THE SEMIRING VARIETY GENERATED BY ANY FINITE NUMBER OF FINITE FIELDS AND DISTRIBUTIVE LATTICES

Yong Shao, Miaomiao Ren, Siniša Crvenković, and Melanija Mitrović

Abstract. We study the semiring variety $V$ generated by any finite number of finite fields $F_1, \ldots, F_k$ and two-element distributive lattice $B_2$, i.e., $V = \text{HSP}\{B_2, F_1, \ldots, F_k\}$. It is proved that $V$ is hereditarily finitely based, and that, up to isomorphism, $B_2$ and all subfields of $F_1, \ldots, F_k$ are the only subdirectly irreducible semirings in $V$.

1. Introduction and preliminaries

Semirings are the natural generalization of rings and distributive lattices. Besides the two well-known examples of semirings: the set of nonnegative integers $\mathbb{N}$ with the usual addition and multiplication as the most trivial one, and the first nontrivial example given by Dedekind [2] in connection with algebra of ideals of commutative ring, history of semirings date back, at least, to Vandiver [22]. The intensive study of semirings was initiated during the late 1960's when their significant applications were found. Thus, nowadays, semirings have both a developed algebraic theory as well as important practical applications. More about applications of semiring theory within analysis, fuzzy set theory, the theory of discrete-event dynamical systems, automata and formal language theory can be found in the trilogy [4]–[6] and in [15]. Recently, new examples of applications of semiring constructions have been investigated in [11]–[14].

All semirings $(S, +, \cdot)$ occurring in the literature satisfy at least the following axioms: $(S, +)$, the additive reduct, and $(S, \cdot)$, the multiplicative reduct of a semiring $S$ are semigroups, and the multiplication distributes over addition from both sides, i.e.,

2010 Mathematics Subject Classification: Primary 16Y60, 08B05; Secondary 20M07.

Key words and phrases: finite field, distributive lattice, subdirectly irreducible, hereditarily finitely based, variety.

The first author is supported by the Natural Science Foundation of Shaanxi Province, Grant 2015JQ210. The third author is supported by the Ministry of Education, Science and Technological Development of Serbia, Grant 174018. The forth author is supported by the Ministry of Education, Science and Technological Development of Serbia, Grant 174026.

Communicated by Žarko Mijajlović.
(SR1) \( x + (y + z) \approx (x + y) + z \);
(SR2) \( x(yz) \approx (xy)z \);
(SR3) \( x(y + z) \approx xy + xz \), \( (x + y)z \approx xz + yz \).

It is, as well, often assumed that \((S,+)\) is commutative, i.e.,
(SR4) \( x + y \approx y + x \).

Note that the variety considered in the present paper satisfy this identity too.

Let \( S \) be a semiring. We can distinguish, in general, the following three subsets of idempotents (if there are any) of \( S \): \( E(S) \bullet \), the set of all multiplicative idempotents of \((S,\cdot)\); \( E(S)_+ \), the set of all additive idempotents of \((S,+)\), and \( E(S) = E(S) \bullet \cap E(S)_+ \). A semiring \( S \) is idempotent if \( S = E(S) \), i.e., if it satisfies
\[ x + x \approx x \approx x^2. \]

An idempotent semiring \( S \) is called a bisemilattice if both the additive and multiplicative reducts \((S,+)\) and \((S,\cdot)\) of \( S \) are semilattices. A distributive lattice is a bisemilattice which satisfies the absorption law
\[ x + xy \approx x. \]

The variety of all distributive lattices is denoted by \( \mathbf{D} \). The smallest nontrivial distributive lattice, the two-element boolean algebra \( B_2 \), given by

\[
\begin{array}{c|cc}
+ & 0 & 1 \\
0 & 0 & 1 \\
1 & 1 & 1 \\
\end{array}
\quad
\begin{array}{c|cc}
\cdot & 0 & 1 \\
0 & 0 & 0 \\
1 & 1 & 1 \\
\end{array}
\]

is the only subdirectly irreducible (moreover, \( B_2 \) is congruence simple too) member of \( \mathbf{D} \) and we have \( \mathbf{D} = HSP\{B_2\} \).

Kelarev in \cite{9} described the ring variety generated by a finite number of finite fields with pairwise distinct characteristics and proved that such varieties are finitely based. Some of their properties, including the one that such a ring variety is arithmetical, are given in \cite{18,25}. Specially, in \cite{10}, it is proved that the ring variety generated by a finite ring is finitely based. Thus, in \cite{23} the ring variety of square root rings is considered, and it is proved that it is generated by the finite field \( F_{2^k} \). In \cite{1} it is proved that the ring variety generated by a finite number of finite fields with pairwise distinct characteristics is finitely based and used in term rewriting. Shao and Ren in \cite{20} proved that the semiring variety generated by distributive lattices and any finite number of prime fields are finitely based. In \cite{21}, it is proved that the semiring variety generated by a finite number of finite fields with pairwise distinct characteristics and distributive lattices are finitely based.

As we know, the “simplest” semiring variety generated by finite fields and distributive lattices is the the variety of Boolean semirings generated by \( B_2 \) and the smallest nontrivial finite field \( Z_2 \), the field of integers modulo 2 or 2-element Boolean ring, given by

\[
\begin{array}{c|cc}
+ & 0 & 1 \\
0 & 0 & 1 \\
1 & 1 & 0 \\
\end{array}
\quad
\begin{array}{c|cc}
\cdot & 0 & 1 \\
0 & 0 & 0 \\
1 & 0 & 1 \\
\end{array}
\]
In [8] it is proved that this variety is finitely based, and it is equivalent to the category of partially Stone spaces. This motivates us to give a little progress in that direction.

The main subject here is the semiring variety \( V = \mathrm{HSP}\{B_2, F_1, \ldots, F_k\} \) generated by \( B_2 \) and any finite number of finite fields \( F_1, \ldots, F_k \). In our consideration, we do not need that finite fields \( F_1, \ldots, F_k \) have pairwise distinct characteristics. We prove that \( V = \mathrm{HSP}\{B_2, F_1, \ldots, F_k\} \) is hereditarily finitely based and characterize all subdirectly irreducible semirings in \( V \). We refer to [4]–[6] as sources of references on semirings. For notions and terminology not given here, we refer to [16] as the background on finite fields, [17] on universal algebras, and [7, 19] for semigroup theory.

2. On the semiring variety \( V = \mathrm{HSP}\{B_2, F_1, \ldots, F_k\} \)

Let \( p_1, \ldots, p_k \) be primes and \( q_1 = p_1^{n_1}, \ldots, q_k = p_k^{n_k} \) for some positive integers \( n_1, \ldots, n_k \). Assume that \( d \) is the least common multiple of \( p_1, \ldots, p_k \) and that \( m \) is a positive integer such that \( m - 1 \) is the product of \( q_1 - 1, \ldots, q_k - 1 \). Let \( W \) denote the variety of semirings defined by identities (SR1–4) and the following ones

\[
(W1) \quad (d + 1) \cdot x \approx x; \\
(W2) \quad x^m \approx x; \\
(W3) \quad d \cdot x^2 \approx d \cdot x; \\
(W4) \quad x + d \cdot xy \approx x; \\
(W5) \quad xy \approx yx.
\]

Let \( S \) be a semiring in \( W \). We denote by \( E(S) \) the set of all idempotents of the additive reduct \((S, +)\) of \( S \). By Theorems 1.1, 1.2, 2.1 and Lemma 2.1 in [21], we have

**Theorem 2.1.** Let \( S \) be a semiring in \( W \). Then the following statements are true:

(i) \( E(S) = \{d \cdot a | a \in S\} \), and \( (E(S), +, \cdot) \) is a distributive lattice;
(ii) \( (S, +) \) is an \( E \)-unitary Clifford semigroup;
(iii) If \( R \) is a subdirectly irreducible semiring in \( W \), then \( R \) is two-element distributive lattice or \( R \) is a finite field.

In this section we assume that \( F_1, \ldots, F_k \) is any given finite number of finite fields with characteristics \( p_1, \ldots, p_k \) and sizes \( q_1, \ldots, q_k \). In what follows the semiring variety \( V = \mathrm{HSP}\{B_2, F_1, \ldots, F_k\} \) will be considered.

It suffices to consider the following cases:

- \( V_1 = \mathrm{HSP}\{B_2, F_1, \ldots, F_k\} \), in which there exist at least two finite fields in \( \{F_1, \ldots, F_k\} \) such that their characteristics are distinct.
- \( V_2 = \mathrm{HSP}\{B_2, F_1, \ldots, F_k\} \), in which \( F_1, \ldots, F_k \) have the same characteristics.

We firstly consider the variety \( V_1 \). Clearly, \( V_1 \) satisfies (W1–5) so it is a subvariety of \( W \). We also have that \( B_2 \) and finite fields \( F_1, \ldots, F_k \) satisfy the following identities

\[
(W6) \quad \frac{d}{p_i} \cdot x^{p_i} \approx \frac{d}{p_i} \cdot x \quad (1 \leq i \leq k),
\]
which implies that $V_1 = \text{HSP}\{B_2, F_1, \ldots, F_k\}$ satisfies (W1–6). In fact, we have

**Theorem 2.2.** Let $V_1 = \text{HSP}\{B_2, F_1, \ldots, F_k\}$. Then

(i) $V_1$ is finitely based;

(ii) if $S$ is a subdirectly irreducible semiring in $V_1$, then $S$ is isomorphic to

$B_2$, or there exists a field $F$ in $\{F_1, \ldots, F_k\}$ such that $S$ is isomorphic to a subfield of $F$.

**Proof.** (i) Let $V^*$ be the variety of semirings defined by (SR1–4) and (W1–6). It is easy to see that $V^*$ is a subvariety of $W$ and that $V_1$ is a subvariety of $V^*$. In what follows we will prove that $V_1 = V^*$.

Suppose that $S$ is a subdirectly irreducible semiring in $V^*$. It follows from Theorem 2.1 that $S$, up to isomorphism, is $B_2$ or a finite field. If $S$ is a finite field, then $S$ satisfies the identity (W1). Thus, the characteristic of $S$ is equal to some $p_i$ ($1 \leq i \leq k$) since $d$ is the least common multiple of $p_1, \ldots, p_k$. Next, $S$ satisfies $d \cdot x^0 = d \cdot x$, which implies that $S$ satisfies $x^d = x$, 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 the variety $V_1 = \text{HSP}\{B_2, F_1, \ldots, F_k\}$, we have that $S$ belongs to $V_1$. This shows that every subdirectly irreducible semiring of $V^*$ is in $V_1$ and so $V^* \subseteq V_1$ and so $V^* = V_1$. This shows that $V_1$ is finitely based.

(ii) If $S$ is a subdirectly irreducible semiring in $V_1$, then it follows directly from the proof of (i) that $S$ is isomorphic to $B_2$, or there exists a field $F$ in $\{F_1, \ldots, F_k\}$ such that $S$ is isomorphic to a subfield of $F$. □

In general, $V_1$ can be a proper subvariety of $W$. This can be shown by the following example.

**Example 2.1.** Let us consider the variety $\text{HSP}\{B_2, F_3, F_{22}, F_{23}, F_{72}\}$ and the semiring variety $W(2, 3, 7, 2017)$ defined by the additional identities

\[\begin{align*}
(1) \quad & x + 42 \cdot x \approx x; \\
(2) \quad & x^{2017} \approx x; \\
(3) \quad & 42 \cdot x^2 \approx 42 \cdot x; \\
(4) \quad & x + 42 \cdot x y \approx x; \\
(5) \quad & x y \approx y x.
\end{align*}\]

It is easy to see that $\text{HSP}\{B_2, F_3, F_{22}, F_{23}, F_{72}\}$ satisfies identities (1)–(5). It is a routine matter to verify that $F_{22}$ is in $W(2, 3, 7, 2017)$. By Theorem 2.2 we have that $F_{22}$ does not belong to $\text{HSP}\{B_2, F_3, F_{22}, F_{23}, F_{72}\}$. This implies that $\text{HSP}\{B_2, F_3, F_{22}, F_{23}, F_{72}\}$ is a proper subvariety of $W(2, 3, 7, 2017)$. This means that, for $V_1$, the identity (W6) is indispensable.

In the following we will discuss the variety $V_2 = \text{HSP}\{B_2, F_1, \ldots, F_k\}$ generated by $B_2$ and a finite number of finite fields with the same characteristic. Without loss of generality, we 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 $|F_i| = p^{n_i}$ ($1 \leq i \leq k$).

Let $n$ be a positive integer such that $n - 1$ is the product of $p^{n_1} - 1, \ldots, p^{n_k} - 1$. It is easy to verify that $V_2$ satisfy

\[\begin{align*}
(FSR1) \quad & (p + 1) \cdot x \approx x; \\
(FSR2) \quad & x^n \approx x;
\end{align*}\]
The semiring variety generated by

(FSR3) \( p \cdot x^2 \approx p \cdot x \);

(FSR4) \( x + p \cdot xy \approx x \);

(FSR5) \( x + (x^{p^{nj}} + (p-1) \cdot x) \cdots (x^{p^{nj}} + (p-1) \cdot x) \approx x \);

(W5) \( xy \approx yx \).

Thus we have

**Theorem 2.3.** Let \( V_2 = \text{HSP}\{B_2, F_1, \ldots, F_k\} \) be the variety generated by \( B_2 \) and a finite number of finite fields with the same characteristic \( p \). Then

(i) \( V_2 \) is finitely based;

(ii) if \( S \) is a subdirectly irreducible semiring in \( V_2 \), then \( S \) is isomorphic to \( B_2 \), or there exists a field \( F \) in \( \{F_1, \ldots, F_k\} \) such that \( S \) is isomorphic to a subfield of \( F \).

**Proof.** (i) We denote by \( V' \) the variety of semirings defined by (SR1–4), (FSR1–5) and (W5). It is easy to see that \( V_2 \) is a subvariety of \( V' \). In what follows, we will prove that \( V_2 = V' \).

Suppose that \( S \) is a subdirectly irreducible semiring in \( V' \). It follows from Theorem 2.1 that \( S \), up to isomorphism, is \( B_2 \) or a finite field. If \( S \) is a finite field, then \( S \) satisfies the identity (FSR1). This implies that the characteristic of \( S \) is equal to \( p \). Since \((S, +, \cdot)\) is a finite field, we denote by 0 and 1 the zero element and the identity of \( S \), respectively. Thus we have that \((S \setminus \{0\}, \cdot)\) is a cyclic group of a finite order. Without loss of generality, we suppose that \((S \setminus \{0\}, \cdot)\) can be generated by the element \( a \) and the order of \((S \setminus \{0\}, \cdot)\) is equal to \( q \), i.e., \(|S \setminus \{0\}| = q \). From (FSR5) we have that \( a + (a^{p^{nj}} + (p-1) \cdot a) \cdots (a^{p^{nj}} + (p-1) \cdot a) = a \). It follows that \( (a^{p^1} + (p-1) \cdot a) \cdots (a^{p^k} + (p-1) \cdot a) = 0 \) since \((S, +)\) is a group. Furthermore, there exists \( 1 \leq j \leq k \) such that \( a^{p^j} + (p-1) \cdot a = 0 \) and so \( a^{p^j} + (p-1) \cdot a + a = a \).

Since the characteristic of \( S \) is equal to \( p \), \( a = a^{p^j} + (p-1) \cdot a + a = a^{p^j} + p \cdot a = a^{p^j+1} \) and so \( a^{p^j+1} \) is 1. This shows the size \( q \) of \((S \setminus \{0\}, \cdot)\) divides \( p^{nj+1} \) and so the size of \( S \) divides \( p^{nj} \). Thus, \( S \) is isomorphic to the subfield of \( F_j \). Since every subfield of \( F_j \) is in the variety \( V_2 = \text{HSP}\{B_2, F_1, \ldots, F_k\} \), we have that \( S \) belongs to \( V_2 \). This shows that every subdirectly irreducible semiring of \( V' \) is in \( V_2 \) and so \( V' = V_2 \). This means that \( V_2 \) is finitely based.

(ii) If \( S \) is a subdirectly irreducible semiring in \( V_2 \), then it follows directly from the proof of (i) that \( S \) is isomorphic to \( B_2 \), or there exists a field \( F \) in \( \{F_1, \ldots, F_k\} \) such that \( S \) is isomorphic to a subfield of \( F \). \( \square \)

In general, \( V_2 \) can be a proper subvariety of \( W \). For example, let us consider the variety \( \text{HSP}\{B_2, F_{3^2}, F_{3^3}, F_{3^3}\} \) and the semiring variety \( W(3, 13754313) \) defined by the additional identities

(1) \( 4 \cdot x \approx x \);

(2) \( x^{13754313} \approx x \);

(3) \( 3 \cdot x^2 \approx 3 \cdot x \);

(4) \( x + 3 \cdot xy \approx x \);

(5) \( xy \approx yx \).

It is easy to see that \( \text{HSP}\{B_2, F_{3^2}, F_{3^3}, F_{3^3}\} \) satisfies identities (1)–(5). It is routine to verify that \( F_{3^2} \) is in \( W(3, 13754313) \). By Theorem 2.3 it follows that \( F_{3^2} \) does not belong to the variety \( \text{HSP}\{B_2, F_{3^2}, F_{3^3}, F_{3^3}\} \). This implies that \( \text{HSP}\{B_2, F_{3^2}, F_{3^3}, F_{3^3}\} \) is a proper subvariety of \( W(3, 13754313) \). This means that, for \( V_2 \), the identity (FSR5) is indispensible.
By Theorems 2.2 and 2.3, we can establish the following result:

**THEOREM 2.4.** Let $V$ be the variety generated by $B_2$ and a finite number of finite fields $\{F_1, \ldots, F_k\}$. Then

(i) $V$ is finitely based;
(ii) if $S$ is a subdirectly irreducible semiring in $V$, then $S$ is isomorphic to $B_2$, or there exists a field $F$ in $\{F_1, \ldots, F_k\}$ such that $S$ is isomorphic to a subfield of $F$.

Theorem 2.4 extends and enriches the main results of [8–10, 20] and [21].

A variety is said to be hereditarily finitely based if every variety contained in it is finitely based. In the rest of this section, we will show that the variety $V$ considered in Theorem 2.4 is hereditarily finitely based. By Theorem 2.4 (ii) we immediately have that, up to isomorphism, there are finitely many subdirectly irreducible members in $V$. Let $T$ denote the set of all subdirectly irreducible members in $V$. Since every subvariety of $V$ is generated by a subset of $T$, it follows that the lattice of all subvarieties of $V$ is finite. Let $A \subseteq T$. To show that $HSP(A)$ is finitely based, we need only to consider the following cases:

- $A = \emptyset$. It is clear that $HSP(A)$ is the trivial variety.
- $A = \{B_2\}$. $HSP(A) = D$ is finitely based.
- $A$ consists of $B_2$ and a finite number of finite fields. Then, by Theorem 2.4 (i) it follows that $HSP(A)$ is finitely based.
- $A$ consists of a finite number of finite fields. Without loss of generality, we assume that $A = \{F_{s_1}, \ldots, F_{s_t}\}$, in which every finite field $F_{s_i}$ is a subfield of some $F_i$. Let $b$ the least common multiple of characteristics of $F_{s_1}, \ldots, F_{s_t}$. It is easy to see that every finite field in $\{F_{s_1}, \ldots, F_{s_t}\}$ satisfies the identity $b \cdot x \approx b \cdot y$, but $B_2$ does not satisfy $b \cdot x \approx b \cdot y$. Thus, $HSP(A)$ is a subvariety of $HSP(A \cup \{B_2\})$ determined by additional identity $b \cdot x \approx b \cdot y$. Suppose that $K$ is a subdirectly irreducible semiring in the subvariety $HSP(A \cup \{B_2\})$ determined by additional identity $b \cdot x \approx b \cdot y$. It follows by Theorem 2.4 (ii) that $K$ is a subfield of some finite field in $A$ and so $K$ belongs to $HSP(A)$. This shows that $HSP(A)$ is the subvariety of $HSP(A \cup \{B_2\})$ determined by additional identity $b \cdot x \approx b \cdot y$. Hence, $HSP(A)$ is finitely based.

From above it follows that every subvariety of $V$ is finitely based. We now have

**THEOREM 2.5.** The semiring variety generated by a two-element distributive lattice and any finite number of finite fields is hereditarily finitely based.

**References**

3. S. Ghosh, A Characterization of semirings which are subdirect product of a distributive lattice and a ring, Semigroup Forum 59 (1999), 106–120.

School of Mathematics
Northwest University
Xian, P. R. China
yongshaomath@126.com
miaomiaoren@yeah.net

Department of Mathematics and Informatics,
University of Novi Sad, Serbia
sima@eunet.rs

Faculty of Mechanical Engineering,
University of Niš, Serbia
meli@masfak.ni.ac.rs