PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE Nouvelle série, tome 98(112) (2015), 45–51

DOI: 10.2298/PIM150404026S

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 \mathbf{V} generated by any finite number of finite fields F_1, \ldots, F_k and two-element distributive lattice B_2 , i.e., $\mathbf{V} = \text{HSP}\{B_2, F_1, \ldots, F_k\}$. It is proved that \mathbf{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 \mathbf{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 discreteevent 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.,

Communicated by Žarko Mijajlović.

45

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 Shannxi Province, Grant 2015JQ1210. 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.

 $\begin{array}{ll} (\mathrm{SR1}) & x+(y+z)\approx (x+y)+z;\\ (\mathrm{SR2}) & x(yz)\approx (xy)z; \end{array}$

(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 **D**. The smallest nontrivial distributive lattice, the two-element boolean algebra B_2 , given by

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

Kelarev in [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 [18, 25]. Specially, in [10], it is proved that the ring variety generated by a finite ring is finitely based. Thus, in [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 [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 [20] proved that the semiring variety generated by distributive lattices and any finite number of prime fields are finitely based. In [21], it is proved that the semiring variety generated by a 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

46

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 $\mathbf{V} = \text{HSP}\{B_2, F_1, \ldots, F_k\}$ 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 $\mathbf{V} = \text{HSP}\{B_2, F_1, \ldots, F_k\}$ is hereditarily finitely based and characterize all subdirectly irreducible semirings in \mathbf{V} . We refer to $[\mathbf{4}]$ - $[\mathbf{6}]$ as sources of references on semirings. For notions and terminology not given here, we refer to $[\mathbf{16}]$ as the background on finite fields, $[\mathbf{17}]$ on universal algebras, and $[\mathbf{7}, \mathbf{19}]$ for semigroup theory.

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

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

 $\begin{array}{ll} (W1) & (d+1) \cdot x \approx x; \\ (W2) & x^m \approx x; \\ (W3) & d \cdot x^2 \approx d \cdot x; \\ (W4) & x + d \cdot xy \approx x; \\ (W5) & xy \approx yx. \end{array}$

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 \mathbf{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 \mathbf{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 $\mathbf{V} = \text{HSP}\{B_2, F_1, \ldots, F_k\}$ will be considered.

It suffices to consider the following cases:

- $\mathbf{V}_1 = \mathrm{HSP}\{B_2, F_1, \dots, F_k\}$, in which there exist at least two finite fields in $\{F_1, \dots, F_k\}$ such that their characteristics are distinct.
- $\mathbf{V}_2 = \mathrm{HSP}\{B_2, F_1, \dots, F_k\}$, in which F_1, \dots, F_k have the same characteristics.

We firstly consider the variety \mathbf{V}_1 . Clearly, \mathbf{V}_1 satisfies (W1-5) so it is a subvariety of \mathbf{W} . We also have that B_2 and finite fields F_1, \ldots, F_k satisfy the following identities

(W6)
$$\frac{d}{p_i} \cdot x^{q_i} \approx \frac{d}{p_i} \cdot x \quad (1 \le i \le k),$$

which implies that $\mathbf{V}_1 = \mathrm{HSP}\{B_2, F_1, \dots, F_k\}$ satisfies (W1-6). In fact, we have

THEOREM 2.2. Let $V_1 = HSP\{B_2, F_1, ..., F_k\}$. Then

- (i) \mathbf{V}_1 is finitely based;
- (ii) if S is a subdirectly irreducible semiring in V₁, then S is isomorphic to B₂, or there exists a field F in {F₁,...,F_k} such that S is isomorphic to a subfield of F.

PROOF. (i) Let \mathbf{V}^* be the variety of semirings defined by (SR1-4) and (W1-6). It is easy to see that \mathbf{V}^* is a subvariety of \mathbf{W} and that \mathbf{V}_1 is a subvariety of \mathbf{V}^* . In what follows we will prove that $\mathbf{V}_1 = \mathbf{V}^*$.

Suppose that S is a subdirectly irreducible semiring in \mathbf{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 $\frac{d}{p_i} \cdot x^{q_i} = \frac{d}{p_i} \cdot x$, which implies that S satisfies $x^{q_i} = x$, 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 $\mathbf{V}_1 = \text{HSP}\{B_2, F_1, \ldots, F_k\}$, we have that S belongs to \mathbf{V}_1 . This shows that every subdirectly irreducible semiring of \mathbf{V}^* is in \mathbf{V}_1 and so $\mathbf{V}^* \subseteq \mathbf{V}_1$ and so $\mathbf{V}^* = \mathbf{V}_1$. This shows that \mathbf{V}_1 is finitely based.

(ii) If S is a subdirectly irreducible semiring in \mathbf{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, \mathbf{V}_1 can be a proper subvariety of \mathbf{W} . This can be shown by the following example.

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

(1) $x + 42 \cdot x \approx x;$ (3) $42 \cdot x^2 \approx 42 \cdot x;$ (5) $xy \approx yx.$ (2) $x^{2017} \approx x;$ (4) $x + 42 \cdot xy \approx x;$

It is easy to see that $\text{HSP}\{B_2, F_3, F_{2^2}, F_{2^3}, F_{7^2}\}$ satisfies identities (1)–(5). It is a routine matter to verify that F_{3^2} is in $\mathbf{W}(2, 3, 7, 2017)$. By Theorem 2.2 we have that F_{3^2} does not belong to $\text{HSP}\{B_2, F_3, F_{2^2}, F_{2^3}, F_{7^2}\}$. This implies that $\text{HSP}\{B_2, F_3, F_{2^2}, F_{2^3}, F_{7^2}\}$ is a proper subvariety of $\mathbf{W}(2, 3, 7, 2017)$. This means that, for \mathbf{V}_1 , the identity (W6) is indispensable.

In the following we will discuss the variety $\mathbf{V}_2 = \text{HSP}\{B_2, F_1, \ldots, F_k\}$ 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 $|F_i| = p^{n_i}$ $(1 \le i \le k)$.

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 \mathbf{V}_2 satisfy

(FSR1) $(p+1) \cdot x \approx x;$ (FSR2) $x^n \approx x;$ (FSR3) $p \cdot x^2 \approx p \cdot x;$ (FSR4) $x + p \cdot xy \approx x;$ (FSR5) $x + (x^{p^{n_1}} + (p-1) \cdot x) \dots (x^{p^{n_k}} + (p-1) \cdot x) \approx x;$ (W5) $xy \approx yx.$ Thus we have

THEOREM 2.3. Let $\mathbf{V}_2 = \text{HSP}\{B_2, F_1, \dots, F_k\}$ be the variety generated by B_2 and a finite number of finite fields with the same characteristic p. Then

- (i) \mathbf{V}_2 is finitely based;
- (ii) if S is a subdirectly irreducible semiring in V₂, then S is isomorphic to B₂, or there exists a field F in {F₁,..., F_k} such that S is isomorphic to a subfield of F.

PROOF. (i) We denote by \mathbf{V}' the variety of semirings defined by (SR1-4), (FSR1-5) and (W5). It is easy to see that \mathbf{V}_2 is a subvariety of \mathbf{V}' . In what follows, we will prove that $\mathbf{V}_2 = \mathbf{V}'$.

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 $a + (a^{p_1^{n_1}} + (p-1) \cdot a) \dots (a^{p_k^{n_k}} + (p-1) \cdot a) = a$. It follows that $(a^{p^{n_1}} + (p-1) \cdot a) \dots (a^{p^{n_k}} + (p-1) \cdot a) = a$. It follows that $(a^{p^{n_1}} + (p-1) \cdot a) \dots (a^{p^{n_k}} + (p-1) \cdot a = 0$ and so $a^{p^{n_j}} + (p-1) \cdot a + a = a$. Since the characteristic of S is equal to $p, a = a^{p^{n_j}} + (p-1) \cdot a + a = a^{p^{n_j}}$ and so $a^{p^{n_j}-1} = 1$. This shows the size q of $(S \setminus \{0\}, \cdot)$ divides $p^{n_j} - 1$ and so the size of S divides p^{n_j} . Thus, S is isomorphisic to the subfield of F_j . Since every subfield of F_i is in the variety $\mathbf{V}_2 = \text{HSP}\{B_2, F_1, \dots, F_k\}$, we have that S belongs to \mathbf{V}_2 . This shows that every subdirectly irreducible semiring of \mathbf{V}' is in \mathbf{V}_2 and so $\mathbf{V}' = \mathbf{V}_2$. This means that \mathbf{V}_2 is finitely based.

(ii) If S is a subdirectly irreducible semiring in \mathbf{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.

In general, \mathbf{V}_2 can be a proper subvariety of \mathbf{W} . For example, let us consider the variety HSP{ $B_2, F_{3^3}, F_{3^5}, F_{3^7}$ } and the semiring variety $\mathbf{W}(3, 13754313)$ defined by the additional identities

 $\begin{array}{lll} (1) & 4 \cdot x \approx x; \\ (2) & x^{13754313} \approx x; \\ \end{array} \begin{array}{lll} (3) & 3 \cdot x^2 \approx 3 \cdot x; \\ (4) & x + 3 \cdot xy \approx x; \\ \end{array} \begin{array}{llll} (5) & xy \approx yx. \\ \end{array}$

It is easy to see that $\text{HSP}\{B_2, F_{3^3}, F_{3^5}, F_{3^7}\}$ satisfies identities (1)–(5). It is routine to verify that F_{3^2} is in $\mathbf{W}(3, 13754313)$. By Theorem 2.3 it follows that F_{3^2} does not belong to the variety $\text{HSP}\{B_2, F_{3^3}, F_{3^5}, F_{3^7}\}$. This implies that $\text{HSP}\{B_2, F_{3^3}, F_{3^5}, F_{3^7}\}$ is a proper subvariety of $\mathbf{W}(3, 13754313)$. This means that, for \mathbf{V}_2 , the identity (FSR5) is indispensable.

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) \mathbf{V} is finitely based;
- (ii) if S is a subdirectly irreducible semiring in V, then S is isomorphic to B₂, or there exists a field F in {F₁,..., 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 \mathbf{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 \mathbf{V} . Let \mathcal{T} denote the set of all subdirectly irreducible members in \mathbf{V} . Since every subvariety of \mathbf{V} is generated by a subset of \mathcal{T} , it follows that the lattice of all subvarieties of \mathbf{V} is finite. Let $\mathcal{A} \subseteq \mathcal{T}$. To show that $\text{HSP}(\mathcal{A})$ is finitely based, we need only to consider the following cases:

- $\mathcal{A} = \emptyset$. It is clear that $HSP(\mathcal{A})$ is the trivial variety.
- $\mathcal{A} = \{B_2\}$. HSP $(\mathcal{A}) = \mathbf{D}$ is finitely based.
- \mathcal{A} consists of B_2 and a finite number of finite fields. Then, by Theorem 2.4(i) it follows that HSP(\mathcal{A}) is finitely based.
- A consists of a finite number of finite fields. Without loss of generality, we assume that A = {F_{s1},...,F_{st}}, in which every finite field F_{sj} is a subfield of some F_i. Let b the least common multiple of characteristics of F_{s1},...,F_{st}. It is easy to see that every finite field in {F_{s1},...,F_{st}} satisfies the identity b · x ≈ b · y, but B₂ does not satisfy b · x ≈ b · y. Thus, HSP(A) is a subvariety of HSP(A ∪ {B₂}) determined by additional identity b · x ≈ b · y. Suppose 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 ∪ {B₂}) determined by additional identity b · x ≈ b · 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 ∪ {B₂}) determined by additional identity b · x ≈ b · y.

From above it follows that every subvariety of \mathbf{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

- S. Burris, J. Lawrence, Term rewrite rules for finite fields, Int. J. Algebra Comput. 1(3) (1991), 353–369.
- R. Dedekind, Über die Theorie derganzen algebraiseen Zahlen, Supplement XI to P.G. Lejeune Dirichlet: Vorlesung über Zahlentheorie 4, Aufl., Druck und Verlag, Braunschweig, 1894.
- S. Ghosh, A Characterization of semirings which are subdirect product of a distributive lattice and a ring, Semigroup Forum 59 (1999), 106–120.

- 4. J. S. Golan, The theory of Semirings with Applications in Mathematics and Theoretical Computer Science, Pitman Monographs and Surveys in Pure Appl. Math., Longman Scientific and Technical, Harlow, 1992.
- 5. _____, Power Algebras over Semirings, Kluwer, Dordrecht, 1999.
- 6. _____, Semirings and Affine Equations over Them, Kluwer, Dordrecht, 2003.
- 7. J. M. Howie, Fundamentals of Semigroup Theory, Oxford Science Publication, Oxford, 1995.
- 8. F. Guzmán, The variety of Boolean semirings, J. Pure Appl. Algebra 78 (1992), 253–270.
- A.V. Kelarev, Semigroup rings in semisimple varieties, Bull. Aust. Math. Soc. 57 (1998), 387–391.
- 10. R. L. Kruse, Identities satisfied by a finite ring, J. Algebra 26 (1973), 298–318.
- D. Y. Gao, A. V. Kelarev, J. L. Yearwood, Optimization of matrix semirings for classification systems, Bull. Aust. Math. Soc. 84 (2011), 492–503.
- J. Abawajy, A.V. Kelarev, J.L. Yearwood, C. Turville, A data mining application of the incidence semirings, Houston J. Math. 39(4) (2013), 1083–1093.
- J. Abawajy, A. V. Kelarev, J. Zeleznikow, Optimization of classification and clustering systems based on Munn semirings, Semigroup Forum 87 (2013), 617–626.
- J. Abawajy, A.V. Kelarev, M. Miller, J. Ryan, *Incidence semirings of graphs and visible bases*, Bull. Aust. Math. Soc. 89 (2014), 451–459.
- W. Kuich, A. Salomaa, Semirings, Automata and Languages, EATCS Monographs on Theoretical Computer Science, Springer Verlag, Berlin, 1986.
- 16. R. Lidl, H. Niederreiter, Finite Fields, (2nd ed.), Cambridge University Press, 1997.
- 17. R. N. McKenzie, G. F. McNulty, W. F. Taylor, *Algebras, Lattices, Varieties*, 1, Monterey: Wadsworth and BrookdCole, 1987.
- G. Michler, R. Wille, Die primitiven Klassen arithmetischer Ringe, Math. Z. 113 (1970), 369–372.
- 19. M. Petrich, Inverse Semigroups, Wiley, New York, 1984.
- Y. Shao, M. M. Ren, The variety of semirings generated by distributive lattices and prime fields, J. Math. Res. Appl. 34(5) (2014), 529–534.
- Y. Shao, S. Crvenkovi]'c, M. Mitrović, Variety generated by distributive lattices and finite fields, Publ. Inst. Math., Nouv. Sér. 95(109), (2014), 101–109.
- H. S. Vandiver, Note on simple type of algebra in which cancellation law of addition does not hold, Bull. Am. Math. Soc. 40 (1934), 914–920.
- J. P. D. Varela, Equivalence between varieties of square root rings and Boolean algebras with a distinguished automorphism, J. Algebra 299 (2006), 190–197.
- B. M. Vernikov, Self-dual varieties of associative rings, Ural. Gos. Univ. Mat. Zap. 14 (1985), 31–37.
- H. Werner, R. Wille, Charakterisierungen der primitiven Klassen arithmetischer Ringe. Math. Z. 115 (1970), 197–200.

(Received 20 02 2015)

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