SEMIRING AND INVOLUTION IDENTITIES OF POWER GROUPS

SERGEY V. GUSEV ⓘ and MIKHAIL V. VOLKOV ⓘ

Communicated by James East

Abstract

For every group G, the set $\mathcal{P}(G)$ of its subsets forms a semiring under set-theoretical union $\cup$ and element-wise multiplication $\cdot$, and forms an involution semigroup under $\cdot$ and element-wise inversion $^{-1}$. We show that if the group G is finite, non-Dedekind, and solvable, neither the semiring $(\mathcal{P}(G), \cup, \cdot)$ nor the involution semigroup $(\mathcal{P}(G), \cdot, ^{-1})$ admits a finite identity basis. We also solve the finite basis problem for the semiring of Hall relations over any finite set.

1. Introduction

An *additively idempotent semiring* (ai-semiring, for short) is an algebra $\mathcal{S} = (S, +, \cdot)$ whose operations $+$ and $\cdot$ are associative and fulfill the distributive laws

$$x(y + z) = xy + xz \quad \text{and} \quad (y + z)x = yx + zx,$$

and furthermore, addition is commutative and fulfills the idempotency law $x + x = x$. We refer to the semigroup $(S, \cdot)$ as to the *multiplicative reduct* of $\mathcal{S}$.

Examples of ai-semirings are plentiful and include many objects of importance for computer science, idempotent analysis, tropical geometry, and algebra such as, for example, semirings of binary relations [17], syntactic semirings of languages [27, 28], tropical semirings [26], endomorphism semirings of semilattices [16]. A natural family of ai-semirings comes from the powerset construction applied to an arbitrary semigroup. Namely, for any semigroup $(S, \cdot)$, one can multiply its subsets element-wise: for any $A, B \subseteq S$, put

$$A \cdot B := \{ab \mid a \in A, \ b \in B\}.$$

It is known and easy to verify that this multiplication distributes over the set-theoretical union of subsets of S. Thus, denoting the powerset of S by $\mathcal{P}(S)$, we see that $(\mathcal{P}(S), \cup, \cdot)$ is an ai-semiring, called the *power semiring* of $(S, \cdot)$. In semigroup theory, there exists a vast literature on *power semigroups*, that is, the multiplicative reducts of power semirings. The interest in power semigroups is mainly motivated by their applications in the algebraic theory of regular languages; see [1, Ch. 11] and references therein. Power semirings have attracted less attention so far, but we think they deserve study no less than power semigroups as $(\mathcal{P}(S), \cup, \cdot)$ carries more information than its multiplicative reduct $(\mathcal{P}(S), \cdot)$. (For instance, it is known that in general, the power semigroup $(\mathcal{P}(S), \cdot)$ does not determine its 'parent' semigroup $(S, \cdot)$ up to isomorphism [21, 22] while it is easy to see that the power semiring $(\mathcal{P}(S), \cup, \cdot)$ does.)

The power semigroups of finite groups have quite a specific structure discussed in detail in [1, Section 11.1]. In particular, they satisfy the following implications:

$$ ef = e^2 = e \ \& \ fe = f^2 = f \rightarrow e = f, \tag{1-1} $$

$$ ef = f^2 = f \ \& \ fe = e^2 = e \rightarrow e = f. \tag{1-2} $$

Semigroups satisfying Equations (1-1) and (1-2) are called *block-groups*. We refer the reader to Pin's survey [25] for an explanation of the name 'block-group' and an overview of the remarkable role played by finite block-groups in the theory of regular languages. In this paper, we deal with power semirings of finite groups, which we call *power groups* for brevity, and more broadly, with ai-semirings whose multiplicative reducts are block-groups. We address the finite axiomatizability question (also known as the finite basis problem) for semiring identities satisfied by such ai-semirings. For power groups, we prove the following theorem.

THEOREM 1.1. *For any finite nonabelian solvable group $(G, \cdot)$, the identities of the power group $(\mathcal{P}(G), \cup, \cdot)$ admit no finite basis.*

In 2009, Dolinka [6, Problem 6.5] asked for a description of finite groups whose power groups have no finite identity basis (provided such finite groups exist, which was unknown at that time). Theorem 1.1 gives a partial answer to Dolinka's question.

Theorem 1.1 is a consequence of quite a general condition ensuring the absence of a finite identity basis for ai-semirings whose multiplicative reducts are block-groups with solvable subgroups (see Theorem 4.2). Yet another application of this condition, combined with a result from [14], gives a complete solution to the finite basis problem for a natural family of semirings of binary relations. Recall that a *Hall relation* on a finite set X is a binary relation that contains all pairs $(x, x\pi)$, $x \in X$, for a permutation $\pi \colon X \to X$. Clearly, the set $H(X)$ of all Hall relations on X is closed under unions and products of relations, and hence $(H(X), \cup, \cdot)$ is a subsemiring of the $(\cup, \cdot)$-semiring of all binary relations on X.

THEOREM 1.2. *The identities of the ai-semiring of all Hall relations on a finite set X admit a finite basis if and only if $|X| = 1$.*

Our techniques apply equally well to yet another algebra carried by the powerset of a group. An *involution semigroup* is a semigroup equipped with an extra unary operation $x \mapsto x^*$ that fulfills the laws

$$(xy)^* = y^* x^* \quad \text{and} \quad (x^*)^* = x.$$

If $(G, \cdot)$ is a group, each $g \in G$ has the inverse g^{-1} and the map $g \mapsto g^{-1}$ naturally extends to the powerset of G: for each $A \in \mathcal{P}(G)$, let $A^{-1} := \{g^{-1} \mid g \in A\}$. Clearly, $(\mathcal{P}(G), \cdot, ^{-1})$ forms an involution semigroup. The finite basis problem for involution semigroups is relatively well studied (see, for example, [2, 3, 7, 19]), but involution power semigroups of groups do not fall into any previously studied class. Our next result applies to involution power semigroups of finite solvable groups containing at least one nonnormal subgroup. Recall that a group all of whose subgroups are normal is called a *Dedekind* group.

THEOREM 1.3. *For any finite non-Dedekind solvable group* $(G, \cdot)$*, the identities of the involution semigroup* $(\mathcal{P}(G), \cdot, ^{-1})$ *admit no finite basis.*

The paper is structured as follows. Section 2 collects the necessary properties of block-groups. The technical core of the paper is Section 3, where we show that every finite block-group with solvable subgroups satisfies certain semigroup identities from a family of identities introduced in our earlier paper [11]. This allows us in Section 4 to quickly deduce Theorems 1.1 and 1.2 from the main result of [11]. In Section 5, we prove an involution semigroup variant of the main result of [11], which allows us to infer Theorem 1.3.

2. Preliminaries

The present paper uses a few basic notions of semigroup theory such as idempotents, ideals, and Rees quotients. They all can be found in the early chapters of any general semigroup theory text, for example, [5, 13]. We also assume the reader's acquaintance with rudiments of group theory, including the concept of a solvable group, see, for example, [12].

We recall the definition of a Brandt semigroup as we will need some calculations in such semigroups. Let I be a nonempty set, $\mathcal{G} = (G, \cdot)$ a group, and $0 \notin G$ a fresh symbol. The *Brandt semigroup* $\mathcal{B}_{G,I}$ over $\mathcal{G}$ has the set $B_{G,I} := I \times G \times I \cup \{0\}$ as its carrier, and the multiplication in $\mathcal{B}_{G,I}$ is defined by

$$(\ell_1, g_1, r_1) \cdot (\ell_2, g_2, r_2) := \begin{cases} (\ell_1, g_1 g_2, r_2) & \text{if } r_1 = \ell_2, \\ 0 & \text{otherwise,} \end{cases} \text{ for all } \ell_1, \ell_2, r_1, r_2 \in I, \ g_1, g_2 \in G,$$

$$(\ell, g, r) \cdot 0 = 0 \cdot (\ell, g, r) = 0 \cdot 0 := 0 \qquad \text{for all } \ell, r \in I, \ g \in G.$$

We register a property of Brandt semigroups that readily follows from the definition.

LEMMA 2.1. *Let I be a nonempty set, let $\mathcal{G} = (G, \cdot)$ be a group, and for any $\ell, r \in I$, let $G_{\ell r} := \{(\ell, g, r) \mid g \in G\}$. Then, $(G_{\ell r}, \cdot)$ is a maximal subgroup of the Brandt semigroup $\mathcal{B}_{G,I}$ if $\ell = r$; otherwise the product of any two elements from $G_{\ell r}$ is 0.*

An element a of a semigroup $(S, \cdot)$ is said to be *regular* if there exists $b \in S$ satisfying $aba = a$ and $bab = b$; any such b is called an *inverse of a*. A semigroup is called *regular* [respectively, *inverse*] if every element has an inverse [respectively, a unique inverse]. Every group $\mathcal{G} = (G, \cdot)$ is an inverse semigroup, and the unique inverse of an element $g \in G$ is nothing but its group inverse g^{-1}. The Brandt semigroup $\mathcal{B}_{G,I}$ over $\mathcal{G}$ is inverse as well: for $\ell, r \in I$ and $g \in G$, the unique inverse of (ℓ, g, r) is (r, g^{-1}, ℓ) and the unique inverse of 0 is 0.

Now we present a few properties of block-groups needed for Section 3. They all are known, but in some cases, we failed to find any reference that could be used directly (rather one has to combine several facts scattered over the literature). In such cases, we include easy direct proofs for the reader's convenience.

The definition of a block-group can be restated in terms of inverse elements, and it is this version of the definition that is often used in the literature to introduce block-groups.

LEMMA 2.2. *A semigroup $(B, \cdot)$ is a block-group if and only if every element in B has at most one inverse.*

PROOF. The 'if' part. Take any $e, f \in B$ that satisfy the antecedent of the implication in Equation (1-1), that is, $ef = e^2 = e$ and $fe = f^2 = f$. Multiplying $ef = e$ by e on the right and using $e^2 = e$, we get $efe = e$, and similarly, multiplying $fe = f$ by f on the right and using $f^2 = f$, we get $fef = f$. Hence, f is an inverse of e. However, we have $e = e^2 = e^3$ so that e is an inverse of itself. Since e has at most one inverse, we conclude that $e = f$ so that Equation (1-1) holds. By symmetry, the implication in Equation (1-2) holds as well.

The 'only if' part. Take any $a \in B$ and suppose that both b and c are inverses of a. Letting $e := ba$ and $f := ca$, we have $ef = baca = ba = e$, $e^2 = baba = e$, and similarly, $fe = caba = ca = f$, $f^2 = caca = f$. Since $(B, \cdot)$ satisfies the implication in Equation (1-1), we get $e = f$, that is, $ba = ca$. By symmetry, the implication in Equation (1-2) ensures $ab = ac$. Now we have $b = bab = cab = cac = c$. $\square$

Lemma 2.2 shows that regular block-groups are inverse, so that one can think of block-groups as nonregular analogs of inverse semigroups.

For any semigroup $(S, \cdot)$, we denote the set of all its idempotents by $E(S)$. A semigroup $(S, \cdot)$ is called *$\mathcal{J}$-trivial* if every principal ideal of $(S, \cdot)$ has a unique generator and *periodic* if every one-generated subsemigroup of $(S, \cdot)$ is finite. In [20, Proposition 2.3], it is proved that a finite monoid $(S, \cdot)$ is a block-group if and only if the subsemigroup $(\langle E(S) \rangle, \cdot)$ generated by $E(S)$ is $\mathcal{J}$-trivial. In fact, the proof in [20] uses periodicity of $(S, \cdot)$ rather than its finiteness and does not use the identity element of $(S, \cdot)$. Thus, we have the following characterization of periodic block-groups.

PROPOSITION 2.3. *A periodic semigroup is a block-group if and only if the subsemi-group generated by its idempotents is $\mathcal{J}$-trivial.*

As a consequence, we have the following observation.

LEMMA 2.4. *If $(S, \cdot)$ is a periodic block-group, then every regular element of the subsemigroup $(\langle E(S) \rangle, \cdot)$ lies in $E(S)$.*

PROOF. Let $a \in \langle E(S) \rangle$ be a regular element and b its inverse. The FitzGerald trick [9, Lemma 1] shows that $b \in \langle E(S) \rangle$ as well. Since $a = aba$ and $b = bab$ generate the same ideal in $(\langle E(S) \rangle, \cdot)$, Proposition 2.3 implies $a = b$. Thus, $a = a^3$, whence a and a^2 also generate the same ideal in $(\langle E(S) \rangle, \cdot)$. Now Proposition 2.3 implies $a = a^2 \in E(S)$.   □

LEMMA 2.5. *If a Brandt semigroup $(B, \cdot)$ occurs as an ideal in a periodic block-group $(S, \cdot)$, then for all $b \in B$, $f \in E(S)$, either $fb = b$ or $fb = 0$.*

PROOF. If the semigroup $(B, \cdot)$ is represented as $\mathcal{B}_{G,I}$ for some group $(G, \cdot)$ and some nonempty set I, then each nonzero idempotent is of the form (i, e, i), where $i \in I$ and e is the identity element of the group $\mathcal{G}$. Take an arbitrary element $b = (\ell, g, r) \in I \times G \times I$. Then $b = (\ell, e, \ell)b$, whence $fb = f(\ell, e, \ell)b$ for each $f \in E(S)$. The product $f(\ell, e, \ell)$ lies in B and so it is regular. By Lemma 2.4, $f(\ell, e, \ell)$ is an idempotent. If $f(\ell, e, \ell) \neq 0$, then $f(\ell, e, \ell) = (j, e, j)$ for some $j \in I$. Multiplying the equality through by (j, e, j) on the right yields $f(\ell, e, \ell)(j, e, j) = (j, e, j)$, whence $j = \ell$. We conclude that either $f(\ell, e, \ell) = (\ell, e, \ell)$ or $f(\ell, e, \ell) = 0$, whence either $fb = b$ or $fb = 0$.   □

A *principal series* of a semigroup $(S, \cdot)$ is a chain

$$S_0 \subset S_1 \subset \cdots \subset S_h = S \qquad (2\text{-}1)$$

of ideals S_j of $(S, \cdot)$ such that S_0 is the least ideal of $(S, \cdot)$ and there is no ideal of $(S, \cdot)$ strictly between S_{j-1} and S_j for $j = 1, \ldots, h$. The *factors* of the series in Equation (2-1) are the Rees quotients $(S_j/S_{j-1}, \cdot)$, $j = 1, \ldots, h$. The number h is called the *height* of the series in Equation (2-1).

Recall that a semigroup $(Z, \cdot)$ with a zero element 0 is called a *zero semigroup* if $ab = 0$ for all $a, b \in Z$. A semigroup $(T, \cdot)$ with a zero element 0 is *0-simple* if it is not a zero semigroup, and $\{0\}$ and T are the only ideals of $(T, \cdot)$. A semigroup $(T, \cdot)$ is *simple* if T is its only ideal. (Observe that a simple semigroup may consist of a single element while any 0-simple semigroup has at least two elements.) By [5, Lemma 2.39], if Equation (2-1) is a principal series, then $(S_0, \cdot)$ is a simple semigroup and every factor $(S_j/S_{j-1}, \cdot)$, $j = 1, \ldots, h$, is either a 0-simple semigroup or a zero semigroup with at least two elements.

Restricting a classical result of semigroup theory (see [5, Theorem 3.5] or [13, Theorem 3.2.3]) to the case of periodic block-groups yields the following lemma.

LEMMA 2.6. *If a periodic block-group is simple, it is a group, and if it is 0-simple, it is a Brandt semigroup.*

COROLLARY 2.7. *If a periodic block-group possesses a principal series, then its least ideal is a group and the nonzero factors of the series are Brandt semigroups.*

We call Equation (2-1) a *Brandt series* if $(S_0, \cdot)$ is a group and every factor $(S_j/S_{j-1}, \cdot)$ with $j = 1, \ldots, h$, which is not a zero semigroup, is a Brandt semigroup. Thus, Corollary 2.7 can be restated as saying that a principal series of a periodic block-group is a Brandt series (provided the series exists). The converse is also true, even without periodicity.

LEMMA 2.8. *If a semigroup possesses a Brandt series, it is a block-group.*

PROOF. Let Equation (2-1) be a Brandt series in a semigroup $(S, \cdot)$. Take any regular element $a \in S$ and let $j \in \{0, 1, \ldots, h\}$ be the least number with $a \in S_j$. Recall that each inverse of a generates the same ideal of $(S, \cdot)$ as does a. Therefore, if $j = 0$, all inverses of a lie in the least ideal of $(S, \cdot)$ which is a group. Then all inverses of a are equal since they coincide with the group inverse of a in the group $(S_0, \cdot)$. If $j > 0$, we have $a \in S_j \setminus S_{j-1}$, and all inverses of a also lie in $S_j \setminus S_{j-1}$. Their images in the Rees quotient $(S_j/S_{j-1}, \cdot)$ are inverses of the image of a, and hence, they coincide as the quotient must be an inverse semigroup. Since nonzero elements of S_j/S_{j-1} are in a 1–1 correspondence with the elements of $S_j \setminus S_{j-1}$, all inverses of a are equal also in this case. Now Lemma 2.2 shows that $(S, \cdot)$ is a block-group. $\square$

We also need the following property of $\mathcal{J}$-trivial semigroups.

LEMMA 2.9 [1, Lemma 8.2.2(iii)]. *If a $\mathcal{J}$-trivial semigroup $(S, \cdot)$ satisfies the identity $x^p = x^{p+1}$ and w is an arbitrary semigroup word, then $(S, \cdot)$ satisfies the identity $w^p = u^p$ where u is the product, in any order, of the variables that occur in w.*

3. Identities holding in block-groups with solvable subgroups

Here we aim to show that every finite block-group with solvable subgroups satisfies certain identities constructed in [11]. For the reader's convenience, we reproduce the construction in detail so that no acquaintance with [11] is necessary for understanding the results and the proofs of this section.

For any $i, h \geq 1$, consider the set $X_i^{(h)} := \{x_{i_1 i_2 \cdots i_h} \mid i_1, i_2, \ldots, i_h \in \{1, 2, \ldots, i\}\}$. We fix arbitrary $n, m \geq 1$ and introduce a family of words $\mathbf{v}_{n,m}^{(h)}$ over $X_{2n}^{(h)}$, $h = 1, 2, \ldots,$ by induction.

For $h = 1$, let

$$\mathbf{v}_{n,m}^{(1)} := x_1 x_2 \cdots x_{2n} (x_n x_{n-1} \cdots x_1 \cdot x_{n+1} x_{n+2} \cdots x_{2n})^{2m-1}. \tag{3-1}$$

Assuming that $h > 1$ and the word $\mathbf{v}_{n,m}^{(h-1)}$ over $X_{2n}^{(h-1)}$ has already been defined, we create $2n$ copies of this word over the alphabet $X_{2n}^{(h)}$ as follows. We start by taking for every $j \in \{1, 2, \ldots, 2n\}$, the substitution $\sigma_{2n,j}^{(h)} : X_{2n}^{(h-1)} \to X_{2n}^{(h)}$ that appends j to the indices of its arguments, that is,

$$\sigma_{2n,j}^{(h)}(x_{i_1 i_2 \ldots i_{h-1}}) := x_{i_1 i_2 \ldots i_{h-1} j} \quad \text{for all } i_1, i_2, \ldots, i_{h-1} \in \{1, 2, \ldots, 2n\}. \tag{3-2}$$

Then we let $\mathbf{v}_{n,m,j}^{(h-1)} := \sigma_{2n,j}^{(h)}(\mathbf{v}_{n,m}^{(h-1)})$ and define

$$\mathbf{v}_{n,m}^{(h)} := \mathbf{v}_{n,m,1}^{(h-1)} \cdots \mathbf{v}_{n,m,2n}^{(h-1)}(\mathbf{v}_{n,m,n}^{(h-1)} \cdots \mathbf{v}_{n,m,1}^{(h-1)} \cdot \mathbf{v}_{n,m,n+1}^{(h-1)} \cdots \mathbf{v}_{n,m,2n}^{(h-1)})^{2m-1}. \qquad (3\text{-}3)$$

Comparing the definitions in Equations (3-1) and (3-3), one readily sees that the word $\mathbf{v}_{n,m}^{(h)}$ is nothing but the image of $\mathbf{v}_{n,m}^{(1)}$ under the substitution $x_j \mapsto \mathbf{v}_{n,m,j}^{(h-1)}$, $j \in \{1, 2, \dots, 2n\}$.

REMARK 1. It is easy to see that the word $\mathbf{v}_{n,m}^{(h+r)}$ is the image of the word $\mathbf{v}_{n,m}^{(h)}$ under a substitution ζ that sends every variable from $X_{2n}^{(h)}$ to a word obtained from $\mathbf{v}_{n,m}^{(r)}$ by renaming its variables. Indeed, in terms of the substitutions $\sigma_{2n,j}^{(h)}$ from Equation (3-2), ζ expresses as follows:

$$\zeta(x_{i_1 i_2 \dots i_h}) := \sigma_{2n,i_h}^{(r+h)}(\cdots(\sigma_{2n,i_2}^{(r+2)}(\sigma_{2n,i_1}^{(r+1)}(\mathbf{v}_{n,m}^{(r)})))\cdots) \quad \text{for all } i_1, i_2, \dots, i_h \in \{1, 2, \dots, 2n\}.$$

For any $n, k \geq 0$ with $n + k > 0$ and any $m \geq 1$, we define the following word over $X_{n+k}^{(1)}$:

$$\mathbf{u}_{n,k,m} := x_1 x_2 \cdots x_{n+k} (x_n x_{n-1} \cdots x_1 \cdot x_{n+1} x_{n+2} \cdots x_{n+k})^{2m-1}.$$

Notice that $\mathbf{u}_{n,n,m} = \mathbf{v}_{n,m}^{(1)}$.

LEMMA 3.1. *Let I be a nonempty set, $\mathcal{G} = (G, \cdot)$ a group, and $\mathcal{B}_{G,I}$ the Brandt semigroup over $\mathcal{G}$. For any $m \geq 1$ and $n, k \geq 0$ with $n + k > 0$ and any substitution $\tau \colon X_{n+k}^{(1)} \to B_{G,I}$, the element $\tau(\mathbf{u}_{n,k,m})$ lies in a subgroup of $\mathcal{B}_{G,I}$.*

PROOF. Lemma 2.1 implies that for any $a \in B_{G,I}$, the power a^{2m} lies in a subgroup of $\mathcal{B}_{G,I}$. Since $\mathbf{u}_{0,k,m} = (x_1 x_2 \cdots x_k)^{2m}$ and $\mathbf{u}_{1,k,m} = (x_1 x_2 \cdots x_{k+1})^{2m}$, the claim holds for $n \in \{0, 1\}$.

For the rest of the proof, assume $n \geq 2$. If $\tau(\mathbf{u}_{n,k,m}) = 0$, there is nothing to prove. Let $\tau(\mathbf{u}_{n,k,m}) \neq 0$. Then all elements $\tau(x_i)$, $i = 1, 2, \dots, n + k$, must lie in the set $I \times G \times I$ of nonzero elements of $\mathcal{B}_{G,I}$. Hence, $\tau(x_i) = (\ell_i, g_i, r_i)$ for some $\ell_i, r_i \in I$ and $g_i \in G$.

First, consider the case $k = 0$. Since $\mathbf{u}_{n,0,m} = x_1 x_2 \cdots x_n (x_n x_{n-1} \cdots x_1)^{2m-1}$, we have $\tau(\mathbf{u}_{n,0,m}) = (\ell_1, g, r_1)$ for some $g \in G$. By Lemma 2.1, we have to show that $\ell_1 = r_1$. We verify that $\ell_j = r_j$ for all $j = n, n-1, \dots, 1$ by backward induction. Since x_n^2 occurs as a factor in the word $\mathbf{u}_{n,0,m}$, we must have $\tau(x_n^2) \neq 0$, whence $\ell_n = r_n$. If $j > 1$, both $x_{j-1}x_j$ and $x_j x_{j-1}$ occur as factors in $\mathbf{u}_{n,0,m}$. We then have

$$\begin{aligned}
r_{j-1} &= \ell_j &&\text{since } \tau(x_{j-1}x_j) \neq 0, \\
&= r_j &&\text{by the induction assumption,} \\
&= \ell_{j-1} &&\text{since } \tau(x_j x_{j-1}) \neq 0.
\end{aligned}$$

Now, let $k > 0$. Since

$$\mathbf{u}_{n,k,m} = x_1 x_2 \cdots x_{n+k} (x_n x_{n-1} \cdots x_1 \cdot x_{n+1} x_{n+2} \cdots x_{n+k})^{2m-1},$$

we have $\tau(\mathbf{u}_{n,k,m}) = (\ell_1, g, r_{n+k})$ for some $g \in G$. Here we have to show that $\ell_1 = r_{n+k}$. Since $\tau(x_1 x_2 \cdots x_n x_{n+1}) \neq 0$ and $\tau(x_{n+k} x_n) \neq 0$, we have

$$r_1 = \ell_2, \; r_2 = \ell_3, \ldots, r_{n-1} = \ell_n, \; r_n = \ell_{n+1} \quad \text{and} \quad r_{n+k} = \ell_n. \tag{3-4}$$

Since $\tau(x_n x_{n-1} \cdots x_1 x_{n+1}) \neq 0$, we also have

$$r_n = \ell_{n-1}, \; r_{n-1} = \ell_{n-2}, \ldots, r_2 = \ell_1, \; r_1 = \ell_{n+1}. \tag{3-5}$$

Therefore, we obtain

$$r_{n+k} \overset{(3\text{-}4)}{=} \ell_n \overset{(3\text{-}4)}{=} r_{n-1} \overset{(3\text{-}5)}{=} \ell_{n-2} \overset{(3\text{-}4)}{=} r_{n-3} = \cdots = \begin{cases} \ell_1 & \text{if } n \text{ is odd,} \\ r_1 & \text{if } n \text{ is even.} \end{cases}$$

In addition, if n is even, then

$$r_1 \overset{(3\text{-}5)}{=} \ell_{n+1} \overset{(3\text{-}4)}{=} r_n \overset{(3\text{-}5)}{=} \ell_{n-1} \overset{(3\text{-}4)}{=} r_{n-2} \overset{(3\text{-}5)}{=} \ell_{n-3} = \cdots = \ell_1.$$

We see that $r_{n+k} = \ell_1$ in either case. □

Several statements in this section deal with semigroups that possess Brandt series and have subgroups subject to certain restrictions. To keep the premises of these statements compact, we introduce a few short names. In what follows:

- groups of exponent dividing m are called *m-groups*;
- solvable m-groups of derived length at most k are called *$[m, k]$-groups*;
- a semigroup with a Brandt series of height h all of whose subgroups are m-groups (respectively, $[m, k]$-groups) is called an *(h, m)-semigroup* (respectively, an *(h, m, k)-semigroup*).

LEMMA 3.2. *Any (h, m)-semigroup satisfies the identity $x^{2^h m} = x^{2^{h+1} m}$.*

PROOF. Let $(S, \cdot)$ be an (h, m)-semigroup and Equation (2-1) its Brandt series. We induct on h. If $h = 0$, then $(S, \cdot)$ is an m-group, and any m-group satisfies $x^m = x^{2m}$.

Let $h > 0$ and let a be an arbitrary element in S; we have to verify that

$$a^{2^h m} = a^{2^{h+1} m}. \tag{3-6}$$

If a lies in a subgroup of $(S, \cdot)$, then $a^m = a^{2m}$ since all subgroups of $(S, \cdot)$ are m-groups. Squaring this h times gives Equation (3-6). If a lies in no subgroup of $(S, \cdot)$, then $a^2 \in S_{h-1}$ — this is clear if $a \in S_{h-1}$ or the factor $(S_h / S_{h-1}, \cdot)$ is a zero semigroup and follows from Lemma 2.1 if $(S_h / S_{h-1}, \cdot)$ is a Brandt semigroup. By the induction assumption, $(a^2)^{2^{h-1} m} = (a^2)^{2^h m}$, that is, Equation (3-6) holds again. □

Recall that if $(S, \cdot)$ is a semigroup, $(\langle E(S) \rangle, \cdot)$ stands for its subsemigroup generated by the set $E(S)$ of all idempotents of $(S, \cdot)$.

LEMMA 3.3. *Let $(S, \cdot)$ be an (h, m)-semigroup. For any $k \geq 1$, if a substitution $\tau \colon X_{2n}^{(k)} \to S$ is such that $\tau(x_{i_1 i_2 \ldots i_k}) \in \langle E(S) \rangle$ for all $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, 2n\}$, then $\tau(\mathbf{v}_{n, 2^h m}^{(k)}) \in E(S)$.*

PROOF. By Lemma 3.2, the semigroup $(S, \cdot)$ satisfies $x^{2^h m} = x^{2^{h+1} m}$, whence for each $p \geq 2^h m$ and each $a \in \langle E(S) \rangle$, the elements a^p and a^{p+1} generate the same ideal in the subsemigroup $(\langle E(S) \rangle, \cdot)$. The periodic semigroup $(S, \cdot)$ is a block-group by Lemma 2.8, whence the subsemigroup $(\langle E(S) \rangle, \cdot)$ is $\mathcal{J}$-trivial by Proposition 2.3. Therefore, we have $a^p = a^{p+1}$, that is, $(\langle E(S) \rangle, \cdot)$ satisfies the identity $x^p = x^{p+1}$.

Letting

$$a_j := \begin{cases} \tau(x_j) & \text{if } k = 1, \\ \tau(\mathbf{v}_{n,2^h m,j}^{(k-1)}) & \text{if } k > 1, \end{cases}$$

for $j = 1, 2, \ldots, 2n$, we have from Equations (3-1) and (3-3)

$$
\begin{aligned}
\tau(\mathbf{v}_{n,2^h m}^{(k)}) &= a_1 a_2 \cdots a_{2n} (a_n a_{n-1} \cdots a_1 \cdot a_{n+1} a_{n+2} \cdots a_{2n})^{2^{h+1} m - 1} \\
&= a_1 a_2 \cdots a_{2n} (a_1 \cdots a_{n-1} a_n \cdot a_{n+1} a_{n+2} \cdots a_{2n})^{2^{h+1} m - 1} \qquad \text{by Lemma 2.9} \\
&= (a_1 \cdots a_{n-1} a_n \cdot a_{n+1} a_{n+2} \cdots a_{2n})^{2^{h+1} m} \\
&= (a_1 \cdots a_{n-1} a_n \cdot a_{n+1} a_{n+2} \cdots a_{2n})^{2^h m} \qquad \text{as } x^{2^h m} = x^{2^{h+1} m} \\
&= ((a_1 \cdots a_{n-1} a_n \cdot a_{n+1} a_{n+2} \cdots a_{2n})^{2^h m})^2 = (\tau(\mathbf{v}_{n,2^h m}^{(k)}))^2.
\end{aligned}
$$

Hence, $\tau(\mathbf{v}_{n,2^h m}^{(k)}) \in E(S)$ as required. $\square$

LEMMA 3.4. *Let $(S, \cdot)$ be an (h, m)-semigroup with Brandt series in Equation (2-1). If $(S_1, \cdot)$ is a Brandt semigroup and $S = \langle E(S) \rangle \cup S_1$, then for an arbitrary substitution $\tau \colon X_{2n}^{(1)} \to S$, the element $\tau(\mathbf{v}_{n,2^h m}^{(1)})$ lies in a subgroup of S.*

PROOF. If $\tau(x_k) \in \langle E(S) \rangle$ for all $k \in \{1, 2, \ldots, 2n\}$, then $\tau(\mathbf{v}_{n,2^h m}^{(1)}) \in E(S)$ by Lemma 3.3. Otherwise, let $\{k_1, k_2, \ldots, k_{p+q}\}$ with

$$1 \leq k_1 < k_2 < \cdots < k_p \leq n < k_{p+1} < k_{p+2} < \cdots < k_{p+q} \leq 2n$$

be the set of all indices k such that $\tau(x_k) \notin \langle E(S) \rangle$. (Here, $p = 0$ or $q = 0$ is possible but $p + q > 0$.) Since $S = \langle E(S) \rangle \cup S_1$, we have $\tau(x_{k_1}), \tau(x_{k_2}), \ldots, \tau(x_{k_{p+q}}) \in S_1$. By Lemma 2.5 and its dual, either $\tau(\mathbf{v}_{n,2^h m}^{(1)}) = 0$ or removing all $\tau(x_k)$ such that $\tau(x_k) \in \langle E(S) \rangle$ does not change the value of $\tau(\mathbf{v}_{n,2^h m}^{(1)})$. If $\tau(\mathbf{v}_{n,2^h m}^{(1)}) = 0$, the claim holds. Otherwise, consider the substitution $\tau' \colon X_{p+q}^{(1)} \to S_1$ given by $\tau'(x_s) := \tau(x_{k_s})$ for all $s \in \{1, 2, \ldots, p + q\}$. Then $\tau(\mathbf{v}_{n,2^h m}^{(1)}) = \tau'(\mathbf{u}_{p,q,2^h m})$. By Lemma 3.1, the element $\tau'(\mathbf{u}_{p,q,2^h m})$ lies in a subgroup of the Brandt semigroup $(S_1, \cdot)$. Therefore, $\tau(\mathbf{v}_{n,2^h m}^{(1)})$ belongs to a subgroup of $(S, \cdot)$. $\square$

LEMMA 3.5. *Any $[m, k]$-group satisfies the identity $\mathbf{v}_{n,m}^{(k)} = 1$.*

PROOF. Let $\mathcal{G} = (G, \cdot)$ be an $[m, k]$-group and $a \in G$. Since a^m is the identity element of $\mathcal{G}$, we have $a^{2m-1} = a^{-1}$. Consider any substitution $\tau \colon X_{2n}^{(1)} \to G$ and let $a_i := \tau(x_i)$. Then

$$\tau(\mathbf{v}_{n,m}^{(1)}) = a_1 a_2 \cdots a_{2n} (a_n a_{n-1} \cdots a_1 \cdot a_{n+1} a_{n+2} \cdots a_{2n})^{-1} = a_1 a_2 \cdots a_n \cdot a_1^{-1} a_2^{-1} \cdots a_n^{-1}. \tag{3-7}$$

Recall that the *commutator* of elements a and b of a group is defined as $[a, b] := a^{-1}b^{-1}ab$. It is easy to verify that the right-hand side of Equation (3-7) can be written as a product of commutators, namely,

$$a_1 a_2 \cdots a_n \cdot a_1^{-1} a_2^{-1} \cdots a_n^{-1} = [a_1^{-1}, a_2^{-1}][(a_2 a_1)^{-1}, a_3^{-1}] \cdots [(a_{n-1}a_{n-2} \cdots a_1)^{-1}, a_n^{-1}]. \tag{3-8}$$

Therefore, $\tau(\mathbf{v}_{n,m}^{(1)})$ belongs to the derived subgroup $(G^{(1)}, \cdot)$ of $\mathcal{G}$. We use this as the induction basis and show by induction on h that any substitution $\theta \colon X_{2n}^{(h)} \to G$ sends the word $\mathbf{v}_{n,m}^{(h)}$ to the hth derived subgroup $(G^{(h)}, \cdot)$ of $\mathcal{G}$.

Indeed, let $h > 1$. Since for each $j \in \{1, 2, \ldots, 2n\}$, the word $\mathbf{v}_{n,m,j}^{(h-1)}$ is obtained from the word $\mathbf{v}_{n,m}^{(h-1)}$ by renaming its variables, $\theta(\mathbf{v}_{n,m,j}^{(h-1)}) \in G^{(h-1)}$ by the induction assumption. Combining Equations (3-3) and (3-7), we see that

$$\theta(\mathbf{v}_{n,m}^{(h)}) = \theta(\mathbf{v}_{n,m,1}^{(h-1)})\theta(\mathbf{v}_{n,m,2}^{(h-1)}) \cdots \theta(\mathbf{v}_{n,m,n}^{(h-1)}) \cdot (\theta(\mathbf{v}_{n,m,1}^{(h-1)}))^{-1}(\theta(\mathbf{v}_{n,m,2}^{(h-1)}))^{-1} \cdots (\theta(\mathbf{v}_{n,m,n}^{(h-1)}))^{-1}.$$

Now rewriting the last expression as in Equation (3-8), we see that $\theta(\mathbf{v}_{n,m}^{(h)})$ is a product of commutators of elements from $G^{(h-1)}$. Hence, $\theta(\mathbf{v}_{n,m}^{(h)}) \in G^{(h)}$. Since the group $\mathcal{G}$ is solvable of derived length at most k, its kth derived subgroup is trivial, whence the word $\mathbf{v}_{n,m}^{(k)}$ is sent to the identity element of G by any substitution $X_{2n}^{(k)} \to G$. This means that $\mathcal{G}$ satisfies the identity $\mathbf{v}_{n,m}^{(k)} = 1$. □

LEMMA 3.6. *Let $(S, \cdot)$ be an (h, m, k)-semigroup and Equation (2-1) its Brandt series. If $S_0 = \{0\}$ and $S = \langle E(S) \rangle \cup S_1$, then $(S, \cdot)$ satisfies the identity $\mathbf{v}_{n,2^h m}^{(k+1)} = (\mathbf{v}_{n,2^h m}^{(k+1)})^2$.*

PROOF. We have to verify that $\tau(\mathbf{v}_{n,2^k m}^{(k+1)}) \in E(S)$ for every substitution $\tau \colon X_{2n}^{(k+1)} \to S$. Recall from Remark 1 that the word $\mathbf{v}_{n,2^h m}^{(k+1)}$ is the image of the word $\mathbf{v}_{n,2^h m}^{(k)}$ under the substitution that sends every variable $x_{i_1 \ldots i_k} \in X_{2n}^{(k)}$ to the word $\mathbf{v}_{n,2^h m, i_1, \ldots, i_k}^{(1)}$ obtained from $\mathbf{v}_{n,2^h m}^{(1)}$ by renaming its variables. Hence, if all elements of the form $\tau(\mathbf{v}_{n,2^h m, i_1, \ldots, i_k}^{(1)})$ lie in $\langle E(S) \rangle$, then $\tau(\mathbf{v}_{n,2^h m}^{(k+1)}) \in E(S)$ by Lemma 3.3. So, we may assume that at least one element of the form $\tau(\mathbf{v}_{n,2^h m, i_1, \ldots, i_k}^{(1)})$ lies in $S_1 \setminus \langle E(S) \rangle$.

By the definition of an (h, m, k)-semigroup, $(S_1, \cdot)$ is either a zero semigroup or a Brandt semigroup over an $[m, k]$-group. If $(S_1, \cdot)$ is a zero semigroup, we have $\tau(\mathbf{v}_{n,2^k m}^{(k+1)}) = 0$ since S_1 is an ideal of $(S, \cdot)$ and each factor of the form $\mathbf{v}_{n,2^h m, i_1, \ldots, i_k}^{(1)}$ occurs in the word $\mathbf{v}_{n,2^k m}^{(k+1)}$ at least twice. If $(S_1, \cdot)$ is a Brandt semigroup, Lemma 2.5 and its dual imply that either $\tau(\mathbf{v}_{n,2^h m}^{(k+1)}) = 0$ or removing all factors $\tau(\mathbf{v}_{n,2^h m, i_1, \ldots, i_k}^{(1)})$ that lie in $\langle E(S) \rangle$ does not change the value of $\tau(\mathbf{v}_{n,2^h m}^{(k+1)})$. In the former case, the claim holds, and in the latter case, the remaining elements belong to subgroups of $(S_1, \cdot)$ by Lemma 3.4. If some of these elements belong to different maximal subgroups of $(S_1, \cdot)$,

then $\tau(\mathbf{v}_{n,2^h m}^{(k+1)}) = 0$ by the definition of multiplication in Brandt semigroups. Thus, it remains to consider only the situation when, for all $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, 2n\}$, all elements $\tau(\mathbf{v}_{n,2^h m,i_1,\ldots,i_k}^{(1)}) \in S_1 \setminus \langle E(S) \rangle$ belong to the same maximal subgroup $(G, \cdot)$ of $(S_1, \cdot)$.

Denote by e the identity element of $(G, \cdot)$ and define the substitution $\overline{\tau} : X_{2n}^{(k)} \to G$ by

$$\overline{\tau}(x_{i_1 \ldots i_k}) := \begin{cases} \tau(\mathbf{v}_{n,2^h m,i_1,\ldots,i_k}^{(1)}) & \text{if } \tau(\mathbf{v}_{n,2^h m,i_1,\ldots,i_k}^{(1)}) \text{ belongs to } G, \\ e & \text{otherwise,} \end{cases}$$

for each $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, 2n\}$. As we know that $\tau(\mathbf{v}_{n,2^h m,i_1,\ldots,i_k}^{(1)}) \in \langle E(S) \rangle \cup G$ for all $i_1, i_2 \ldots, i_k \in \{1, 2, \ldots, 2n\}$ and $fg = gf = g$ for all $g \in G$, $f \in E(S)$, we conclude that $\tau(\mathbf{v}_{n,2^h m}^{(k+1)}) = \overline{\tau}(\mathbf{v}_{n,2^h m}^{(k)})$. Since $(G, \cdot)$ is an $[m, k]$-group (and so a $[2^h m, k]$-group), it satisfies the identity $\mathbf{v}_{n,2^h m}^{(k)} = 1$ by Lemma 3.5. Hence, $\tau(\mathbf{v}_{n,2^k m}^{(k+1)}) = \overline{\tau}(\mathbf{v}_{n,2^h m}^{(k)}) = e$. Since the substitution τ is arbitrary, $(S, \cdot)$ satisfies the identity $\mathbf{v}_{n,2^h m}^{(k+1)} = (\mathbf{v}_{n,2^h m}^{(k+1)})^2$. □

PROPOSITION 3.7. *Let $(S, \cdot)$ be an (h, m, k)-semigroup with Brandt series in Equation (2-1) and $S_0 = \{0\}$. For any $n \geq 2$, $(S, \cdot)$ satisfies the identity*

$$\mathbf{v}_{n,2^h m}^{(kh+h)} = (\mathbf{v}_{n,2^h m}^{(kh+h)})^2. \tag{3-9}$$

PROOF. We induct on h. If $h = 1$, then the claim follows from Lemma 3.6. Let $h > 1$. The Rees quotient $(S/S_1, \cdot)$ is an $(h-1, m, k)$-semigroup whose Brandt series starts with the zero term. By the induction assumption, $(S/S_1, \cdot)$ satisfies the identity $\mathbf{v}_{n,2^{h-1} m}^{(kh-k+h-1)} = (\mathbf{v}_{n,2^{h-1} m}^{(kh-k+h-1)})^2$ for any $n \geq 2$. By Lemma 3.2, $(S/S_1, \cdot)$ satisfies the identity $\mathbf{v}_{n,2^h m}^{(kh-k+h-1)} = (\mathbf{v}_{n,2^h m}^{(kh-k+h-1)})^2$ as well. This readily implies that any substitution $X_{2n}^{(kh-k+h-1)} \to S$ sends the word $\mathbf{v}_{n,2^h m}^{(kh-k+h-1)}$ to either an idempotent in $S \setminus S_1$ or an element in S_1. Recall from Remark 1 that the word $\mathbf{v}_{n,2^h m}^{(kh+h)}$ is the image of the word $\mathbf{v}_{n,2^h m}^{(k+1)}$ under the substitution that sends every variable $x_{i_1 \ldots i_{k+1}} \in X_{2n}^{(k+1)}$ to the word $\mathbf{v}_{n,2^h m,i_1,\ldots,i_{k+1}}^{(kh-k+h-1)}$ obtained from $\mathbf{v}_{n,2^h m}^{(kh-k+h-1)}$ by renaming its variables. Therefore, for every substitution $\tau : X_{2n}^{(kh+h)} \to S$, all elements of the form $\tau(\mathbf{v}_{n,2^h m,i_1,\ldots,i_{k+1}}^{(kh-k+h-1)})$ lie in either $E(S)$ or S_1.

Now consider the substitution $\overline{\tau} : X_{2n}^{(k+1)} \to E(S) \cup S_1$ defined by

$$\overline{\tau}(x_{i_1 \ldots i_{k+1}}) := \tau(\mathbf{v}_{n,2^h m,i_1,\ldots,i_{k+1}}^{(kh-k+h-1)}) \quad \text{for each } i_1, i_2, \ldots, i_{k+1} \in \{1, 2, \ldots, 2n\}.$$

Clearly, $\tau(\mathbf{v}_{n,2^h m}^{(kh+h)}) = \overline{\tau}(\mathbf{v}_{n,2^h m}^{(k+1)})$. However, $(\langle E(S) \rangle \cup S_1, \cdot)$ is an (h, m, k)-semigroup satisfying the assumption of Lemma 3.6. By this lemma, the semigroup $(\langle E(S) \rangle \cup S_1, \cdot)$ satisfies the identity $\mathbf{v}_{n,2^h m}^{(k+1)} = (\mathbf{v}_{n,2^h m}^{(k+1)})^2$. This ensures that the element $\tau(\mathbf{v}_{n,2^h m}^{(kh+h)}) = \overline{\tau}(\mathbf{v}_{n,2^h m}^{(k+1)})$ is an idempotent. Since the substitution τ is arbitrary, $(S, \cdot)$ satisfies the identity in Equation (3-9). □

Finally, we remove the restriction $S_0 = \{0\}$.

PROPOSITION 3.8. *The identity* $\mathbf{v}_{n,2^hm}^{(kh+h+k)} = (\mathbf{v}_{n,2^hm}^{(kh+h+k)})^2$ *with* $n \geq 2$ *holds in each* (h, m, k)-*semigroup.*

PROOF. Let $(S, \cdot)$ be an (h, m, k)-semigroup with Brandt series in Equation (2-1). Consider the Rees quotient $(S/S_0, \cdot)$. This is an (h, m, k)-semigroup whose Brandt series starts with the zero term. By Proposition 3.7, the semigroup $(S/S_0, \cdot)$ satisfies Equation (3-9). Recall from Remark 1 that the word $\mathbf{v}_{n,2^hm}^{(kh+h+k)}$ is the image of the word $\mathbf{v}_{n,2^hm}^{(k)}$ under the substitution that sends every variable $x_{i_1 \ldots i_k} \in X_{2n}^{(k)}$ to the word $\mathbf{v}_{n,2^hm,i_1,i_2,\ldots,i_k}^{(hk+h)}$ obtained from $\mathbf{v}_{n,2^hm}^{(hk+h)}$ by renaming its variables. Then, for every substitution $\tau \colon X_{2n}^{(kh+h+k)} \to S$, the element $\tau(\mathbf{v}_{n,2^hm,i_1,\ldots,i_k}^{(kh+h)})$ is an idempotent of $(S/S_0, \cdot)$. Therefore, $\tau(\mathbf{v}_{n,2^hm,i_1,\ldots,i_k}^{(kh+h)})$ lies in either $E(S) \setminus S_0$ or S_0. Recall that by the definition of an (h, m, k)-semigroup, $(S_0, \cdot)$ is an $[m, k]$-group. Denote by e the identity element of this group. For each $f \in E(S)$, the product fe lies in S_0 because S_0 is an ideal in S. Then fe is an idempotent in S_0 by Lemma 2.4 which applies since $(S, \cdot)$ is a periodic block-group by Lemmas 3.2 and 2.8. Hence, $fe = e$ since a group has no idempotents except its identity element. Consequently, for every $g \in S_0$, we have $fg = feg = eg = g$. Dually, $gf = g$ for all $g \in S_0$, $f \in E(S)$. Now consider the substitution $\bar{\tau} \colon X_{2n}^{(k)} \to S_0$ defined by

$$\bar{\tau}(x_{i_1 \ldots i_k}) := \begin{cases} \tau(\mathbf{v}_{n,2^hm,i_1,\ldots,i_k}^{(kh+h)}) & \text{if } \tau(\mathbf{v}_{n,m,i_1,\ldots,i_k}^{(kh+h)}) \text{ belongs to } S_0, \\ e & \text{otherwise,} \end{cases}$$

for each $i_1, i_2, \ldots, i_k \in \{1, 2, \ldots, 2n\}$. As we know that $\tau(\mathbf{v}_{n,2^hm,i_1,\ldots,i_k}^{(kh+h)}) \in E(S) \cup S_0$ for all $i_1, i_2 \ldots, i_k \in \{1, 2, \ldots, 2n\}$ and $fg = gf = g$ for all $g \in S_0$, $f \in E(S)$, we conclude that $\tau(\mathbf{v}_{n,2^hm}^{(kh+h+k)}) = \bar{\tau}(\mathbf{v}_{n,2^hm}^{(k)})$. Since $(S_0, \cdot)$ is an $[m, k]$-group (and so a $[2^hm, k]$-group), it satisfies the identity $\mathbf{v}_{n,2^hm}^{(k)} = 1$ by Lemma 3.5. Hence, $\tau(\mathbf{v}_{n,2^hm}^{(kh+h+k)}) = \bar{\tau}(\mathbf{v}_{n,2^hm}^{(k)}) = e$. Since the substitution τ is arbitrary, $(S, \cdot)$ satisfies the identity $\mathbf{v}_{n,2^hm}^{(kh+h+k)} = (\mathbf{v}_{n,2^hm}^{(kh+h+k)})^2$. □

Now we are ready to complete the mission of this section.

PROPOSITION 3.9. *For each finite block-group* $(S, \cdot)$ *with solvable subgroups, there exist positive integers q and r such that $(S, \cdot)$ satisfies the identities* $\mathbf{v}_{n,q}^{(r)} = (\mathbf{v}_{n,q}^{(r)})^2$ *for all* $n \geq 2$.

PROOF. Clearly, each finite semigroup possesses a principal series. By Corollary 2.7, every principal series of a block-group is a Brandt series. Let h be the height of a Brandt series of $(S, \cdot)$, let m be the least common multiple of the exponents of subgroups of $(S, \cdot)$, and let k be the maximum of the derived lengths of these subgroups. Then $(S, \cdot)$ is an (h, m, k)-semigroup. Now Proposition 3.8 applies, showing that $(S, \cdot)$ satisfies all identities $\mathbf{v}_{n,2^hm}^{(kh+h+k)} = (\mathbf{v}_{n,2^hm}^{(kh+h+k)})^2$ with $n \geq 2$. Hence, one can choose $q = 2^hm$ and $r = kh + k + h$. □

Proposition 3.9 gives a vast generalization of [11, Proposition 2.4] where a similar result was established for finite inverse semigroups with abelian subgroups.

4. Proofs of Theorems 1.1 and 1.2

Recall that the 6-*element Brandt monoid* $(B_2^1, \cdot)$ is formed by the following zero–one 2×2-matrices

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{4-1}$$

under the usual matrix multiplication $\cdot$. In terms of the construction for Brandt semigroups presented in Section 2, $(B_2^1, \cdot)$ is obtained by adjoining the identity element to the Brandt semigroup over the trivial group with the 2-element index set. It is known and easy to verify that the set B_2^1 admits a unique addition $+$ such that $\mathcal{B}_2^1 := (B_2^1, +, \cdot)$ becomes an ai-semiring. The addition is nothing but the Hadamard (entry-wise) product of matrices:

$$(a_{ij}) + (b_{ij}) := (a_{ij} b_{ij}).$$

The identities of the semiring $\mathcal{B}_2^1$ were studied by the second author [31] and, independently, by Jackson *et al.* [14]; it was proved that these identities admit no finite basis. Moreover, in [11], we proved that this property of $\mathcal{B}_2^1$ is very contagious: if all identities of an ai-semiring hold in $\mathcal{B}_2^1$, then under some rather mild conditions, the identities have no finite basis. Here is the key result of [11] stated in the notation adopted here.

THEOREM 4.1 [11, Theorem 4.2]. *Let S be an ai-semiring whose multiplicative reduct satisfies the identities $\mathbf{v}_{n,q}^{(r)} = (\mathbf{v}_{n,q}^{(r)})^2$ for all $n \geq 2$ and some $q, r \geq 1$. If all identities of S hold in the ai-semiring $\mathcal{B}_2^1$, then the identities admit no finite basis.*

In [11], Theorem 4.1 was applied to finite ai-semirings whose multiplicative reducts were inverse semigroups with abelian subgroups. Due to Proposition 3.9, we are in a position to enlarge its application range as follows.

THEOREM 4.2. *Let $S = (S, +, \cdot)$ be a finite ai-semiring whose multiplicative reduct is a block-group with solvable subgroups. If all identities of S hold in the ai-semiring $\mathcal{B}_2^1$, then the identities admit no finite basis.*

PROOF. Proposition 3.9 implies that the semigroup $(S, \cdot)$ satisfies the identities $\mathbf{v}_{n,q}^{(r)} = (\mathbf{v}_{n,q}^{(r)})^2$ for all $n \geq 2$ and some $q, r \geq 1$, and therefore, Theorem 4.1 applies. □

We are ready to deduce Theorems 1.1 and 1.2.

PROOF OF THEOREM 1.1. We aim to prove that for any finite nonabelian solvable group $\mathcal{G} = (G, \cdot)$, the identities of the power group $(\mathcal{P}(G), \cup, \cdot)$ admit no finite basis. It is shown in [24, Proposition 2.4], see also [1, Proposition 11.1.2], that the semigroup $(\mathcal{P}(G), \cdot)$ is a block-group and all maximal subgroups of $(\mathcal{P}(G), \cdot)$ are of the form

$(N_G(H)/H, \cdot)$, where $(H, \cdot)$ is a subgroup of $\mathcal{G}$ and $N_G(H) := \{g \in G \mid gH = Hg\}$ is the normalizer of $(H, \cdot)$ in $\mathcal{G}$. Hence, each subgroup of $(\mathcal{P}(G), \cdot)$ embeds into a quotient of a subgroup of $\mathcal{G}$ and so it is solvable. We see that the multiplicative reduct of $(\mathcal{P}(G), \cup, \cdot)$ is a block-group with solvable subgroups.

First, suppose that $\mathcal{G}$ is not a Dedekind group, that is, some subgroup $(H, \cdot)$ is not normal in $\mathcal{G}$. Then, of course, $1 < |H| < |G|$ and one can find an element $g \in G$ with $g^{-1}Hg \neq H$. Denote by E the singleton subgroup of $\mathcal{G}$, let $J := \{A \subseteq G \mid |A| > |H|\}$, and consider the following subset of $\mathcal{P}(G)$:

$$B := \{E, H, g^{-1}H, Hg, g^{-1}Hg\} \cup J. \tag{4-2}$$

Observe that $g^{-1}H \neq Hg$: indeed $g^{-1}H \cdot Hg = g^{-1}Hg$ while $Hg \cdot g^{-1}H = H$, so that the assumption $g^{-1}H = Hg$ forces the equality $g^{-1}Hg = H$ which contradicts the choice of g. It is easy to verify that B is closed under union and element-wise multiplication of subsets so that $(B, \cup, \cdot)$ is a subsemiring in $(\mathcal{P}(G), \cup, \cdot)$. Define a map $B \to \mathcal{B}_2^1$ via the following rule:

$$
\begin{array}{cccccc}
A \in J & E & Hg & g^{-1}H & H & g^{-1}Hg \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} &
\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &
\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} &
\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} &
\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} &
\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} .
\end{array} \tag{4-3}
$$

It can be routinely verified that this map is a homomorphism from the subsemiring $(B, \cup, \cdot)$ onto the ai-semiring $\mathcal{B}_2^1$. Since $\mathcal{B}_2^1$ is the homomorphic image of a subsemiring in $(\mathcal{P}(G), \cup, \cdot)$, all identities of $(\mathcal{P}(G), \cup, \cdot)$ hold in $\mathcal{B}_2^1$. Thus, Theorem 4.2 applies to $(\mathcal{P}(G), \cup, \cdot)$, showing that its identities admit no finite basis.

If $\mathcal{G}$ is a Dedekind group, then since $\mathcal{G}$ is nonabelian, it has a subgroup isomorphic to the 8-element quaternion group; see [12, Theorem 12.5.4]. This subgroup is isomorphic to a subgroup in $(\mathcal{P}(G), \cdot)$, and by [14, Theorem 6.1], the identities of every ai-semiring whose multiplicative reduct possesses a nonabelian nilpotent subgroup admit no finite basis. We see that $(\mathcal{P}(G), \cup, \cdot)$ has no finite identity basis in this case as well. □

REMARK 2. Given a semigroup $(S, \cdot)$, one sometimes considers, along with the power semigroup $(\mathcal{P}(S), \cdot)$, its subsemigroup $(\mathcal{P}'(S), \cdot)$, where $\mathcal{P}'(S)$ is the set of all *nonempty* subsets of S; see, for example, [1, Ch. 11]. Clearly, the empty set serves as a zero in power semigroups so that one can think of $(\mathcal{P}(S), \cdot)$ as the result of adjoining a new zero to $(\mathcal{P}'(S), \cdot)$. It is well known that the property of a semigroup to have or not to have a finite identity basis does not change when a new zero is adjoined; see [30, Section 3]. Therefore, $(\mathcal{P}(S), \cdot)$ and $(\mathcal{P}'(S), \cdot)$ admit or do not admit a finite identity basis simultaneously.

Since the set $\mathcal{P}'(S)$ is closed under unions, one can consider the semiring $(\mathcal{P}'(S), \cup, \cdot)$. The power semiring $(\mathcal{P}(S), \cup, \cdot)$ can be thought of as the result of adjoining a new element, which is both an additive identity and multiplicative zero, to $(\mathcal{P}'(S), \cup, \cdot)$. However, it is not yet known whether adjoining such an element preserves

the property of having/not having a finite identity basis. Nevertheless, the above proof of Theorem 1.1 applies without a hitch to ai-semirings of the form $(\mathcal{P}'(G), \cup, \cdot)$, where $(G, \cdot)$ is any finite nonabelian solvable group and shows that the identities of every such ai-semiring admit no finite basis.

REMARK 3. It is quite natural to consider $(\mathcal{P}(S), \cup, \cdot, \varnothing)$ as an algebra with an extra nullary operation of taking the constant $\varnothing$; this was actually the setting adopted by Dolinka [6]. One can verify that the conclusion of Theorem 1.1 persists in this case as well. The 'non-Dedekind' part of the proof of Theorem 1.1 invokes our results from [11] via Theorem 4.2. These results continue to work for ai-semirings with multiplicative zero treated as a constant; this is explicitly registered in [11, Remark 3]. In the part of the proof that deals with Dedekind groups, one should refer to [14, Theorem 7.6] which transfers the result of [14, Theorem 6.1] to semirings with multiplicative zero treated as a constant.

PROOF OF THEOREM 1.2. The theorem claims that the identities of the semiring $(H(X), \cup, \cdot)$ of all Hall relations on a finite set X admit a finite basis if and only if $|X| = 1$. The 'if' part is obvious, since if $|X| = 1$, then $|H(X)| = 1$, and the identities of the trivial semiring have a basis consisting of the single identity $x = y$.

For the 'only if' part, assume that $X = X_n := \{1, 2, \ldots, n\}$ and $n \geq 2$. The semigroup $(H(X_n), \cdot)$ is a block-group; see, for example, [10, Proposition 2]. It can be easily verified that the ai-semiring $\mathcal{B}_2^1$ embeds into $(H(X_2), \cup, \cdot)$ via the following map:

$$
\begin{array}{cccccc}
\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} & \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}
\end{array} .
$$

The matrices in the bottom row are matrices over the Boolean semiring $\mathbb{B} := (\{0, 1\}, +, \cdot)$ with $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0 + 0 = 0$, $1 \cdot 1 = 1 + 0 = 0 + 1 = 1 + 1 = 1$, and we mean the standard representation of binary relations as matrices over the Boolean semiring (in which Hall relations correspond to matrices with permanent 1). Obviously, the ai-semiring $(H(X_2), \cup, \cdot)$ embeds into $(H(X_n), \cup, \cdot)$ for each $n \geq 2$, whence so does $\mathcal{B}_2^1$. Therefore, all identities of $(H(X_n), \cup, \cdot)$ hold in $\mathcal{B}_2^1$.

Let Sym_n stand for the group of all permutations of the set X_n. It is known that all subgroups of the semigroup of all binary relations on X_n embed into Sym_n; see, for example, [23, Theorem 3.5]. In particular, all subgroups of the semigroup $(H(X_n), \cdot)$ with $n \leq 4$ embed into Sym_4, and hence, are solvable. We see that Theorem 4.2 applies to the ai-semiring $(H(X_n), \cup, \cdot)$ with $n = 2, 3, 4$, whence the identities of the ai-semiring admit no finite basis.

To cover the case $n > 4$, observe that the semigroup $(H(X_n), \cdot)$ has Sym_n as its group of units, and for $n > 4$ (even for $n \geq 4$), this group possesses nonabelian nilpotent subgroups, for instance, the 8-element dihedral group. By [14, Theorem 6.1], the ai-semiring $(H(X_n), \cup, \cdot)$ has no finite identity basis in this case as well.   □

In the introduction, we mentioned Dolinka's problem [6, Problem 6.5] as the main motivation of our study. Recall that the problem asks for a description of finite groups whose power groups have no finite identity basis. Combining Theorem 1.1 of the present paper and [14, Theorem 6.1] reduces the problem to two special cases.

First, the problem remains open for nonsolvable groups whose nilpotent subgroups are abelian. The structure of such groups is well understood, see [4]; an interesting example here is the sporadic simple group of order 175 560 found by Janko [15]. While the arguments in the proof of Theorem 1.1 do not cover this case, we conjecture that the conclusion of the theorem persists. In other words, we believe that the power group of any finite nonabelian group has no finite identity basis.

Second, the problem is open for the majority of abelian groups. This may seem surprising as power groups of abelian groups have commutative multiplication, but finite ai-semirings with commutative multiplication and without finite identity basis are known to exist, see [14, Corollary 4.11]. This does not exclude, of course, that all power groups of finite abelian groups admit a finite identity basis, but to the best of our knowledge, the only group for which such a basis is known is the 2-element group. Namely, Ren and Zhao [29] have shown that the identities $xy = yx$ and $x = x^3$ form a basis for identities of a 4-element ai-semiring that can be easily identified with the power group of the 2-element group.

5. Proof of Theorem 1.3

Recall that in an inverse semigroup $(S, \cdot)$, every element has a unique inverse; the inverse of $a \in S$ is denoted a^{-1}. This defines a unary operation on S, and it is well known (and easy to verify) that $(S, \cdot, {}^{-1})$ is an involution semigroup. In particular, the 6-element Brandt monoid can be considered as an involution semigroup. (Observe that in terms of the matrix representation in Equation (4-1), the involution of $(B_2^1, \cdot, {}^{-1})$ is just the usual matrix transposition.)

We need the following result that translates Theorem 4.1 into the language of involution semigroups. Its proof is parallel to that of [11, Theorem 4.2].

THEOREM 5.1. *Let* $\mathcal{S} = (S, \cdot, {}^*)$ *be an involution semigroup whose multiplicative reduct satisfies the identities* $\mathbf{v}_{n,q}^{(r)} = (\mathbf{v}_{n,q}^{(r)})^2$ *for all* $n \geq 2$ *and some* $q, r \geq 1$. *If all identities of* $\mathcal{S}$ *hold in the involution semigroup* $(B_2^1, \cdot, {}^{-1})$, *then the identities admit no finite basis.*

PROOF. As in the proof of [11, Theorem 4.2], we employ a family of inverse semi-groups constructed by Kad'ourek in [18, Section 2]. First, for all $n, h \geq 1$, define terms $\mathbf{w}_n^{(h)}$ of the signature $(\cdot, {}^{-1})$ over the alphabet $X_n^{(h)} = \{x_{i_1 i_2 \cdots i_h} \mid i_1, i_2, \ldots, i_h \in \{1, 2, \ldots, n\}\}$ by induction on h. Put

$$\mathbf{w}_n^{(1)} := x_1 x_2 \cdots x_n x_1^{-1} x_2^{-1} \cdots x_n^{-1}.$$

Then, assuming that, for any $h > 1$, the unary term $\mathbf{w}_n^{(h-1)}$ over the alphabet $X_n^{(h-1)}$ has already been defined, we create n copies of this term over the alphabet $X_n^{(h)}$ as follows.
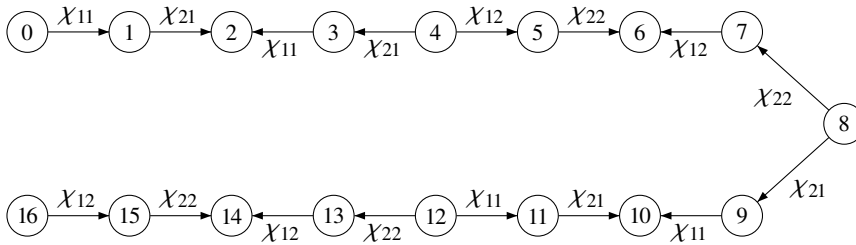
FIGURE 1. The generators of the inverse semigroup $(S_2^{(2)}, \cdot, ^{-1})$.

For every $j \in \{1, 2, \ldots, n\}$, we put

$$\mathbf{w}_{n,j}^{(h-1)} := \sigma_{n,j}^{(h)}(\mathbf{w}_n^{(h-1)}),$$

where the substitution $\sigma_{n,j}^{(h)} : X_n^{(h-1)} \to X_n^{(h)}$ appends j to the indices of its arguments, that is,

$$\sigma_{n,j}^{(h)}(x_{i_1 i_2 \ldots i_{h-1}}) := x_{i_1 i_2 \ldots i_{h-1} j} \quad \text{for all } i_1, i_2, \ldots, i_{h-1} \in \{1, 2, \ldots, n\}.$$

Then we put

$$\mathbf{w}_n^{(h)} := \mathbf{w}_{n,1}^{(h-1)} \mathbf{w}_{n,2}^{(h-1)} \cdots \mathbf{w}_{n,n}^{(h-1)} (\mathbf{w}_{n,1}^{(h-1)})^{-1} (\mathbf{w}_{n,2}^{(h-1)})^{-1} \cdots (\mathbf{w}_{n,n}^{(h-1)})^{-1}.$$

Now, for any $n \geq 2$ and $h \geq 1$, let $(S_n^{(h)}, \cdot, ^{-1})$ stand for the inverse semigroup of partial one-to-one transformations on the set $\{0, 1, \ldots, 2^h n^h\}$ generated by n^h transformations $\chi_{i_1 i_2 \ldots i_h}$ with arbitrary indices $i_1, i_2, \ldots, i_h \in \{1, 2, \ldots, n\}$ defined as follows:

- $\chi_{i_1 i_2 \ldots i_h}(p - 1) = p$ if and only if in the term $\mathbf{w}_n^{(h)}$, the element in the p th position from the left is $x_{i_1 i_2 \ldots i_h}$;
- $\chi_{i_1 i_2 \ldots i_h}(p) = p - 1$ if and only if in the term $\mathbf{w}_n^{(h)}$, the element in the p th position from the left is $x_{i_1 i_2 \ldots i_h}^{-1}$.

We borrow the following illustrative example from [11]. Let $n = 2$, $h = 2$; then

$$\mathbf{w}_2^{(2)} = \underbrace{x_{11} x_{21} x_{11}^{-1} x_{21}^{-1}}_{\mathbf{w}_{2,1}^{(1)}} \underbrace{x_{12} x_{22} x_{12}^{-1} x_{22}^{-1}}_{\mathbf{w}_{2,2}^{(1)}} \underbrace{x_{21} x_{11} x_{21}^{-1} x_{11}^{-1}}_{(\mathbf{w}_{2,1}^{(1)})^{-1}} \underbrace{x_{22} x_{12} x_{22}^{-1} x_{12}^{-1}}_{(\mathbf{w}_{2,2}^{(1)})^{-1}},$$

and the generators of the inverse semigroup $(S_2^{(2)}, \cdot, ^{-1})$ act as shown in Figure 1.

We need two properties of the inverse semigroups $(S_n^{(h)}, \cdot, ^{-1})$.

(A) [18, Corollary 3.2] For each $n \geq 2$ and $h \geq 1$, any inverse subsemigroup of $(S_n^{(h)}, \cdot, ^{-1})$ generated by less than n elements satisfies all identities of the involution semigroup $(B_2^1, \cdot, ^{-1})$.

(B) [11, Proposition 3.3] For each $n \geq 2$ and $h \geq 1$ and any $m \geq 1$, the semigroup $(S_n^{(h)}, \cdot)$ violates the identity $\mathbf{v}_{n,m}^{(h)} = (\mathbf{v}_{n,m}^{(h)})^2$.

Now, arguing by contradiction, assume that for some k, the involution semigroup S has an identity basis Σ such that each identity in Σ involves less than k variables. Fix an arbitrary identity $\mathbf{u} = \mathbf{v}$ in Σ and let $x_1, x_2, \ldots, x_\ell$ be all variables that occur in $\mathbf{u}$ or $\mathbf{v}$. Consider an arbitrary substitution $\tau \colon \{x_1, x_2, \ldots, x_\ell\} \to S_k^{(r)}$ and let $(T, \cdot, ^{-1})$ be the inverse subsemigroup of $(S_k^{(r)}, \cdot, ^{-1})$ generated by the elements $\tau(x_1), \tau(x_2), \ldots, \tau(x_\ell)$. Since $\ell < k$, property (A) implies that $(T, \cdot, ^{-1})$ satisfies all identities of the involution semigroup $(B_2^1, \cdot, ^{-1})$. Since by the condition of the theorem, $(B_2^1, \cdot, ^{-1})$ satisfies all identities of S, the identity $\mathbf{u} = \mathbf{v}$ holds in $(B_2^1, \cdot, ^{-1})$. Hence, the identity $\mathbf{u} = \mathbf{v}$ holds also in the involution semigroup $(T, \cdot, ^{-1})$, and so $\mathbf{u}$ and $\mathbf{v}$ take the same value under every substitution of elements of T for the variables $x_1, \ldots, x_\ell$. In particular, $\tau(\mathbf{u}) = \tau(\mathbf{v})$. Since the substitution τ is arbitrary, the identity $\mathbf{u} = \mathbf{v}$ holds in the involution semigroup $(S_k^{(r)}, \cdot, ^{-1})$. Since $\mathbf{u} = \mathbf{v}$ is an arbitrary identity from the identity basis Σ of S, we see that $(S_k^{(r)}, \cdot, ^{-1})$ satisfies all identities of S. In particular, the multiplicative reduct $(S_k^{(r)}, \cdot)$ satisfies all identities of the multiplicative reduct $(S, \cdot)$ of S. By the condition of the theorem, $(S, \cdot)$ satisfies the identity $\mathbf{v}_{k,q}^{(r)} = (\mathbf{v}_{k,q}^{(r)})^2$. However, property (B) shows that this identity fails in $(S_k^{(r)}, \cdot)$, which is a contradiction. □

Now, we deduce Theorem 1.3 from Theorem 5.1, applying exactly the same construction that was used in the 'non-Dedekind' part of the proof of Theorem 1.1.

PROOF OF THEOREM 1.3. We aim to prove that for any finite non-Dedekind solvable group $\mathcal{G} = (G, \cdot)$, the identities of the involution semigroup $(\mathcal{P}(G), \cdot, ^{-1})$ admit no finite basis. As observed in the first paragraph of the proof of Theorem 1.1, the multiplicative reduct $(\mathcal{P}(G), \cdot)$ is a block-group with solvable subgroups. By Proposition 3.9, the reduct satisfies the identities $\mathbf{v}_{n,q}^{(r)} = (\mathbf{v}_{n,q}^{(r)})^2$ for all $n \geq 2$ and some $q, r \geq 1$.

As the group $(G, \cdot)$ is not Dedekind, one can choose a subgroup $(H, \cdot)$ of $\mathcal{G}$ and an element $g \in G$ such that $g^{-1}Hg \neq H$. Consider the subset B of $\mathcal{P}(G)$ defined by Equation (4-2). Applying the element-wise inversion to the elements of B, we see that

$$E^{-1} = E, \ H^{-1} = H, \ (g^{-1}H)^{-1} = Hg, \ (Hg)^{-1} = g^{-1}H, \ (g^{-1}Hg)^{-1} = g^{-1}Hg,$$

and $A^{-1} \in J$ for all $A \in J$. Hence, $(B, \cdot, ^{-1})$ is an involution subsemigroup of $(\mathcal{P}(G), \cdot, ^{-1})$ and the map in Equation (4-3) is a homomorphism of this involution subsemigroup onto $(B_2^1, \cdot, ^{-1})$. Hence, all identities of $(\mathcal{P}(G), \cdot, ^{-1})$ hold in the involution semigroup $(B_2^1, \cdot, ^{-1})$. Now Theorem 5.1 applies to $(\mathcal{P}(G), \cdot, ^{-1})$ and shows that its identities have no finite basis. □

REMARK 4. The analogy between Theorems 1.1 and 1.3 is not complete since the latter theorem does not cover finite groups that are Dedekind but nonabelian. In particular, we do not know whether the involution power semigroup of the 8-element quaternion group admits a finite identity basis.

REMARK 5. The semigroup of all binary relations on a set X has a useful involution: for each $\rho \subseteq X \times X$, one sets $\rho^{-1} := \{(y, x) \mid (x, y) \in \rho\}$. The set $H(X)$ of all Hall relations on X is closed under this involution so that one can consider the involution semigroup $(H(X), \cdot, ^{-1})$. The reader might wonder if a result related to Theorem 1.2 as Theorem 1.3 relates to Theorem 1.1 holds, and if it does, why it is missing from this paper. In fact, the exact analog of Theorem 1.2 does hold: the identities of the involution semigroup of all Hall relations on a finite set X admit a finite basis if and only if $|X| = 1$. This follows from [2, Remark 3.6] which establishes a stronger fact that we briefly describe now.

Recall that an involution semigroup is said to be *weakly finitely based* if it fulfills a finite set Σ of identities such that every finitely generated involution semigroup that satisfies Σ is finite. An involution semigroup that is not weakly finitely based is called *inherently nonfinitely based*. In [2, Remark 3.6], it is shown that the involution semigroup $(H(X), \cdot, ^{-1})$ with $|X| > 1$ is inherently nonfinitely based. This property is known to be much stronger than the absence of a finite identity basis and it cannot be achieved via the approach of the present paper.

In contrast, Dolinka [8, Theorem 6] has proved that for every finite group $(G, \cdot)$, the involution semigroup $(\mathcal{P}(G), \cdot, ^{-1})$ is weakly finitely based. This means that the finite basis problem for involution power semigroups of groups is out of the range of methods developed in [2, 7], and therefore, this justifies including Theorem 1.3.

REMARK 6. An *involution ai-semiring* is an algebra $(S, +, \cdot, ^*)$ such that $(S, +, \cdot)$ is an ai-semiring, $(S, \cdot, ^*)$ is an involution semigroup and, in addition to that, the law

$$(x + y)^* = x^* + y^*$$

holds. It is easy to see that $(\mathcal{P}(G), \cup, \cdot, ^{-1})$ is an involution ai-semiring for any group $\mathcal{G} = (G, \cdot)$. The above proofs of Theorems 1.1 and 1.3 can be fused to show that this involution ai-semiring has no finite identity basis whenever the group $\mathcal{G}$ is finite, solvable, and non-Dedekind.

References

[1] J. Almeida, *Finite Semigroups and Universal Algebra*, Series in Algebra, 3 (World Scientific, Singapore, 1995).
[2] K. Auinger, I. Dolinka and M. V. Volkov, 'Matrix identities involving multiplication and transposition', *J. Eur. Math. Soc. (JEMS)* **14** (2012), 937–969.
[3] K. Auinger, I. Dolinka and M. V. Volkov, 'Equational theories of semigroups with involution', *J. Algebra* **369** (2012), 203–225.
[4] A. M. Broshi, 'Finite groups whose Sylow subgroups are abelian', *J. Algebra* **17** (1971), 74–82.
[5] A. H. Clifford and G. B. Preston, *The Algebraic Theory of Semigroups*, Vol. I, Mathematical Surveys and Monographs, 7(I) (American Mathematical Society, Providence, RI, 1961).
[6] I. Dolinka, 'A class of inherently nonfinitely based semirings', *Algebra Universalis* **60** (2009), 19–35.
[7] I. Dolinka, 'On identities of finite involution semigroups', *Semigroup Forum* **80** (2010), 105–120.
[8] I. Dolinka, 'Power semigroups of finite groups and the INFB property', *Algebra Universalis* **63** (2010), 239–242.

[9]   D. G. FitzGerald, 'On inverses of products of idempotents in regular semigroups', *J. Aust. Math. Soc.* **13** (1972), 335–337.

[10] A. M. Gaysin and M. V. Volkov, 'Block-groups and Hall relations', in: *Semigroups, Categories, and Partial Algebras*, Springer Proceedings in Mathematics and Statistics, 345 (eds. P. G. Romeo, M. V. Volkov and A. R. Rajan) (Springer, Singapore, 2021), 25–32.

[11] S. V. Gusev and M. V. Volkov, 'Semiring identities of finite inverse semigroups', *Semigroup Forum* (to appear), see also Preprint, 2022, arXiv:2204.10514v2.

[12] M. Hall Jr, *The Theory of Groups* (Macmillan, New York, 1959).

[13] J. M. Howie, *Fundamentals of Semigroup Theory* (Clarendon Press, Oxford, 1995).

[14] M. Jackson, M. Ren and X. Zhao, 'Nonfinitely based ai-semirings with finitely based semigroup reducts', *J. Algebra* **611** (2022), 211–245.

[15] Z. Janko, 'A new finite simple group with abelian Sylow 2-subgroups and its characterization', *J. Algebra* **3** (1966), 147–186.

[16] J. Ježek, T. Kepka and M. Maróti, 'The endomorphism semiring of a semilattice', *Semigroup Forum* **78** (2009), 21–26.

[17] P. Jipsen, 'Relation algebras, idempotent semirings and generalized bunched implication algebras', in: *Relational and Algebraic Methods in Computer Science*, Lecture Notes in Computer Science, 10226 (eds. P. Höfner, D. Pous and G. Struth) (Springer, Cham, 2017), 144–158.

[18] J. Kad'ourek, 'On bases of identities of finite inverse semigroups with solvable subgroups', *Semigroup Forum* **67** (2003), 317–343.

[19] E. W. H. Lee, 'Equational theories of unstable involution semigroups,' *Electron. Res. Announc. Math. Sci.* **24** (2017), 10–20.

[20] S. W. Margolis and J.-É. Pin, 'Varieties of finite monoids and topology for the free monoid', in: *Proceedings of the 1984 Marquette Conference on Semigroups* (eds. K. Byleen, P. Jones and F. Pastijn) (Marquette University, Milwaukee, 1985), 113–129.

[21] E. M. Mogiljanskaja, 'The solution to a problem of Tamura', in: *Modern Analysis and Geometry* (eds. I. Ya. Bakelman *et al.*) (Leningrad. Gos. Ped. Inst., Leningrad, 1972), 148–151 (in Russian).

[22] E. M. Mogiljanskaja, 'Non-isomorphic semigroups with isomorphic semigroups of subsets', *Semigroup Forum* **6** (1973), 330–333.

[23] J. S. Montague and R. J. Plemmons, 'Maximal subgroups of the semigroup of relations', *J. Algebra* **13** (1969), 575–587.

[24] J.-É. Pin, 'Variétés de langages et monoïde des parties', *Semigroup Forum* **20** (1980), 11–47 (in French).

[25] J.-É. Pin, 'BG = PG, a success story', in: *Semigroups, Formal Languages and Groups*, Nato Science Series C, 466 (ed. J. Fountain) (Kluwer Academic Publishers, Dordrecht–Boston–London, 1995), 33–47.

[26] J.-É. Pin, 'Tropical semirings', in: *Idempotency*, Publications of the Newton Institute, 11 (ed. J. Gunawardena) (Cambridge University Press, Cambridge, 1998), 50–69.

[27] L. Polák, 'Syntactic semiring of a language', in: *Mathematical Foundations of Computer Science 2001*, Lecture Notes in Computer Science, 2136 (eds. J. Sgall, A. Pultr and P. Kolman) (Springer, Berlin–Heidelberg, 2001), 611–620.

[28] L. Polák, 'Syntactic semiring and universal automaton', In: *Developments in Language Theory 2003*, Lecture Notes in Computer Science, 2710 (eds. Z. Ésik and Z. Fülöp) (Springer, Berlin–Heidelberg, 2003), 411–422.

[29] M. Ren and X. Zhao, 'The varieties of semilattice-ordered semigroups satisfying $x^3 \approx x$ and $xy \approx yx$', *Period. Math. Hungar.* **72** (2016), 158–170.

[30] M. V. Volkov, 'The finite basis problem for finite semigroups', *Sci. Math. Jpn.* **53** (2001), 171–199, a periodically updated version is available under http://csseminar.math.ru/MATHJAP_revisited.pdf.

[31] M. V. Volkov, 'Semiring identities of the Brandt monoid', *Algebra Universalis* **82** (2021), Article no. 42.

SERGEY V. GUSEV, Institute of Natural Sciences and Mathematics,
Ural Federal University, 620000 Ekaterinburg, Russia
e-mail: sergey.gusb@gmail.com

MIKHAIL V. VOLKOV, Institute of Natural Sciences and Mathematics,
Ural Federal University, 620000 Ekaterinburg, Russia
e-mail: m.v.volkov@urfu.ru