MULTIPLICATIVELY IDEMPOTENT SEMIRINGS

Ivan Chajda, Olomouc, Helmut Länger, Wien,
Filip Švrček, Olomouc

(Received December 11, 2012)

Abstract. Semirings are modifications of unitary rings where the additive reduct does not form a group in general, but only a monoid. We characterize multiplicatively idempotent semirings and Boolean rings as semirings satisfying particular identities. Further, we work with varieties of enriched semirings. We show that the variety of enriched multiplicatively idempotent semirings differs from the join of the variety of enriched unitary Boolean rings and the variety of enriched bounded distributive lattices. We get a characterization of this join.

Keywords: semiring; commutative semiring; multiplicatively idempotent semiring; semiring of characteristic 2; simple semiring; unitary Boolean ring; bounded distributive lattice

MSC 2010: 16Y60, 06E20

1. Introduction

Boolean rings are important algebras used both in mathematics and applications. Several characterizations of Boolean rings were settled in [1], [2] and [8]. However, in some considerations in Computer Science as well as in Propositional Calculus we need to work with similar algebras which need not be rings. In particular, we often use semirings satisfying the condition $xx = x$ and hence forming a certain generalization of Boolean rings. Of course, every unitary Boolean ring is a semiring satisfying this condition. However, also every bounded distributive lattice can be considered as a semiring satisfying $xx = x$. Hence, our class of semirings under consideration is broad enough to be treated from several points of view.

We recall the definition of a semiring from [5].

Support of the research of the first two authors by the Austrian Science Fund (FWF) and the Czech Science Foundation (GAČR), Project I 1923-N25, and by AKTION Austria–Czech Republic, Grant No. 71p3, is gratefully acknowledged.

Definition 1.1. A *semiring* is an algebra $\mathcal{S} = (S, +, \cdot, 0, 1)$ of type $(2, 2, 0, 0)$ satisfying the following conditions:

(i) $(S, +, 0)$ is a commutative monoid.
(ii) $(S, \cdot, 1)$ is a monoid.
(iii) '$\cdot$' is distributive with respect to '+'.
(iv) $x0 = 0x = 0$ for all $x \in S$.

A *semiring* $\mathcal{S} = (S, +, \cdot, 0, 1)$ is called *trivial* if $|S| = 1$ (i.e. $0 = 1$), *commutative* if '$\cdot$' is commutative, i.e., $xy = yx$ for all $x, y \in S$, *multiplicatively idempotent* if $xx = x$ for all $x \in S$, of *characteristic* 2 if $x + x = 0$ for all $x \in S$ and *simple* (cf. [5]) if $x+1 = 1$ for all $x \in S$. For the sake of brevity, multiplicatively idempotent semirings will be called simply *idempotent semirings* throughout the paper.

Remark 1.2. A semiring $\mathcal{S}$ is of characteristic 2 if and only if $1 + 1 = 0$. In this case $\mathcal{S}$ is a ring since $(S, +)$ is a group.

Hence, if $\mathcal{S} = (S, +, \cdot, 0, 1)$ is a commutative idempotent semiring then its reduct $(S, \cdot, 0, 1)$ is a bounded meet-semilattice.

Now we introduce a notation concerning the additive multiple of an element of a semiring.

Notation. Let $\mathcal{S} = (S, +, \cdot, 0, 1)$ be a semiring, n a positive integer and $a \in S$. Then na and a^n denotes the sum and product, respectively, of n elements a. Moreover $0a := 0$ and $a^0 := 1$. Especially, we write n instead of $n1$, so $na = (1 + \ldots + 1)a$ (with n 1's).

It is well-known that if $\mathcal{R} = (R, +, \cdot, 0, 1)$ is a unitary Boolean ring, i.e., a ring satisfying $xx = x$, then $\mathcal{R}$ is commutative and of characteristic 2. In what follows we show that for idempotent semirings the situation differs.

Theorem 1.3. *For commutative semirings, idempotency $xx = x$ and characteristic 2 are independent properties.*

The proof is composed by the following two examples:

Example 1.4. Consider the semiring $\mathcal{S} = (\{0, a, 1\}, +, \cdot, 0, 1)$ defined by

$+$	0	a	1
0	0	a	1
a	a	a	a
1	1	a	1

and

$\cdot$	0	a	1
0	0	0	0
a	0	a	a
1	0	a	1

The distributive law $(x + y)z = xz + yz$ holds if $0 \in \{x, y\}$ or $z \in \{0, 1\}$. The remaining cases can be checked directly:

$$\begin{aligned}
(a+a)a &= aa = a = a + a = aa + aa, \\
(a+1)a &= aa = a = a + a = aa + 1a, \\
(1+1)a &= 1a = a = a + a = 1a + 1a.
\end{aligned}$$

$\mathcal{S}$ is commutative and idempotent, but not of characteristic 2 since $a + a = a \neq 0$.

Example 1.5. Consider the semiring

$$\mathcal{S} = \left(\left\{\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}, +, \cdot, \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)$$

of 2×2-matrices over $\mathbb{Z}_2$. Then $\mathcal{S}$ is commutative and of characteristic 2, but not idempotent since $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$.

Nevertheless, we can show that idempotency and characteristic 2 yield commutativity as well as a stronger property, see the following lemma.

Lemma 1.6. *Let $\mathcal{S} = (S, +, \cdot, 0, 1)$ be a semiring.*

(i) *$\mathcal{S}$ is idempotent if and only if there exist positive integers p and s with $s \geqslant 2$ such that $x^{p+1} = x^p$ and $x^s = x$ for all $x \in S$.*

(ii) *$\mathcal{S}$ is idempotent and of characteristic 2 if and only if it is a unitary Boolean ring.*

Proof. (i) The necessity of the conditions is clear. Conversely, assume the conditions to hold. Let $a \in S$. Induction on k yields $a^{s^k} = a$ for all positive integers k. Let n be a positive integer with $s^n \geqslant p$. Then we have

$$aa = a^{s^n}a = a^{s^n+1} = a^{p+1}a^{s^n-p} = a^p a^{s^n-p} = a^{s^n} = a.$$

(ii) If $\mathcal{S}$ is a unitary Boolean ring then it is an idempotent semiring of characteristic 2. If, conversely, $\mathcal{S}$ is an idempotent semiring of characteristic 2 then the reduct $(S, +, 0)$ is an involutory Abelian group and hence $\mathcal{S}$ is a ring, i.e., a Boolean ring. $\square$

Remark 1.7. For rings, the condition $x^s = x$ in (i) can be dropped (cf. [1]). This is not the case for semirings since the nonidempotent semiring $(\{0, a, 1\}, +, \cdot, 0, 1)$ defined by

$+$	0	a	1
0	0	a	1
a	a	a	1
1	1	1	1

and

$\cdot$	0	a	1
0	0	0	0
a	0	0	a
1	0	a	1

satisfies $x^3 = x^2$. Moreover, the condition $x^{p+1} = x^p$ in (i) cannot be dropped either (not even for rings) since the three-element field is nonidempotent and satisfies $x^3 = x$.

An example of a non-commutative idempotent semiring is the following

Example 1.8. It can be easily checked that the semiring consisting of the five matrices

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

over the two-element lattice $\{0, 1\}$ (considered as a semiring) is an idempotent semiring. Because of

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

it is not commutative.

2. Structure of idempotent semirings

Since unitary Boolean rings and bounded distributive lattices are important examples of idempotent semirings, we are interested in the characterization of them among idempotent semirings. Although one simple characterization of unitary Boolean rings is given in Lemma 1.6 (ii), we are going to get a bit more sophisticated one. First, we characterize bounded distributive lattices as follows:

Theorem 2.1. *Let $\mathcal{S} = (S, +, \cdot, 0, 1)$ be a semiring. Then $\mathcal{S}$ is a bounded distributive lattice if and only if $\mathcal{S}$ is commutative, simple and idempotent.*

Proof. The necessity of the conditions is clear. Conversely, assume the conditions to hold. Then $(S, +)$ and $(S, \cdot)$ are commutative semigroups. Let $a, b \in S$. Then

$$(a + b)a = aa + ba = a + ba = 1a + ba = (1 + b)a = (b + 1)a = 1a = a$$

and

$$ab + a = ab + a1 = a(b + 1) = a1 = a.$$

Hence the absorption laws hold and therefore $(S, +, \cdot)$ is a lattice. Moreover, $0 + a = a$ and $a + 1 = 1$, i.e., $0 \leqslant a \leqslant 1$. Hence $\mathcal{S}$ is a bounded lattice. Since '$\cdot$' is distributive with respect to '$+$', $\mathcal{S}$ is a bounded distributive lattice. $\square$

Next we characterize unitary Boolean rings as certain semirings.

Theorem 2.2. *Let $\mathcal{S} = (S, +, \cdot, 0, 1)$ be a semiring. Then $\mathcal{S}$ is a unitary Boolean ring if and only if there exist positive integers p, s and t such that $x^{p+1} = x^p$ and $x^s(x+1)^t = 0$ for all $x \in S$.*

P r o o f. The necessity of the conditions is clear. Conversely, assume the conditions to hold. We have

$$2^t = 1^s(1+1)^t = 0. \tag{2.1}$$

Let k be a positive integer with $k \equiv -1 \pmod{2^t}$. If p is odd then

$$k^p 2^t - k^p + k^{p+1} \equiv -(-1)^p + (-1)^{p+1} = 2 \pmod{2^t}$$

and hence there exists a non-negative integer u with $k^p 2^t - k^p + k^{p+1} = u2^t + 2$. Thus, using this and (2.1), we compute

$$2 = u2^t + 2 = (k^p 2^t - k^p) + k^{p+1} = (k^p 2^t - k^p) + k^p = k^p 2^t = 0.$$

If p is even then $p+1$ is odd and $x^{(p+1)+1} = x^{p+1}$ for all $x \in S$. Let $a \in S$. Then in any case $a + a = a1 + a1 = a(1+1) = a0 = 0$, i.e., $\mathcal{S}$ is a unitary ring of characteristic 2 satisfying $x^{p+1} = x^p$ for some positive integer p and all $x \in S$. According to Theorem 4 in [1] and Lemma 1.6 (ii), $\mathcal{S}$ is a unitary Boolean ring. $\square$

Finally, we consider Boolean subrings of idempotent semirings.

Definition 2.3. By a *Boolean subring* of a semiring $\mathcal{S} = (S, +, \cdot, 0, 1)$ we mean a Boolean subring of $(S, +, \cdot)$.

Let $\mathcal{S} = (S, +, \cdot, 0, 1)$ be an idempotent semiring. We can ask when does it contain a Boolean subring. Of course, $\mathcal{S}$ contains the trivial Boolean subring $(\{0\}, +, \cdot)$ (for which 0 is also the unit element). However, we are interested in the existence of maximal Boolean subrings of $\mathcal{S}$. We can state the following

Theorem 2.4. *Let $\mathcal{S} = (S, +, \cdot, 0, 1)$ be an idempotent semiring and put $B := \{x \in S;\ x + x = 0\}$. Then the union of the Boolean subrings of $\mathcal{S}$ is the Boolean subring $(B, +, \cdot)$ of $\mathcal{S}$. Moreover, $\mathcal{S}$ is a Boolean ring if and only if it contains a Boolean subring containing* 1.

P r o o f. Let $a, b \in S$. It is evident that B is closed under addition and $0 \in B$. If $a, b \in B$ then $ab + ab = a(b + b) = a0 = 0$ and hence $ab \in B$. Therefore $(B, +, \cdot)$ is a subalgebra of $(S, +, \cdot)$. Since $(B, +)$ is an involutory Abelian group, $(B, +, \cdot)$ is a subring of $(S, +, \cdot)$, i.e., a Boolean subring of $(S, +, \cdot, 0, 1)$. It is evident that this subring is the greatest Boolean subring of $(S, +, \cdot, 0, 1)$. If $\mathcal{S}$ contains a Boolean subring $(R, +, \cdot)$ containing 1 then $1+1 = 0$. Hence $a+a = a1+a1 = a(1+1) = a0 = 0$ for each $a \in S$ and, by Lemma 1.6 (ii), $(S, +, \cdot)$ is a Boolean ring. The converse statement is clear. $\square$

Of course, not every commutative idempotent semiring is either a unitary Boolean ring or a bounded distributive lattice, see the following

Example 2.5. If $\mathbb{Z}_2 = (\mathbb{Z}_2, +, \cdot, 0, 1)$ denotes the ring of residue classes of the integers modulo 2 and $\mathcal{L} = (L, \vee, \wedge, 0, 1)$ is a bounded distributive lattice with $|L| > 1$ then $\mathcal{S} := \mathbb{Z}_2 \times \mathcal{L}$ is a commutative idempotent semiring which is neither a ring, since $(0,1) + (0,0) = (0,1) = (0,1) + (0,1)$ and $(0,0) \neq (0,1)$, nor a lattice, since $(1,0) + (1,0) = (0,0) \neq (1,0)$. According to Theorem 2.4, $(\{(0,0),(1,0)\}, +, \cdot)$ is the greatest Boolean subring of $\mathcal{S}$.

3. Varieties of enriched semirings

In [3] and [7], D. J. Clouse and F. Guzmán introduced another generalization of unitary Boolean rings, the so-called Boolean semirings (see also [4]). In the terminology adopted in our paper, by a Boolean semiring we mean an idempotent semiring satisfying the additional identity

$$1 + x + x = 1.$$

Of course, both the unitary Boolean rings and the bounded distributive lattices satisfy this identity. The idempotent semiring of Example 1.4 is even commutative but it does not satisfy this identity since $1+a+a = a \neq 1$ and hence it is not Boolean. As shown in [7], Theorem 1.6, the variety of Boolean semirings is a minimal cover of the variety of unitary Boolean rings and of the variety of bounded distributive lattices. For idempotent semirings, the situation is not so simple. For example, the commutative idempotent semiring of Example 1.4 is neither a unitary Boolean ring nor a bounded distributive lattice and, moreover, it is not isomorphic to a direct product of the semirings mentioned because it is directly indecomposable (since it has just three elements). Hence, in order to study varieties of idempotent semirings, it can be of advantage to use a bit more general concept which we call an enriched semiring.

Definition 3.1. An *enriched semiring* is an algebra $\mathcal{S} = (S, +, \cdot, \circ, 0, 1)$ of type $(2,2,2,0,0)$ such that its reduct $(S, +, \cdot, 0, 1)$ is a semiring. An *enriched unitary Boolean ring* is an algebra $\mathcal{B} = (B, +, \cdot, +, 0, 1)$ where $(B, +, \cdot, 0, 1)$ is a unitary Boolean ring. An *enriched bounded distributive lattice* is an algebra $\mathcal{D} = (D, \vee, \wedge, \wedge, 0, 1)$ where $(D, \vee, \wedge, 0, 1)$ is a bounded distributive lattice.

Hence $\mathcal{B}$ is an enriched semiring where $\circ = +$ and $\mathcal{D}$ is an enriched semiring where $\circ = \wedge$.

In what follows, denote by $\mathbf{B}$, $\mathbf{D}$, $\mathbf{C}$, and $\mathbf{V}$, the variety of enriched unitary Boolean rings, enriched bounded distributive lattices, enriched commutative idempotent semirings, and enriched idempotent semirings, respectively. Of course, $\mathbf{B}\cup\mathbf{D} \subseteq \mathbf{C} \subseteq \mathbf{V}$, but $\mathbf{C} \neq \mathbf{V}$ (see Example 1.8) and $\mathbf{B}\cup\mathbf{D} \neq \mathbf{C}$ (see Example 2.5).

In order to describe $\mathbf{B}\vee\mathbf{D}$ we recall the following

Definition 3.2. Let $\mathbf{V}_1$ and $\mathbf{V}_2$ be varieties of the same type. We say that $\mathbf{V}_1$ and $\mathbf{V}_2$ are *independent* if there exists a binary term t in their common type such that $\mathbf{V}_1$ satisfies the identity $t(x, y) = x$ and $\mathbf{V}_2$ satisfies the identity $t(x, y) = y$. The term $t(x, y)$ is called an *independence term* for $\mathbf{V}_1$ and $\mathbf{V}_2$. If $\mathbf{V}_1$ and $\mathbf{V}_2$ are independent subvarieties of a variety $\mathbf{W}$ then their join $\mathbf{V}_1 \vee \mathbf{V}_2$ in the lattice of subvarieties of $\mathbf{W}$ is called an *independent join*.

The following assertions are included in [6]:

Proposition 3.3. *Let $\mathbf{W}$ be the independent join of its subvarieties $\mathbf{V}_1$ and $\mathbf{V}_2$. Then* (i) *and* (ii) *hold:*

- (i) *Every algebra $\mathcal{A} \in \mathbf{W}$ is isomorphic to a direct product $\mathcal{A}_1 \times \mathcal{A}_2$ where $\mathcal{A}_1 \in \mathbf{V}_1$ and $\mathcal{A}_2 \in \mathbf{V}_2$. These algebras $\mathcal{A}_1$ and $\mathcal{A}_2$ are determined uniquely up to isomorphism.*
- (ii) *If $\mathcal{B}$ is a subalgebra of $\mathcal{A} = \mathcal{A}_1 \times \mathcal{A}_2$ with $\mathcal{A}_1 \in \mathbf{V}_1$ and $\mathcal{A}_2 \in \mathbf{V}_2$ then there exist subalgebras $\mathcal{B}_1$ of $\mathcal{A}_1$ and $\mathcal{B}_2$ of $\mathcal{A}_2$ such that $\mathcal{B} = \mathcal{B}_1 \times \mathcal{B}_2$.*

Using the fact that every unitary Boolean ring is commutative and of characteristic 2 we can easily prove the following theorem.

Theorem 3.4. *The varieties $\mathbf{B}$ and $\mathbf{D}$ are independent and the independence term is*

$$t(x, y) = y + (y \circ x). \tag{3.1}$$

Proof. Consider the term $t(x, y) := y + (y \circ x)$. Then in $\mathbf{B}$ we have $t(x, y) = y + (y + x) = (y + y) + x = 0 + x = x$ and in $\mathbf{D}$ we have $t(x, y) = y \vee (y \wedge x) = y$ proving independence of $\mathbf{B}$ and $\mathbf{D}$. □

Theorem 3.5. *Within $\mathbf{C}$ the variety $\mathbf{B}\vee\mathbf{D}$ is fully determined by the identities*

$$x + x = t(0, x),$$
$$1 + x = 1 + t(x, 1)$$

where $t(x, y)$ denotes the above independence term (3.1) *for $\mathbf{B}$ and $\mathbf{D}$.*

P r o o f. Let us first note that within $\mathbf{V}$ the variety $\mathbf{B}$ is fully determined by the identity $x+x=0$ (which witnesses that each member of $\mathbf{B}$ is an enriched ring) according to Lemma 1.6 (ii), and within $\mathbf{V}$ the variety $\mathbf{D}$ is fully determined by the identities $x+1=1$ and $xy=yx$ according to Theorem 2.1. Since according to Proposition 3.3 (i) every enriched idempotent semiring belonging to $\mathbf{B}\vee\mathbf{D}$ is isomorphic to a direct product of an enriched Boolean ring and an enriched bounded distributive lattice we can apply the term (3.1). If $\mathcal{A}\in\mathbf{B}\vee\mathbf{D}$ then according to Proposition 3.3 (i) we have $\mathcal{A}\cong\mathcal{A}_1\times\mathcal{A}_2$ with $\mathcal{A}_1\in\mathbf{B}$ and $\mathcal{A}_2\in\mathbf{D}$. For $\mathcal{A}_1$ we have

$$\begin{aligned} t(0,x)&=0,\\ 1+t(x,1)&=1+x, \end{aligned}$$

whereas for $\mathcal{A}_2$ we have

$$\begin{aligned} t(0,x)&=x,\\ 1+t(x,1)&=1+1=1\vee 1=1. \end{aligned}$$

The rest follows from Lemma 1.6 (ii) and Theorem 2.1.

□

References

[1] *I. Chajda, F. Švrček*: Lattice-like structures derived from rings. Contributions to General Algebra 20, Proceedings of the 81st Workshop on General Algebra Salzburg, Austria (J. Czermak et al., eds.). Johannes Heyn, Klagenfurt, 2012, pp. 11–18. zbl MR

[2] *I. Chajda, F. Švrček*: The rings which are Boolean. Discuss. Math., Gen. Algebra Appl. *31* (2011), 175–184. zbl MR

[3] *D. J. Clouse, F. Guzmán*: The dual geometry of Boolean semirings. Algebra Univers. *64* (2010), 231–249. zbl MR

[4] *J. S. Golan*: Semirings and Affine Equations over Them: Theory and Applications. Mathematics and Its Applications 556, Kluwer Academic Publishers, Dordrecht, 2003. zbl MR

[5] *J. S. Golan*: Semirings and Their Applications. Kluwer Academic Publishers, Dordrecht, 1999. zbl MR

[6] *G. Grätzer, H. Lakser, J. Płonka*: Joins and direct products of equational classes. Can. Math. Bull. *12* (1969), 741–744. zbl MR

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

[8] *P. Jedlička*: The rings which are Boolean, Part II. Acta Univ. Carol., Math. Phys. *53* (2012), 73–75. zbl MR

Authors' addresses: *Ivan Chajda*, Department of Algebra and Geometry, Faculty of Science, Palacký University Olomouc, 17. listopadu 12, 771 46 Olomouc, Czech Republic, e-mail: `ivan.chajda@upol.cz`; *Helmut Länger*, Institute of Discrete Mathematics and Geometry, Faculty of Mathematics and Geoinformation, Vienna University of Technology, Wiedner Hauptstraße 8-10, 1040 Wien, Austria, e-mail: `helmut.laenger@tuwien.ac.at`; *Filip Švrček*, Department of Algebra and Geometry, Faculty of Science, Palacký University Olomouc, 17. listopadu 12, 771 46 Olomouc, Czech Republic, e-mail: `filip.svrcek@upol.cz`.