J}(K[M(X,r)])$ and prime radical $\mathcal{B}(K[M(X,r)])$ of $K[M(X,r)]$.

In the final section, Section 7, we prove a matrix-type representation of the prime algebra $K[M(X,r)]/P$ for each prime ideal P of $K[M(X,r)]$. It is shown that the classical ring of quotients $\mathrm{Q_{cl}}(K[M(X,r)]/P)$ of $K[M(X,r)]/P$ is the same as $\mathrm{Q_{cl}}(\mathrm{M}_v(K[G]/P_0))$, where P_0 is a prime ideal of a group algebra $K[G]$ with G the group of quotients of a cancellative subsemigroup of $M(X,r)$ and $v\geqslant 1$ is determined by the number of orthogonal cancellative subsemigroups of an ideal in $M(X,r)/(P\cap M(X,r))$. As a consequence, we show that if, furthermore, $K[M(X,r)]$ is semiprime, then there exist finitely many finitely generated abelian-by-finite groups, say $G_1,\dots,G_m$, each being the group of quotients of a cancellative subsemigroup of $M(X,r)$ such that $K[M(X,r)]$ embeds into $\mathrm{M}_{v_1}(K[G_1])\times\cdots\times\mathrm{M}_{v_m}(K[G_m])$ for some $v_1,\dots,v_m\geqslant 1$.

1. Preliminaries

Let X be a non-empty set and let $r\colon X \times X \to X \times X$ be a map denoted as

$$r(x,y) = (\lambda_x(y), \rho_y(x))$$

for $x, y \in X$. Then (X,r) is a solution of the Yang–Baxter equation if and only if, for any $x,y,z \in X$, the following equalities hold:

$$\lambda_x(\lambda_y(z)) = \lambda_{\lambda_x(y)}(\lambda_{\rho_y(x)}(z)), \tag{1}$$

$$\lambda_{\rho_{\lambda_y(z)}(x)}(\rho_z(y)) = \rho_{\lambda_{\rho_y(x)}(z)}(\lambda_x(y)), \tag{2}$$

$$\rho_z(\rho_y(x)) = \rho_{\rho_z(y)}(\rho_{\lambda_y(z)}(x)).$$

For a solution (X,r) we define its structure monoid (we use the terminology introduced in [16]; in [19] this is called the monoid associated with (X,r))

$$M(X,r) = \langle X \mid xy = \lambda_x(y)\rho_y(x) \quad \text{for all } x,y \in X\rangle.$$

It turns out that in the study of $M(X,r)$ the derived structure monoid (we use terminology similar to [46] in the context of groups)

$$A(X,r) = \langle X \mid x\lambda_x(y) = \lambda_x(y)\lambda_{\lambda_x(y)}(\rho_y(x)) \quad \text{for all } x,y \in X\rangle$$

plays a crucial role. If we put $z = \lambda_x(y)$, then the defining relations of $A(X,r)$ can be rewritten as $xz = z\sigma_z(x)$, where $\sigma_z(x) = \lambda_z(\rho_{\lambda_x^{-1}(z)}(x))$. Hence,

$$A(X,r) = \langle X \mid xz = z\sigma_z(x) \text{ for all } x,z \in X\rangle.$$

Moreover, if (X,r) is bijective left non-degenerate, it can be proved that (X,r^{-1}) is automatically a left non-degenerate solution. In this case, writing $r^{-1}(x,y) = (\hat{\lambda}_x(y), \hat{\rho}_y(x))$ for $x,y \in X$, it can be verified that

$$\sigma_z(x) = \lambda_z(\rho_{\lambda_x^{-1}(z)}(x)) = \lambda_z(\hat{\lambda}_z^{-1}(x)) \tag{3}$$

for all $x,z \in X$. Notice that the second equality in (3) leads to $\sigma_z \in \mathrm{Sym}(X)$. Note also that if the solution (X,r) is involutive, then $\sigma_x = \mathrm{id}$ for all $x \in X$ and thus $A(X,r)$ is the free abelian monoid of rank $|X|$.

Since the defining relations of $M(X,r)$ and $A(X,r)$ are homogeneous, both these monoids inherit a gradation determined by the length function on words in the free monoid on X. We shall freely use this fact throughout the paper. Moreover, the length of an element s in one of the monoids under consideration will be denoted by $|s|$.

Let (X,r) and (Y,s) be solutions of the Yang–Baxter equation. We say that a map $f\colon X \to Y$ is a morphism of solutions (and we write $f\colon (X,r) \to (Y,s)$) if $(f \times f) \circ r = s \circ (f \times f)$ or, in other words, if the following diagram

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

is commutative. Moreover, the solutions (X,r) and (Y,s) are called isomorphic provided there exists a bijective morphism of solutions $f\colon (X,r) \to (Y,s)$. Two involutive non-degenerate solutions (X,r) and (Y,s) are isomorphic if and only if their structure monoids $M(X,r)$ and $M(Y,s)$ are isomorphic. To see this, it is sufficient to induce an action of r on the words of length two in the alphabet X and observe that these orbits are of size two or smaller. However, the following example shows that this is no longer true for non-involutive solutions.

Example 1.1. Let $X = \{x_1, x_2, x_3\}$. Define $\sigma_1 = (2,3)$, $\sigma_2 = (1,3)$, $\sigma_3 = (1,2)$ and consider the maps $r, s\colon X \times X \to X \times X$ given by

$$r(x_i, x_j) = (x_j, x_{\sigma_j(i)}) \qquad \text{and} \qquad s(x_i, x_j) = (x_{\sigma_i(j)}, x_i).$$

It is easy to check that both (X, r) and (X, s) are bijective (in fact, $r^3 = s^3 = \mathrm{id}$) non-degenerate solutions of the Yang–Baxter equation. Moreover, $M(X, r) = A(X, r) = A(X, s) = M(X, s)$. However, (X, r) and (X, s) are not isomorphic as solutions. Indeed, if $f\colon (X, r) \to (X, s)$ were an isomorphism of solutions, then, in particular, $f \circ \sigma_x = f$ for all $x \in X$, which would lead to $\sigma_x = \mathrm{id}$, a contradiction.

The remaining part of this section is based on the work of Lebed and Vendramin [32]. For completeness' sake and to translate their results on bijective 1-cocycles into the language of regular submonoids, which will be crucial to all sections in this paper, we include detailed proofs.

By an action of a monoid M on a monoid A we mean a left action by automorphisms, that is, a morphism of monoids $\theta\colon M \to \mathrm{Aut}(A)$ (multiplication in $\mathrm{Aut}(A)$ will often be written as a juxtaposition). Recall that a map $\varphi\colon M \to A$ is called a bijective 1-cocycle with respect to the action θ provided φ is bijective, $\varphi(1) = 1$ (i.e., φ preserves units of monoids) and satisfies the 1-cocycle condition

$$\varphi(xy) = \varphi(x)\theta(x)(\varphi(y))$$

for all $x, y \in M$.

Lemma 1.2. *Assume that $\theta\colon M \to \mathrm{Aut}(A)$ is an action and $\varphi\colon M \to A$ is a bijective 1-cocycle with respect to θ. For a congruence η on M define*

$$\varphi(\eta) = \{(\varphi(x), \varphi(y)) : (x, y) \in \eta\} \subseteq A \times A.$$

If the congruence η satisfies the following properties:

(1) $\eta \subseteq \operatorname{Ker}\theta = \{(x, y) \in M \times M : \theta(x) = \theta(y)\}$ *and*
(2) $\varphi(\eta) = \{(\theta(z)(\varphi(x)), \theta(z)(\varphi(y))) : (x, y) \in \eta\}$ *for all $z \in M$,*

then $\varphi(\eta)$ is a congruence on A. Moreover, θ induces an action $\overline{\theta}\colon M/\eta \to \mathrm{Aut}(A/\varphi(\eta))$ and φ induces a bijective 1-cocycle $\overline{\varphi}\colon M/\eta \to A/\varphi(\eta)$ with respect to $\overline{\theta}$.

Proof. Using bijectivity of φ it is easy to verify that $\varphi(\eta)$ is an equivalence relation on A. To check that $\varphi(\eta)$ is a left congruence fix $(a, b) \in \varphi(\eta)$ and $c \in A$. Since φ is bijective, we can write $c = \varphi(z)$ for some $z \in M$. By (2) we get $a = \theta(z)(\varphi(x))$ and $b = \theta(z)(\varphi(y))$ for some $(x, y) \in \eta$. Now

$$ca = \varphi(z)\theta(z)(\varphi(x)) = \varphi(zx) \qquad \text{and} \qquad cb = \varphi(z)\theta(z)(\varphi(y)) = \varphi(zy).$$

Because η is a left congruence we get $(zx, zy) \in \eta$, and thus $(ca, cb) \in \varphi(\eta)$. To prove that $\varphi(\eta)$ is a right congruence assume that $(a, b) \in \varphi(\eta)$ and $c \in A$. By the definition of $\varphi(\eta)$ there exists $(x, y) \in \eta$ such that $(a, b) = (\varphi(x), \varphi(y))$. By (1) we know that $\theta(x) = \theta(y)$. Moreover, bijectivity of φ assures that $c = \theta(x)(\varphi(z)) = \theta(y)(\varphi(z))$ for some $z \in M$. Now

$$ac = \varphi(x)\theta(x)(\varphi(z)) = \varphi(xz) \qquad \text{and} \qquad bc = \varphi(y)\theta(y)(\varphi(z)) = \varphi(yz).$$

Since η is a right congruence we get $(xz, yz) \in \eta$. Hence $(ac, bc) \in \varphi(\eta)$.

To finish the proof observe that (1) implies that there exists an action of M/η on A induced by θ. Moreover, (2) guarantees that the latter action induces an action $\overline{\theta}\colon M/\eta \to \operatorname{Aut}(A/\varphi(\eta))$. Finally, it is clear that φ induces a map $\overline{\varphi}\colon M/\eta \to A/\varphi(\eta)$ satisfying $\overline{\varphi}(1) = 1$ and the cocycle condition with respect to $\overline{\theta}$. Moreover, bijectivity of $\overline{\varphi}$ follows easily from bijectivity of φ. □

Lemma 1.3. *Assume that $\theta\colon M \to \operatorname{Aut}(A)$ is an action and $\varphi\colon M \to A$ is a bijective 1-cocycle with respect to θ. Let $\mathcal{G} = \theta(M) \subseteq \operatorname{Aut}(A)$, which is a submonoid of $\operatorname{Aut}(A)$. Then the map $f\colon M \to A \rtimes \mathcal{G}$ defined as $f(x) = (\varphi(x), \theta(x))$ for $x \in M$ is an injective morphism of monoids. In particular,*

$$M \cong f(M) = \{(a, \phi(a)) : a \in A\} \subseteq A \rtimes \mathcal{G},$$

where the map $\phi = \theta \circ \varphi^{-1}\colon A \to \mathcal{G}$ satisfies $\phi(a)\phi(b) = \phi(a\phi(a)(b))$ for $a, b \in A$.

Proof. We have $f(1) = (\varphi(1), \theta(1)) = (1, \mathrm{id})$. Moreover, if $x, y \in M$, then

$$\begin{aligned} f(xy) &= (\varphi(xy), \theta(xy)) \\ &= (\varphi(x)\theta(x)(\varphi(y)), \theta(x)\theta(y)) \\ &= (\varphi(x), \theta(x))(\varphi(y), \theta(y)) \\ &= f(x)f(y). \end{aligned}$$

Since φ is injective, f is injective as well. Finally, if $a, b \in A$, then $a = \varphi(x)$ and $b = \varphi(y)$ for some $x, y \in M$. Therefore

$$\phi(a)\phi(b) = \theta(x)\theta(y) = \theta(xy) = \phi(\varphi(xy)) = \phi(\varphi(x)\theta(x)(\varphi(y))) = \phi(a\phi(a)(b)).$$

Hence the result follows. □

Proposition 1.4. *Assume that (X, r) is a left non-degenerate solution of the Yang–Baxter equation. Let $A = A(X, r)$, $M = M(X, r)$, and $\mathcal{G} = \mathcal{G}(X, r) = \operatorname{gr}(\lambda_x \mid x \in X) \subseteq \operatorname{Sym}(X)$.*

(1) *There exists an action $\theta\colon M \to \operatorname{Aut}(A)$ and a bijective 1-cocycle $\varphi\colon M \to A$ with respect to θ satisfying $\theta(x) = \lambda_x$ and $\varphi(x) = x$ for $x \in X$. In particular, $\mathcal{G} = \theta(M)$.*
(2) *The map $f\colon M \to A \rtimes \mathcal{G}$ defined as $f(x) = (\varphi(x), \theta(x))$ for $x \in M$ is an injective morphism of monoids. In particular,*

$$M \cong f(M) = \{(a, \phi(a)) : a \in A\} \subseteq A \rtimes \mathcal{G},$$

where the map $\phi = \theta \circ \varphi^{-1}\colon A \to \mathcal{G}$ satisfies $\phi(a)\phi(b) = \phi(a\phi(a)(b))$ for $a, b \in A$. That is, M is a regular submonoid of the semidirect product $A \rtimes \mathcal{G}$.
(3) *If the set X is finite, then $\mathcal{G}$ is a finite group.*

Proof. Let F denote the free monoid on X. Define the action $\vartheta\colon F \to \operatorname{Aut}(F)$ by the rule $\vartheta(x) = \lambda_x$ for $x \in X$. Similarly, let $\psi\colon F \to F$ be the bijective 1-cocycle with respect to ϑ induced by the rule $\psi(x) = x$ for $x \in X$. Denote by η the congruence on F generated by pairs $(xy, \lambda_x(y)\rho_y(x))$ for all $x, y \in X$. Clearly, we have $F/\eta \cong M$. Moreover, it follows from equation (1) that $\eta \subseteq \operatorname{Ker}\vartheta$. Now, fix $x, y, z \in X$ and put

$$u = \lambda_z(x) \in X \qquad \text{and} \qquad v = \lambda_{\rho_x(z)}(y) \in X.$$

Then using equation (1) we get

$$\begin{aligned}\vartheta(z)(\psi(xy)) &= \lambda_z(x\lambda_x(y))\\ &= \lambda_z(x)\lambda_z(\lambda_x(y))\\ &= \lambda_z(x)\lambda_{\lambda_z(x)}(\lambda_{\rho_x(z)}(y))\\ &= u\lambda_u(v)\\ &= \psi(uv).\end{aligned}$$

Furthermore, equations (1) and (2) yield

$$\begin{aligned}\vartheta(z)(\psi(\lambda_x(y)\rho_y(x))) &= \lambda_z(\lambda_x(y)\lambda_{\lambda_x(y)}(\rho_y(x)))\\ &= \lambda_z(\lambda_x(y))\lambda_z(\lambda_{\lambda_x(y)}(\rho_y(x)))\\ &= \lambda_{\lambda_z(x)}(\lambda_{\rho_x(z)}(y))\lambda_{\lambda_z(\lambda_x(y))}(\lambda_{\rho_{\lambda_x(y)}(z)}(\rho_y(x)))\\ &= \lambda_{\lambda_z(x)}(\lambda_{\rho_x(z)}(y))\lambda_{\lambda_{\lambda_z(x)}(\lambda_{\rho_x(z)}(y))}(\rho_{\lambda_{\rho_x(z)}(y)}(\lambda_z(x)))\\ &= \lambda_u(v)\lambda_{\lambda_u(v)}(\rho_v(u))\\ &= \psi(\lambda_u(v)\rho_v(u)).\end{aligned}$$

Hence $\psi(\eta) = \{(\vartheta(z)(x), \vartheta(z)(y)) : (x, y) \in \eta\}$ for all $z \in F$. Concluding, the congruence η satisfies both conditions (1) and (2) from Lemma 1.2. Thus $\psi(\eta)$ is a congruence on F. Moreover, the congruence $\psi(\eta)$ is generated by pairs

$$(\psi(xy), \psi(\lambda_x(y)\rho_y(x))) = (x\lambda_x(y), \lambda_x(y)\lambda_{\lambda_x(y)}(\rho_y(x)))$$

for all $x, y \in X$. Therefore $F/\psi(\eta) \cong A$ and both statements (1) and (2) of the proposition are direct consequences of Lemmas 1.2 and 1.3. Since statement (3) is obvious, the result is proved. □

It is worth adding that for a solution (X, r) we can also define a “right analog” $A'(X, r)$ of the monoid $A(X, r)$ as

$$A'(X, r) = \langle X \mid \rho_y(x)y = \rho_{\rho_y(x)}(\lambda_x(y))\rho_y(x) \quad \text{for all } x, y \in X\rangle.$$

If the solution (X, r) is right non-degenerate, then one can show (in a similar manner as in Proposition 1.4) that there exist a right action of $M(X, r)$ on $A'(X, r)$ and a bijective (right) 1-cocycle $M(X, r) \to A'(X, r)$ with respect to this action. Hence, one obtains that the structure monoid $M(X, r)$ is isomorphic to the regular submonoid $\{(\phi'(a), a) : a \in A'(X, r)\}$ of the semidirect product $\mathcal{G}'(X, r)^{\mathrm{op}} \ltimes A'(X, r)$, where $\mathcal{G}'(X, r) = \mathrm{gr}(\rho_x \mid x \in X) \subseteq \mathrm{Sym}(X)$ and the map $\phi' \colon A'(X, r) \to \mathcal{G}'(X, r)$ satisfies $\phi'(b)\phi'(a) = \phi'(\phi'(b)(a)b)$ for all $a, b \in A'(X, r)$.

2. Structure of the monoid $A(X, r)$ and its algebra

The following lemma and proposition are proved in [46] and [34] for right non-degenerate solutions. We include the proofs for completeness' sake.

Lemma 2.1. *Let (X, r) be a left non-degenerate solution of the Yang–Baxter equation. Then*

$$\lambda_x \circ \sigma_y = \sigma_{\lambda_x(y)} \circ \lambda_x$$

for all $x, y \in X$, where σ_z for $z \in X$ is defined by the first equality in (3).

Proof. Let $z \in X$. By (3) and (1) we get

$$\lambda_x(\sigma_y(z)) = \lambda_x(\lambda_y(\rho_{\lambda_z^{-1}(y)}(z))) = \lambda_{\lambda_x(y)}(\lambda_{\rho_y(x)}(\rho_{\lambda_z^{-1}(y)}(z))).$$

Denote $t = \lambda_z^{-1}(y) \in X$. Then using (2) the previous equation becomes

$$\lambda_{\lambda_x(y)}(\lambda_{\rho_{\lambda_z(t)}(x)}(\rho_t(z))) = \lambda_{\lambda_x(y)}(\rho_{\lambda_{\rho_z(x)}(t)}(\lambda_x(z))) = \lambda_{\lambda_x(y)}(\rho_{\lambda_{\rho_z(x)}(\lambda_z^{-1}(y))}(\lambda_x(z))).$$

Applying (1) and (3) once more, we get that this is equal to

$$\lambda_{\lambda_x(y)}(\rho_{\lambda^{-1}_{\lambda_x(z)}(\lambda_x(y))}(\lambda_x(z))) = \sigma_{\lambda_x(y)}(\lambda_x(z)),$$

and the result follows. □

Proposition 2.2. *Assume that (X, r) is a left non-degenerate solution of the Yang–Baxter equation. Define $s\colon X \times X \to X \times X$ by $s(x, y) = (y, \sigma_y(x))$. Then (X, s) is a left non-degenerate solution of the Yang–Baxter equation satisfying $M(X, s) = A(X, s) = A(X, r)$. Moreover, the solution (X, r) is bijective if and only if (X, s) is bijective if and only if (X, s) is right non-degenerate, and in this case (X, s) is called the rack solution associated to (X, r).*

Proof. Let $r_1 = \mathrm{id} \times r$, $r_2 = r \times \mathrm{id}$, $s_1 = \mathrm{id} \times s$, and $s_2 = s \times \mathrm{id}$. Our aim is to show that

$$s_1 \circ s_2 \circ s_1 = s_2 \circ s_1 \circ s_2.$$

We shall prove that $s_i = J \circ r_i \circ J^{-1}$ for $1 \leqslant i \leqslant 2$, where the map $J\colon X \times X \times X \to X \times X \times X$ is defined as $J(x, y, z) = (x, \lambda_x(y), \lambda_x(\lambda_y(z)))$, which clearly implies what we need. First note that J is indeed a bijection with the inverse given by $J^{-1}(x, y, z) = (x, \lambda_x^{-1}(y), \lambda^{-1}_{\lambda_x^{-1}(y)}(\lambda_x^{-1}(z)))$. Put

$$u = \lambda_x^{-1}(y) \in X \qquad \text{and} \qquad v = \lambda_x^{-1}(z) \in X.$$

Then we have $J^{-1}(x, y, z) = (x, u, \lambda_u^{-1}(v))$. Since $\lambda_y(\rho_u(x)) = \sigma_y(x)$ by (3) and

$$\lambda_y(\lambda_{\rho_u(x)}(\lambda_u^{-1}(v))) = \lambda_{\lambda_x(u)}(\lambda_{\rho_u(x)}(\lambda_u^{-1}(v))) = \lambda_x(\lambda_u(\lambda_u^{-1}(v))) = \lambda_x(v) = z$$

by (1), we obtain

$$\begin{aligned}(J \circ r_1 \circ J^{-1})(x, y, z) &= J(r_1(x, u, \lambda_u^{-1}(v))) \\ &= J(y, \rho_u(x), \lambda_u^{-1}(v)) \\ &= (y, \lambda_y(\rho_u(x)), \lambda_y(\lambda_{\rho_u(x)}(\lambda_u^{-1}(v)))) \\ &= (y, \sigma_y(x), z) \\ &= s_1(x, y, z).\end{aligned}$$

Moreover, because $\lambda_v(\rho_{\lambda_u^{-1}(v)}(u)) = \sigma_v(u)$ by (3) and

$$\lambda_x(\lambda_v(\rho_{\lambda_u^{-1}(v)}(u))) = \lambda_x(\sigma_v(u)) = \sigma_{\lambda_x(v)}(\lambda_x(u)) = \sigma_z(y)$$

by Lemma 2.1, we conclude that

$$\begin{aligned}(J \circ r_2 \circ J^{-1})(x, y, z) &= J(r_2(x, u, \lambda_u^{-1}(v))) \\ &= J(x, v, \rho_{\lambda_u^{-1}(v)}(u)) \\ &= (x, z, \lambda_x(\lambda_v(\rho_{\lambda_u^{-1}(v)}(u)))) \\ &= (x, z, \sigma_z(y)) \\ &= s_2(x, y, z).\end{aligned}$$

Hence the first part of the result is proved. To finish the proof it is enough to observe that $s = I \circ r \circ I^{-1}$, where the bijection $I\colon X \times X \to X \times X$ is defined as $I(x,y) = (x, \lambda_x(y))$. □

Moreover, in case the solution (X,r) is bijective, if we define $x \triangleleft y = \sigma_y(x)$ for $x, y \in X$, then the resulting structure $(X, \triangleleft)$ is a rack. If, furthermore, $\sigma_y(y) = y$ for all $y \in X$, this is a quandle (see also [16]).

Remark 2.3. Note that if (X,r) is a bijective left non-degenerate solution, then, by virtue of the defining relations, every element x of X is normal in $A = A(X,r)$. Hence each element of A is normal; i.e., $aA = Aa$ for all $a \in A$. If $X = \{x_1, \dots, x_n\}$ is a finite set, then

$$A = \{x_1^{k_1} \cdots x_n^{k_n} : k_1, \dots, k_n \geqslant 0\}.$$

In essence, Proposition 2.2 boils down to the equality

$$\sigma_x \circ \sigma_y = \sigma_{\sigma_x(y)} \circ \sigma_x$$

for all $x, y \in X$. Moreover, the above equality assures that the action of $A = A(X,r)$ on A, given as

$$\sigma_a = \sigma_{x_n} \circ \cdots \circ \sigma_{x_1} \qquad \text{and} \qquad \sigma_a(b) = \sigma_a(y_1) \cdots \sigma_a(y_m)$$

for $a = x_1 \cdots x_n \in A$ and $b = y_1 \cdots y_m \in A$, where $x_i, y_j \in X$, is well-defined. We shall freely use this fact throughout the paper.

Proposition 2.4. *Assume that (X,r) is a bijective left non-degenerate solution of the Yang–Baxter equation. Then there exist a set I and σ-invariant submonoids A_i of $A = A(X,r)$ for $i \in I$ (i.e., $\sigma_a(A_i) \subseteq A_i$ for all $a \in A$ and $i \in I$) such that A is the subdirect product of the family $(A_i)_{i\in I}$ and $A_iA_j = A_jA_i$ for all $i, j \in I$. Furthermore, if X is a finite set, then I can be taken as a finite set.*

Proof. For $x, y \in X$ we declare that $x \sim y$ if and only if there exists $a \in A$ such that $\sigma_a(x) = y$. It is clear that $\sim$ is an equivalence relation on X. So, let $X = \bigcup_{i\in I} X_i$ be the partition of X with respect to $\sim$. Let $A_i = \langle X_i \rangle$ for $i \in I$ denote the submonoid of A generated by X_i. Clearly, each monoid A_i is σ-invariant. Moreover, as each element of A is normal, it follows that A is the subdirect product of the family $(A_i)_{i\in I}$. □

Lemma 2.5. *Assume that (X,r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Then there exists $d \geqslant 1$ such that a^d is a central element of $A = A(X,r)$ for each $a \in A$.*

Proof. As X is a finite set, it follows that there exists $d \geqslant 1$ (we can choose d as a divisor of $n!$, where $n = |X|$) such that $\sigma_a^d = \mathrm{id}$ for each $a \in A$. Now, if $b \in A$, then

$$ba^d = a\sigma_a(b)a^{d-1} = \cdots = a^d\sigma_a^d(b) = a^d b,$$

and the result follows. □

Remark 2.6. Moreover, if $ac = bc$ or $ca = cb$ holds for some $a, b, c \in A$, then $az^i = bz^i$ for some $i \geqslant 1$, where $z = x_1^d \cdots x_n^d \in \mathrm{Z}(A)$ (here $d \geqslant 1$ is defined as in Lemma 2.5). Hence the monoid A is left cancellative if and only if it is right cancellative if and only if the central elements of A are cancellable.

Theorem 2.7. *Assume that (X,r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Then $A = A(X,r)$ is a central-by-finite monoid; i.e., $A = \bigcup_{f\in F} Cf$ for a central submonoid $C \subseteq A$ and a finite subset $F \subseteq A$. In particular, if K is a field, then $K[A]$ is a finite module over a central affine subalgebra of $K[A]$. Hence, $K[A]$ is a Noetherian PI-algebra satisfying*

$$\operatorname{clKdim} K[A] = \operatorname{GKdim} K[A] = \operatorname{rk} A \leqslant |X|,$$

and the equality holds if and only if the solution (X,r) is involutive.

Proof. Write $X = \{x_1,\dots,x_n\}$ with $n = |X|$. By Lemma 2.5 we know that there exists $d \geqslant 1$ such that $x_1^d,\dots,x_n^d$ are central elements of A. Define $C = \langle x_1^d,\dots,x_n^d\rangle$. Clearly C is a central submonoid of A. Moreover, Remark 2.3 yields $A = \bigcup_{f\in F} Cf$, where

$$F = \{x_1^{k_1}\cdots x_n^{k_n} : 0 \leqslant k_1,\dots,k_n < d\} \subseteq A.$$

In particular, $K[A] = \sum_{f\in F} K[C]f$ is a finite module over the central affine subalgebra $K[C]$ of $K[A]$. Therefore, the algebra $K[A]$ is Noetherian and PI. Hence $\operatorname{clKdim} K[A] = \operatorname{GKdim} K[A] = \operatorname{rk} A$ by [37, Theorem 14, p. 284]. Because the commutative algebra $K[C]$ can be generated by n elements, we get $\operatorname{GKdim} K[A] = \operatorname{GKdim} K[C] \leqslant n$, as desired.

Finally, it is clear that if (X,r) is involutive, then the equality $\operatorname{clKdim} K[A] = \operatorname{GKdim} K[A] = \operatorname{rk} A = n$ holds as A is a free abelian monoid of rank n. Whereas if (X,r) is not involutive, then we claim that $\sigma_x(y) \neq y$ for some $x,y\in X$. Indeed, otherwise $\sigma_x = \mathrm{id}$ for all $x\in X$ and then $\lambda_x = \hat\lambda_x$ by (3). Since

$$\rho_y(x) = \hat\lambda^{-1}_{\lambda_x(y)}(x) = \lambda^{-1}_{\hat\lambda_x(y)}(x) = \hat\rho_y(x),$$

we get $\rho_y = \hat\rho_y$ for all $y\in X$. Thus $r = r^{-1}$ and (X,r) is involutive, a contradiction. Hence $\sigma_x(y)\neq y$ for some $x,y\in X$. Now $y^d x = x\sigma_x(y)^d = \sigma_x(y)^d x$ yields $(y^d - \sigma_x(y)^d)x^d = 0 \in K[C]$. Therefore, if $\mathfrak{p}$ is a prime ideal of $K[C]$, then $x^d\in\mathfrak{p}$ or $y^d - \sigma_x(y)^d \in \mathfrak{p}$. Thus the commutative algebra $K[C]/\mathfrak{p}$ can be generated by fewer than n elements, and it follows that $\operatorname{clKdim} K[A] = \operatorname{clKdim} K[C] < n$. ☐

Theorem 2.8. *Assume that (X,r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Let $A = A(X,r)$. If K is a field, then the following conditions are equivalent:*

1. *(X,r) is an involutive solution.*
2. *A is a free abelian monoid of rank $|X|$.*
3. *A is a cancellative monoid.*
4. $\operatorname{rk} A = |X|$.
5. *$K[A]$ is a prime algebra.*
6. *$K[A]$ is a domain.*
7. $\operatorname{clKdim} K[A] = |X|$.
8. $\operatorname{GKdim} K[A] = |X|$.

Proof. It is obvious that (1) $\Longrightarrow$ (2) $\Longrightarrow$ (8). Moreover, we have (1) $\Longleftrightarrow$ (4) $\Longleftrightarrow$ (7) $\Longleftrightarrow$ (8) by Theorem 2.7. Since clearly (2) $\Longrightarrow$ (6) $\Longrightarrow$ (5), and (5) $\Longrightarrow$ (3) follows by Remark 2.3, it is enough to show that (3) $\Longrightarrow$ (2). So assume (3) and observe first that $xx = x\sigma_x(x)$ yields $\sigma_x(x) = x$ for each $x\in X$. Now, choose $d\geqslant 1$ such that $a^d \in \mathrm{Z}(A)$ for each $a\in A$. Then for $x,y\in X$ we have

$$y^d x = y^{d-1}x\sigma_x(y) = \cdots = x\sigma_x(y)^d = \sigma_x(y)^d x,$$

which leads to $\sigma_x(y)^d = y^d$. Because the elements y^d and $\sigma_x(y)^d$ cannot be rewritten using the defining relations of A (the only way to rewrite the word z^d for $z \in X$ would be to use a relation of the form $z\sigma_z(z) = zz = \sigma_z^{-1}(z)z$), we conclude that $\sigma_x(y) = y$. Hence $\sigma_x = \mathrm{id}$ and (2) follows. This finishes the proof. □

Assume that (X, r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Let $A = A(X, r)$ and define

$$\eta_A = \{(a, b) \in A \times A : ac = bc \quad \text{for some } c \in A\}.$$

By Remark 2.3 it follows that η_A is the cancellative congruence of the monoid A, that is, the smallest congruence η on A such that the quotient monoid A/η is cancellative. Moreover, $\eta_A = \bigcup_{i=1}^{\infty} \eta_i$ is a union of the ascending chain of congruences $\eta_i = \{(a, b) \in A \times A : az^i = bz^i\}$ (here $z = \prod_{x \in X} x^d \in \mathrm{Z}(A)$ is defined as in Remark 2.3). Note that the lattice of congruences on A can be embedded into the lattice of ideals of the algebra $K[A]$ (here K is an arbitrary field) by associating to a congruence η on A the ideal

$$I(\eta) = \mathrm{Span}_K\{a - b : (a, b) \in \eta\},$$

the K-linear span of the set consisting of all elements $a - b$ with $(a, b) \in \eta$. We conclude by Theorem 2.7 that the monoid A satisfies the ascending chain condition on congruences. Hence there exists $t \geqslant 1$ such that $\eta_i = \eta_t$ for each $i \geqslant t$, and thus $\eta_A = \eta_t$. Therefore, we have proved the following result.

Proposition 2.9. *Assume that (X, r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Then there exists $t \geqslant 1$ such that*

$$\eta_A = \{(a, b) \in A \times A : az^i = bz^i\}$$

for all $i \geqslant t$, where $z = \prod_{x \in X} x^d \in \mathrm{Z}(A)$ is defined as in Remark 2.3. In particular, the ideal Az^t is cancellative, and if K is a field, then $I(\eta_A) = \mathrm{Ann}_{K[A]}(z^i)$ for all $i \geqslant t$.

3. Prime ideals of $A(X, r)$ and $K[A(X, r)]$

We shall begin this section with the following description of prime ideals of the monoid $A = A(X, r)$. The prime spectra of A and $K[A]$ (for a field K) are denoted as $\mathrm{Spec}(A)$ and $\mathrm{Spec}(K[A])$, respectively.

Proposition 3.1. *Assume that (X, r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Let $A = A(X, r)$ and*

$$\mathcal{Z} = \mathcal{Z}(X, r) = \{Z \subseteq X : \varnothing \neq Z \neq X \quad \text{and} \quad \sigma_x(Z) = Z \quad \text{for all } x \in X \setminus Z\}.$$

Define $P(Z) = \bigcup_{z \in Z} Az$ for $Z \in \mathcal{Z}$. Then the maps

$$\mathcal{Z} \to \mathrm{Spec}(A)\colon Z \mapsto P(Z) \qquad \text{and} \qquad \mathrm{Spec}(A) \to \mathcal{Z}\colon P \mapsto X \cap P$$

are mutually inverse bijections.

Proof. Since the elements of A are normal it is clear that if $P \in \mathrm{Spec}(A)$, then $\varnothing \neq X \cap P \neq X$ and $P = \bigcup_{x \in X \cap P} Ax$. Moreover, if $x \in X \cap P$ and $y \in X \setminus P$, then $y\sigma_y(x) = xy \in P$. Hence $y \notin P$ implies that $\sigma_y(x) \in P$. Therefore, $\sigma_y(X \cap P) = X \cap P$ and $X \cap P \in \mathcal{Z}$.

Conversely, if $Z \in \mathcal{Z}$, then we claim that $P(Z)$ is a prime ideal of A. To show this observe that if $x_1 \cdots x_n \in P(Z)$ for some $x_1, \ldots, x_n \in X$, then necessarily $x_i \in P(Z)$ for some $1 \leqslant i \leqslant n$. Otherwise $x_1, \ldots, x_n \in X \setminus Z$, and then each word in the free monoid on X representing the element $x_1 \cdots x_n \in A$ must be a product of letters in $X \setminus Z$, which leads to a contradiction. Indeed, if $x, y \in X \setminus Z$, then the only way to rewrite the word xy is to use one of the relations $xy = y\sigma_y(x)$ and $xy = \sigma_x^{-1}(y)x$. Since $\sigma_x(Z) = \sigma_y(Z) = Z$, we get $\sigma_x(X \setminus Z) = \sigma_y(X \setminus Z) = X \setminus Z$. Hence both $\sigma_y(x)$ and $\sigma_x^{-1}(y)$ are elements of $X \setminus Z$. □

Our next result provides an inductive description of all prime ideals of the monoid algebra $K[A(X,r)]$ over a field K in terms of prime ideals of group algebras over K of certain finitely generated FC-groups (finite conjugacy groups) closely related to the monoid $A(X,r)$. Recall that for such a group $G = \Delta(G)$ the torsion elements form a finite characteristic subgroup $G^+ = \Delta^+(G)$ such that G/G^+ is a finitely generated free abelian group (see, e.g., [39, Section 4.1]).

Proposition 3.2. *Assume that (X,r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Let $A = A(X,r)$ and $\mathcal{Z} = \mathcal{Z}(X,r)$. If K is a field and P is a prime ideal of the algebra $K[A]$, then $X \cap P \in \mathcal{Z} \cup \{\varnothing, X\}$. Moreover, for such a prime ideal P the following properties hold:*

(1) *There exists an inclusion preserving bijection between the set of prime ideals Q of $K[A]$ with the property $X \cap Q = X \cap P$ and the set of all prime ideals of the algebra $K[A \setminus P]$. Moreover, the monoid $A \setminus P$ has the following presentation:*

$$A \setminus P \cong \langle X \setminus P \mid xy = y\sigma_y(x) \quad \textit{for all } x, y \in X \setminus P\rangle.$$

(2) *There exists an inclusion-preserving bijection between the set of prime ideals Q of $K[A]$ satisfying $Q \cap A = \varnothing$ and the set of all prime ideals of the group algebra $K[G]$, where*

$$G = \mathrm{gr}(X \mid xy = y\sigma_y(x) \quad \textit{for all } x, y \in X).$$

Furthermore, the cancellative monoid $\overline{A} = A/\eta_A$ has a group of quotients which is equal to the central localization $\overline{A}\langle z\rangle^{-1}$ for some $z \in \mathrm{Z}(\overline{A})$, and $G \cong \overline{A}\langle z\rangle^{-1}$. Clearly, G is a finitely generated FC-group.

Proof. Clearly $P \cap A$ is a prime ideal of A and $X \cap (P \cap A) = X \cap P$. Hence, from Proposition 3.1, we get that $X \cap P \in \mathcal{Z}$ if $\varnothing \neq X \cap P \neq X$. Therefore, the first part of the proposition follows.

Since $Q \cap A = \bigcup_{x \in Q \cap X} Ax$, it is clear that the set of prime ideals Q of $K[A]$ with the property $X \cap Q = X \cap P$ is in an inclusion-preserving bijection with the set of all prime ideals of the algebra $K[A]/K[P \cap A] \cong K_0[A/(P \cap A)]$, the contracted semigroup algebra of $A/(P \cap A)$ (recall that the contracted semigroup algebra $K_0[S]$, for a semigroup S with zero element θ, is defined as $K[S]/K\theta$). By Proposition 3.1 we get $A \setminus P = \langle X \setminus P\rangle \subseteq A$ and also $A \setminus P \cong \langle X \setminus P \mid xy = y\sigma_y(x)$ for all $x, y \in X \setminus P\rangle$. Therefore, $A/(P \cap A) \cong (A \setminus P) \cup \{\theta\}$. Hence $K_0[A/(P \cap A)] \cong K[A \setminus P]$, and (1) follows.

Assume now that Q is a prime ideal of $K[A]$ such that $Q \cap A = \varnothing$. We claim that Q contains the ideal $I(\eta_A)$. Indeed, if $a, b \in A$ satisfy $ac = bc$ for some central element $c \in A$, then

$$(a - b)K[A]c = (a - b)cK[A] = 0 \subseteq Q.$$

Since $c \notin Q$, we get $a - b \in Q$. Therefore the ideals of $K[A]$ intersecting A trivially correspond bijectively to the prime ideals of the algebra $K[A]/I(\eta_A) \cong K[\overline{A}]$ and hence also to the prime ideals of the central localization $K[\overline{A}]\langle z\rangle^{-1} \cong K[\overline{A}\langle z\rangle^{-1}]$, where $z = \prod_{x\in X} x^d \in \mathrm{Z}(A)$ (here $d \geqslant 1$ is defined as in Lemma 2.5). So, it remains to show that the group G is isomorphic to $\overline{A}\langle z\rangle^{-1}$, which is clearly equal to the group of quotients of the monoid $\overline{A}$. Observe that the natural morphism $A \to G$ factors through $\overline{A}$ and thus also through $\overline{A}\langle z\rangle^{-1}$. Hence we get a natural morphism of groups $\varphi\colon \overline{A}\langle z\rangle^{-1} \to G$.

Surjectivity of φ is obvious. Let $\overline{a}, \overline{b} \in \overline{A}\langle z\rangle^{-1}$ such that $\varphi(\overline{a}) = \varphi(\overline{b})$. We may assume that $\overline{a}, \overline{b} \in \overline{A}$, as we can multiply them by their highest denominator in z. Consider a and b as words in the free group F with generators in X. By adding the relation $xy = y\sigma_y(x)$ on the free group F, we get the group G, where the words corresponding to a and b are equal. Hence, they are equal in every group generated in X, satisfying the relation $xy = y\sigma_y(x)$. Thus, $\overline{a} = \overline{b}$ in the group $\overline{A}\langle z\rangle^{-1}$. Therefore, φ is injective, which finishes the proof. □

As Example 3.3 shows, it is possible that the algebra $K[A(X,r)]$ does not admit prime ideals intersecting the monoid $A(X,r)$ non-trivially, even if the group $\Sigma = \mathrm{gr}(\sigma_x \mid x \in X) \subseteq \mathrm{Sym}(X)$ is cyclic.

However, it is clear that for a prime ideal P of $K[A(X,r)]$ we have $P \cap A(X,r) \neq \varnothing$ if and only if $z \in P$, where the element $z = \prod_{x\in X} x^d \in \mathrm{Z}(A(X,r))$ is defined as in Remark 2.3. Thus, the maximal ideal containing $1-z$ is a prime ideal that intersects $A(X,r)$ trivially. Hence the algebra $K[A(X,r)]$ always has minimal prime ideals intersecting the monoid $A(X,r)$ trivially.

Example 3.3. Let X be a finite non-empty set. Fix $\sigma \in \mathrm{Sym}(X)$ and define $r\colon X\times X \to X \times X$ as $r(x,y) = (y, \sigma(x))$. Clearly (X,r) is a bijective non-degenerate solution of the Yang–Baxter equation. Let $A = A(X,r)$ and let K be a field. If $x, y \in X$, then $y(x-\sigma(x)) = (x-\sigma(x))\sigma(y)$ in $K[A]$. Thus $x - \sigma(x)$ is a normal element of $K[A]$, and hence $K[A](x-\sigma(x))$ is an ideal of $K[A]$. We claim that this ideal is nilpotent. Indeed, observe first that the equality $x\sigma(x) = \sigma(x)^2$ yields

$$(x-\sigma(x))^2 = x^2 - x\sigma(x) - \sigma(x)x + \sigma(x)^2 = (x-\sigma(x))x,$$

which leads to $(x-\sigma(x))^{n+1} = (x-\sigma(x))x^n$ for each $n \geqslant 1$. In particular, if $d \geqslant 1$ is equal to the order σ, then $(x-\sigma(x))^d = 0$. Indeed, if $d = 1$, then the equality is obvious. Whereas, if $d \geqslant 2$, then

$$(x-\sigma(x))^d = (x-\sigma(x))x^{d-1} = x^d - \sigma(x)x^{d-1} = x^d - x^{d-1}\sigma^d(x) = 0.$$

Thus $(K[A](x-\sigma(x)))^d = K[A](x-\sigma(x))^d = 0$, as claimed. Hence the ideal $P = \sum_{x\in X} K[A](x-\sigma(x))$ is nilpotent. Note that if $x, y \in X$, then $xy - yx = x(y-\sigma(y)) \in P$. Moreover, if $x \in X$ and $n \geqslant 1$, then

$$x - \sigma^n(x) = \sum_{i=1}^{n} (\sigma^{i-1}(x) - \sigma^i(x)) \in P.$$

These facts easily lead to a conclusion that $K[A]/P \cong K[t_1, \ldots, t_s]$, the commutative polynomial algebra in s commuting variables, where s is the number of disjoint cycles in the decomposition of σ. Hence the ideal P is also semiprimitive. Therefore, $\mathcal{B}(K[A]) = \mathcal{J}(K[A]) = P$ is the unique minimal prime ideal of $K[A]$. In particular, $\mathrm{clKdim}\, K[A] = s$ may be equal to any prescribed integer between 1 and $|X|$.

Moreover, as Example 3.4 shows, the description of the minimal primes of the algebra $K[A(X,r)]$ depends on the characteristic of a base field K.

Example 3.4. Consider the solution (X, r) defined in Example 1.1. Let $A = A(X, r)$ and assume that K is a field. The following facts can be verified (using the theory of Gröbner bases and the fact that the algebras under consideration are $\mathbb{Z}$-graded). If $\operatorname{char} K = 3$, then the minimal prime ideals of the algebra $K[A]$ are of the form

$$P_1 = (x_2, x_3), \qquad P_2 = (x_1, x_3), \qquad P_3 = (x_1, x_2), \qquad P_4 = (x_1 - x_2, x_2 - x_3).$$

Whereas, if $\operatorname{char} K \neq 3$, then the minimal primes of $K[A]$ consist of the ideals P_1, P_2, P_3, P_4 together with the ideal

$$P_5 = (x_1 + x_2 + x_3, x_1^2 - x_2^2, x_2^2 - x_3^2) = (x_1 + x_2 + x_3, x_1^2 - x_2^2).$$

Furthermore, if $\operatorname{char} K = 3$, then $0 \neq x_1(x_2 - x_3) \in \mathcal{B}(K[A])$, whereas if $\operatorname{char} K \neq 3$, then the algebra $K[A]$ is semiprime.

Our next aim is to determine the classical Krull dimension (which is equal to the Gelfand–Kirillov dimension; see Theorem 2.7) of the algebra $K[A(X, r)]$ over a field K in terms of certain purely combinatorial properties of the permutations σ_x for $x \in X$.

Theorem 3.5. *Assume that (X, r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Let $A = A(X, r)$ and let $G = \operatorname{gr}(X \mid xy = y\sigma_y(x)$ for all $x, y \in X)$. If K is a field and P is a minimal prime ideal of the algebra $K[A]$ satisfying $P \cap A = \varnothing$, then*

$$\operatorname{clKdim} K[A]/P = \operatorname{clKdim} K[G] = s,$$

where s is the number of orbits of X with respect to the action of the group $\Sigma = \operatorname{gr}(\sigma_x \mid x \in X) \subseteq \operatorname{Sym}(X)$.

Proof. By Lemma 2.5 there exists $d \geqslant 1$ such that $\sigma_x^d = \mathrm{id}$ for each $x \in X$. Define $C = \langle x^d \mid x \in X \rangle \subseteq A$. Clearly, C is a central submonoid of A. First, we shall prove that

$$\operatorname{clKdim} K[A]/P \leqslant s. \tag{4}$$

Note that if $x \in X$ and $a \in A$, then $ax^d = x^d\sigma_x^d(a) = x^d a = a\sigma_a(x)^d$. Hence

$$aK[A](x^d - \sigma_a(x)^d) = K[A]a(x^d - \sigma_a(x)^d) = 0 \subseteq P.$$

Thus $a \notin P$ leads to $x^d - \sigma_a(x)^d \in P$. Since $K[C]$ is a central subalgebra of $K[A]$, the ideal $\mathfrak{p} = P \cap K[C]$ is prime. Moreover, $x^d - \sigma_a(x)^d \in \mathfrak{p}$ for all $x \in X$ and $a \in A$. Therefore, $\operatorname{clKdim} K[C]/\mathfrak{p} \leqslant s$ because the commutative algebra $K[C]/\mathfrak{p}$ can be generated by s elements (the image of the set $\{x^d : x \in X\} \subseteq C$ in $K[C]/\mathfrak{p}$ has cardinality $\leqslant s$). Since $K[A]/P$ is a PI-algebra, which is a finite module over the central subalgebra $K[C]/\mathfrak{p}$, we conclude by [35, Theorem 13.8.14] that $\operatorname{clKdim} K[A]/P = \operatorname{clKdim} C/\mathfrak{p} \leqslant s$, as desired.

Next we shall prove that

$$\operatorname{clKdim} K[G] \leqslant \operatorname{clKdim} K[A]/P. \tag{5}$$

By Proposition 3.2 we know that P corresponds bijectively to a minimal prime ideal $\overline{P}$ of the algebra $K[A/\eta_A]$ and also to a minimal prime ideal P_G of the group algebra $K[G]$. Let $z = \prod_{x \in X} x^d \in C$. The images of z in the algebras $K[A/\eta_A]$

and $K[A]/P$, still denoted by z, are central and regular elements of these algebras. Since $K[A/\eta_A]\langle z\rangle^{-1} \cong K[G]$ by Proposition 3.2, it follows easily that

$$(K[A]/P)\langle z\rangle^{-1} \cong (K[A/\eta_A]/\overline{P})\langle z\rangle^{-1} \cong K[G]/P_G.$$

Hence

$$\operatorname{clKdim} K[G]/P_G = \operatorname{clKdim}(K[A]/P)\langle z\rangle^{-1} \leqslant \operatorname{clKdim} K[A]/P.$$

Thus, to prove (5) it is enough to show that $\operatorname{clKdim} K[G]/P_G = \operatorname{clKdim} K[G]$. By [39, Lemma 4.1.8] we know that there exists a finitely generated free abelian subgroup $F \subseteq G$ of finite index. Therefore, $K[G] \cong K[F] * (G/F)$, a crossed product of the finite group G/F over the Laurent polynomial algebra $K[F]$. Hence [38, Theorem 16.6] guarantees that

$$\operatorname{ht} Q = \operatorname{ht} Q \cap K[F] \qquad \text{and} \qquad \operatorname{clKdim} K[G]/Q = \operatorname{clKdim} K[F]/(Q \cap K[F])$$

for each $Q \in \operatorname{Spec}(K[G])$. By Schelter's theorem (see [35, Theorem 13.10.12]) we get

$$\operatorname{ht} \mathfrak{p} + \operatorname{clKdim} K[F]/\mathfrak{p} = \operatorname{clKdim} K[F]$$

for each $\mathfrak{p} \in \operatorname{Spec}(K[F])$. Since $\operatorname{clKdim} K[G] = \operatorname{clKdim} K[F]$, we conclude that

$$\operatorname{ht} Q + \operatorname{clKdim} K[G]/Q = \operatorname{clKdim} K[G]$$

for each $Q \in \operatorname{Spec}(K[G])$. In particular, as $\operatorname{ht} P_G = 0$, we obtain $\operatorname{clKdim} K[G]/P_G = \operatorname{clKdim} K[G]$, as desired.

Finally, let us observe that the ideal P_0 of $K[G]$ generated by elements $x - y$ for all $x, y \in X$ which are in the same orbit of X with respect to the action of Σ satisfies $K[G]/P_0 \cong K[t_1^{\pm 1}, \ldots, t_s^{\pm 1}]$, the Laurent polynomial algebra in s commuting variables. Hence

$$s = \operatorname{clKdim} K[G]/P_0 \leqslant \operatorname{clKdim} K[G]. \tag{6}$$

Putting (4), (5), and (6) together we get $\operatorname{clKdim} K[A]/P = \operatorname{clKdim} K[G] = s$, which finishes the proof. □

Motivated by Propositions 3.1 and 3.2 and Theorem 3.5 we define

$$\Sigma_Z = \operatorname{gr}(\sigma_x \mid x \in X \setminus Z) \subseteq \operatorname{Sym}(X)$$

and

$$s(Z) = \text{the number of orbits of } X \setminus Z \text{ with respect to the action of } \Sigma_Z$$

for each $Z \in \mathcal{Z}_0 = \mathcal{Z} \cup \{\varnothing\}$, where $\mathcal{Z} = \mathcal{Z}(X, r)$.

By Proposition 3.1 we know that all sets in $\mathcal{Z}$ are of the form $X \cap P$ for a prime ideal P of $A = A(X, r)$. On the other hand, Proposition 3.2 assures that if Q is a prime ideal of the algebra $K[A]$ over a field K, then $X \cap Q \in \mathcal{Z}_0$ or $X \cap Q = X$. But if Q is a minimal prime ideal of $K[A]$, then the latter possibility is excluded. Indeed, otherwise Q would strictly contain the prime ideal Q_0 generated by elements $x - y$ for all $x, y \in X$. However, as Example 3.6 shows, not all sets in $\mathcal{Z}_0$ are of the form $X \cap Q$ for a minimal prime ideal Q of $K[A]$.

Example 3.6. Let $X = \{x_1, x_2, x_3, x_4, x_5\}$. Define $\sigma_1 = \sigma_2 = (1, 2)$, $\sigma_3 = \sigma_5 = \mathrm{id}$, and $\sigma_4 = (3, 5)$. Let $r \colon X \times X \to X \times X$ be defined as $r(x_i, x_j) = (x_j, x_{\sigma_j(i)})$. It is easy to check that (X, r) is a bijective non-degenerate solution of the Yang–Baxter equation. If K is a field and $A = A(X, r)$, then

$$x_4(x_3 - x_5) = 0, \qquad x_1(x_1 - x_2) = 0, \qquad x_2(x_1 - x_2) = 0$$

in $K[A]$. Clearly, the first equality assures that each prime ideal P of $K[A]$ contains x_4 or x_3-x_5. Moreover, the second and third equalities guarantee that $x_1-x_2 \in P$. Because $P_1 = (x_1 - x_2, x_4)$ and $P_2 = (x_1 - x_2, x_3 - x_5)$ are prime ideals of $K[A]$ (actually, we have $K[A]/P_1 \cong K[A]/P_2 \cong K[t_1, t_2, t_3]$, the polynomial algebra in three commuting variables), P_1 and P_2 are the only minimal prime ideals of $K[A]$. However, the set $Z = \{x_3, x_5\} \in \mathcal{Z}(X, r)$ satisfies $Z \neq X \cap P_1 = \{x_4\}$ and $Z \neq X \cap P_2 = \varnothing$.

Note that Example 3.6 shows also that the algebra $K[A]$, where $A = A(X, r)$, may contain minimal prime ideals of mixed type (i.e., prime ideals P of $K[A]$ satisfying $P \cap A \neq \varnothing$ but $P \neq K[P \cap A]$), even if the group $\Sigma = \mathrm{gr}(\sigma_x \mid x \in X) \subseteq \mathrm{Sym}(X)$ is abelian. This is in contrast to what happens in the cancellative case (see [24]).

Moreover, Example 3.7 shows that it is possible that the algebra $K[A]$ contains prime ideals of the form $P = K[P \cap A]$, even if each orbit of X with respect to the action of the group Σ has cardinality larger than 1.

Example 3.7. Let $X = \{x_1, x_2, x_3, x_4\}$. Define $\sigma_1 = \sigma_2 = \mathrm{id}$ and $\sigma_3 = \sigma_4 = (1, 2)(3, 4)$. Moreover, let $r\colon X \times X \to X \times X$ be defined as $r(x_i, x_j) = (x_j, x_{\sigma_j(i)})$, a bijective non-degenerate solution of the Yang–Baxter equation. If K is a field and $A = A(X, r)$, then

$$x_3(x_3 - x_4) = 0, \qquad x_4(x_3 - x_4) = 0, \qquad x_3(x_1 - x_2) = 0, \qquad x_4(x_1 - x_2) = 0$$

in $K[A]$. The above equalities assure that each prime ideal of $K[A]$ contains x_3, x_4, or $x_1 - x_2, x_3 - x_4$. Since $P = (x_3, x_4)$ is a prime ideal of $K[A]$ (actually, we have $K[A]/P \cong K[t_1, t_2]$, the polynomial algebra in two commuting variables), it is a minimal prime ideal of $K[A]$.

Theorem 3.8. *Assume that (X, r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Let $A = A(X, r)$ and let $\mathcal{Z}_0 = \mathcal{Z} \cup \{\varnothing\}$, where $\mathcal{Z} = \mathcal{Z}(X, r)$. If K is a field, then*

$$\mathrm{clKdim}\, K[A] = \max\{s(Z) : Z \in \mathcal{Z}_0\}.$$

Proof. Define $s = \max\{s(Z) : Z \in \mathcal{Z}_0\}$. If P is a minimal prime ideal of $K[A]$, then $X \cap P \in \mathcal{Z}_0$ and P corresponds to a minimal prime ideal P' of the algebra $K[A \setminus P]$ such that $P' \cap (A \setminus P) = \varnothing$ and $K[A]/P \cong K[A \setminus P]/P'$ (see Proposition 3.2). Therefore, Theorem 3.5 implies that

$$\mathrm{clKdim}\, K[A]/P = \mathrm{clKdim}\, K[A \setminus P]/P' = s(X \cap P) \leqslant s.$$

Since we have $\mathrm{clKdim}\, K[A] = \mathrm{clKdim}\, K[A]/P$ for some minimal prime ideal P of $K[A]$, the inequality $\mathrm{clKdim}\, K[A] \leqslant s$ follows.

To show that $\mathrm{clKdim}\, K[A] \geqslant s$ we have to check that $\mathrm{clKdim}\, K[A] \geqslant s(Z)$ for each $Z \in \mathcal{Z}_0$. So, let us fix $Z \in \mathcal{Z}_0$. If $Z = \varnothing$, then we are done by Theorem 3.5. Whereas, if $Z \in \mathcal{Z}$, then $A = P(Z) \cup A(Z)$, where $P(Z) = \bigcup_{z \in Z} Az$ and $A(Z) = A \setminus P(Z) = \langle X \setminus Z \rangle \subseteq A$ is the submonoid of A generated by $X \setminus Z$. Therefore, $K[A]/K[P(Z)] \cong K_0[A/P(Z)] \cong K[A(Z)]$, which leads to

$$\mathrm{clKdim}\, K[A] \geqslant \mathrm{clKdim}\, K[A]/K[P(Z)] = \mathrm{clKdim}\, K[A(Z)] \geqslant s(Z),$$

where the last inequality is a consequence of the fact that the ideal P_0 of $K[A(Z)]$, generated by elements of the form $x - y$ for all $x, y \in X \setminus Z$ which are in the same orbit of $X \setminus Z$ with respect to the action of the group Σ_Z, satisfies

$K[A(Z)]/P_0 \cong K[t_1, \ldots, t_{s(Z)}]$, the polynomial algebra in $s(Z)$ commuting variables. Hence the result follows. ☐

4. Structure of the monoid $M(X, r)$ and its algebra

If (X, r) is a left non-degenerate solution, then by Proposition 1.4 we may (and we shall) identify the structure monoid $M = M(X, r)$ with its image $\{(a, \phi(a)) : a \in A = A(X, r)\}$ in the semidirect product $A \rtimes \mathcal{G}$, where $\mathcal{G} = \mathcal{G}(X, r) = \mathrm{gr}(\lambda_x \mid x \in X) \subseteq \mathrm{Sym}(X)$, and the map $\phi \colon A \to \mathcal{G}$ satisfies $\phi(a)\phi(b) = \phi(a\phi(a)(b))$ for $a, b \in A$.

Lemma 4.1. *Assume that (X, r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. If $xz = yz$ or $zx = zy$ for some $x, y, z \in M$, then there exists $w \in \mathrm{Z}(M)$ such that $xw = yw$.*

Proof. Suppose that $xz = yz$ (the proof in case $zx = zy$ is completely similar) and write $z = (a, \phi(a))$ for some $a \in A$. Because $z^n = (a\phi(a)(a) \cdots \phi(a)^{n-1}(a), \phi(a)^n)$ for each $n \geqslant 1$, replacing z by some z^n we may assume that $\phi(a) = \mathrm{id}$. Moreover, since $a^d \in \mathrm{Z}(A)$ for some $d \geqslant 1$ (see Lemma 2.5) then replacing z by $z^d = (a^d, \mathrm{id})$, we may assume that $a \in \mathrm{Z}(A)$. Since $g(\mathrm{Z}(A)) = \mathrm{Z}(A)$ for each $g \in \mathcal{G} = \mathcal{G}(X, r)$, the element $c = \prod_{g \in \mathcal{G}} g(a) \in \mathrm{Z}(A)$ is well-defined. It is clear that $g(c) = c$ for each $g \in \mathcal{G}$. Moreover, by induction we prove that $\phi(c^k) = \phi(c)^k$ for $k \geqslant 1$. Indeed,

$$\phi(c^k) = \phi(c^{k-1}c) = \phi(c^{k-1}\phi(c^{k-1})(c)) = \phi(c^{k-1})\phi(c) = \phi(c)^{k-1}\phi(c) = \phi(c)^k$$

for each $k \geqslant 1$. Hence, replacing c by some c^k, we may assume that $\phi(c) = \mathrm{id}$. Define $w = (c, \mathrm{id}) \in M$. Clearly $w \in \mathrm{Z}(M)$. Moreover,

$$w = (c, \mathrm{id}) = (\prod_{g \in \mathcal{G}} g(a), \mathrm{id}) = \prod_{g \in \mathcal{G}} (g(a), \mathrm{id}) = zu,$$

where $u = \prod_{\mathrm{id} \neq g \in \mathcal{G}} (g(a), \mathrm{id}) \in A \rtimes \mathcal{G}$ (note that the element u may not lie in M). It follows that $xw = yw$, which completes the proof. ☐

As an immediate consequence of Lemma 4.1 we obtain that the monoid M is left cancellative if and only if it is right cancellative. Moreover, defining

$$\eta_M = \{(x, y) \in M \times M : xz = yz \quad \text{for some } z \in M\},$$

we see that η_M is the cancellative congruence of M, that is, the smallest congruence η on M such that the quotient monoid M/η is cancellative. The following proposition gives a description of η_M in terms of the cancellative congruence η_A of $A = A(X, r)$.

Proposition 4.2. *Assume that (X, r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. If $A = A(X, r)$ and $M = M(X, r)$, then*

$$\eta_M = \{((a, \phi(a)), (b, \phi(b))) : (a, b) \in \eta_A \quad \text{and} \quad \phi(a) = \phi(b)\}.$$

Moreover, there exist $w \in \mathrm{Z}(M)$ and $t \geqslant 1$ such that

$$\eta_M = \{(x, y) \in M \times M : xw^i = yw^i\}$$

for all $i \geqslant t$. In particular, the ideal Mw^t is cancellative, and if K is a field, then $I(\eta_M) = \mathrm{Ann}_{K[M]}(w^i)$ for all $i \geqslant t$.

Proof. If $(x, y) \in \eta_M$ for some $x = (a, \phi(a)) \in M$ and $y = (b, \phi(b)) \in M$, then, by the proof of Lemma 4.1, there exists $c \in \mathrm{Z}(A)$ such that $g(c) = c$ for each $g \in \mathcal{G} = \mathcal{G}(X, r)$, $\phi(c) = \mathrm{id}$, and $xw = yw$ for $w = (c, \mathrm{id}) \in \mathrm{Z}(M)$. Hence

$$(ac, \phi(a)) = (a, \phi(a))(c, \mathrm{id}) = xw = yw = (b, \phi(b))(c, \mathrm{id}) = (bc, \phi(b)).$$

Thus $\phi(a) = \phi(b)$ and $ac = bc$, which gives $(a, b) \in \eta_A$. Conversely, if $(a, b) \in \eta_A$ and $\phi(a) = \phi(b)$, then $ac = bc$ for some $c \in \mathrm{Z}(A)$. Replacing c by $\prod_{g\in\mathcal{G}} g(c) \in cA \cap \mathrm{Z}(A)$ we may assume that $g(c) = c$ for each $g \in \mathcal{G}$. Now,

$$(a, \phi(a))(c, \phi(c)) = (ac, \phi(a)\phi(c)) = (bc, \phi(b)\phi(c)) = (b, \phi(b))(c, \phi(b)).$$

Hence $x = (a, \phi(a)) \in M$ and $y = (b, \phi(b)) \in M$ satisfy $xz = yz$, where $z = (c, \phi(c)) \in M$ and thus $(x, y) \in \eta_M$.

To obtain the second equality define $z = \prod_{x\in X} x^d \in \mathrm{Z}(A)$ (here $d \geqslant 1$ is defined as in Lemma 2.5). Let $t \geqslant 1$ be such that $\eta_A = \{(a, b) \in A \times A : az^i = bz^i\}$ for all $i \geqslant t$ (see Proposition 2.9). Since $g(z) = z$ for each $g \in \mathcal{G}$, we get $(z, \phi(z))^n = (z^n, \phi(z)^n) = (z^n, \mathrm{id})$ for some $n \geqslant 1$. Define $w = (z^n, \mathrm{id}) \in \mathrm{Z}(M)$. Now, if $x = (a, \phi(a)) \in M$ and $y = (b, \phi(b)) \in M$, then for $i \geqslant t$ we obtain, by Proposition 2.9,

$$\begin{aligned}(x, y) \in \eta_M &\iff (a, b) \in \eta_A \quad \text{and} \quad \phi(a) = \phi(b)\\ &\iff az^{ni} = bz^{ni} \quad \text{and} \quad \phi(a) = \phi(b)\\ &\iff xw^i = yw^i,\end{aligned}$$

because

$$xw^i = (a, \phi(a))(z^{ni}, \mathrm{id}) = (az^{ni}, \phi(a)) \quad \text{and} \quad yw^i = (b, \phi(b))(z^{ni}, \mathrm{id}) = (bz^{ni}, \phi(b)).$$

□

One says that a square-free left non-degenerate solution (X, r) of the Yang–Baxter equation satisfies the so-called exterior cyclic condition if $r(x, y) = (u, v)$ for some $x, y, u, v \in X$ implies that there exists $z \in X$ such that $r(v, y) = (u, z)$. This condition was crucial in the study of monoids of I-type (see [24]). In [19] it is shown that the exterior cyclic condition holds for a square-free left non-degenerate solution of the Yang–Baxter equation. Considering the importance of this condition, we include the following generalization of the result in [19], which can be proved in a similar fashion as in [19].

Corollary 4.3. *Assume that (X, r) is a left non-degenerate solution of the Yang–Baxter equation such that for any $x \in X$ there exists a unique $y \in X$ satisfying $r(x, y) = (x, y)$. If $x, y, y', u, v, u' \in X$ are such that $r(x, y) = (u, v)$, $r(y, y') = (y, y')$, and $r(u, u') = (u, u')$, then there exists $z \in X$ such that $r(v, y') = (u', z)$.*

Theorem 4.4. *Assume that (X, r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Then the structure monoid $M = M(X, r)$ is central-by-finite. In particular, if K is a field, then $K[M]$ is a finite module over a central affine subalgebra of $K[M]$. Hence, $K[M]$ is a Noetherian PI-algebra. Moreover, if $A = A(X, r)$, then*

$$\begin{aligned}\mathrm{clKdim}\, K[M] = \mathrm{GKdim}\, K[M] = \mathrm{rk}\, M = \mathrm{clKdim}\, K[A] = \mathrm{GKdim}\, K[A] = \mathrm{rk}\, A\\ \leqslant |X|,\end{aligned}$$

and the equality holds if and only if the solution (X, r) is involutive.

Proof. By Lemma 2.5 there exists $d \geqslant 1$ such that the elements $c_x = x^d \in A$, for $x \in X$, are central. Define $C = \langle c_x \mid x \in X\rangle \subseteq A$ and $z_x = \prod_{g\in\mathcal{G}} g(c_x) \in A$ for $x \in X$, where $\mathcal{G} = \mathcal{G}(X, r)$. Because $g(X) = X$ for each $g \in \mathcal{G}$, it is easy to see that $Z = \langle z_x \mid x \in X\rangle \subseteq C$. We claim that $K[C]$ is a finite $K[Z]$-module. Indeed, let

$$C_0 = \{c \in C : g(c) = c \quad \text{for all } g \in \mathcal{G}\}$$

denote the submonoid of $\mathcal{G}$-invariants of C. For $c \in C$ define $p(t) = \prod_{g\in\mathcal{G}}(t - g(c))$. It is clear that $p(t)$ is a monic polynomial with coefficients in $K[C_0]$ and $p(c) = 0$. Hence $K[C_0] \subseteq K[C]$ is an integral extension. Since the algebra $K[C]$ is affine, we conclude that $K[C]$ is a finite $K[C_0]$-module. Now, if $c = \prod_{x\in X} c_x^{n_x} \in C_0$, then $g(c) = c$ for each $g \in \mathcal{G}$ and thus

$$c^{|\mathcal{G}|} = \prod_{g\in\mathcal{G}} g(c) = \prod_{g\in\mathcal{G}}\prod_{x\in X} g(c_x)^{n_x} = \prod_{x\in X}\Big(\prod_{g\in\mathcal{G}} g(c_x)\Big)^{n_x} = \prod_{x\in X} z_x^{n_x} \in Z.$$

Thus the extension $K[Z] \subseteq K[C_0]$ is integral as well. Because the algebra $K[C_0]$ is affine (by the Artin–Tate lemma [35, Lemma 13.9.10]; equivalently, C_0 is a finitely generated monoid), $K[C_0]$ is a finite $K[Z]$-module. Concluding, $K[C]$ is a finite $K[C_0]$-module and $K[C_0]$ is a finite $K[Z]$-module, which assures that $K[C]$ is a finite $K[Z]$-module.

If $z \in Z$, then $g(z) = z$ for each $g \in \mathcal{G}$. This leads to $(z, \phi(z))^n = (z^n, \phi(z)^n)$ for all $n \geqslant 1$. Hence there exists $k \geqslant 1$ such that $\phi(z_x)^k = \mathrm{id}$ for all $x \in X$. Define $Z_0 = \langle z_x^k \mid x \in X\rangle \subseteq Z$. Then $g(z) = z$ for each $z \in Z_0$ and $g \in \mathcal{G}$. Moreover, $\phi(z) = \mathrm{id}$ for each $z \in Z_0$ (this is an easy consequence of $\mathrm{id} = \phi(a)\phi(b) = \phi(a\phi(a)(b)) = \phi(ab)$ for $a, b \in A$ satisfying $\phi(a) = \phi(b) = \mathrm{id}$). Further, if $(a, \phi(a)) \in M$ and $z \in Z_0$, then

$$\begin{aligned}(z, \mathrm{id})(a, \phi(a)) &= (za, \phi(a)) = (az, \phi(a)),\\ (a, \phi(a))(z, \mathrm{id}) &= (a\phi(a)(z), \phi(a)) = (az, \phi(a)).\end{aligned}$$

Thus $Z_0' = Z_0 \times \{\mathrm{id}\}$ is a central submonoid of M. Clearly $K[Z_0] \subseteq K[Z]$ is an integral extension, and because the algebra $K[Z]$ is affine, $K[Z]$ is a finite $K[Z_0]$-module. Putting this together with the claim from the first paragraph of the proof, we obtain that $K[C]$ is a finite $K[Z_0]$-module. Furthermore, $K[A]$ is a finite $K[C]$-module (see the proof of Theorem 2.7), which leads to a conclusion that $K[A] = \sum_{f\in F} K[Z_0]f$ for some finite subset $F \subseteq A$. Finally, because

$$(zf, \phi(zf)) = (zf, \phi(f)) = (z, \mathrm{id})(f, \phi(f))$$

for $z \in Z_0$ and $f \in F$, we get that $K[M] = \sum_{f\in F} K[Z_0'](f, \phi(f))$ is a finite module over the central affine subalgebra $K[Z_0']$ of $K[M]$. Hence the algebra $K[M]$ is Noetherian and PI. Thus [37, Theorem 14, p. 284] yields $\operatorname{clKdim} K[M] = \operatorname{GKdim} K[M] = \operatorname{rk} M$. Moreover,

$$\operatorname{GKdim} K[M] = \operatorname{GKdim} K[Z_0'] = \operatorname{GKdim} K[Z_0] = \operatorname{GKdim} K[A].$$

Hence, the remaining part of our theorem follows by Theorem 2.7. □

We finish this section with a positive answer to Conjecture 3.20 posed by Gateva-Ivanova in [19].

Theorem 4.5. *Assume that (X, r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Let $M = M(X, r)$. If K is a field, then the following conditions are equivalent:*

(1) *(X, r) is an involutive solution.*
(2) *M is a cancellative monoid.*
(3) $\operatorname{rk} M = |X|$.
(4) *$K[M]$ is a prime algebra.*
(5) *$K[M]$ is a domain.*
(6) $\operatorname{clKdim} K[M] = |X|$.
(7) $\operatorname{GKdim} K[M] = |X|$.

Proof. Clearly (5) $\Longrightarrow$ (4), and (4) $\Longrightarrow$ (2) follows by Lemma 4.1. Moreover, the implication (1) $\Longrightarrow$ (5) is a well-known fact (cf. [21, Corollary 1.5]). Since (1) $\Longleftrightarrow$ (3) $\Longleftrightarrow$ (6) $\Longleftrightarrow$ (7) by Theorem 4.4, it is enough to check that (2) $\Longrightarrow$ (1). But if M is cancellative and $ca = cb$ for some $a, b, c \in A = A(X, r)$, then

$$(c, \phi(c))(\phi(c)^{-1}(a), \phi(\phi(c)^{-1}(a))) = (ca, \phi(ca))$$
$$= (cb, \phi(cb)) = (c, \phi(c))(\phi(c)^{-1}(b), \phi(\phi(c)^{-1}(b))).$$

Hence, by cancellativity of M, we get

$$(\phi(c)^{-1}(a), \phi(\phi(c)^{-1}(a))) = (\phi(c)^{-1}(b), \phi(\phi(c)^{-1}(b))).$$

Thus $\phi(c)^{-1}(a) = \phi(c)^{-1}(b)$ and $a = b$ follows. Hence A is cancellative, and thus (X, r) is an involutive solution by Theorem 2.8. □

Note that in [28] it is shown that the quadratic monoid is of I-type if and only if it is cancellative and satisfies the cyclic condition.

5. Prime ideals of $M(X, r)$ and $K[M(X, r)]$

In this section we give a description of certain prime ideals of the algebra $K[M(X, r)]$ over a field K for a square-free finite bijective left non-degenerate solution (X, r) of the Yang–Baxter equation. We start with some observations and introduce some notation. As before we make an identification $M = M(X, r) = \{(a, \phi(a)) : a \in A = A(X, r)\} \subseteq A \rtimes \mathcal{G}$, where $\mathcal{G} = \mathcal{G}(X, r) = \operatorname{gr}(\lambda_x \mid x \in X) \subseteq \operatorname{Sym}(X)$, and the map $\phi\colon A \to \mathcal{G}$ satisfies $\phi(a)\phi(b) = \phi(a\phi(a)(b))$ for $a, b \in A$. We first describe all the prime ideals of $M(X, r)$.

Because elements of A are normal, each one-sided ideal of A is a two-sided ideal. For an ideal I of A put

$$I^e = \{(a, \phi(a)) : a \in I\}.$$

Similarly, if J is an ideal of M, then put

$$J^c = \{a \in A : (a, \phi(a)) \in J\}.$$

It is clear that J^c is an ideal of A, and I^e is a right ideal of M. Moreover, I^e is an ideal of M if and only if I satisfies $a\phi(a)(I) \subseteq I$ for each $a \in A$ (of course it is enough to consider $a \in A \setminus I$; let us call such ideals ϕ-invariant). Thus the rules

$$I \mapsto I^e \qquad \text{and} \qquad J \mapsto J^c$$

define mutually inverse bijections (actually mutually inverse lattice isomorphisms) between the set consisting of all ϕ-invariant ideals of A and the set consisting of all ideals of M.

Lemma 5.1. *Assume that (X, r) is a finite left non-degenerate solution of the Yang–Baxter equation. If P is a prime ideal of $M = M(X, r)$, then $P = I^e$ with I a semiprime ideal of $A = A(X, r)$. Thus $P = (Q_1 \cap \cdots \cap Q_r)^e$ for some prime ideals $Q_1, \ldots, Q_r$ of A that are minimal over I.*

Proof. Let $P = I^e$ be a prime ideal of M. We need to prove that I is a semiprime ideal of A. To do so, assume J is an ideal of A that contains I and such that J/I is nil. We claim that $I = J$. First we show that the right ideal $J^e = \{(j, \phi(j)) : j \in J\}$ of M is nil modulo P. Indeed, take $x = (j, \phi(j)) \in J^e$. For any $n \geqslant 1$ we have that

$$x^n = (j\phi(j)(j) \cdots \phi(j)^{n-1}(j), \phi(j)^n).$$

Hence for a large enough $n \geqslant 1$, we have $x^n = (y, \mathrm{id})$ with $y \in J$, and thus for some $m \geqslant 1$, we get that $x^{nm} = (y^m, \mathrm{id}) \in I^e$ and $y^m \in I$. This proves that J^e is indeed nil modulo P. Hence, J^e/P is nil submonoid of the monoid M/P. Since M and thus also M/P satisfies the ascending chain condition, it is well-known (cf. [17, Proposition 17.22] or [24, Theorem 2.4.10]) that J^e/P is nilpotent. Since P is a prime ideal we get that $J^e \subseteq P = I^e$ and thus $J = I$, as desired. ☐

With notation as above, since P is a left ideal we have that $a\phi(a)(Q_1 \cap \cdots \cap Q_r) \subseteq Q_1 \cap \cdots \cap Q_r$ for every $a \in A$. As $\phi(a) \in \mathrm{Aut}(A)$ this condition is equivalent to

(7) for every $1 \leqslant i \leqslant r$ and for every $a \in A \setminus Q_i$ there exists $1 \leqslant j \leqslant r$ such that $\phi(a)(Q_j) \subseteq Q_i$.

Renumbering, if necessary, we may assume that $Q_1, \ldots, Q_k$ are all the prime ideals of least height among all primes $Q_1, \ldots, Q_r$. Then, condition (7) yields that for every $1 \leqslant i \leqslant k$ and for every $a \in A \setminus Q_i$ there exists $1 \leqslant j \leqslant k$ such that $\phi(a)(Q_j) = Q_i$. Hence $(Q_1 \cap \cdots \cap Q_k)^e$ is an ideal of M. We claim that $k = r$. Suppose the contrary, i.e., suppose $k < r$. First note that $(Q_{k+1} \cap \cdots \cap Q_r)^e$ and $(Q_1 \cap \cdots \cap Q_k)^e$ are right ideals of M. Furthermore,

$$\begin{aligned}
&(Q_{k+1} \cap \cdots \cap Q_r)^e (Q_1 \cap \cdots \cap Q_k)^e \\
&\quad \subseteq \bigcup_{a \in Q_{k+1} \cap \cdots \cap Q_r} (a\phi(a)(Q_1 \cap \cdots \cap Q_k), \phi(a\phi(a)(Q_1 \cap \cdots \cap Q_k))) \\
&\quad \subseteq (Q_1 \cap \cdots \cap Q_k \cap Q_{k+1} \cap \cdots \cap Q_r)^e = P.
\end{aligned}$$

Thus, $(Q_{k+1} \cap \cdots \cap Q_r)^e \subseteq P$ or $(Q_1 \cap \cdots \cap Q_k)^e \subseteq P$. The former would imply that $Q_s \subseteq Q_1$ for some $k+1 \leqslant s \leqslant r$. Hence, since all the primes involved are minimal over I, we would get $Q_s = Q_1$, a contradiction.

Hence, we have proved the first part of the following lemma. The second part is then a translation of condition (7).

Lemma 5.2. *Assume that (X, r) is a finite left non-degenerate solution of the Yang–Baxter equation. If P is a prime ideal of $M = M(X, r)$, then $P = I^e$ with I a semiprime ideal of $A = A(X, r)$. Thus $P = (Q_1 \cap \cdots \cap Q_r)^e$ where $Q_1, \ldots, Q_r$ are prime ideals of A all of the same height, and furthermore,*

for every $1 \leqslant i \leqslant r$ and for every $a \in A \setminus Q_i$ there exists $1 \leqslant j \leqslant r$ such that $\phi(a)^{-1}(Q_i) = Q_j$.

The set of prime ideals $\{Q_1, \ldots, Q_r\}$ will be denoted as $\mathrm{Spec}(P)$. Consequently

if $Q \in \mathrm{Spec}(P)$, then $\{\phi(a)^{-1}(Q) : a \in A \setminus Q\} \subseteq \mathrm{Spec}(P)$.

We now focus on the converse process and investigate whether for a prime ideal Q of A there exists a prime ideal P of M such that $Q \in \mathrm{Spec}(P)$. To do so we recursively introduce some sets $\mathcal{S}_n = \mathcal{S}_n(Q)$ consisting of prime ideals of A. Put

$$\mathcal{S}_1 = \mathcal{S}_1(Q) = \{Q\}$$

and

$$\mathcal{S}_{n+1} = \mathcal{S}_{n+1}(Q) = \{\phi(a)^{-1}(Q') : Q' \in \mathcal{S}_n \quad \text{and} \quad a \in A \setminus Q'\}.$$

Since $1 \in A \setminus Q'$ for $Q' \in \mathcal{S}_n$ and $\phi(1) = \mathrm{id}$ we get $\mathcal{S}_n \subseteq \mathcal{S}_{n+1}$. Because A has only finitely many prime ideals there exists $n = n(Q) \geqslant 1$ such that $\mathcal{S}_i = \mathcal{S}_n$ for all $i \geqslant n$. Put

$$P(Q) = \bigcap_{Q' \in \mathcal{S}_n} Q'.$$

We also need the following lemma for square-free solutions. Actually, it is enough to assume that $\lambda_x(x) = x$ for all $x \in X$.

Lemma 5.3. *Assume that (X, r) is a finite square-free bijective left non-degenerate solution of the Yang–Baxter equation. Then there exists $t \geqslant 1$ such that $\phi(a^t) = \mathrm{id}$ for each $a \in A = A(X, r)$.*

Proof. By Lemma 2.5 we know that there exists $d \geqslant 1$ such that $a^d \in \mathrm{Z}(A)$ for all $a \in A$. Because of the square-free assumption, there exists $d' \geqslant 1$ such that $\phi(x^{d'}) = \mathrm{id}$ for all $x \in X$. Replacing d and d' by a common multiple we may assume that $d = d'$. Let $C = \langle x^d \mid x \in X \rangle$, a submonoid of $\mathrm{Z}(A)$. Let $\sim$ denote the equivalence relation on A defined by $a_1 \sim a_2$ if $c_1 a_1 = c_2 a_2$ for some $c_1, c_2 \in C$. Because C is a central submonoid of A we have that $\sim$ is a congruence on A. Denote by $\overline{a}$ the natural image of $a \in A$ in the monoid $\overline{A} = A/{\sim}$. Clearly $\overline{A} = \langle \overline{x} \mid x \in X \rangle$. As $\overline{x}^d = \overline{x^d} = \overline{1}$, the monoid $\overline{A}$ is a group, and, by Remark 2.3, it follows that $\overline{A}$ is a finite group, say of order t. Then, for every $a \in A$, we obtain that $\overline{a}^t = \overline{1}$. Hence, for every $a \in A$ there exist $c_1, c_2 \in C$ such that $c_1 a^t = c_2$. Since $\phi(c_1) = \phi(c_2) = \mathrm{id}$, we conclude that

$$\phi(a^t) = \phi(c_1)\phi(a^t) = \phi(c_1 \phi(c_1)(a^t)) = \phi(c_1 a^t) = \phi(c_2) = \mathrm{id},$$

as desired. □

Lemma 5.4. *Assume that (X, r) is a finite square-free bijective left non-degenerate solution of the Yang–Baxter equation. If Q is a prime ideal of $A = A(X, r)$, then $P(Q)^e$ is a prime ideal of $M = M(X, r)$.*

Proof. First we show that $P(Q)^e$ is an ideal of M. For this we need to show that condition (7) holds for the set of primes $\mathcal{S}_n$ (where $n = n(Q)$). So, let $Q' \in \mathcal{S}_n$ and $a \in A \setminus Q'$. Then by the definition of $\mathcal{S}_n$ we have that $\phi(a)^{-1}(Q') \in \mathcal{S}_{n+1} = \mathcal{S}_n$, and thus condition (7) follows.

Second we prove that $P(Q)^e$ is a prime ideal of M. To do so, consider

$$\mathcal{F} = \{I^e : I \text{ is an ideal of } A \text{ such that } I \subseteq Q \text{ and } I^e \text{ is an ideal of } M\}.$$

By the first part $P(Q)^e \in \mathcal{F}$, and thus $\mathcal{F} \neq \varnothing$. Because of Zorn's lemma, there exists a maximal (for the inclusion relation) element of $\mathcal{F}$, say I^e. We claim that I^e is a prime ideal of M. To prove this, suppose J^e and K^e are ideals of M, with J and K ideals of A that properly contain I such that $J^e K^e \subseteq I^e$. Then, because of the maximality, there exist $j \in J \setminus Q$ and $k \in K \setminus Q$ and $(j, \phi(j))M(k, \phi(k)) \subseteq I^e$. Because of Lemma 5.3, let $d \geqslant 1$ be such that $\phi(j^d) = \mathrm{id}$. Then,

$$\begin{aligned}(j, \phi(j)) \cdot (\phi(j)^{-1}(j^{d-1}), \phi(\phi(j)^{-1}(j^{d-1}))) \cdot (k, \phi(k)) &= (j^d, \mathrm{id}) \cdot (k, \phi(k)) \\ &= (j^d k, \phi(k)) \in I^e.\end{aligned}$$

Hence $j^d k \in I \subseteq Q$, in contradiction with Q being a prime ideal in the monoid A that consists of normal elements. So, indeed I^e is a prime ideal of M.

Hence, by Lemmas 5.1 and 5.2 we know that $I = Q_1 \cap \cdots \cap Q_r$, an intersection of prime ideals of A of the same height, and $\mathcal{S}_n(Q) \subseteq \mathrm{Spec}(I^e)$. So $I \subseteq P(Q) \subseteq Q$, and thus $I^e \subseteq P(Q)^e$. Since $P(Q)^e \in \mathcal{F}$, the maximality condition yields that $I^e = P(Q)^e$, and the result follows. ☐

The previous lemmas together with results from Section 3 give a full description of the prime ideals in $M(X, r)$.

Proposition 5.5. *Assume that (X, r) is a finite square-free bijective left non-degenerate solution of the Yang–Baxter equation. The prime ideals of $M = M(X, r)$ are precisely the ideals $P(Q)^e$, where Q runs through the prime ideals of $A = A(X, r)$. Further,*

$$P(Q) = \bigcap_{Q' \in \mathcal{S}_{n(Q)}(Q)} Q'$$

is an intersection of prime ideals of A of the same height and $\mathrm{ht}\, P(Q)^e = \mathrm{ht}\, Q$. In particular, the map

$$\mathrm{Spec}(A) \to \mathrm{Spec}(M) \colon Q \mapsto P(Q)^e$$

satisfies going-up, going-down, and incomparability.

Proof. The first part has been proved. The second part follows now at once. ☐

We also have the following analog of the second part of Proposition 3.2. That is, prime ideals of the algebra $K[M(X, r)]$ over a field K not intersecting the monoid $M(X, r)$ are determined by prime ideals of the group algebra $K[G(X, r)]$.

Proposition 5.6. *Assume that (X, r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Let $M = M(X, r)$. If K is a field, then there exists an inclusion-preserving bijection between the set of prime ideals P of $K[M]$ satisfying $P \cap M = \varnothing$ and the set of all prime ideals of the group algebra $K[G]$, where*

$$G = G(X, r) = \mathrm{gr}(X \mid xy = \lambda_x(y)\rho_y(x) \quad \text{for all } x, y \in X).$$

Moreover, the cancellative monoid $\overline{M} = M/\eta_M$ has a group of quotients which is equal to the central localization $\overline{M}\langle z \rangle^{-1}$ for some $z \in \mathrm{Z}(\overline{M})$, and $G \cong \overline{M}\langle z \rangle^{-1}$.

Proof. By Lemma 2.5 there exists $d \geqslant 1$ such that $\phi(a)^d = \mathrm{id}$ and $a^d \in \mathrm{Z}(A)$ for each $a \in A = A(X, r)$. Moreover, if $x \in X$, then $(x, \phi(x))^{d^2} = (y, \mathrm{id})^d = (a_x, \mathrm{id})$, where $y = x\phi(x)(x) \cdots \phi(x)^{d-1}(x) \in A$ and $a_x = y^d \in \mathrm{Z}(A)$. Define $c_x = \prod_{g \in \mathcal{G}} g(a_x)$, where $\mathcal{G} = \mathcal{G}(X, r)$. Clearly $c_x \in \mathrm{Z}(A)$ and $g(c_x) = c_x$ for each $g \in \mathcal{G}$. If $b_x = \prod_{\mathrm{id} \neq g \in \mathcal{G}} g(a_x) \in \mathrm{Z}(A)$, then $a_x b_x = c_x$, and thus

$$(x, \phi(x))^{d^2}(b_x, \phi(b_x)) = (a_x, \mathrm{id})(b_x, \phi(b_x)) = (a_x b_x, \phi(b_x)) = (c_x, \phi(c_x)).$$

Moreover, $\phi(c_x^d) = \phi(c_x)^d = \mathrm{id}$. Hence $[(x,\phi(x))^{d^2}(b_x,\phi(b_x))]^d = (c_x,\phi(c_x))^d = (c_x^d,\mathrm{id})$, and it follows that if

$$z = \prod_{x\in X}(c_x^d,\mathrm{id}) = (\prod_{x\in X} c_x^d,\mathrm{id}),$$

then $z \in \mathrm{Z}(M)$ and the central localization $\overline{M}\langle z\rangle^{-1}$ (here by z we understand the image of $z \in M$ in $\overline{M}$) is equal to the group of quotients of $\overline{M}$. Finally, the remaining part of the proof is similar to the proof of Proposition 3.2. Thus the result follows. □

6. Divisibility in $M(X,r)$

In the previous section we have shown that prime ideals are sets that are determined by divisibility of some generators. In this section, we go deeper into this. This has been done earlier, but for different quadratic monoids, in several papers to prove that the algebra is Noetherian and PI, which we already know. As before, throughout this section (X,r) denotes a finite bijective left non-degenerate solution of the Yang–Baxter equation. Let us now relate the structure of $M = M(X,r)$ to substructures determined by divisibility by generators. Since each element of $A = A(X,r)$ is a normal element, left divisibility in A by an element is the same as right divisibility by that element. In the monoid M we will have to use the terminology left and right divisible. Let $|X| = n$. For $1 \leqslant i \leqslant n$ put

$$A_i = \{a \in A : a \text{ is divisible by at least } i \text{ elements of } X\}$$

and

$$M_i = \{(a,\phi(a)) \in M : (a,\phi(a)) \text{ is left divisible by at least } i \text{ generators } (x,\phi(x)) \text{ with } x \in X\}.$$

Clearly,

$$M_i = A_i^e = \{(a,\phi(a)) : a \in A_i\}.$$

Since A_i is a ϕ-invariant ideal of A, it follows that each M_i is an ideal of M. Hence we get an ideal chain in M:

$$M_n \subseteq M_{n-1} \subseteq \cdots \subseteq M_1 \subseteq M.$$

Note that the equality $M_i = M_{i+1}$ is possible; for instance the structure monoid $M = M(X,r)$ of the solution (X,r) defined in Example 1.1 satisfies $M_1 = M_2$.

The following lemmas, propositions, and proofs are completely analogous to those for monoids of skew type given in [24]. We have included them for completeness' sake.

For a non-empty subset $Y \subseteq X$ define

$$M_Y = \bigcap_{y\in Y}(y,\phi(y))M \qquad \text{and} \qquad D_Y = M_Y \setminus \bigcup_{x\in X\setminus Y} M_{\{x\}}.$$

Clearly, the set M_Y consists of all elements of M that are left divisible by generators $(y,\phi(y))$ with $y \in Y$, and the set D_Y consists of all elements of M that are precisely left divisible by those generators. Obviously, for each $1 \leqslant i \leqslant n$ we have

$$M_i = \bigcup_{Y\subseteq X,\, |Y|=i} M_Y.$$

The following lemma is clear by using the fact that $M_i = A_i^e$ and A_i are ϕ-invariant ideals of A.

Lemma 6.1 (Cf. [24, Theorem 9.3.7]). *Assume that (X, r) is a finite left non-degenerate solution of the Yang–Baxter equation. If $M = M(X, r)$ and $n = |X|$, then*

$$M_X = M_n \subseteq M_{n-1} \subseteq \cdots \subseteq M_1 \subseteq M$$

is a chain of ideals in M.

The following technical lemma will prove to be crucial in the proof of the main result of this section. It proves that under certain conditions we can show left divisibility by words.

Lemma 6.2 (Cf. [24, Lemma 9.3.8]). *Assume that (X, r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Let $M = M(X, r)$ and $n = |X|$. Suppose that $Y \subseteq X$ and $|Y| = i$, where $1 \leqslant i \leqslant n$. If $\varnothing \neq Z \subseteq Y$ and $s \in D_Z$ satisfies $|s| = k$, then*

$$M_i^k \cap D_Y \subseteq sM.$$

Proof. If $k = 1$, then the claim is obvious. So assume $k \geqslant 2$. To shorten the notation put

$$s_x = (x, \phi(x)) \in M$$

for $x \in X$ and write $s = s_{x_1} \cdots s_{x_k}$ with $x_1, \ldots, x_k \in X$. Let $a = a_1 \cdots a_k \in D_Y$, where $a_1, \ldots, a_k \in M_i$. Since $D_Y \subseteq M_i \setminus M_{i+1}$ and M_{i+1} is an ideal of M, if non-empty, it is clear that $a_1, \ldots, a_k \in M_i \setminus M_{i+1}$. As $s \in D_Z$ and $Z \subseteq Y$, it follows that $x_1 \in Y$. Because $a \in D_Y$, we obtain $a_1 \in D_Y$. Hence, there exists $b_1 \in M$ such that $a_1 = s_{x_1} b_1$. Thus, $a_1 a_2 = s_{x_1} c_1$, where $c_1 = b_1 a_2$. Clearly, $a_1 a_2 \in M_i \setminus M_{i+1}$, which implies that $c_1 \in M_i \setminus M_{i+1}$. Suppose we have shown that

$$a_1 \cdots a_j = s_{x_1} \cdots s_{x_{j-1}} c_{j-1}$$

for some $1 < j < k$ and $c_{j-1} \in M_i \setminus M_{i+1}$. We claim that $c_{j-1} \in s_{x_j} M$. Let $W \subseteq X$ be such that $|W| = i$ and $c_{j-1} \in D_W$. Consider the set

$$U = \{x \in X : s_{x_1} \cdots s_{x_{j-1}} s_x \in D_V \quad \text{for some } V \subseteq Y\}.$$

As (X, r) is left non-degenerate, it follows that $|U| \leqslant |Y| = i$. Since $a \in D_Y$, it follows that $a_1 \cdots a_j \in D_Y$. Because $c_{j-1} \in D_W$, we obtain that $W \subseteq U$. Thus $|U| = i$ and $W = U$. Since $s_{x_1} \cdots s_{x_j}$ is a left initial segment of $s \in D_Z$ and $Z \subseteq Y$, we also get that $x_j \in U = W$. As $c_{j-1} \in D_W$, it follows that $c_{j-1} \in s_{x_j} M$, as claimed.

Now, write $c_{j-1} = s_{x_j} b_j$ for some $b_j \in M$. Then

$$a_1 \cdots a_j a_{j+1} = s_{x_1} \cdots s_{x_{j-1}} s_{x_j} b_j a_{j+1}.$$

Define $c_j = b_j a_{j+1}$. Then $c_j \in M_i \setminus M_{i+1}$. Thus, by induction, we obtain that $a = a_1 \cdots a_k \in s_{x_1} \cdots s_{x_k} M = sM$, and the result is shown. ☐

Recall that by

$$I(\eta) = \operatorname{Span}_K\{x - y : (x, y) \in \eta\},$$

the K-linear span of the set consisting of all elements $x - y$ with $(x, y) \in \eta$, we understand the ideal of the algebra $K[M]$ associated to a congruence η on the monoid M. Moreover, η_M denotes the cancellative congruence of M (see Proposition 4.2 and the comment above).

Lemma 6.3. *Assume that (X,r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Let $M = M(X,r)$. If K is a field, then*

$$I(\eta_M) = \operatorname{Ann}_{K[M]}(w^m) = \operatorname{Ann}_{K[M]}(M_X^m)$$

for some $w \in M_X \cap \mathrm{Z}(M)$ and some $m \geqslant 1$.

Proof. Let $A = A(X,r)$. Define $z = \prod_{x\in X} x^d \in \mathrm{Z}(A)$ and $w = (z^n, \mathrm{id}) \in \mathrm{Z}(M)$ as in the proof of Proposition 4.2. Clearly $w \in M_X$. Therefore, Lemma 6.2 implies that $M_X^k \subseteq wM \subseteq M_X$, where $k = |w|$. Now, if $t \geqslant 1$ is such that $I(\eta_M) = \operatorname{Ann}_{K[M]}(w^i)$ for all $i \geqslant t$ (see Proposition 4.2), then, since $w^{kt}M \subseteq M_X^{kt} \subseteq w^t M$, we conclude that

$$I(\eta_M) = \operatorname{Ann}_{K[M]}(w^t) \subseteq \operatorname{Ann}_{K[M]}(M_X^{kt}) \subseteq \operatorname{Ann}_{K[M]}(w^{kt}) = I(\eta_M).$$

This shows the result with $m = kt$. □

The following proposition provides us information on prime ideals P of the algebra $K[M(X,r)]$, which intersect the monoid $M(X,r)$ non-trivially.

Proposition 6.4 (Cf. [24, Proposition 9.5.3])**.** *Assume that (X,r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Let $M = M(X,r)$. If K is a field and P is a prime ideal of $K[M]$ such that $P \cap M \neq \varnothing$, then*

$$P \cap M = \bigcup_{Y\in\mathcal{F}} D_Y,$$

where $\mathcal{F} = \{Y \subseteq X : Y \neq \varnothing \quad \text{and} \quad D_Y \cap P \neq \varnothing\}$. Moreover, if $Y \in \mathcal{F}$ and $Y \subseteq Z \subseteq X$, then $D_Z \subseteq P$.

Proof. The inclusion $P \cap M \subseteq \bigcup_{Y\in\mathcal{F}} D_Y$ is obvious. We prove the reverse inclusion by contradiction. So, suppose that there exists $Y \in \mathcal{F}$ such that $D_Y \nsubseteq P$. Choose such a set Y with maximal $i = |Y|$. We claim that $i < |X|$. Indeed, if $s \in P \cap M$, then $ws \in P \cap M_X$ (we use the notation introduced in the proof of Lemma 6.3). Therefore, by Lemma 6.2, we get $M_X^n \subseteq wsM \subseteq P$, where $n = |ws|$. Hence $D_X = M_X \subseteq P$, and thus $Y \neq X$, as claimed. Let $a \in D_Y \cap P$ and set $k = |a|$. Consider an arbitrary subset $Z \subseteq X$ such that $Y \subseteq Z$ and $D_Z \neq \varnothing$. By Lemma 6.2,

$$D_Z^k \cap D_Z \subseteq aM \subseteq P. \tag{8}$$

If $Z \neq Y$ and $D_Z^k \cap D_Z \neq \varnothing$, then $|Z| > i$ and $D_Z \cap P \neq \varnothing$ by (8). Hence, by the definition of i, we get $D_Z \subseteq P$. Whereas, if $Z \neq Y$ and $D_Z^k \cap D_Z = \varnothing$, then $D_Z^k \subseteq \bigcup_{Z\subsetneq V} D_V$. In the latter case the given argument can be applied to every $V \subseteq X$ such that $Z \subsetneq V$ and $D_V \neq \varnothing$. Continuing this process, after a finite number of steps, we obtain that $I = \bigcup_{Y\subsetneq Z} D_Z$ is nilpotent modulo P. Since I is a right ideal of M and because $P \cap M$ is a prime ideal of M, it follows that $I \subseteq P$. Applying (8) to $Z = Y$, we thus have proved that

$$D_Y^k \subseteq (D_Y^k \cap D_Y) \cup I \subseteq P.$$

As $D_Y \cup I = \bigcup_{Y\subseteq Z} D_Z$ is a right ideal of M and it is nilpotent modulo P, we conclude that $D_Y \subseteq P$, a contradiction. The second part of the result follows from the proof above. □

We now are in a position to prove the main result of this section.

Theorem 6.5 (Cf. [24, Proposition 9.5.2])**.** *Assume that (X, r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. If $M = M(X, r)$ and K is a field, then the following properties hold:*

(1) $I(\eta_M) = \mathrm{Ann}_{K[M]}(w^m) = \mathrm{Ann}_{K[M]}(M_X^m)$ *for some* $w \in M_X \cap \mathrm{Z}(M)$ *and some* $m \geqslant 1$.
(2) $I(\eta_M) \subseteq P$ *for any prime ideal* P *of* $K[M]$ *such that* $P \cap M = \varnothing$.
(3) $M_X \subseteq P$ *for any prime ideal* P *of* $K[M]$ *such that* $P \cap M \neq \varnothing$. *In particular,* $w \in P$.
(4) *There exists at least one minimal prime ideal* P *of* $K[M]$ *such that* $P \cap M = \varnothing$.
(5) *If* $\mathrm{char}\, K = 0$, *then*

$$\mathcal{J}(K[M]) = \mathcal{B}(K[M]) = I(\eta_M) \cap \bigcap_{P \in \mathcal{P}} P,$$

where $\mathcal{P} = \{P \in \mathrm{Spec}(K[M]) : P \cap M \neq \varnothing\} = \{P \in \mathrm{Spec}(K[M]) : w \in P\}$.

Proof. (1), (2), and (3) follow from Lemma 6.3 and Propositions 4.2 and 6.4, respectively. Clearly $M \cap \mathcal{B}(K[M]) = \varnothing$ (elements of M are not nilpotent). Therefore, $w \notin \mathcal{B}(K[M])$, and (4) also follows. If $\mathrm{char}\, K = 0$, then the algebra $K[M/\eta_M] \cong K[M]/I(\eta_M)$ is semiprime (see [24, Theorem 3.2.8]). Hence $\mathcal{B}(K[M]) \subseteq I(\eta_M)$ and $I(\eta_M)$ is equal to the intersection of all prime ideals P of $K[M]$ such that $I(\eta_M) \subseteq P$. Thus the second equality in (5) follows. Since the Jacobson radical of an affine PI-algebra is nilpotent (cf. [9]), it equals the prime radical, which ends the proof. ☐

7. Prime images of $K[M(X, r)]$.

Assume that (X, r) is a finite bijective left non-degenerate solution of the Yang–Baxter equation. Let $M = M(X, r)$ and let K be a field. The aim in this section is to provide a matrix-type representation of the prime algebra $K[M]/P$ for each prime ideal P of $K[M]$. We do this by showing that the classical ring of quotients $\mathrm{Q_{cl}}(K[M]/P)$ is the same as $\mathrm{Q_{cl}}(\mathrm{M}_v(K[G]/P_0))$, where P_0 is a prime ideal of a group algebra $K[G]$ with G the group of quotients of a cancellative subsemigroup of M and $v \geqslant 1$ is determined by the number of orthogonal cancellative subsemigroups of an ideal in $M/(P \cap M)$. If P is such that $P \cap M = \varnothing$, then this has been shown in Proposition 5.6. Hence, in the remainder of this section we assume that P is a prime ideal of $K[M]$ with $P \cap M \neq \varnothing$. Note that $K[M]/P$ is an epimorphic image of the contracted monoid algebra $K_0[M/(P \cap M)]$. Hence we determine a representation of

$$S = M/(P \cap M).$$

As a first step we make use of a result of Anan'in (see [24, Theorem 3.5.2] or [2]) that yields that the Noetherian PI-algebra $K_0[S]$ embeds into a matrix algebra $\mathrm{M}_m(L)$ over a field extension L of K. Thus, we will consider S as a submonoid of the multiplicative monoid $\mathrm{M}_m(L)$. By [24, Proposition 5.1.1] (and the fact that S satisfies the ascending chain condition on left and right ideals) it follows that S intersects non-trivially finitely many $\mathcal{H}$-classes of $\mathrm{M}_m(L)$ (i.e., the maximal subgroups of $\mathrm{M}_m(L)$), say $G_1, \dots, G_k$. Since $K_0[S]$ is a PI-algebra, also each $K[S \cap G_i]$ is a PI-algebra. Hence, $S \cap G_i$ has a group of quotients $\mathrm{gr}(S \cap G_i)$ which is abelian-by-finite (cf. [24, Theorem 3.1.9]).

For every $1 \leqslant i \leqslant k$, let e_i denote the idempotent of the maximal subgroup G_i and fix $s_i \in S \cap G_i$. Because of Lemma 2.5 we may choose s_i in the center of $A(X,r)$. So, $e_i = s_i s_i^{-1}$, where s_i^{-1} denotes the inverse of s_i in G_i. Without loss of generality, we may assume that $s_i = (a_i, \mathrm{id})$ with a_i in the center of $A(X,r)$. One then proves as in [28, Lemma 2.4] that $e_i e_j = e_j e_i$ for all $1 \leqslant i, j \leqslant k$. Hence,

$$\langle e_1, \ldots, e_k \rangle \cup \{\theta\} = \{e_1, \ldots, e_k\} \cup \{\theta\}$$

is an abelian semigroup (where θ is the zero element of S). By [36, Theorem 3.5] we get that the linear semigroup S has an ideal chain

$$S_0 \subseteq T_1 \subseteq S_1 \subseteq \cdots \subseteq S_{m-1} \subseteq T_m \subseteq S_m = S \tag{9}$$

with each

$$N_j = T_j/S_{j-1} = (T_j \setminus S_{j-1}) \cup \{\theta\} \quad \text{a nilpotent ideal of } S/S_{j-1}$$

(and it actually is a union of nilpotent ideals of nilpotency index 2) and each

$$S_j/T_j = (S_j \setminus T_j) \cup \{\theta\} \subseteq \mathcal{M}_j/\mathcal{M}_{j-1}$$

a 0-disjoint union of uniform subsemigroups (for the terminology see [24, Section 2.2]), say $U_\alpha^{(j)}$ (with α in an indexing set $\mathcal{A}_j$), of $\mathcal{M}_j/\mathcal{M}_{j-1}$ that intersect different $\mathcal{R}$-classes and different $\mathcal{L}$-classes of $\mathcal{M}_j/\mathcal{M}_{j-1}$ (here $\mathcal{M}_j$ denotes the ideal in $\mathrm{M}_m(L)$ consisting of matrices of rank at most j). Recall that it is well-known that $\mathcal{M}_j$ are the only ideals of the multiplicative monoid $\mathrm{M}_m(L)$ and $\mathcal{M}_j/\mathcal{M}_{j-1}$ is a completely 0-simple semigroup with maximal subgroups isomorphic to $\mathrm{GL}_j(L)$. Moreover,

$$\text{each } N_j \text{ does not intersect } \mathcal{H}\text{-classes of } \mathcal{M}_j/\mathcal{M}_{j-1} \text{ intersected by } S_j \setminus T_j,$$

and

$$U_\alpha^{(j)} U_\beta^{(j)} \subseteq N_j \quad \text{for all } \alpha \neq \beta \quad \text{and} \quad U_\alpha^{(j)} N_j U_\alpha^{(j)} = \{\theta\} \quad \text{in } \mathcal{M}_j/\mathcal{M}_{j-1}.$$

In particular, each $U_\alpha^{(j)}$ can be considered as an ideal in S/T_j.

Because S is a prime monoid with 0-element, it follows that the lowest non-zero ideal in the chain (9) is of the type S_j (i.e., $T_j = \{\theta\}$). So $N_j = \{\theta\}$, and thus $S_j \subseteq \mathcal{M}_j/\mathcal{M}_{j-1}$ is a 0-disjoint union of the uniform subsemigroups $U_\alpha^{(j)}$, and each $U_\alpha^{(j)}$ is an ideal of S. As $U_\alpha^{(j)} U_\beta^{(j)} \subseteq N_j = \{\theta\}$ for $\alpha \neq \beta$, and because S is a prime monoid we get that $S_j = U_\alpha^{(j)}$ for some α, and it is a uniform subsemigroup of the completely 0-simple semigroup $\mathcal{M}_j/\mathcal{M}_{j-1}$. Renumbering $G_1, \ldots, G_k$, if necessary, we may assume that $G_1, \ldots, G_v$ are all the maximal subgroups of $\mathcal{M}_j$ that intersect S non-trivially. So, for each $1 \leqslant r \leqslant v$, the semigroup $S \cap G_r$ is cancellative.

We also know that $S_j = U_\alpha^{(j)}$ is contained in the smallest completely 0-simple subsemigroup $\widehat{U}_\alpha^{(j)}$ of $\mathcal{M}_j/\mathcal{M}_{j-1}$ (see, e.g., [24, Proposition 2.2.1]). That is, $U_\alpha^{(j)}$ intersects all non-zero $\mathcal{H}$-classes of $\widehat{U}_\alpha^{(j)}$, and every maximal subgroup H of $\widehat{U}_\alpha^{(j)}$ is generated by $U_\alpha^{(j)} \cap H$ (so $H = \mathrm{gr}(S \cap G_i)$ for some i and $\mathrm{gr}(S \cap G_1) \cong \cdots \cong \mathrm{gr}(S \cap G_v)$ is an abelian-by-finite group).

To simplify notation, we write $U_\alpha^{(j)}$ as U and $\widehat{U}_\alpha^{(j)}$ as $\widehat{U}$. By the above, the idempotents of $\widehat{U}$ commute. Since $\widehat{U}$ is completely 0-simple, this implies that these idempotents are pairwise orthogonal. Since S intersects non-trivially only finitely $\mathcal{H}$-classes of $\mathcal{M}_j/\mathcal{M}_{j-1}$, the completely 0-simple semigroup $\widehat{U}$ has only finitely many rows and columns. It follows that the sandwich matrix of $\widehat{U}$ contains precisely one non-zero element in each row and column. So, reindexing if necessary, we may assume that the sandwich matrix is a diagonal matrix, and thus also $\widehat{U}$ has the same number of rows and columns. It is then well-known (see, e.g., [14, Lemma 3.6]) that

$$\widehat{U} \cong \mathcal{M}(G, v, v, I)$$

with G a maximal subgroup of $\widehat{U}$ (that is, this is isomorphic to $\mathrm{gr}(S \cap G_1)$) and G is abelian-by-finite (we denote by I the identity matrix of degree v). Put $\widehat{S} = (S \setminus U) \cup \widehat{U}$, a disjoint union. Note that $\widehat{S}$ also is a subsemigroup of $\mathrm{M}_m(L)$ and $\widehat{U}$ is an ideal of $\widehat{S}$ (cf. [24, Lemma 2.5.2]). Hence, $K_0[S]$ is a subalgebra of $K_0[\widehat{S}]$, and it has $K_0[\widehat{U}]$ as an ideal. The ideal $K_0[\widehat{U}]$ has $e = e_1 + \cdots + e_v$ as an identity, and thus this is a central element of $K_0[\widehat{S}]$. We also have a natural epimorphism

$$f_P\colon K_0[S] \to K_0[S]e \subseteq K_0[\widehat{U}].$$

Hence, $K_0[S]e$ is a Noetherian algebra and $K_0[S]e \subseteq K_0[\widehat{U}] \cong \mathrm{M}_v(K[G])$. By [24, Proposition 2.5.6] we also know that G is finitely generated. So, G is a finitely generated abelian-by-finite group. Note that

$$\operatorname{Ker} f_P = \{\alpha \in K_0[S] : \alpha e = 0\} = \{\alpha \in K_0[S] : \alpha U = 0\}.$$

Since the ideal $K_0[U]$ is not contained in the prime ideal $P/K[P \cap M]$, we get $\operatorname{Ker} f_P \subseteq P/K[P \cap M]$.

We are now in a position to prove the main result of this section (in the statement and proof of this result we use the notation introduced in this section).

Theorem 7.1. *If P is a prime ideal of $K[M]$, then there exists an ideal I_P of $K[M]$ contained in P and a prime ideal P_0 of $K[G]$ such that $K[M]/I_P \subseteq \mathrm{M}_v(K[G])$ and $K[M]/P \subseteq \mathrm{M}_v(K[G]/P_0)$ for some $v \geqslant 1$. Moreover, $\mathrm{M}_v(K[G])$ is a localization of $K[M]/I_P$. In particular, $\mathrm{Q}_{\mathrm{cl}}(K[M]/P) \cong \mathrm{Q}_{\mathrm{cl}}(\mathrm{M}_v(K[G]/P_0))$. If, furthermore, $K[M]$ is semiprime, then there exist finitely many finitely generated abelian-by-finite groups, say $G_1, \ldots, G_m$, each being the group of quotients of a cancellative subsemigroup of M such that $K[M]$ embeds into $\mathrm{M}_{v_1}(K[G_1]) \times \cdots \times \mathrm{M}_{v_m}(K[G_m])$ for some $v_1, \ldots, v_m \geqslant 1$.*

Proof. Let P be a prime ideal of $K[M]$. If $P \cap M = \varnothing$, then the first part of the result has been shown in Proposition 5.6. So, assume that $P \cap M \neq \varnothing$. Let $S = M/(P \cap M)$. From the above we know that $K_0[S]/\operatorname{Ker} f_P \subseteq K_0[\widehat{U}] \cong \mathrm{M}_v(K[G])$, where G is the group of fractions of a cancellative subsemigroup of U. Furthermore, $K_0[\widehat{U}]$ is a localization of $K_0[U]$ with respect to diagonal matrices (with entries in G) that belong to $K_0[U]$. Such matrices are regular in $K_0[\widehat{U}]$, and thus they also are regular elements in $K_0[S]/\operatorname{Ker} f_P$. Hence the Noetherian algebra $K_0[\widehat{U}]$ is a localization of $K_0[S]/\operatorname{Ker} f_P$. Therefore, as is well-known (see [24, Theorem 3.2.6]), there exists a prime ideal $P_0' = \mathrm{M}_v(P_0)$ of $\mathrm{M}_v(K[G])$ (with P_0 a prime ideal of $K[G]$) such that $P_0' \cap (K_0[S]/\operatorname{Ker} f_P) = P/\operatorname{Ker} f_P$. Let I_P denote the ideal of $K[M]$ containing $K[P \cap M]$ that naturally projects onto $\operatorname{Ker} f_P$ in $K_0[S]$. It follows that $K[M]/I_P \subseteq \mathrm{M}_v(K[G])$ and $K[M]/P \subseteq \mathrm{M}_v(K[G]/P_0)$ and $K[M]/P$ is a localization of $\mathrm{M}_v(K[G]/P_0)$. Hence the first part of the result follows.

Assume now that the algebra $K[M]$ is semiprime. Because $K[M]$ is Noetherian (see Theorem 4.4), it has finitely many minimal prime ideals, say $P_1, \ldots, P_m$. By the first part, for each P_i there exists an ideal $I_{P_i} \subseteq P_i$ such that $K[M]/I_{P_i} \subseteq \mathrm{M}_{v_i}(K[G_i])$, for some finitely generated abelian-by-finite group G_i that is the group of fractions of a cancellative subsemigroup of M. Since $\bigcap_{i=1}^{m} I_i \subseteq \bigcap_{i=1}^{m} P_i = 0$, we get that $K[M]$ embeds into $K[M]/I_{P_1} \times \cdots \times K[M]/I_{P_m}$. Hence the result follows. □

References

[1] B. Amberg, O. Dickenschied, and Ya. P. Sysak, *Subgroups of the adjoint group of a radical ring*, Canad. J. Math. **50** (1998), no. 1, 3–15, DOI 10.4153/CJM-1998-001-9. MR1618706

[2] A. Z. Anan′in, *An intriguing story about representable algebras*, Ring theory 1989 (Ramat Gan and Jerusalem, 1988/1989), Israel Math. Conf. Proc., vol. 1, Weizmann, Jerusalem, 1989, pp. 31–38. MR1029294

[3] David Bachiller, *Solutions of the Yang-Baxter equation associated to skew left braces, with applications to racks*, J. Knot Theory Ramifications **27** (2018), no. 8, 1850055, 36, DOI 10.1142/S0218216518500554. MR3835326

[4] David Bachiller, *Extensions, matched products, and simple braces*, J. Pure Appl. Algebra **222** (2018), no. 7, 1670–1691, DOI 10.1016/j.jpaa.2017.07.017. MR3763276

[5] David Bachiller, *Classification of braces of order p^3*, J. Pure Appl. Algebra **219** (2015), no. 8, 3568–3603, DOI 10.1016/j.jpaa.2014.12.013. MR3320237

[6] David Bachiller, Ferran Cedó, and Eric Jespers, *Solutions of the Yang-Baxter equation associated with a left brace*, J. Algebra **463** (2016), 80–102, DOI 10.1016/j.jalgebra.2016.05.024. MR3527540

[7] D. Bachiller, F. Cedó, E. Jespers, and J. Okniński, *Asymmetric product of left braces and simplicity; new solutions of the Yang–Baxter equation*, Commun. Contemp. Math. (2018), 1850042, doi.org/10.1142/S0219199718500426.

[8] Rodney J. Baxter, *Partition function of the eight-vertex lattice model*, Ann. Physics **70** (1972), 193–228, DOI 10.1016/0003-4916(72)90335-1. MR0290733

[9] Amiram Braun, *The nilpotency of the radical in a finitely generated PI ring*, J. Algebra **89** (1984), no. 2, 375–396, DOI 10.1016/0021-8693(84)90224-2. MR751151

[10] Francesco Catino, Ilaria Colazzo, and Paola Stefanelli, *Semi-braces and the Yang-Baxter equation*, J. Algebra **483** (2017), 163–187, DOI 10.1016/j.jalgebra.2017.03.035. MR3649817

[11] Ferran Cedó, *Left braces: solutions of the Yang-Baxter equation*, Adv. Group Theory Appl. **5** (2018), 33–90. MR3824447

[12] Ferran Cedó, Tatiana Gateva-Ivanova, and Agata Smoktunowicz, *On the Yang-Baxter equation and left nilpotent left braces*, J. Pure Appl. Algebra **221** (2017), no. 4, 751–756, DOI 10.1016/j.jpaa.2016.07.014. MR3574204

[13] Ferran Cedó, Eric Jespers, and Jan Okniński, *Braces and the Yang-Baxter equation*, Comm. Math. Phys. **327** (2014), no. 1, 101–116, DOI 10.1007/s00220-014-1935-y. MR3177933

[14] A. H. Clifford and G. B. Preston, *The algebraic theory of semigroups. Vol. I*, Mathematical Surveys, No. 7, American Mathematical Society, Providence, R.I., 1961. MR0132791

[15] V. G. Drinfel′d, *On some unsolved problems in quantum group theory*, Quantum groups (Leningrad, 1990), Lecture Notes in Math., vol. 1510, Springer, Berlin, 1992, pp. 1–8, DOI 10.1007/BFb0101175. MR1183474

[16] Pavel Etingof, Travis Schedler, and Alexandre Soloviev, *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. **100** (1999), no. 2, 169–209, DOI 10.1215/S0012-7094-99-10007-X. MR1722951

[17] Carl Faith, *Algebra. II*, Ring theory, Grundlehren der Mathematischen Wissenschaften, No. 191, Springer-Verlag, Berlin-New York, 1976. MR0427349

[18] Tatiana Gateva-Ivanova, *Set-theoretic solutions of the Yang-Baxter equation, braces and symmetric groups*, Adv. Math. **338** (2018), 649–701, DOI 10.1016/j.aim.2018.09.005. MR3861714

[19] T. Gateva-Ivanova, *A combinatorial approach to noninvolutive set-theoretic solutions of the Yang–Baxter equation*, preprint, arXiv:1808.03938, 2018.

[20] T. Gateva-Ivanova, Eric Jespers, and Jan Okniński, *Quadratic algebras of skew type and the underlying monoids*, J. Algebra **270** (2003), no. 2, 635–659, DOI 10.1016/j.jalgebra.2003.06.005. MR2019633

[21] Tatiana Gateva-Ivanova and Michel Van den Bergh, *Semigroups of I-type*, J. Algebra **206** (1998), no. 1, 97–112, DOI 10.1006/jabr.1997.7399. MR1637256

[22] Isabel Goffa and Eric Jespers, *Monoids of IG-type and maximal orders*, J. Algebra **308** (2007), no. 1, 44–62, DOI 10.1016/j.jalgebra.2006.07.029. MR2290908

[23] L. Guarnieri and L. Vendramin, *Skew braces and the Yang-Baxter equation*, Math. Comp. **86** (2017), no. 307, 2519–2534, DOI 10.1090/mcom/3161. MR3647970

[24] Eric Jespers and Jan Okniński, *Noetherian semigroup algebras*, Algebra and Applications, vol. 7, Springer, Dordrecht, 2007. MR2301033

[25] Eric Jespers and Jan Okniński, *Monoids and groups of I-type*, Algebr. Represent. Theory **8** (2005), no. 5, 709–729, DOI 10.1007/s10468-005-0342-7. MR2189580

[26] Eric Jespers, Jan Okniński, and Maya Van Campenhout, *Finitely generated algebras defined by homogeneous quadratic monomial relations and their underlying monoids*, J. Algebra **440** (2015), 72–99, DOI 10.1016/j.jalgebra.2015.05.017. MR3373388

[27] Eric Jespers and Arne Van Antwerpen, *Left semi-braces and solutions of the Yang-Baxter equation*, Forum Math. **31** (2019), no. 1, 241–263, DOI 10.1515/forum-2018-0059. MR3898225

[28] Eric Jespers and Maya Van Campenhout, *Finitely generated algebras defined by homogeneous quadratic monomial relations and their underlying monoids II*, J. Algebra **492** (2017), 524–546, DOI 10.1016/j.jalgebra.2017.09.011. MR3709164

[29] Seiichi Kamada, *Knot invariants derived from quandles and racks*, Invariants of knots and 3-manifolds (Kyoto, 2001), Geom. Topol. Monogr., vol. 4, Geom. Topol. Publ., Coventry, 2002, pp. 103–117, DOI 10.2140/gtm.2002.4.103. MR2002606

[30] A. Konovalov, A. Smoktunowicz, and L. Vendramin, *On skew braces and their ideals*, Exp. Math., online (2018), `doi.org/10.1080/10586458.2018.1492476`.

[31] Victoria Lebed, *Cohomology of idempotent braidings with applications to factorizable monoids*, Internat. J. Algebra Comput. **27** (2017), no. 4, 421–454, DOI 10.1142/S0218196717500229. MR3668103

[32] V. Lebed and L. Vendramin, *On structure groups of set-theoretic solutions to the Yang–Baxter equation*, Proc. Edinb. Math. Soc., online (2019), `doi.org/10.1017/S0013091518000548`.

[33] Victoria Lebed and Leandro Vendramin, *Cohomology and extensions of braces*, Pacific J. Math. **284** (2016), no. 1, 191–212, DOI 10.2140/pjm.2016.284.191. MR3530867

[34] Jiang-Hua Lu, Min Yan, and Yong-Chang Zhu, *On the set-theoretical Yang-Baxter equation*, Duke Math. J. **104** (2000), no. 1, 1–18, DOI 10.1215/S0012-7094-00-10411-5. MR1769723

[35] J. C. McConnell and J. C. Robson, *Noncommutative Noetherian rings*, with the cooperation of L. W. Small, Revised edition, Graduate Studies in Mathematics, vol. 30, American Mathematical Society, Providence, RI, 2001. MR1811901

[36] Jan Okniński, *Semigroups of matrices*, Series in Algebra, vol. 6, World Scientific Publishing Co., Inc., River Edge, NJ, 1998. MR1785162

[37] Jan Okniński, *Semigroup algebras*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 138, Marcel Dekker, Inc., New York, 1991. MR1083356

[38] Donald S. Passman, *Infinite crossed products*, Pure and Applied Mathematics, vol. 135, Academic Press, Inc., Boston, MA, 1989. MR979094

[39] Donald S. Passman, *The algebraic structure of group rings*, Pure and Applied Mathematics, Wiley-Interscience [John Wiley & Sons], New York-London-Sydney, 1977. MR470211

[40] J. E. Roseblade, *Prime ideals in group rings of polycyclic groups*, Proc. London Math. Soc. (3) **36** (1978), no. 3, 385–447, DOI 10.1112/plms/s3-36.3.385. MR0491797

[41] Wolfgang Rump, *Braces, radical rings, and the quantum Yang-Baxter equation*, J. Algebra **307** (2007), no. 1, 153–170, DOI 10.1016/j.jalgebra.2006.03.040. MR2278047

[42] Wolfgang Rump, *Modules over braces*, Algebra Discrete Math. **2** (2006), 127–137. MR2320986

[43] Wolfgang Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation*, Adv. Math. **193** (2005), no. 1, 40–55, DOI 10.1016/j.aim.2004.03.019. MR2132760

[44] Agata Smoktunowicz, *On Engel groups, nilpotent groups, rings, braces and the Yang-Baxter equation*, Trans. Amer. Math. Soc. **370** (2018), no. 9, 6535–6564, DOI 10.1090/tran/7179. MR3814340

[45] Agata Smoktunowicz and Leandro Vendramin, *On skew braces (with an appendix by N. Byott and L. Vendramin)*, J. Comb. Algebra **2** (2018), no. 1, 47–86, DOI 10.4171/JCA/2-1-3. MR3763907

[46] Alexander Soloviev, *Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation*, Math. Res. Lett. **7** (2000), no. 5-6, 577–596, DOI 10.4310/MRL.2000.v7.n5.a4. MR1809284

[47] C. N. Yang, *Some exact results for the many-body problem in one dimension with repulsive delta-function interaction*, Phys. Rev. Lett. **19** (1967), 1312–1315, DOI 10.1103/PhysRevLett.19.1312. MR0261870

Department of Mathematics, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussel, Belgium

Email address: Eric.Jespers@vub.be

Department of Mathematics, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussel, Belgium

Email address: Lukasz.Kubat@vub.be

Department of Mathematics, Vrije Universiteit Brussel, Pleinlaan 2, 1050 Brussel, Belgium

Email address: Arne.Van.Antwerpen@vub.be