Czechoslovak Mathematical Journal

Ivan Chajda; M. Kotrle

Boolean semirings

Czechoslovak Mathematical Journal, Vol. 44 (1994), No. 4, 763–767

Persistent URL: http://dml.cz/dmlcz/128495

Czechoslovak Mathematical Journal, 44 (119) 1994, Praha

BOOLEAN SEMIRINGS

I. CHAJDA, M. KOTRLE, Olomouc

(Received January 13, 1993)

By a *semiring* we mean an algebra $A = (A; +, \cdot, 0)$ with two associative binary operations $+$, $\cdot$ where $+$ is, moreover, commutative, and with a nullary operation 0 satisfying the distributive laws, i.e.

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (b + c) \cdot a = b \cdot a + c \cdot a$$

and $0 \cdot a = 0$ for each $a \in A$.

A semiring $A = (A; +, \cdot, 0)$ is called *commutative* if the operation $\cdot$ is commutative. An element $1 \in A$ is called a *weak unit* if $(a \cdot b) \cdot 1 = a \cdot b$ for each a, $b \in A$. If 1 is a distinguished weak unit of a semiring A, then A is called a *unitary semiring.*

For a semiring $A = (A; +, \cdot, 0)$, denote by $S(A) = \{a + b; a \in A, b \in B\}$ the so called *skeleton* of A. It is immediately clear that $0 \in S(A)$ since

$$0 + 0 = 0 \cdot a + 0 \cdot a = 0 \cdot (a + a) = 0 \quad \text{for each } a \in A.$$

A semiring $A = (A; +, \cdot, 0)$ is *skeletal* if $(S(A), +)$ is a group with the unit 0.

Hence, if a semiring $A = (A; +, \cdot, 0)$ is skeletal then $(S(A); +, \cdot, 0)$ is the ring which is a subsemiring of A.

Let $A = (A; +, \cdot, 0)$ be a semiring. If there exists the least integer $n > 0$ such that $a + \ldots + a = 0$ (n arguments on the left hand side) for each $a \in A$, it is called the *characteristic of* A; we denote it by $\operatorname{char} A$.

An element a of a semiring A is called an *idempotent* if $a \cdot a = a$.

Definition 1. By a *Boolean semiring* we mean a unitary skeletal semiring $A = (A; +, \cdot, 0)$ whose weak unit 1 is an idempotent of A and which satisfies the following two conditions for each a, $b \in A$:

(1) $a \cdot a = a + 0$;

(2) $a \cdot b + 0 = a \cdot b$.

Lemma 1. *Let $A = (A; +, \cdot, 0)$ be a Boolean semiring. Then:*

(a) $1 + 0 = 1$;

(b) $(a \cdot a) \cdot b = a \cdot b$ *for each* $a, b \in A$;

(c) $a \cdot a = a \cdot 1$ *for each* $a \in A$;

(d) *if* $c \in A$ *is an idempotent then* $c \cdot 1 = c$.

Proof. (a) Since 1 is an idempotent of A, we have $1 + 0 = 1 \cdot 1 + 0 = 1 \cdot 1 = 1$ by (2) of Definition 1.

(b) By (1), (2) and the distributivity laws, we obtain $(a \cdot a) \cdot b = (a + 0) \cdot b = a \cdot b + 0 \cdot b = a \cdot b + 0 = a \cdot b$.

(c) By (1) and (2) we immediately infer $a \cdot a = (a \cdot a) \cdot 1 = (a + 0) \cdot 1 = a \cdot 1 + 0 \cdot 1 = a \cdot 1 + 0 = a \cdot 1$.

(d) If $c \in A$ is an idempotent, then (c) implies $c = c \cdot c = c \cdot 1$. □

Theorem 1. *Every Boolean semiring A is commutative,* char $A = 2$ *and $S(A)$ is equal to the set of all idempotents of A.*

Proof. (i) Let $a \in A$. Then $a + a \in S(A)$, thus $a + a = (a + a) + 0 = (a + a) \cdot (a + a) = a \cdot a + a \cdot a + a \cdot a + a \cdot a = (a + 0) + (a + 0) + (a + 0) + (a + 0) = (a + a) + (a + a) + 0 = (a + a) + (a + a)$. Since $S(A)$ is a group, we have $0 = a + a$ which proves $\operatorname{char} A = 2$.

(ii) If $a, b \in A$ then $a + b \in S(A)$ whence $a + b = (a + b) + 0 = (a + b) \cdot (a + b) = a \cdot a + a \cdot b + b \cdot a + b \cdot b = (a + 0) + a \cdot b + b \cdot a + (b + 0) = a + b + a \cdot b + b \cdot a$. Since $S(A)$ is a group, we have $0 = a \cdot b + b \cdot a$, thus by (2)

$$b \cdot a = b \cdot a + 0 = 0 + b \cdot a = a \cdot b + b \cdot a + b \cdot a = a \cdot b + 0 = a \cdot b$$

in spite of $\operatorname{char} A = 2$. Hence A is commutative.

(iii) Let $a \in S(A)$. Then $a = b + c$ for some $b, c \in A$. Hence $a \cdot a = (b + c) \cdot (b + c) = b \cdot b + b \cdot c + c \cdot b + c \cdot c = (b + 0) + b \cdot c + b \cdot c + (c + 0) = (b + c) + 0 = b + c = a$, thus a is an idempotent of A.

Conversely, let a be an idempotent of A. Then, by (1), we obtain $a = a \cdot a = a + 0 \in S(A)$. □

The meaning of a Boolean semiring for q-algebras is the same as that of Boolean rings for Boolean algebras, see e.g. [1]. Recall that an algebra $A = (A; \vee, \wedge, ', 0, 1)$ of the type $(2, 2, 1, 0, 0)$ is a *q-algebra*, see [2], [3] (or the *algebra of quasiordered logic* in the terminology of [3]), if the following axioms are satisfied:

associativity: $a \vee (b \vee c) = (a \vee b) \vee c \quad a \wedge (b \wedge c) = (a \wedge b) \wedge c$

commutativity: $a \vee b = b \vee a \quad a \wedge b = b \wedge a$

weak absorption: $a \vee (b \wedge a) = a \vee a \quad a \wedge (b \vee a) = a \wedge a$

weak idempotence: $a \vee (b \vee b) = a \vee b \quad a \wedge (b \wedge b) = a \wedge b$

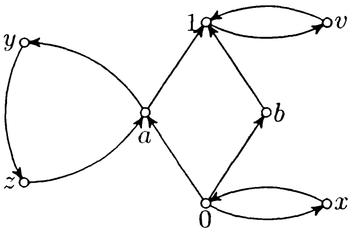
equalization: $a \vee a = a \wedge a$

distributivity: $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

complementation: $a \vee a' = 1$ and $a \wedge a' = 0$

$0 - 1$ *axioms*: $a \vee 1 = 1$ and $a \wedge 0 = 0$.

Evidently, every Boolean algebra is a q-algebra but not vice versa, see [3]. An example of a q-algebra A which is not a Boolean algebra is in Fig. 1.



(0, a, b, 1 are idempotents of A and the operations $\vee$, $\wedge$, $'$ are given in the tables)

$\vee$	0	x	a	y	z	b	1	v
0	0	0	a	a	a	b	1	1
x	0	0	a	a	a	b	1	1
a	a	a	a	a	a	1	1	1
y	a	a	a	a	a	1	1	1
z	a	a	a	a	a	1	1	1
b	b	b	1	1	1	b	1	1
1	1	1	1	1	1	1	1	1
v	1	1	1	1	1	1	1	1

$\wedge$	0	x	a	y	z	b	1	v
0	0	0	0	0	0	0	0	0
x	0	0	0	0	0	0	0	0
a	0	0	a	a	a	0	a	a
y	0	0	a	a	a	0	a	a
z	0	0	a	a	a	0	a	a
b	0	0	0	0	0	b	b	b
1	0	0	a	a	a	b	1	1
v	0	0	a	a	a	b	1	1

	0	x	a	y	z	b	1	v
$'$	1	1	b	b	b	a	0	0

Fig. 1.

Theorem 2. *Let* $A = (A; \vee, \wedge, ', 0, 1)$ *be a q-algebra. Put* $x + y = (x \wedge y') \vee (x' \wedge y)$ *and* $x \cdot y = x \wedge y$. *Then* $(A; +, \cdot, 0)$ *is a Boolean semiring (where* 1 *is the weak unit).*

Proof. Commutativity and associativity of $+$, $\cdot$ is a direct consequence of these properties for $\vee$ and $\wedge$. Also the distributivity laws can be proved quite analogously as for Boolean rings [1]. Clearly $0 \cdot a = 0 \wedge a = 0$. Let us prove the remaining axioms of Boolean semirings. By weak idempotence, we infer $(a \cdot b) \cdot (a \cdot b) = (a \cdot a) \cdot (b \cdot b) = (a \wedge a) \wedge (b \wedge b) = (a \wedge a) \wedge b = a \wedge b = a \cdot b$, thus $a \cdot b$ is an idempotent of $(A; +, \cdot, 0)$ for each $a, b \in A$. Since $a \cdot b = a \wedge b$ is an idempotent, we have $(a \cdot b) \cdot 1 = (a \wedge b) \wedge 1 = a \wedge b = a \cdot b$, thus 1 is a weak unit and $(A; +, \cdot, 0)$ is a unitary semiring.

It is easy to see that if x, $y \in S(A)$, i.e. $x = a + b$ and $y = c + d$ for some a, b, c, d from A, then also $x + y \in S(A)$. Moreover, $x + 0 = (x \wedge 0') \vee (x' \wedge 0) = (x \wedge 1) \vee (x' \wedge 0) = (x \wedge 1) \vee 0$.

Since $x \wedge 1$ is an idempotent of $(A; \vee, \wedge, ', 0, 1)$ (see e.g. [3], [4]), we have $x + 0 = x \wedge 1$. Since $x = a + b$, it is also an idempotent of the q-algebra whence $x \wedge 1 = x$ (see [3]), thus $x + 0 = x$.

Further, $x + x = (x \wedge x') \vee (x \wedge x') = 0 \vee 0 = 0$, thus $(S(A); +)$ is a group with the unit 0, i.e. the semiring $(A; +, \cdot, 0)$ is also skeletal.

By 0–1 axioms and equalization, the weak unit 1 is an idempotent of $(A; +, \cdot, 0)$. Prove (1) and (2) of Definition 1. Let $a \in A$. By [3], $a + 0$ is an idempotent of the q-algebra, thus $a+0 = (a+0) \wedge (a+0) = (a+0) \cdot (a+0) = a \cdot a + 0 \cdot a + a \cdot 0 + 0 \cdot 0 = a \cdot a$. If a, $b \in A$ then $a \cdot b + 0 = (a \cdot b \wedge 1) \vee \big((a \cdot b)' \wedge 0\big) = a \cdot b \wedge 1$. Since $a \cdot b = a \wedge b$ is an idempotent of the q-algebra, we have $a \wedge b \wedge 1 = a \wedge b$, thus $a \cdot b + 0 = a \cdot b$, which proves that $(A; +, \cdot, 0)$ is a Boolean semiring. □

Theorem 3. *Let $A = (A; +, \cdot, 0)$ be a Boolean semiring with the weak unit 1. Introduce $a \vee b = a + b + (a \cdot b)$, $a \wedge b = a \cdot b$, $a' = 1 + a$. Then $(A; \vee, \wedge, ', 0, 1)$ is a q-algebra.*

P r o o f. Commutativity of $\vee$, $\wedge$ and associativity of $\wedge$ follow directly from the commutativity and associativity of $+$, $\cdot$. Prove associativity of $\vee$:

$$a \vee (b \vee c) = a + (b + c + b \cdot c) + a \cdot (b + c + b \cdot c) = a + b + a \cdot b + c + c \cdot (a + b + a \cdot b) = (a \vee b) \vee c.$$

Weak absorption:

$$a \vee (b \wedge a) = a + b \cdot a + a \cdot (b \cdot a) = a + b \cdot a + (a \cdot a) \cdot b = a + b \cdot a + b \cdot a.$$

Since char $A = 2$, we obtain $a \vee (b \wedge a) = a + 0 = a \cdot a = a \vee a$ by (1) of Definition 1. Further, by (1), (2) of Definition 1 and by (b) of Lemma 1:

$$\begin{aligned} a \wedge (b \vee a) &= a \cdot (b + a + b \cdot a) = a \cdot b + a \cdot a + a \cdot b \cdot a = a \cdot b + a \cdot b + a \cdot a \\ &= 0 + a \cdot a = a \cdot a = a \wedge a. \end{aligned}$$

Weak idempotence:

$$\begin{aligned} a \vee (b \vee b) &= a + b + b + b \cdot b + a \cdot (b + b + b \cdot b) = a + b \cdot b + a \cdot (b \cdot b) \\ &= a + (b + 0) + a \cdot b = a + b + a \cdot b = a \vee b, \\ a \wedge (b \wedge b) &= a \cdot (b \cdot b) = a \cdot b = a \wedge b. \end{aligned}$$

Distributivity:

$$\begin{aligned}(a \vee b) \wedge (a \vee c) &= (a+b+a\cdot b)\cdot(a+c+a\cdot c)\\ &= a\cdot a + a\cdot c + (a\cdot a)\cdot c + b\cdot a + b\cdot c + b\cdot a\cdot c + a\cdot b\cdot a + b\cdot a\cdot c\\ &\quad + a\cdot b\cdot a + a\cdot b\cdot c + (a\cdot b)\cdot(a\cdot c)\\ &= a\cdot a + b\cdot c + a\cdot b\cdot c = (a+0) + b\cdot c + a\cdot b\cdot c\\ &= a + b\cdot c + a\cdot b\cdot c = a\vee(b\wedge c).\end{aligned}$$

Equalization:

$$a\vee a = a+a+a\cdot a = a\cdot a = a\wedge a.$$

Complementation:

$$a\vee a' = a + (1+a) + a(1+a) = 1 + a\cdot 1 + a\cdot a = 1 + a\cdot a + a\cdot a = 1$$

(by using (c) of Lemma 1),

$$a\wedge a' = a\cdot(1+a) = a\cdot 1 + a\cdot a = a\cdot a + a\cdot a = 0.$$

0–1 axioms:

$$a\wedge 0 = 0\wedge a = 0\cdot a = 0,$$

$a\vee 1 = a+1+a\cdot 1$. Since $a+1\in S(A)$, we have $a+1=(a+1)\cdot(a+1)$ by Theorem 1, and, by (c) of Lemma 1, we infer $a+1=(a+1)\cdot(a+1)=(a+1)\cdot 1$. Thus

$$a\vee 1 = (a+1)\cdot 1 + a\cdot 1 = a\cdot 1 + 1\cdot 1 + a\cdot 1 = 1\cdot 1 = 1\wedge 1 = 1$$

since 1 is an idempotent of the q-algebra, see [3]. □

Let A be a q-algebra. Denote by $\mathscr{B}(A)$ the Boolean semiring derived from A by Theorem 2. Let B be a Boolean semiring. Denote by $\mathscr{A}(B)$ the q-algebra obtained from B by Theorem 3. The proof of the following statement is straightforward and hence omitted:

Theorem 4. *For any Boolean semiring B, $\mathscr{B}(\mathscr{A}(B))$ is isomorphic to B. For any q-algebra A, $\mathscr{A}(\mathscr{B}(A))$ is isomorphic to A.*

References

[1] *G. Birkhoff*: Lattice Theory. Publ. AMS (3rd edition), Providence (USA), 1967.

[2] *I. Chajda*: Lattices in quasiordered sets. Acta Univ. Palackiensis Olomouc *31* (1992), 6–12.

[3] *I. Chajda*: Algebra of quasiordered logic. Math. Bohemica, submitted.

[4] *I. Chajda, M. Kotrle*: Subdirectly irreducible and congruence distributive q-lattices. Czech. Math. J., to appear 1993.

Authors' address: Katedra algebry a geometrie, PF PU Olomouc, Tomkova 38, 779 00 Olomouc, Czech Republic.