PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 95 (109) (2014), 101–109 DOI: 10.2298/PIM1409101S

THE VARIETY OF SEMIRINGS GENERATED BY DISTRIBUTIVE LATTICES AND FINITE FIELDS

Yong Shao, Siniša Crvenković, and Melanija Mitrović

Communicated by Žarko Mijajlović

Abstract. A semiring variety is *d-semisimple* if it is generated by the distributive lattice of order two and a finite number of finite fields. A d-semisimple variety $\mathbf{V} = \mathbf{HSP}\{B_2, F_1, \dots, F_k\}$ plays the main role in this paper. It will be proved that it is finitely based, and that, up to isomorphism, the two-element distributive lattice B_2 and all subfields of $F_1, \dots, F_k$ are the only subdirectly irreducible members in it.

1. Introduction and preliminaries

Semirings, following [**5**], "abound in the mathematical world around us. Indeed, the first mathematical structure we encounter-the set of natural numbers-is a semiring." The very begining of their study is connected with the study of ideals of commutative ring [**3**], but semirings per se were firstly considered explicitly in [**18**]. Besides of its more than one century long history, the intensive study of semiring theory was initiated during the late 1960's when their significant applications were found. 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 [**5**–**7**] and in [**12**]. Thus, nowadays, semirings have both a developed algebraic theory as well as important practical applications.

All semirings $(S, +, \cdot)$ occuring in the literature satisfy at least the following axioms: $S_+ = (S, +)$, the *additive reduct*, and $S_\bullet = (S, \cdot)$, the *multiplicative reduct* of a semiring S are semigroups, and the multiplication distributes over addition

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

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

The first author is supported by China Postdoctoral Science Foundation, Grant 2011M501466 and the Natural Science Foundation of Shannxi Province, Grant 2011JQ1017. The second author is Supported by the Ministry of Education, Science and Technological Development of Serbia, Grant 174018. The third author is Supported by the Ministry of Education, Science and Technological Development of Serbia, Grant 174026.

from the both sides, i.e., we have

$$x + (y + z) \approx (x + y) + z, \tag{SR1}$$

$$x(yz) \approx (xy)z, \tag{SR2}$$

$$x(y + z) \approx xy + xz, \quad (x + y)z \approx xz + yz. \tag{SR3}$$

It is, as well, often assumed that S_+ is commutative, i.e.,

$$x + y \approx y + x. \tag{SR4}$$

Let $\mathcal{C}$ be a class of semigroups. A semiring S is an *additively* $\mathcal{C}$ semiring, or, shortly $a - \mathcal{C}$ semiring, if S_+ is a semigroup from the class $\mathcal{C}$. In a similar manner we can define a *multiplicative* $\mathcal{C}$ semiring, or, shortly, $m - \mathcal{C}$ semiring. If both S_+ and $S_\bullet$ are from the class $\mathcal{C}$, then S is a $\mathcal{C}$ semiring. A subset I of a semiring S is an *ideal* of S if $x + y \in I$, $sx, xs \in I$, for any $x, y \in I$ and $s \in S$. An ideal I of S is *k-ideal* or *subtractive ideal* of S if $a \in I$, and either $a + x \in I$ or $x + a \in I$, for some $x \in S$, implies $x \in I$. We can distinguish, in general, the following three subsets of idempotents (if there are any) of a semiring S: $E(S)_\bullet$ set of all multiplicative idempotents of $S_\bullet$; $E(S)_+$ set of all additive idempotents of S_+, and $E(S) = E(S)_\bullet \cap E(S)_+$. Going through the literature (for example, [**4**, **17**]) it can be seen that $E(S)_+$, which is an ideal of a semiring S, plays an important role in the study of semiring's structure. A semiring S is a *subtractive semiring* if $E(S)_+$ is a k-ideal of S. By $\mathcal{H}^+$ and σ^+ will be denoted the Green's relation $\mathcal{H}$ and the minimum group congruence on S_+. A semiring S is *idempotent* if $S = E(S)$, i.e., if it satisfies the following additional identities

$$x + x \approx x \approx x^2.$$

An idempotent semiring S is called a *bisemilattice* if both S_+ and $S_\bullet$ are semilattices. A *distributive lattice* is a bisemilattice which satisfies the absorption law

$$x + xy \approx x.$$

It is well known that an interesting problem in universal algebra is the connection between the structure of a certain algebra and the identities it satisfies. The study of varieties provides some insight into this problem. Through this paper we are concerned mainly about certain varieties of semirings. Vandiver [**18**], worked very hard to make semirings recognized as fundamental algebraic structure, "being basically the best structure which include both rings and distributive lattices." The variety (class) of all distributive lattices is denoted by $\mathbf{D}$. The smallest nontrivial distributive lattice B_2 is the only subdirectly irreducible (moreover, B_2 is congruence simple too) member of $\mathbf{D}$ and we have $\mathbf{D} = \mathbf{HSP}\{B_2\}$. In the theory of ring varieties important place have the so called *semisimple varieties.* A variety is called *semisimple* if it is generated by a finite number of finite fields. Such varieties are finitely based [**15**]. Some of their properties, including the one that such a variety is arithmetical, are given in [**15**, **21**]. Specially, in [**11**], it is proved that the variety generated by a finite ring is finitely based. Semisimple varieties occur in the solutions of several natural problems. Thus, in [**19**] the variety of square root rings are considered, and it is proved that this variety is generated by the finite field

F_{2^k}. In [**2**] it is proved that the variety generated by finitely many finite fields with pairwise distinct characteristics is finitely based and used in term rewriting. The list of the adequate references on semisimple varieties and its applications can be found in [**10**]. Among that list is [**20**] as well, where it is proved that a semisimple variety is self-dual (i.e., lattice of of its subvarieties is self-dual) if and only if it can be generated by a finite number of finite fields with pairwise distinct characteristics. Semigroup rings which belong to self-dual semisimple varieties are described in [**10**]. Coming back to the theory of semiring varieties, we can find applications of semisimple varieties as well, [**1**], where it is proved that an a-commutative semiring S is a lattice of rings from a semisimple variety $\mathbf{R}$ iff it S a subdirect product of a ring from $\mathbf{R}$ and a (distributive) lattice iff S is in the join $\mathbf{R} \vee \mathbf{D}$.

There is another way to use finite fields within semiring variety case. We will stop for a moment to give the following definition. A semiring variety is *d-semisimple* if it is generated by the distributive lattice of order two and a finite number of finite fields. The "simplest" *d-semisimple* semiring variety, the variety of Boolean rings, is the variety 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

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$.

In [**9**], it is proved that this variety is finitely based, and that it is equivalent to the category of partially Stone spaces. This motivates us to give a little progress in that direction.

Finite fields (also called *Galois fields*) are fields with finitely many elements. We start this section with three (wellknown) fundamental properties of finite fields which we are going to use till the end of this paper without special announcement.

THEOREM 1.1. *Let F be a finite field. Then F has p^k elements, where the prime p is the* characteristic *of F, k is a positive integer.*

THEOREM 1.2 (Existence and Uniqueness). *For every prime p and every positive integer k there exists a finite field with p^k elements. Any finite field with $q = p^k$ elements is isomorphic to the splitting field of $x^{p^k} - x$ over F_p.*

THEOREM 1.3 (Subfield Criterion). *Let F_q be a finite field with $q = p^k$ elements. Then every subfield of F_q has order p^m, where m is a positive divisor of k. Conversely, if m is a positive divisor of k, then there is exactly one subfield of F_q with p^m elements.*

Theorem 1.1 gives justification for talking about *finite field with q elements* or *finite field of order q*. We denote this field with F_q, having in mind that q is a power of the prime characteristic p of F_q. A great progress is made during last decades in connection with algorithmic and computational aspects of finite fields so important in the areas of computer algebra and symbolic computation. The numerous applications of finite fields in combinatorics, cryptology, algebraic coding theory, pseudorandom number generating and electronical engineering, besides of their important application within mathematics, were and are stimulus for intensive developing of the theory of finite fields. For notions and notations in connection to finite fields not given in this paper, as well as about more of their applications, we refer to [**13**].

The main subject of this paper is *d-semisimple* semiring variety

$$\mathbf{V} = \mathbf{HSP}\{B_2, F_1, \ldots, F_k\},$$

the variety generated by B_2 and finite fields $F_1, \ldots, F_k$ with distinct characteristcs. We will prove that this variety is finitely based. To do that we will define variety **DFSR** by certain finite number of identities, describe it, and then prove that **V** is its proper subvariety.

We refer to [**5**–**7**] as sources of references on semirings. For notions and terminologies not given in this paper, we refer to [**14**] as a background on universal algebra, and [**8**, **16**] for semigroup theory.

2. DFSR variety

Till the end of this paper let $F_1, \ldots, F_k$ be a fixed list of finite fields with distinct characteristics $p_1, \ldots, p_k$, i.e., with respective sizes $q_1 = {p_1}^{n_1}, \ldots, q_k = {p_k}^{n_k}$, for some positive integers $n_1, \ldots, n_k$. Let $c = p_1 \cdots p_k$, and let n be a positive integer such that $n-1$ is the least common multiple of $q_1 - 1, \ldots, q_k - 1$. It is easy to verify that B_2, $F_1, \ldots, F_k$ satisfy the following identities:

(DFSR1) $$(c+1) \cdot x \approx x;$$

(DFSR2) $$x^n \approx x;$$

(DFSR3) $$c \cdot x^2 \approx c \cdot x;$$

(DFSR4) $$x + c \cdot xy \approx x;$$

(DFSR5) $$xy \approx yx.$$

Let us denote by **DFSR** the variety of semirings defined by the identities (SR1–4) and (DFSR1–5). We will start with some results about semirings which are members of **DFSR**.

THEOREM 2.1. *Let S be a semiring in* **DFSR**. *Then:*

(i) *$E(S)_+ = \{c \cdot a \mid a \in S\}$, and $(E(S)_+, +, \cdot)$ is a distributive lattice;*
(ii) *S_+ is an E-unitary Clifford semigroup;*
(iii) *S is a subtractive Clifford semiring;*
(iv) *S is (isomorphic to) a subdirect product of the distributive lattice $S/\mathcal{H}^+$ and the ring S/σ^+.*

PROOF. Let $(S, +, \cdot)$ be a semiring in **DFSR**.

(i) It is obvious that $c \cdot a + c \cdot a = c \cdot a$, for any $a \in S$. Thus we have that $E(S)_+ = \{c \cdot a \mid a \in S\}$. By (SR4), $(E(S)_+, +)$ is a semilattice. Let $e \in E(S)_+$. Then, by (DFSR3), we have

$$e^2 = (c \cdot e)(c \cdot e) = c^2 \cdot e^2 = c \cdot (c \cdot e^2) = c \cdot (c \cdot e) = c \cdot e = e.$$

Thus $(E(S)_+, \cdot)$ is a band, and, by (DFSR5), a semilattice. We have, by (DFSR1) and (DFSR4), that $e + ef = e + c \cdot ef = e$. Thus, $(E(S)_+, +, \cdot)$ is a distributive lattice.

(ii) (DFSR1) implies regularity of the addition, even more, we have

$$(c-1) \cdot a + a = a + (c-1) \cdot a,$$

for any $a \in S$. So, S_+ is completely regular. By (SR4), S_+ is a Clifford semigroup.

Let $a + e \in E(S)_+$, $a \in S$ and $e \in E(S)_+$, i.e., there is $f \in E(S)_+$ such that $a + e = f$ and $a + e + f = f$. On the other hand, by (i) and (DFSR5), we have

$$\begin{aligned} e + f &= e + f + ef = e + f + e(a + e) \\ &= e + f + e + ea = e + f + ea \\ &= f + e(e + a) = f + ef = f + fe = f. \end{aligned}$$

Thus, $a+e+f = e+f$, and (left-)multiplying it by a, we have $a^2+a(e+f) = a(e+f)$, which implies

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

If we, further, add $(c-1) \cdot a(e + f)$ to both sides, we get

$$a^2 + a + c \cdot a(e + f) = a + c \cdot a(e + f).$$

Now, by (DFSR4), we have $a^2+a = a$, and, multiplying it by a, we have $a^3+a^2 = a^2$, which implies $a + a^3 + a^2 = a + a^2$. Thus $a^3 + a = a$. By induction, it can easily be shown that $a^m + a = a$ for any positive integer m. By (DFSR2), it follows that $a + a = a$, i.e., $a \in E(S)_+$. Therefore, S_+ is E-unitary.

(iii) $S_\bullet$ is a Clifford semigroup by (DFSR2). By this and *(ii)*, S is a Clifford semiring. By *(ii)* again, $E(S)_+$ is a k-ideal. Thus, S is a subtractive Clifford semiring.

(iv) By *(iii)* and [**4**, Theorem 3.5], S is a subdirect product of a distributive lattice and a ring. By *(ii)* and [**8**, Proposition 5.9.1], we have $\sigma^+ \cap \mathcal{H}^+ = 1_S$, which, by [**16**, Lemma I.4.18], implies that S is a subdirect product of $S/\mathcal{H}^+$ and S/σ^+.

(SR4), [**8**, Theorem 4.1.3], [**8**, Theorem 4.2.1] and (ii), implies that $\mathcal{H}^+$ is the least semilattice congruence on S_+ with $\mathcal{H}^+$-classes as the maximal subgroups of S_+. Recall that [**8**, Proposition 5.1.2],

$$\mathcal{H}^+ = \{(x, y) \in S \times S \mid x + x' = y + y'\},$$

and $\mathcal{H}^+$-class of an element x is the group $H^+_{x+x'}$. On the other hand, as $\mathcal{H}^+$ is a congruence, we have $c \cdot x \in H^+_{x+x'}$. By (i), $c \cdot x \in E(S)_+$, which implies $c \cdot x = x + x'$. So we have

$$\mathcal{H}^+ = \{(x, y) \in S \times S \mid c \cdot x = c \cdot y\}.$$

It is easy to check that the mapping $f : E(S)_+ \to S/\mathcal{H}^+$, defined by $f(c \cdot x) = H^+_{c \cdot x}$ is an isomorphism. Thus $S/\mathcal{H}^+$, by (i), is a distributive lattice.

It is easy to verify that a relation

$$\sigma^+ = \{(x, y) \in S \times S \mid (\exists e \in E(S)_+) x + e = y + e\}$$

is the least ring congruence on S. □

Now, to determine subdirectly irreducible members of **DFSR**.

Lemma 2.1. *Let R be a ring in* **DFSR**. *If R is subdirectly irreducible, then R is a finite field.*

Proof. Let R be a subdirectly irreducible ring in the semiring variety **DFSR**. Then R has the unique minimal nontrivial ideal J. For any $a \neq 0$ in J, if $aa = 0$, then $0 = a^2 \cdot a^{n-2} = a^n = a$, which is a contradiction. This implies that $aa \neq 0$ and so $\{0\} \subset aJ$. Since $(aJ)R = a(JR) \subseteq aJ$, it follows that aJ is an ideal. Also, $\{0\} \subset aJ \subseteq J$. This shows that $aJ = J$ since J is the unique minimal nontrivial ideal.

For any $a, b \in J \smallsetminus \{0\}$, we have that $aJ = bJ = J$. Thus, there exist $c, d \in J \smallsetminus \{0\}$ such that $a = bc, b = ad$. It follows from (DFSR5) that $a^{n-1} = b^{n-1}c^{n-1}$ and $b^{n-1} = a^{n-1}d^{n-1}$. Since

$$b^{n-1}a^{n-1} = b^{n-1}b^{n-1}c^{n-1} = b^n b^{n-2}c^{n-1} = b^{n-1}c^{n-1} = a^{n-1},$$

we have that $b^{n-1}a^{n-1} = a^{n-1}$. Similarly, we obtain $a^{n-1}b^{n-1} = b^{n-1}$. Thus $a^{n-1} = b^{n-1}$. For any $a, b \in J \smallsetminus \{0\}$, if $ab = 0$, then, by (DFSR5), $a^{n-1}b^{n-1} = 0$ and so $a^{n-1} = a^{n-1}a^{n-1} = a^{n-1}b^{n-1} = 0$. Moreover, $a = a^{n-1}a = 0 \cdot a = 0$, which is a contradiction. This shows that $(J \smallsetminus \{0\}, \cdot)$ is a multiplicative subsemigroup of J.

Since $a^{n-1} = b^{n-1}$ for any $a, b \in J \smallsetminus \{0\}$, without loss of generality, we let $e = a^{n-1}$ for any $a \in J \smallsetminus \{0\}$. It is easy to see that $b = be = eb$ for any $b \in J \smallsetminus \{0\}$. Thus, e is the identity element of the semigroup $(J \smallsetminus \{0\}, \cdot)$. Also, it is obvious that every element in $(J \smallsetminus \{0\}, \cdot)$ has a multiplicative inverse since $e = a^{n-2}a = aa^{n-2}$ for any $a \in J \smallsetminus \{0\}$. This shows that $(J \smallsetminus \{0\}, \cdot)$ is a group and so J is a field.

Let $I = \{a \mid ea = 0\}$. It is easy to verify that I is an ideal of R. If $a \in I \bigcap J$ and $a \neq 0$, then $ea = a^{n-1}a = a = 0$, which is a contradiction. Thus, $I = \{0\}$. For any $r \in R$, we have that $e(r - er) = 0$ and so $r - er = 0$, i.e., $r = er$. Since J is an ideal and $e \in J$, it follows that $r = er \in J$. This shows that R is a field.

R satisfies $x^n \approx x$, that is to say that every element of R is a root of the polynomial $x^n - x$. Since the polynomial $x^n - x$ has at most n roots in a field, we have that the size of the field R is less than or equal to n. This shows that R is a finite field. □

Remark. Lemma 2.1 is an equivalent of Jacobson's theorem [**14**, p. 175].

It is a well known fact that subdirectly irreducible members, in general, need not be congruence simple. For example, let Z_4 be the integer residue ring modulo 4 with addition and multiplication table

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

.

It is easy to verify that $\{\bar{0}, \bar{2}\}$ is the unique nontrival ideal of Z_4. Thus Z_4 is subdirectly irreducible, but it is not congruence simple. For subdirectly irreducible members from **DFSR**, as a consequence of Lemma 2.1, we have

Corollary 2.1. *A semiring S from* **DFSR** *is subdirectly irreducible if and only if it is congruence simple.*

How many subdirectly irreducible members are there in **DFSR**? The main result of this section will give the answer.

Theorem 2.2. *There exist, up to isomorphism, finitely many finite fields in* **DFSR**.

Proof. Let F be a finite field in **DFSR**. By (DFSR1) we have that F satisfies $c \cdot x \approx 0$. This implies that the characteristic of F divides c, so the characteristic is some $p_i(1 \leqslant i \leqslant k)$ since $c = p_1 \cdots p_k$. Without loss of generality, we let the characteristic of F be p_j. Then, there exists a positive integer t such that the size of F is ${p_j}^t$. Hence, F satisfies $x^{{p_j}^t} \approx x$, Clearly, F satisfies (DFSR2), thus we have that ${p_j}^t - 1$ divides $n-1$. Since $n-1$ has finitely many divisors, it follows that, up to isomorphism, there are finitely many finite fields in **DFSR**. □

Here are, given below, some consequences of Theorem 2.2

Corollary 2.2. *Let F be a finite field. Then F belongs to* **DFSR** *if and only if there exists a prime q which is a divisor of c and a positive integer t such that the characteristic of F is q, the size of F is q^t and $q^t - 1$ divides $n-1$.*

Corollary 2.3. *There are finitely many subdirectly irreducible members in* **DFSR**.

3. The *d*-semisimple semiring variety

In what follows the d-semisimple semiring variety $\mathbf{V} = \mathbf{HSP}\{B_2, F_1, \ldots, F_k\}$ will be considered. Clearly, $\mathbf{V}$ satisfies (DFSR1-5) so it is a subvariety of **DFSR**. We also have that B_2 and finite fields $F_1, \ldots, F_k$, [**2**, Lemma 1.1], satisfy the following identities

$$\text{(DFSR6)} \qquad \frac{c}{p_i} \cdot x^{q_i} = \frac{c}{p_i} \cdot x \quad (1 \leqslant i \leqslant k),$$

which implies that $\mathbf{V} = \mathbf{HSP}\{B_2, F_1, \ldots, F_k\}$ satisfies (DFSR1-6). The following theorem is the main result of this section.

Theorem 3.1. *Let $\mathbf{V} = \mathbf{HSP}\{B_2, F_1, \ldots, F_k\}$. Then*

(i) $\mathbf{V}$ *is finitely based;*

(ii) *if S is a subdirectly irreducible semiring in $\mathbf{V}$, 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.*

Proof. (i) We denote by $\mathbf{V}^*$ the variety of semirings defined by (SR1-4) and (DFSR1-6). It is easy to see that $\mathbf{V}^*$ is a subvariety of **DFSR** and that $\mathbf{V}$ is a subvariety of $\mathbf{V}^*$. In the following we will prove that $\mathbf{V} = \mathbf{V}^*$.

Suppose that S is a subdirectly irreducible semiring in $\mathbf{V}^*$. It follows from Theorem 2.1 and Theorem 2.2 that S, up to isomorphism, is B_2 or a finite field. If S is a finite field, then S satisfies $c \cdot x \approx 0$. Thus, the characteristic of S is equal to some $p_i (1 \leqslant i \leqslant k)$ since $c = p_1 \cdots p_k$. Next, S satisfies $\dfrac{c}{p_i} \cdot x^{q_i} = \dfrac{c}{p_i} \cdot x$ 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 $\mathbf{V} = \mathbf{HSP}\{B_2, F_1, \dots, F_k\}$, we have that S belongs to $\mathbf{V}$. This shows that every subdirectly irreducible semiring of $\mathbf{V}^*$ is in $\mathbf{V}$ and so $\mathbf{V}^* \subseteq \mathbf{V}$. Thus we have that $\mathbf{V}$ is finitely based.

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

In general, $\mathbf{V}$ is a proper subvariety of $\mathbf{DFSR}$ which is shown by the following example.

Example. Let us consider the variety $\mathbf{HSP}\{B_2, Z_3, F_{7^2}\}$ and the variety $\mathbf{DFSR}(3, 7, 97)$ defined by the identities

$$x + 21 \cdot x \approx x; \tag{1}$$

$$x^{97} \approx x; \tag{2}$$

$$x + 21 \cdot xy \approx x; \tag{3}$$

$$21 \cdot x^2 \approx 21 \cdot x; \tag{4}$$

$$xy \approx yx. \tag{5}$$

It is easy to see that $\mathbf{HSP}\{B_2, Z_3, F_{7^2}\}$ satisfies identities (1)–(5). Since 3^2 is not a divisor of 7^2, we have by Theorem 3.1 that F_{3^2} does not belong to the variety $\mathbf{HSP}\{B_2, Z_3, F_{7^2}\}$. It is routine to verify that F_{3^2} is in $\mathbf{DFSR}(3, 7, 97)$. This implies that $\mathbf{HSP}\{B_2, Z_3, F_{7^2}\}$ is a proper subvariety of $\mathbf{DFSR}(3, 7, 97)$.

By Corollary 2.2 and Theorem 3.1, we have

Corollary 3.1. $\mathbf{HSP}\{B_2, F_1, \dots, F_k\} = \mathbf{DFSR}$ *if and only if every finite field in* $\mathbf{DFSR}$ *is isomorphic to a subfield of some* F_i $(1 \leqslant i \leqslant k)$.

References

1. H.-J. Bandelt, M. Petrich, *Subdirect products of rings and distributive lattices*, Proc. Edinburgh Math. Soc., II. Series **25** (1982), 155–171.
2. S. Burris, J. Lawrence, *Term rewrite rules for finite fields*, Internat. J. Algebra Comput. **1**(3) (1991), 353–369.
3. R. Dedekind, *Über die Theorie derganzen algebraiscen Zahlen*, Supplement XI to P. G. Lejeune Dirichlet: *Vorlesung über Zahlentheorie* 4, Aufl., Druck und Verlag, Braunschweig, 1894.
4. S. Ghosh, *A characterization of semirings which are subdirect product of a distributive lattice and a ring*, Semigroup Forum **59** (1999), 106–120.
5. 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.
6. ———, *Power Algebras Over Semirings*, Kluwer, Dordrecht, 1999.

7. ______, *Semirings and Affine Equations Over Them*, Kluwer, Dordrecht, 2003.
8. J. M. Howie, *Fundamentals of Semigroup Theory*, Oxford Science Publication, 1995.
9. F. Guzmń, *The variety of Boolean semirings*, J. Pure Appl. Algebra **78** (1992), 253–270.
10. A. V. Kelarev, *Semigroup rings in semisimple varieties*, Bull. Austral. Math. Soc. **57** (1998), 387–391.
11. R. L. Kruse, *Identities satisfied by a finite rings*, J. Algebra **26** (1973), 298–318.
12. W. Kuich, A. Salomaa, *Semirings, Automata and Languages*, EATCS Monographs on Theoretical Computer Science, Springer-Verlag, Berlin, 1986.
13. R. Lidl, H. Niederreiter, *Finite Fields*, (2nd ed.), Cambridge University Press, 1997.
14. R. N. McKenzie, G. F. McNulty, W. F. Taylor, *Algebras, Lattices, Varieties*, Vol. 1, Wadsworth and BrookdCole, Monterey, 1987.
15. G. Michler, R. Wille, *Die primitiven Klassen arithmetischer Ringe*, Math. Z. **113** (1970), 369–372.
16. M. Petrich, *Inverse Semigroups*, Wiley, New York, 1984.
17. M. K. Sen, S. Ghosh, P. Mukhopadhyay, *Congruences on inversive semirings*, Algebras and Combinatorics, Proceedings ICAC 97 (HK), Springer-Verlag, 1991, 391–400.
18. 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.
19. J. P. D. Varela, *Equivalence between varieties of square root rings and Boolean algebras with a distinguished automorphism*, J. Algebra **299** (2006), 190–197.
20. B. M. Vernikov, *Self-dual varieties of associative rings*, Ural. Gos. Univ. Mat. Zap. **14** (1985), 31–37.
21. H. Werner, R. Wille, *Charakterisierungen der primitiven Klassen arithmetischer Ringe*, Math. Z. **115** (1970), 197–200.

(Revised 24 06 2013)

Department of Mathematics
Northwest University
Xian
P.R. China
yongshaomath@gmail.com

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