Publ. Math. Debrecen
93/1-2 (2018), 73–86
DOI: 10.5486/PMD.2018.8022

On a semiring variety satisfying $x^n \approx x$

By AIFA WANG (Xi'an) and YONG SHAO (Xi'an)

Abstract. In this paper, we study the semiring variety determined by the additional identities $x^n \approx x$ and $x + (2^n - 2)xyx \approx x$. We give a decomposition theorem of semirings in this variety. Moreover, we characterize all subdirectly irreducible rings in this variety, and show that each subvariety of this variety is finitely based. This generalizes and extends the results of [1], [6], [7], [9], [13], [17] and [19].

1. Introduction and preliminaries

By a *semiring* we mean an algebra $(S, +, \cdot)$ such that

- $(S, +)$ is a commutative semigroup;
- $(S, \cdot)$ is a semigroup;
- the distributive laws $x(y + z) \approx xy + xz$ and $(y + z)x \approx yx + zx$ hold in S.

A semiring S is called *multiplicatively idempotent* (resp., *additively idempotent*) if the identity $x \cdot x \approx x$ (resp., $x + x \approx x$) holds in S. A semiring S is said to be *idempotent* if it is both multiplicatively idempotent and additively idempotent. We say that a semiring S is commutative if the identity $xy \approx yx$ holds in S.

A *variety* of algebras is a class of algebras of the same type that is closed under the formation of subalgebras, homomorphic images and direct products. It is well known (Birkhoff's theorem) that a class of algebras of the same type

Mathematics Subject Classification: 08B15, 16Y60, 20M07.
Key words and phrases: semiring, variety, identity, finitely based.
This paper is supported by Grants of Natural Science Foundation of China (11571278, 11701449), and a Grant of Scientific and Technological Research Program of Chongqing Municipal Education Commission (KJ1600930).
The second author is the corresponding author.

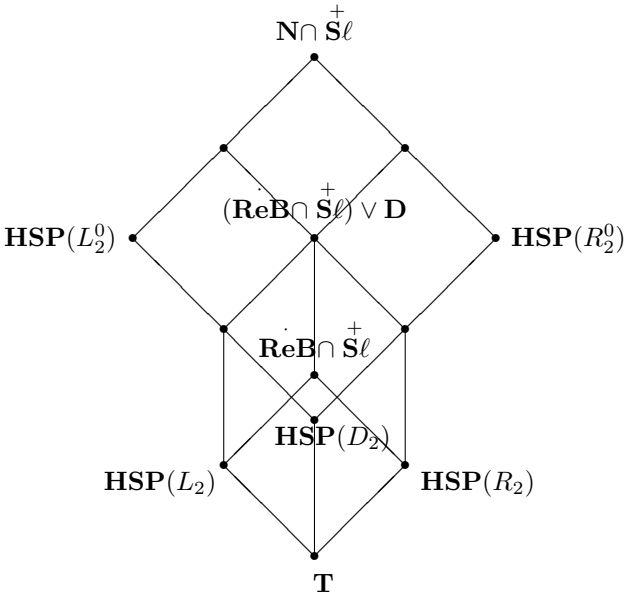
is a variety if and only if it is an equational class. Let $\mathbf{V}$ be a variety, and X a fixed countably infinite set of variables. We denote by $\mathrm{Id}_{\mathbf{V}}(X)$ the set of all identities over X holding in $\mathbf{V}$. If there exists a finite subset Σ of $\mathrm{Id}_{\mathbf{V}}(X)$ such that $\mathrm{var}(\Sigma) = \mathbf{V}$, then $\mathbf{V}$ is said to be *finitely based*, where $\mathrm{var}(\Sigma)$ denotes the variety determined by Σ. In other words, $\mathbf{V}$ is finitely based if there exists a finite subset Σ of $\mathrm{Id}_{\mathbf{V}}(X)$ such that every identity in $\mathrm{Id}_{\mathbf{V}}(X)$ can be derived from Σ. Otherwise, we say that $\mathbf{V}$ is *nonfinitely based*. An algebra A is said to be *finitely based* (resp., *nonfinitely based*) if the variety $\mathbf{HSP}(A)$ generated by A is finitely based (resp., nonfinitely based).

The finite basis problem for finite algebras can be posed as follows: is there an algorithm that when given an effective description of a finite algebra A decides if A is finitely based or not? Over the last decades, several authors have considered the finite basis problem for various semiring (ring) varieties generated by finitely many finite semirings (rings). Kruse [14] and L'vov [15] proved that the variety generated by a finite ring is finitely based. Burris and Lawrence [1], and later Kelarev [13] studied the ring varieties generated by a finite number of finite fields with pairwise distinct characteristics, and proved that such varieties are finitely based. Guzmán [9] proved that the semiring variety generated by two-element distributive lattice D_2 and two-element finite field Z_2 is finitely based. Ghosh, Pastijn and Zhao [8] studied the variety $\overset{+}{\mathbf{S}}\ell$ of idempotent semirings which is generated by two specific semirings of order four. They showed that $\overset{+}{\mathbf{S}}\ell$ has 78 subvarieties and every subvariety of $\overset{+}{\mathbf{S}}\ell$ is finitely based. Shao and Ren [18] investigated the variety generated by all additively idempotent semirings of order two, and proved that every subvariety of this variety is finitely based. Shao, Crvenković and Mitrović [17] studied the variety generated by two-element distributive lattice D_2 and any finite number of finite fields. They showed that this variety is finitely based. Vechtomov and Petrov [19] proved that the variety generated by all commutative multiplicatively idempotent semirings of order two is finitely based. Recently, Chajda and Länger [3] proved that the variety generated by a multiplicatively idempotent semiring of order three is finitely based.

From Birkhoff's theorem [2, Chapter 2, Theorem 8.6], every member of a variety is isomorphic to the subdirect product of its subdirectly irreducible members. Therefore, it is also one of the important research contents of the semiring varieties to characterize subdirectly irreducible semirings in a given semiring variety. Guzmán [9] proved that two-element distributive lattice D_2 and two-element finite field Z_2 are the only subdirectly irreducible members in the Boolean semiring

variety. CHAJDA and LÄNGER [4] gave a complete description of all subdirectly irreducible members of the commutative multiplicatively idempotent semiring variety. VECHTOMOV and PETROV [19] provided necessary conditions under which semirings from the variety generated by all commutative multiplicatively idempotent semirings of order two are subdirectly irreducible.

The class of all rings satisfying the identity $x^n \approx x$ is denoted by $\mathbf{R}_n$. Thus, $\mathbf{R}_2$ denotes the class of all Boolean rings. It is easy to check that $\mathbf{R}_n$ is the semiring variety determined by the additional identities $x^n \approx x$, $(2^n - 1)x \approx x$ and $(2^n - 2)x \approx (2^n - 2)y$. Let $\mathbf{ReB} \cap \overset{+}{\mathbf{S}}\ell$ be the subvariety of $\overset{+}{\mathbf{S}}\ell$ determined by the additional identity $x \approx xyx$ and $\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$ the subvariety of $\overset{+}{\mathbf{S}}\ell$ determined by the additional identity $x \approx x + xyx$. Obviously, the distributive lattice variety $\mathbf{D}$ is a proper subvariety of $\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$ and $\mathbf{D} = \mathbf{HSP}(D_2)$. It is shown [8] that the lattice of all subvarieties of $\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$ is as follows:



where L_2 is the two-element semiring with the following addition and multiplication tables:

$+$	0	1
0	0	1
1	1	1

and

$.$	0	1
0	0	0
1	1	1

;

and R_2 is the (multiplicative) left-right dual of L_2. For $L_2\,[R_2]$ we denote by

$L_2^0\,[R_2^0]$ the semiring obtained from $L_2\,[R_2]$, by adding an element 0, where $a = 0 + a = a + 0$, $0 = 0a = a0$ for every $a \in L_2^0\,[R_2^0]$.

The Mal'cev product of two classes $\mathbf{V}$ and $\mathbf{W}$ of semirings, denoted by $\mathbf{V} \circ \mathbf{W}$, is the class of all semirings S on which there exists a congruence ρ such that $S/\rho \in \mathbf{W}$ and every ρ-class that is a subsemiring of S belongs to $\mathbf{V}$. Thus, in this way, some classes of semirings can be constructed by considering the Mal'cev products of some given classes of semirings. In general, a semiring in the Mal'cev product of two semiring varieties $\mathbf{V}$ and $\mathbf{W}$ is not necessarily isomorphic to the subdirect product of a semiring in $\mathbf{V}$ and a semiring in $\mathbf{W}$. For example, the quotient semiring $L_2^0/\dot{D}$ by the Green $\mathcal{D}$-relation belongs to $\mathbf{D}$ (see [8, Theorem 4.5]). It is easy to check that every $\dot{D}$-class of L_2^0 is a semiring in $\dot{\mathbf{ReB}} \cap \overset{+}{\mathbf{S}}\ell$. Thus, $L_2^0 \in (\dot{\mathbf{ReB}} \cap \overset{+}{\mathbf{S}}\ell) \circ \mathbf{D}$. By [8, Theorem 4.5], $L_2^0 \notin (\dot{\mathbf{ReB}} \cap \overset{+}{\mathbf{S}}\ell) \vee \mathbf{D}$. Therefore, L_2^0 is not isomorphic to the subdirect product of a semiring in $\dot{\mathbf{ReB}} \cap \overset{+}{\mathbf{S}}\ell$ and a semiring in $\mathbf{D}$. Galbiati, Veronesi [6] and Ghosh [7] proved that each member in $\mathbf{R}_2 \circ \mathbf{D}$ is isomorphic to the subdirect product of a ring in $\mathbf{R}_2$ and a semiring in $\mathbf{D}$, which implies that $\mathbf{R}_2 \vee \mathbf{D} = \mathbf{R}_2 \circ \mathbf{D}$. Vechtomov and Petrov proved that the multiplicatively idempotent semiring variety determined by the additional identity $x + 2xyx \approx x$ is equal to $\mathbf{R}_2 \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ (see [19, Theorem 2.1]).

In this paper, we give a decomposition theorem of semirings in the Mal'cev product $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$. Furthermore, we prove that $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ is a finitely based semiring variety, and $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell) = \mathbf{R}_n \vee (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$. We also characterize all subdirectly irreducible rings in this variety, and prove that every subvariety of $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ is finitely based.

For other notation and terminology we use in this paper, the reader is referred to [2], [10] and [11].

2. On the semiring variety $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$

Let $n\,(n \geqslant 2)$ be a positive integer. If $S \in \mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$, then there exists a congruence ρ on S such that $S/\rho \in \mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$ and every ρ-class belongs to $\mathbf{R}_n$. That is to say, for any $a \in S$, the ρ-class ρ_a containing a is a ring in $\mathbf{R}_n$. Thus, $(\rho_a, +)$ is a commutative group. From $S/\rho \in \mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$ it follows that $(S/\rho, +)$ is a semilattice, which means that the additive reduct $(S, +)$ of S is a semilattice of commutative groups. Hence, by [11, Theorem 4.2.1], $(S, +)$ is a commutative

Clifford semigroup. From $\rho_a \in \mathbf{R}_n$ it follows that $a^n = a$, and so S satisfies the identity

$$x^n \approx x. \tag{1}$$

By identity (1), we have $a + a = (a + a)^n = 2^n \cdot a$. Since $(S, +)$ is completely regular, $(2^n - 1) \cdot a = a$. Thus, S satisfies the identity

$$(2^n - 1)x \approx x. \tag{2}$$

For a semiring $(S, +, \cdot)$, we denote Green's $\mathcal{H}$ relation on the additive reduct $(S, +)$ by $\mathcal{H}^+$. By Theorem II.1.4 and Corollary II.1.5 in [16], $\mathcal{H}^+$ is the least semilattice congruence of the additive reduct $(S, +)$ of S, moreover, every $\mathcal{H}^+$-class is a maximal subgroup of $(S, +)$. For any $a \in S$, we denote by $\mathcal{H}_a^+$ the $\mathcal{H}^+$-class containing a, and 0_a the identity of $\mathcal{H}_a^+$, respectively. It is easily seen that $0_a = (2^n - 2)a$ and $a\mathcal{H}^+b$ if and only if $(2^n - 2)a = (2^n - 2)b$ for any $a, b \in S$. Let $E^+(S)$ denote the set of all idempotents of $(S, +)$, i.e., $E^+(S) = \{e \in S \mid e + e = e\}$. Since $E^+(S)$ is a semilattice, by identity (2), we have $E^+(S) = \{(2^n - 2)a \mid a \in S\}$. For a commutative Clifford semigroup $(C, +)$, we say that $(C, +)$ is *E-unitary* (see [11]) if for any $e \in E^+(C)$ and $a \in C$,

$$e + a \in E^+(C) \Rightarrow a \in E^+(C).$$

A commutative Clifford semigroup $(C, +)$ is an E-unitary commutative Clifford semigroup if $(C, +)$ is E-unitary.

Define a binary relation σ on S as follows:

$$(\forall a, b \in S)\, a\sigma b \Leftrightarrow (\exists e \in E^+(S))\, a + e = b + e.$$

It follows from [11, Proposition 5.3.1] that σ is the least group congruence on the additive reduct $(S, +)$ of S. Assume that $a, b \in S$ and $a\sigma b$. Then there exists $e \in E^+(S)$ such that $a + e = b + e$. For any $c \in S$, we have $ca + ce = cb + ce$. Since $ce + ce = c(e + e) = ce$, $ce \in E^+(S)$, and so $ca\,\sigma cb$. Dually, we have $ac\,\sigma bc$. This shows that σ is a semiring congruence on S. In the following, we shall give a decomposition theorem of semirings in $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$.

Theorem 2.1. *If S is a semiring in $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$, then S is isomorphic to the subdirect product of the member S/σ of $\mathbf{R}_n$ and the member $S/\mathcal{H}^+$ of $\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$.*

PROOF. Let S be a semiring. If $S \in \mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$, then there exists a congruence ρ on S such that $S/\rho \in \mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$ and every ρ-class belongs to $\mathbf{R}_n$. It follows that $(S/\rho, +)$ is a semilattice, and so $\mathcal{H}^+ \subseteq \rho$, since $\mathcal{H}^+$ is the least semilattice congruence on $(S, +)$. On the other hand, since ρ_u (the ρ-class containing u) belongs to $\mathbf{R}_n$ for any $u \in S$, the additive reduct of ρ_u is an abelian subgroup of $(S, +)$. Thus, $\rho_u \subseteq \mathcal{H}_u^+$, which implies that $\rho \subseteq \mathcal{H}^+$. Therefore, $\rho = \mathcal{H}^+$, and so $S/\mathcal{H}^+ \in \mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$. It is easy to check that $S/\sigma \in \mathbf{R}_n$, since S satisfies identity (1) and σ is a semiring congruence on S.

Let $a \in S$, $e \in E^+(S)$. If $a + e \in E^+(S)$, then there exists $f \in E^+(S)$ such that $a + e = f$. It follows that $a + (e + f) = e + f$, and so

$$a^3 + a(e + f)a = a(e + f)a.$$

Thus, $a^3 + a + a(e + f)a = a + a(e + f)a$, furthermore,

$$a^3 + a + (2^n - 2)a(e + f)a = a + (2^n - 2)a(e + f)a. \tag{3}$$

Since $E^+(S) = \{(2^n - 2)a \mid a \in S\}$, we can define a mapping from $E^+(S)$ to $S/\mathcal{H}^+$ as follows:

$$\varphi((2^n - 2)a) = \mathcal{H}^+_{(2^n-2)a}.$$

It is routine to verify that φ is an isomorphism. Thus, by $S/\mathcal{H}^+ \in \mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$, $E^+(S)$ satisfies the identity $x + xyx \approx x$. From $(2^n - 2)a$, $e + f \in E^+(S)$, we have

$$(2^n - 2)a + (2^n - 2)a \cdot (e + f) \cdot (2^n - 2)a = (2^n - 2)a,$$

and so $(2^n - 2)a + (2^n - 2)a(e + f)a = (2^n - 2)a$. Thus,

$$a + (2^n - 2)a + (2^n - 2)a(e + f)a = a + (2^n - 2)a. \tag{4}$$

By identities (2), (3) and (4), we can deduce that $a^3 + a = a$. From $a^3 + a(e + f)a = a(e + f)a$, we also have

$$a^4 + a(e + f)a^2 = a(e + f)a^2.$$

Thus, $a^4 + a + a(e + f)a^2 = a + a(e + f)a^2$, furthermore,

$$a^4 + a + (2^n - 2)a(e + f)a^2 = a + (2^n - 2)a(e + f)a^2,$$

which implies that $a^4 + a = a$. By induction, we can show that $a^k + a = a$ for any $k \geq 3$. In particular, we have $a^n + a = a$, i.e., $a + a = a$. This shows that $a \in E^+(S)$. Therefore, $(S, +)$ is an E-unitary commutative Clifford semigroup. It follows from [11, Proposition 5.9.1] that $\mathcal{H}^+ \cap \sigma = \imath_S$. Thus, by [2, Lemma 8.2], S is isomorphic to the subdirect product of $S/\mathcal{H}^+$ and S/σ. □

Theorem 2.1 tells us that if $S \in \mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$, then S is isomorphic to the subdirect product of S/σ and $S/\mathcal{H}^+$, that is, S is isomorphic to a subsemiring of $S/\sigma \times S/\mathcal{H}^+$. Since $\mathbf{R}_n \vee (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ is the smallest variety containing $\mathbf{R}_n$ and $\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$, we have that $S \in \mathbf{R}_n \vee (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ and so $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell) \subseteq \mathbf{R}_n \vee (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$. It is obvious that $\mathbf{R}_n \vee (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell) \subseteq \mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$. This shows that $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell) = \mathbf{R}_n \vee (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$.

If S satisfies identity (1) and

$$x + (2^n - 2)xyx \approx x, \tag{5}$$

then, by the proof of the Theorem 2.1, $S \in \mathbf{R}_n \vee (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$. It is easy to check that both $\mathbf{R}_n$ and $\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$ satisfy identities (1) and (5), which implies that $\mathbf{R}_n \vee (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ also satisfies identities (1) and (5). Thus we have

Theorem 2.2. *The Mal'cev product $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ is a semiring variety determined by identities* (1) *and* (5)*, and $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell) = \mathbf{R}_n \vee (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$.*

Since $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ is a semiring variety, it follows from [2, Theorem 9.6] that every semiring in $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ is isomorphic to a subdirect product of subdirectly irreducible semirings in this variety. By Theorem 2.1, we need only to study subdirectly irreducible idempotent semirings in $\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$ and subdirectly irreducible rings in $\mathbf{R}_n$. In the following, we shall characterize all subdirectly irreducible rings in $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$.

Theorem 2.3. *Let S be a ring in $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$. If S is subdirectly irreducible, then S is a finite field.*

Proof. Assume that S is a subdirectly irreducible ring in $\mathbf{R}_n$. Then S has the unique minimal nontrivial ideal J. From [12, Theorem 11], we have that $(S, \cdot)$ is commutative since S satisfies identity (1). For any $a \neq 0$, if $a^2 = 0$, then $a^n = a = 0$. This implies that $a^2 \neq 0$, and so $\{0\} \subsetneq aJ$. Since $(aJ)R = a(JR) \subseteq aJ$, it follows that aJ is an ideal of S. Thus, $aJ = J$, since J is the unique minimal nontrivial ideal.

For any $a, b \in J \setminus \{0\}$, we have $aJ = bJ = J$. Thus, there exists $c, d \in J \setminus \{0\}$ such that $a = bc, b = ad$. Hence,

$$a^{n-1} = (bc)^{n-1} = b^{n-1}c^{n-1}, \quad b^{n-1} = (ad)^{n-1} = a^{n-1}d^{n-1}.$$

It follows that

$$b^{n-1}a^{n-1} = b^{n-1}b^{n-1}c^{n-1} = b^{n-1}c^{n-1} = a^{n-1},$$
$$a^{n-1}b^{n-1} = a^{n-1}a^{n-1}d^{n-1} = a^{n-1}d^{n-1} = b^{n-1},$$

and so $a^{n-1} = b^{n-1}$. It is also easy to check that $ab \in J \setminus \{0\}$, and so $(J \setminus \{0\}, \cdot)$ is a subsemigroup of J. Moreover, by identity (1), we have $a \cdot a^{n-1} = a^{n-1} \cdot a = a$ and $a \cdot a^{n-2} = a^{n-2} \cdot a = a^{n-1}$. This implies that $(J \setminus \{0\}, \cdot)$ is a group, and so $(J, +, \cdot)$ is a field.

Without loss of generality, we let $e = a^{n-1} = b^{n-1}$ be the identity of $(J \setminus \{0\}, \cdot)$. Consider the set $I = \{a \,|\, ae = 0\}$. It is easy to verify that I is also an ideal of S. If I is nontrivial, then $J \subseteq I$. Hence, for any $a \in I \cap J$ and $a \neq 0$, $ea = a^{n-1}a = a = 0$, a contradiction. Thus, $I = \{0\}$. For any $r \in S$, from $e(r - er) = (r - er)e = 0$ we have $r - er = 0$, and so $r = er$. Since J is an ideal and $e \in J$, it follows that $r = er \in J$. This shows that S is a field.

It is easily seen that every element of S is a root of the polynomial $x^n - x$. Since $x^n - x$ has at most n roots in a field, $|S| \leq n$. This shows that S is a finite field. □

Corollary 2.4. *A finite field F with q elements is in $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ if and only if there exist a prime p and a positive integer t such that $q = p^t$, $p \,|\, 2^n - 2$ and $p^t - 1 \,|\, n - 1$. Furthermore, there exist, up to isomorphism, finitely many finite fields in $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$.*

Proof. Let F be a finite field in $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$. By identity (1), we have that F satisfies $(2^n - 2)x \approx 0$. This implies that the characteristic of F divides $2^n - 2$, and so the characteristic of F is some prime divisor p of $2^n - 2$. Hence, there exists a positive integer t such that the size of F is equal to p^t, i.e., F satisfies $x^{p^t} \approx x$. Clearly, F satisfies identity (1), thus, $p^t - 1$ divides $n - 1$. Since both $2^n - 2$ and $n - 1$ have finitely many divisors, it follows that, up to isomorphism, there are finitely many finite fields in $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$.

Conversely, if there exist a prime p and a positive integer t such that $q = p^t$, $p \,|\, 2^n - 2$ and $p^t - 1 \,|\, n - 1$, then F satisfies identities (1) and (5). Thus, by Theorem 2.2, $F \in \mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$. □

Suppose that $(S, +, \cdot)$ is a semiring in $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$. Then, for each $a \in S$ we have $a = aa^{n-1}a$, $a^n = aa^{n-1} = a^{n-1}a$, which means that a is a completely regular element in the multiplicative reduct $(S, \cdot)$ of S. That is to say, $(S, \cdot)$ is

a completely regular semigroup. Let $\mathcal{H}^{\cdot}$ denote the Green-$\mathcal{H}$ relation on $(S, \cdot)$. It follows that every $\mathcal{H}^{\cdot}$ class is a maximal subgroup of $(S, \cdot)$. We use $E^{\cdot}(S)$ to represent the set of all idempotents of $(S, \cdot)$. Then $E^{\cdot}(S) = \{b^{n-1} \mid b \in S\}$. Recall that a *cryptogroup* is a completely regular semigroup in which $\mathcal{H}^{\cdot}$ is a congruence. A cryptogroup $(S, \cdot)$ is called a *normal orthocryptogroup* if $S/\mathcal{H}^{\cdot}$ is a normal band, and $E^{\cdot}(S)$ is a normal band (see [16]). In the following, we shall characterize the multiplicative reduct $(S, \cdot)$ of S.

Corollary 2.5. *If $S \in \mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$, then $(S, \cdot)$ is a normal orthocryptogroup, and every maximal subgroup of $(S, \cdot)$ is commutative.*

Proof. Suppose that S belongs to $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$. Since both $\mathbf{R}_n$ and $(\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ satisfy the identities $(xy)^{n-1} \approx x^{n-1}y^{n-1}$ and $x^{n-1}y^{n-1}z^{n-1}x^{n-1} \approx x^{n-1}z^{n-1}y^{n-1}x^{n-1}$, it follows from Theorem 2.1 that S satisfies the identities $(xy)^{n-1} \approx x^{n-1}y^{n-1}$ and $x^{n-1}y^{n-1}z^{n-1}x^{n-1} \approx x^{n-1}z^{n-1}y^{n-1}x^{n-1}$. This implies that $E^{\cdot}(S)$ is a normal band and $\mathcal{H}^{\cdot}$ is a congruence on $(S, \cdot)$. By [16, Theorem IV.2.7], $(S, \cdot)$ is a normal orthocryptogroup.

Assume that $a \in S$. Since $\mathcal{H}_a^+$ is a ring, we have $a\mathcal{H}^+a^2$, and so $(2^n - 2)a = (2^n - 2)a^2$. By induction, we can show that $(2^n - 2)a = (2^n - 2)a^k$ for any $k \geq 1$. On the other hand, for any $a, b \in S$, if $a\mathcal{H}^{\cdot}b$, then $a^{n-1} = b^{n-1}$, and so $(2^n - 2)a^{n-1} = (2^n - 2)b^{n-1}$. Thus, $(2^n - 2)a = (2^n - 2)b$, and so $a\mathcal{H}^+b$. Since every $\mathcal{H}^+$-class of S is a ring in $\mathbf{R}_n$, by [12, Theorem 11], we have $ab = ba$. This shows that every maximal subgroup of $(S, \cdot)$ is commutative. □

3. On the subvarieties of $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$

For every subvariety $\mathbf{V}$ of $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$, from Theorem 2.1 we have that $\mathbf{V}$ is generated by some subdirectly irreducible rings in $\mathbf{R}_n$ and some subdirectly irreducible idempotent semirings in $\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$. Now let $\mathcal{SI}(\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ denote the set of all subdirectly irreducible semirings in $\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$. For any subset A of $\mathcal{SI}(\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$, from [8] we have that $\mathbf{HSP}(A)$ is equal to a semiring variety generated by some subset of $\{D_2, L_2, R_2, L_2^0, R_2^0\}$ (denoted by $\mathcal{A}$). On the other hand, we have that, up to isomorphism, there are finitely many subdirectly irreducible rings (finite fields) in $\mathbf{R}_n$ (see Theorem 2.3 and Corollary 2.4). Thus, every subvariety of $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ can be generated by some members in $\mathcal{A}$ and some subdirectly irreducible rings in $\mathbf{R}_n$. Let $\mathcal{T}$ denote the set of all members in $\mathcal{A}$ and all subdirectly

irreducible rings in $\mathbf{R}_n$, and B denote the subset of $\mathcal{T}$. To show that $\mathbf{HSP}(B)$ is finitely based, we need only to consider the following four cases:

Case 1. $B = \emptyset$. It is clear that $\mathbf{HSP}(B)$ is the trivial variety.

Case 2. $B \neq \emptyset$, $B \subseteq \mathcal{A}$. $\mathbf{HSP}(B)$ is finitely based (see the following Table 1 obtained in [8]).

Semiring variety	Determined by additional identities
$\mathbf{HSP}(L_2)$	$x^2 \approx x$, $xy \approx x$
$\mathbf{HSP}(R_2)$	$x^2 \approx x$, $xy \approx y$
$\mathbf{HSP}(L_2, R_2)$	$x^2 \approx x$, $xyx \approx x$
$\mathbf{HSP}(D_2)$	$x^2 \approx x$, $xy \approx yx, x + xy \approx x$
$\mathbf{HSP}(D_2, L_2)$	$x^2 \approx x$, $xyz \approx xzy$, $x \approx x + xy$, $xy + z \approx xy + z + xz$
$\mathbf{HSP}(D_2, R_2)$	$x^2 \approx x$, $xyz \approx yxz$, $x \approx x + yx$, $xy + z \approx xy + z + zy$
$\mathbf{HSP}(D_2, L_2, R_2)$	$x^2 \approx x$, $x + xyx \approx x$, $xy + z \approx xy + z + xz$, $xy + z \approx xy + z + zy$
$\mathbf{HSP}(L_2^0)$	$x^2 \approx x$, $xyz \approx xzy$, $x + xy \approx x$
$\mathbf{HSP}(L_2^0, R_2)$	$x^2 \approx x$, $x + xyx \approx x$, $xy + z \approx xy + z + zy$
$\mathbf{HSP}(R_2^0)$	$x^2 \approx x$, $xyz \approx yxz$, $x + yx \approx x$
$\mathbf{HSP}(R_2^0, L_2)$	$x^2 \approx x$, $x + xyx \approx x$, $xy + z \approx xy + z + xz$
$\mathbf{HSP}(L_2^0, R_2^0)$	$x^2 \approx x$, $x + xyx \approx x$

Table 1

Case 3. B consists of the subdirectly irreducible idempotent semirings in $\mathcal{A}$ and a finite number of subdirectly irreducible rings (finite fields) in $\mathbf{R}_n$. Suppose that A is a non-empty subset of $\mathcal{A}$. Let $\mathbf{V}_A = \mathbf{HSP}(A)$. Since $\mathbf{V}_A$ is finitely based, there exists finite subset Σ_A of $\mathrm{Id}_{\mathbf{V}_A}(X)$ such that each identity in $\mathrm{Id}_{\mathbf{V}_A}(X)$ can be derived from Σ_A.

For any $i \in \{1, 2, \ldots, k\}$, let F_i be a finite field of characteristic p_i in $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ and size $q_i = p_i^{n_i}$ for some positive integer n_i, and let d be the least common multiple of $p_1, \ldots, p_k$. Since F_i satisfies identities (1) and (2), p_i is a prime factor of $2^n - 2$ and $p_i^{n_i} - 1$ is a factor of $n - 1$.

We need to consider the following two subcases:

Subcase 3.1. $B_1 = A \cup \{F_1, \ldots, F_k\}$, in which there exist at least two finite fields in $\{F_1, \ldots, F_k\}$ such that their characteristics are distinct.

Subcase 3.2. $B_2 = A \cup \{F_1, \ldots, F_k\}$, in which $F_1, \ldots, F_k$ have the same characteristics.

We first consider Subcase 3.1. It is easy to verify that $\mathbf{HSP}(B_1)$ satisfies identities (1), (5), and the following

$$(d+1)x \approx x, \tag{6}$$

$$\frac{d}{p_i} \cdot x^{q_i} \approx \frac{d}{p_i} \cdot x, \quad (1 \leq i \leq k), \tag{7}$$

$$d \cdot u_1 + \cdots + d \cdot u_m \approx d \cdot v_1 + \cdots + d \cdot v_\ell, \tag{8}$$

where $u_1 + \cdots + u_m \approx v_1 + \cdots + v_\ell \in \Sigma_A$.

We thus have

Theorem 3.1. *Let $B_1 = A \cup \{F_1, \ldots, F_k\}$, in which there exist at least two finite fields in $\{F_1, \ldots, F_k\}$ such that their characteristics are distinct. Then $\mathbf{HSP}(B_1)$ is finitely based.*

Proof. Let $\mathbf{V}^*$ be the variety of semirings defined by additional identities (1), (5), (6), (7) and (8). It is easy to see that $\mathbf{V}^*$ is a subvariety of $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$, and that $\mathbf{HSP}(B_1)$ is a subvariety of $\mathbf{V}^*$. In what follows, we shall prove that $\mathbf{HSP}(B_1) = \mathbf{V}^*$.

Suppose that S is a subdirectly irreducible semiring in $\mathbf{V}^*$. It follows from Theorems 2.1 and 2.3 that S, up to isomorphism, is a member of $\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell$ or a finite field. If S is a finite field, then, by identity (6), the characteristic of S is equal to some p_i $(1 \leqslant i \leqslant k)$. Since S satisfies

$$\frac{d}{p_i} \cdot x^{q_i} \approx \frac{d}{p_i} \cdot x,$$

S satisfies $x^{q_i} \approx x$, and so the size of S divides q_i. Thus, up to isomorphism, S is a subfield of F_i. Since every subfield of F_i is in $\mathbf{HSP}(B_1)$, we have that S belongs to $\mathbf{HSP}(B_1)$. If S is a subdirectly irreducible idempotent semiring in $\mathbf{V}^*$, then, by identity (8), S belongs to $\mathbf{HSP}(A)$, and so $S \in \mathbf{HSP}(B_1)$. That is to say, every subdirectly irreducible semiring of $\mathbf{V}^*$ is in $\mathbf{HSP}(B_1)$, which implies that $\mathbf{V}^* \subseteq \mathbf{HSP}(B_1)$. This shows that $\mathbf{HSP}(B_1)$ is finitely based. □

Next, we shall discuss Subcase 3.2. Without loss of generality, assume that there exists a prime p such that the characteristics of $F_1, \ldots, F_k$ are equal to p. Thus, there exist positive integers $n_1, \ldots, n_k$ such that $|F_i| = p^{n_i}$ $(1 \leqslant i \leqslant k)$.

It is easy to verify that $\mathbf{HSP}(B_2)$ satisfy identities (1), (5), and the following

$$(p+1)\cdot x \approx x, \tag{9}$$

$$x + (x^{p^{n_1}} + (p-1)\cdot x)\cdots(x^{p^{n_k}} + (p-1)\cdot x) \approx x, \tag{10}$$

$$p\cdot u_1 + \cdots + p\cdot u_m \approx p\cdot v_1 + \cdots + p\cdot v_\ell, \tag{11}$$

where $u_1 + \cdots + u_m \approx v_1 + \cdots + v_\ell \in \Sigma_A$.

We thus have

Theorem 3.2. *Let $B_2 = A \cup \{F_1, \ldots, F_k\}$, in which $F_1, \ldots, F_k$ have the same characteristics. Then $\mathbf{HSP}(B_2)$ is finitely based.*

Proof. We denote by $\mathbf{V}'$ the semiring variety determined by additional identities (1), (5), (9), (10) and (11). It is easy to see that $\mathbf{HSP}(B_2)$ is a subvariety of $\mathbf{V}'$. In the following, we shall show that $\mathbf{HSP}(B_2) = \mathbf{V}'$.

Suppose that S is a subdirectly irreducible semiring in $\mathbf{V}'$. It follows from Theorems 2.1 and 2.3 that S, up to isomorphism, is a number of $\mathbf{N}\cap\overset{+}{\mathbf{S}}\ell$ or a finite field. If S is a finite field, then, by identity (9), the characteristic of S is equal to p. We denote by 0 and 1 the zero element and the identity of S, respectively. Then $(S\setminus\{0\},\cdot)$ is a cyclic group of a finite order. Without loss of generality, suppose that $(S\setminus\{0\},\cdot)$ can be generated by a, and that the order of $(S\setminus\{0\},\cdot)$ is equal to q. From identity (10), we have

$$a + (a^{p^{n_1}} + (p-1)\cdot a)\cdots(a^{p^{n_k}} + (p-1)\cdot a) = a.$$

Furthermore,

$$(a^{p^{n_1}} + (p-1)\cdot a)\cdots(a^{p^{n_k}} + (p-1)\cdot a) = 0,$$

since $(S,+)$ is a group. Therefore, there exists $1 \leqslant j \leqslant k$ such that $a^{p^{n_j}} + (p-1)\cdot a = 0$, and so

$$a^{p^{n_j}} + (p-1)\cdot a + a = a.$$

That is to say, $a = a^{p^{n_j}} + (p-1)\cdot a + a = a^{p^{n_j}} + p\cdot a = a^{p^{n_j}}$, which implies that $a^{p^{n_j}-1} = 1$. This shows that the size q of $(S\setminus\{0\},\cdot)$ divides $p^{n_j}-1$, and so the size of S divides p^{n_j}. Thus, up to isomorphism, S is a subfield of F_j. Since every subfield of F is in the variety $\mathbf{HSP}(B_2)$, S belongs to $\mathbf{HSP}(B_2)$. If S is a subdirectly irreducible idempotent semiring in $\mathbf{V}'$, then, by identity (11), S belongs to $\mathbf{HSP}(A)$, and so $S \in \mathbf{HSP}(B_2)$. This shows that every subdirectly irreducible semiring of $\mathbf{V}'$ is in $\mathbf{HSP}(B_2)$, and so $\mathbf{V}' = \mathbf{HSP}(B_2)$. It follows that $\mathbf{HSP}(B_2)$ is finitely based. □

Case 4. B consists of a finite number of subdirectly irreducible rings (finite fields). Let $B_3 = \{F_1, \ldots, F_k\}$. It is obvious that $\mathbf{HSP}(B_3)$ satisfies identities (6), (7), and the following

$$d \cdot x \approx d \cdot y. \tag{12}$$

Furthermore, we have

Theorem 3.3. *Let* $B_3 = \{F_1, \ldots, F_k\}$. *Then* $\mathbf{HSP}(B_3)$ *is finitely based.*

Proof. Let $\mathbf{V}''$ be the subvariety of $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ determined by additional identities (1), (5), (6), (7) and (12). It is easy to see that $\mathbf{HSP}(B_3) \subseteq \mathbf{V}''$. In the following, we shall show that $\mathbf{HSP}(B_3) = \mathbf{V}''$.

Suppose that S is a subdirectly irreducible semiring in $\mathbf{V}''$. Since S satisfies identity (12), it follows from Theorems 2.1 and 2.3 that S, up to isomorphism, is a finite field. By identity (6), the characteristic of S is equal to p_i $(1 \leqslant i \leqslant k)$. Since S satisfies identity (7), the sizes of S is a factor of q_i. Thus, by $q_i = p_i^{n_i}$, S is a subfield of F_i, and so $S \in \mathbf{HSP}(B_3)$. This shows that $\mathbf{HSP}(B_3) = \mathbf{V}''$, and so $\mathbf{HSP}(B_3)$ is finitely based. □

Hence, for any non-empty subset B of $\mathcal{T}$, by Theorems 3.1, 3.2 and 3.3, $\mathbf{HSP}(B)$ is finitely based.

Recall that a variety is said to be *hereditarily finitely based* if every variety contained in it is finitely based. From the above, it follows that every subvariety of $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ is finitely based. We have now

Corollary 3.4. $\mathbf{R}_n \circ (\mathbf{N} \cap \overset{+}{\mathbf{S}}\ell)$ *is hereditarily finitely based.*

Acknowledgements. The authors are particularly grateful to the referees for an unusually careful reading of this paper and for proposing modifications which led to the substantial improvement of this paper.

References

[1] S. Burris and J. Lawrence, Term rewrite rules for finite fields, *Internat. J. Algebra Comput.* **1** (1991), 353–369.

[2] S. Burris and H. P. Sankappanavar, A Course in Universal Algebra, *Springer-Verlag, New York – Berlin*, 1981.

[3] I. Chajda and H. Länger, On a variety of commutative multiplicatively idempotent semirings, *Semigroup Forum* **94** (2017), 610–617.

[4] I. Chajda and H. Länger, Subdirectly irreducible commutative multiplicatively idempotent semirings, *Algebra Universalis* **76** (2016), 327–337.

[5] I. Dolinka, A class of inherently nonfinitely based semirings, *Algebra Universalis* **60** (2009), 19–35.

[6] J. L. Galbiati and M. L. Veronesi, Sui semianelli di Boole, *Istit. Lombardo Accad. Sci. Lett. Rend. A* **114** (1980), 73–88.

[7] S. Ghosh, A characterization of semirings which are subdirect product of a distributive lattice and a ring, *Semigroup Forum* **59** (1999), 106–120.

[8] S. Ghosh, F. Pastijn and X. Z. Zhao, Varieties Generated by Ordered Bands. I, *Order* **22** (2005), 109–128.

[9] F. Guzmán, The variety of Boolean semirings, *J. Pure Appl. Algebra* **78** (1992), 253–270.

[10] U. Hebisch and H. J. Weinert, Semirings: Algebraic Theory and Applications in Computer Science, *World Scientific*, *Singapore*, 1998.

[11] J. M. Howie, Fundamentals of Semigroup Theory, *The Clarendon Press, Oxford University Press*, *New York*, 1995.

[12] N. Jacobson, Structure theory for algebraic algebras of bounded degree, *Ann. of Math. (2)* **46** (1945), 695–707.

[13] A. V. Kelarev, Semigroup rings in semisimple varieties, *Bull. Austral. Math. Soc.* **57** (1998), 387–391.

[14] R. L. Kruse, Identities satisfied by a finite ring, *J. Algebra* **26** (1973), 298–318.

[15] I. V. L'vov, Varieties of associative rings. I, *Algebra and Logic* **12** (1973), 150–167.

[16] M. Petrich and N. R. Reilly, Completely Regular Semigroups, *John Wiley & Sons*, *New York*, 1999.

[17] Y. Shao, S. Crvenković and M. Mitrović, The variety of semirings generated by distributive lattices and finite fields, *Publ. Inst. Math. (Beograd) (N.S.)* **95** (2014), 101–109.

[18] Y. Shao and M. M. Ren, On the varieties generated by all ai-semirings of order two, *Semigroup Forum* **91** (2015), 171–184.

[19] E. M. Vechtomov and A. A. Petrov, Multiplicatively idempotent semirings, *J. Math. Sci. (N.Y.)* **206** (2015), 634–653.

AIFA WANG
SCHOOL OF MATHEMATICS
NORTHWEST UNIVERSITY
XI'AN, SHAANXI, 710127
P. R. CHINA

AND

SCHOOL OF SCIENCE
CHONGQING UNIVERSITY OF TECHNOLOGY
CHONGQING, 400054
P. R. CHINA

E-mail: wangaf@cqut.edu.cn

YONG SHAO
SCHOOL OF MATHEMATICS
NORTHWEST UNIVERSITY
XI'AN, SHAANXI, 710127
P. R. CHINA

E-mail: yongshaomath@126.com

(Received April 26, 2017; revised January 6, 2018)