Discussiones Mathematicae
General Algebra and Applications 31 (2011) 175–184

THE RINGS WHICH ARE BOOLEAN*

Ivan Chajda

Department of Algebra and Geometry
Palacký University Olomouc, 17. listopadu 12
771 46 Olomouc, Czech Republic
e-mail: ivan.chajda@upol.cz

and

Filip Švrček

Department of Algebra and Geometry
Palacký University Olomouc, 17. listopadu 12
771 46 Olomouc, Czech Republic
e-mail: filip.svrcek@upol.cz

Abstract

We study unitary rings of characteristic 2 satisfying identity $x^p = x$ for some natural number p. We characterize several infinite families of these rings which are Boolean, i.e., every element is idempotent. For example, it is in the case if $p = 2^n - 2$ or $p = 2^n - 5$ or $p = 2^n + 1$ for a suitable natural number n. Some other (more general) cases are solved for p expressed in the form $2^q + 2m + 1$ or $2^q + 2m$ where q is a natural number and $m \in \{1, 2, \ldots, 2^q - 1\}$.

Keywords: Boolean ring, unitary ring, characteristic 2.

2010 Mathematics Subject Classification: 06E20, 16R40.

A ring $\mathcal{R} = (R; +, \cdot)$ is called *Boolean* if every its element is idempotent, i.e., if $\mathcal{R}$ satisfies the identity $x^2 = x$. Boolean rings play an important role in propositional logic and in theoretical computer science as well as in lattice theory, see e.g. [2]. In particular, every unitary Boolean ring

*This work is supported by the Research and Development Council of the Czech Government via the project MSM6198959214.

can be converted into a Boolean algebra and vice versa. This motivated us to classify Boolean rings among rings with restricted powers, i.e., rings satisfying the identity $x^p = x$ for a natural number $p > 2$.

A sample result is the following.

Lemma 1. *Let $\mathcal{R} = (R; +, \cdot)$ be a ring satisfying the identity $x^p = x$ for some integer $p \geq 2$. The following are equivalent:*

(a) *$\mathcal{R}$ is Boolean;*

(b) *$\mathcal{R}$ satisfies the identity $x^{q+1} = x^q$ for some natural number $q \leq p$.*

Proof. (a) $\Rightarrow$ (b): It is evident, because $x^2 = x$ implies $x^{q+1} = x^q$ for every natural number q.

(b) $\Rightarrow$ (a): Then $\mathcal{R}$ satisfies also $x^{p+1} = x^p$ and hence

$$x^2 = x \cdot x = x \cdot x^p = x^{p+1} = x^p = x,$$

thus $\mathcal{R}$ is Boolean. ■

It is an easy consequence of $x^2 = x$ that every Boolean ring is of characteristic 2, i.e., it satisfies the identity $x + x = 0$. Due to this fact, we restrict our treaty only to rings of characteristic 2.

A ring $\mathcal{R} = (R; +, \cdot)$ is called *unitary* if it contains a unit, i.e., an element denoted by 1 such that $x \cdot 1 = x = 1 \cdot x$ for each $x \in R$. For further information and notation on rings, the reader is refered to basic monographs [1, 4–6].

As a motivation, we can serve with the following two particular cases.

Lemma 2. *Let $\mathcal{R} = (R; +, \cdot)$ be a unitary ring of characteristic 2 satisfying the identity $x^3 = x$. Then $\mathcal{R}$ is Boolean.*

Proof. Every element of $\mathcal{R}$ can be written in the form $x + 1$ because $x = (x + 1) + 1$, due to the fact that $\mathcal{R}$ is unitary and of characteristic 2. Hence, we get

$$\begin{aligned} 1 + x = (1 + x)^3 &= (1 + x) \cdot (1 + x)^2 = (1 + x) \cdot (1 + x^2) \\ &= 1 + x + x^3 + x^2 = 1 + x + x + x^2 = 1 + x^2 \end{aligned}$$

whence $x = x^2$ proving that $\mathcal{R}$ is Boolean. ■

On the contrary, we can show that there exists a unitary ring of characteristic 2 satisfying the identity $x^4 = x$ which is not Boolean. In fact, we can show the whole infinite family of identities $x^p = x$, i.e., an infinite set of natural numbers p such that a unitary ring of characteristic 2 satisfying the identity $x^p = x$ need not be Boolean, see the following.

Lemma 3. *For each natural number k there exists a unitary commutative ring of characteristic 2 satisfying the identity $x^{3k+1} = x$ which is not Boolean.*

Proof. Consider the four-element ring $\mathcal{R}$ whose operations $+$ and $\cdot$ are determined by the tables

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

It is an immediate reflexion that $\mathcal{R}$ is unitary, commutative and of characteristic 2. Moreover, $\mathcal{R}$ satisfies $x^{3k+1} = x$ for every natural number k. However, $\mathcal{R}$ is not Boolean because e.g. $2 \cdot 2 = 3 \neq 2$. ∎

Remark 4. Let us note that if $\mathcal{R} = (R; +, \cdot)$ is a unitary ring satisfying the identity $x^p = x$ for some even p then we need not suppose that $\mathcal{R}$ is of characteristic 2. In fact, in this case there exists an element $-1 \in R$ and from the identity $x^p = x$ for $x = -1$ we get $1 = (-1)^p = -1$. Then for each $x \in R$ we have $-x = (-1) \cdot x = 1 \cdot x = x$ whence $x + x = x + (-x) = 0$.

Similarly as in Lemma 2, we can determine infinite sets of natural numbers p for which $x^p = x$ implies that $\mathcal{R}$ is Boolean.

Theorem 5. *Let $\mathcal{R} = (R; +, \cdot)$ be a unitary ring and n be a natural number.*

(i) *If $\mathcal{R}$ satisfies $x^{2^n-2} = x$ for $n > 1$ then $\mathcal{R}$ is Boolean.*

(ii) *If $\mathcal{R}$ is of characteristic 2 and satisfies $x^{2^n-5} = x$ for $n > 3$ then $\mathcal{R}$ is Boolean.*

Proof. (i): As mentioned above, $\mathcal{R}$ is of charactic 2. If $\mathcal{R}$ satisfies $x^{2^n-2} = x$ then it satisfies also $x^{2^n} = x^3$ thus by Lemma 3(a) from [3]

$$1 + x^{2^n} = (1+x)^{2^n} = (1+x)^3 = 1 + 3 \times x + 3 \times x^2 + x^3.$$

Since $x^{2^n} = x^3$, we conclude $3 \times (x + x^2) = x + x^2 = 0$, whence $x = x^2$.

(ii): If $\mathcal{R}$ satisfies $x^{2^n-5} = x$ for some natural number $n > 3$ then it satisfies also $x^{2^n} = x^6$ and therefore, by [3], Lemma 3(a),

$$\begin{aligned} 1 + x^6 = 1 + x^{2^n} &= (1+x)^{2^n} = (1+x)^6 = (1+x)^4 \cdot (1+x)^2 \\ &= (1+x^4) \cdot (1+x^2) = 1 + x^2 + x^4 + x^6 \end{aligned}$$

whence $x^2 = x^4$. This yields

$$x^3 = x^5 = x^7 = \cdots = x^{2^n-5} = x$$

and, applying Lemma 2, we conclude that $\mathcal{R}$ is Boolean. ∎

Similarly, we can also decide the following case.

Lemma 6. *Let $\mathcal{R} = (R; +, \cdot)$ be a unitary ring of characteristic 2 satisfying $x^{2^q+1} = x$ for a natural number q. Then $\mathcal{R}$ is Boolean.*

Proof. We compute

$$\begin{aligned} 1 + x = (1+x)^{2^q+1} &= (1+x) \cdot (1+x)^{2^q} = (1+x) \cdot (1 + x^{2^q}) \\ &= 1 + x + x^{2^q} + x^{2^q+1} = 1 + x + x^{2^q} + x = 1 + x^{2^q}, \end{aligned}$$

i.e., for $p = 2^q + 1$ we have $x^p = x = x^{2^q} = x^{p-1}$. By Lemma 1, $\mathcal{R}$ is Boolean. ∎

Another relative large set of odd natural numbers p, for which a unitary ring of characteristic 2 satisfying $x^p = x$ is Boolean, is discerned by the following result.

Theorem 7. *Let $\mathcal{R} = (R; +, \cdot)$ be a unitary ring of characteristic 2 satisfying $x^p = x$ where $p = 2^q + 2m + 1$ for some natural number q and $m \in \{1, 2, \dots, 2^{q-1} - 1\}$. If $2^q - 2m = 2^a + 2^b$ where a,b are integers such that $q > a > b \geq 1$ then $\mathcal{R}$ is Boolean provided $2^a - 2^b$ divides $2m$.*

Proof. Assume $p = 2^q + 2m + 1$ with $2^q - 2m = 2^a + 2^b$ for some integers q, m, a, b such that $q > a > b \geq 1$ and $m \in \{1, 2, \ldots, 2^{q-1} - 1\}$. If $2^a - 2^b$ divides $2m$ then $2m = r(2^a - 2^b)$ for some natural number r. Since $x^{2^q+2m+1} = x$, we have

$$x^{2^{q+1}} = x^{2^q+2m+1} \cdot x^{2^q-2m-1} = x \cdot x^{2^q-2m-1} = x^{2^q-2m}.$$

Hence, using [3], Lemma 3(a),

$$\begin{aligned} 1 + x^{2^q-2m} &= 1 + x^{2^{q+1}} = (1+x)^{2^{q+1}} = (1+x)^{2^q-2m} = (1+x)^{2^a+2^b} \\ &= (1+x)^{2^a} \cdot (1+x)^{2^b} = (1 + x^{2^a}) \cdot (1 + x^{2^b}) \\ &= 1 + x^{2^a} + x^{2^b} + x^{2^a+2^b} = 1 + x^{2^a} + x^{2^b} + x^{2^q-2m} \end{aligned}$$

This yields $0 = x^{2^a} + x^{2^b}$, thus $x^{2^a} = x^{2^b}$. Since $2m = r \cdot (2^a - 2^b)$ and $2^q + 2m + 1 > 2^q + 1 > 2^a$, we conclude

$$\begin{aligned} x^{2^q+1} &= x^{2^q+(2^a-2^b)+1} = \cdots = x^{2^q+r\cdot(2^a-2^b)+1} \\ &= x^{2^q+2m+1} = x^p = x. \end{aligned}$$

By Lemma 6, $\mathcal{R}$ is Boolean. ■

Corollary 8. *Let $\mathcal{R} = (R; +, \cdot)$ be a unitary ring of characteristic 2 satisfying $x^p = x$ where $p = 2^q + 2m + 1$ for some natural number q and $m \in \{1, 2, \ldots, 2^{q-1} - 1\}$. If $2^q - 2m = 2^{a+1} + 2^a$ for some integer a such that $q - 1 > a \geq 1$ then $\mathcal{R}$ is Boolean.*

Proof. If $2^q - 2m = 2^{a+1} + 2^a$ for some integers q, m, a such that $q - 1 > a \geq 1$, $m \in \{1, 2, \ldots, 2^{q-1} - 1\}$ then $2^{a+1} - 2^a = 2^a$. Thus it divides

$$2m = 2^q - 2^{a+1} - 2^a = 2^a \cdot (2^{q-a} - 3),$$

which, by Theorem 7, means that $\mathcal{R}$ is Boolean. ■

Hence, we get the sequence of numbers

$$p = 3, 5, 9, 17, 33, \ldots, \tag{S}$$

by Lemma 6, for which a unitary ring of characteristic 2 satisfying the identity $x^p = x$ is Boolean. In what follows, we will detect other natural numbers p of this property.

Remark 9. We can recognize that (ii) of Theorem 5 can be included in the cases treated in Theorem 7. Namely, if $p = 2^n - 5$ for some integer $n > 3$ then we can compute

$$p = 2^{n-1} + (2^{n-1} - 5) = 2^{n-1} + (2^{n-1} - 6) + 1.$$

Using the notation from Theorem 7 we have

$$2^q - 2m = 2^{n-1} - (2^{n-1} - 6) = 6 = 2^2 + 2^1.$$

Thus, applying Corollary 8, we obtain that $\mathcal{R}$ is Boolean. Hence, we can extend our sequence (S) with numbers

$$p = 11, 27, 59, 123, \ldots,$$

Moreover, Corollary 8 enables us to insert also numbers of the form $2^n - 11$ ($n > 4$), i.e.,

$$p = 21, 53, 117, 245, \ldots,$$

further numbers of the form $2^n - 23$ ($n > 5$), i.e.,

$$p = 41, 105, 233, 489, \ldots,$$

etc. We can generalize this approach in the following result.

Theorem 10. *Let $\mathcal{R} = (R; +, \cdot)$ be a unitary ring of characteristic 2 satisfying $x^p = x$ for some natural number p of the form $2^n - (3 \cdot 2^l - 1)$ where n, l are arbitrary natural numbers such that $n - 3 \geq l$. Then $\mathcal{R}$ is Boolean.*

Proof. If $p = 2^n - (3 \cdot 2^l - 1)$ for some natural numbers satisfying $n - 3 \geq l$ then

$$3 \cdot 2^l \leq 3 \cdot 2^{n-3} < 4 \cdot 2^{n-3} = 2^{n-1}$$

and, therefore, $p = 2^{n-1} + (2^{n-1} - 3 \cdot 2^l) + 1$. We put $q = n - 1$, $2m = 2^{n-1} - 3 \cdot 2^l$ and then obtain

$$2^q - 2m = 2^{n-1} - (2^{n-1} - 3 \cdot 2^l) = 3 \cdot 2^l = 2 \cdot 2^l + 2^l = 2^{l+1} + 2^l$$

which, due to Corollary 8, means that $\mathcal{R}$ is Boolean. ∎

In the next theorem, we will analyse the case of Theorem 7 in more details to obtain a general method how to produce sequences of p's for which $\mathcal{R}$ is Boolean.

Theorem 11. *Let $\mathcal{R} = (R; +, \cdot)$ be a unitary ring of characteristic 2 satisfying $x^p = x$ where $p = 2^q + 2m + 1$ for some natural number q and $m \in \{1, 2, \dots, 2^{q-1} - 1\}$ such that $2^q - 2m = 2^a + 2^b$ where a, b are integers satisfying $a > b \geq 1$ and, moreover, $q = (a+1) + k \cdot (a-b)$ for some nonnegative integer k. Then $\mathcal{R}$ is Boolean.*

Proof. Consider a unitary ring $\mathcal{R}$ of characteristic 2 satisfying the identity $x^p = x$ for a number p possessing the assumption. Then

$$\begin{aligned}
2m &= 2^q - 2^a - 2^b = 2^{(a+1)+k\cdot(a-b)} - 2^a - 2^b \\
&= 2^b \cdot \left(2^{(a+1)+k\cdot(a-b)-b} - 2^{a-b} - 1\right) \\
&= 2^b \cdot \left(2^{(k+1)\cdot(a-b)+1} - 2^{a-b} - 1\right) \\
&= 2^b \cdot \left(2 \cdot 2^{(k+1)\cdot(a-b)} - 2^{a-b} - 1\right) \\
&= 2^b \cdot \left[\left(\left(2^{a-b}\right)^{k+1} - 2^{a-b}\right) + \left(\left(2^{a-b}\right)^{k+1} - 1\right)\right] \\
&= 2^b \cdot \left[2^{a-b} \cdot \left(\left(2^{a-b}\right)^{k} - 1\right) + \left(\left(2^{a-b}\right)^{k+1} - 1\right)\right] \\
&= 2^b \cdot \Big[2^{a-b} \cdot \left(2^{a-b} - 1\right) \cdot \left(\left(2^{a-b}\right)^{k-1} + \dots + 2^{a-b} + 1\right) \\
&\qquad + \left(2^{a-b} - 1\right) \cdot \left(\left(2^{a-b}\right)^{k} + \dots + 2^{a-b} + 1\right)\Big] \\
&= 2^b \cdot \left(2^{a-b} - 1\right) \cdot \left(2 \cdot \left(2^{a-b}\right)^{k} + \dots + 2 \cdot 2^{a-b} + 1\right) \\
&= \left(2^a - 2^b\right) \cdot \left(2 \cdot \left(2^{a-b}\right)^{k} + \dots + 2 \cdot 2^{a-b} + 1\right).
\end{aligned}$$

Hence, $2^a - 2^b$ divides $2m$ and, by Theorem 7, $\mathcal{R}$ is Boolean. ∎

Remark 12. Theorem 11 shows us how to construct numbers p for which the unitary ring of characteristic 2 satisfying $x^p = x$ is Boolean.

It is enough to choose arbitrary integers a, b such that $a > b \geq 1$ then to take $q = (a+1) + k \cdot (a-b)$ for some nonnegative integer k and to compute $2m = 2^q - 2^a - 2^b$. Then $p = 2^q + 2m + 1$ is the number which we look for.

Example 13. If we take $a = 8$, $b = 3$ and $k = 1$, we have $q = (8+1) + 1 \cdot (8-3) = 14$ and, consequently, $2m = 2^{14} - 2^8 - 2^3 = 16120$. In fact, we have proved that the unitary ring of characteristic 2 satisfying the identity $x^{32505} = x$ is Boolean, because $32505 = 2^{14} + 16120 + 1$.

Until now, except Lemma 5(i) and partially also Lemma 3, we have dealed with unitary rings of characteristic 2 satisfying the identity $x^p = x$ only for odd natural numbers p. Further, we will discuss some cases when p is even.

It is worth noticing that we have already solved the case of unitary ring satisfying $x^{2^r} = x$ for r even. As mentioned in Remark 4, such a ring is of characteristic 2 and we can write here $2^r = 3k + 1$ for some odd natural number k. Hence, by Lemma 3, such a ring need not be Boolean.

If we consider a unitary ring satisfying $x^{2^r} = x$ for r odd then this ring is of characteristic 2 and we can express 2^r in the form $3k + 2$ for some even k. Such a ring also need not be Boolean in general, see the following example for $r = 3$.

Example 14. The eight-element ring $\mathcal{R}$ whose operations $+$ and $\cdot$ are determined by the tables

$+$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	6	7	4	5
2	2	3	0	1	5	4	7	6
3	3	2	1	0	7	6	5	4
4	4	6	5	7	0	2	1	3
5	5	7	4	6	2	0	3	1
6	6	4	7	5	1	3	0	2
7	7	5	6	4	3	1	2	0

$\cdot$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	5	3	7	1	6
3	0	3	5	6	7	1	4	2
4	0	4	3	7	5	6	2	1
5	0	5	7	1	6	2	3	4
6	0	6	1	4	2	3	7	5
7	0	7	6	2	1	4	5	3

is unitary, of characteristic 2, but it is evidently not Boolean.

We finish with the result which solves the problem for even natural numbers p which are sum of two consequently standing powers of two, i.e. for numbers

$$p = 6, 12, 24, 48, \dots \ .$$

Theorem 15. *Let $\mathcal{R} = (R; +, \cdot)$ be a unitary ring satisfying the identity $x^p = x$ where $p = 2^{a+1} + 2^a$ for some natural number a. Then $\mathcal{R}$ is Boolean.*

Proof. Consider a unitary ring $\mathcal{R}$ satisfying $x^{2^{a+1}+2^a} = x$ for some natural number a. By Remark 4, this ring is of characteristic 2 and, by [3], Lemma 3(a), we have

$$\begin{aligned} 1 + x &= (1+x)^{2^{a+1}+2^a} = (1+x)^{2^{a+1}} \cdot (1+x)^{2^a} \\ &= (1 + x^{2^{a+1}}) \cdot (1 + x^{2^a}) = 1 + x^{2^a} + x^{2^{a+1}} + x^{2^{a+1}+2^a}. \end{aligned}$$

Hence, $x^{2^{a+1}} = x^{2^a}$, and further

$$\begin{aligned} x^{2^{a+2}} &= x^{2^{a+1}+2^{a+1}} = x^{2^{a+1}} \cdot x^{2^{a+1}} = x^{2^{a+1}} \cdot x^{2^a} \\ &= x^{2^{a+1}+2^a} = x^p = x. \end{aligned}$$

From the identity $x^p = x^{2^{a+1}+2^a} = x$ we can also obtain

$$x^{2^{a+2}} = x^{(2^{a+1}+2^a)+(2^{a+1}-2^a)} = x^{1+(2^{a+1}-2^a)} = x^{1+2^a}.$$

Altogether we have $x = x^{2^{a+2}} = x^{2^a+1}$, and, by Lemma 6, $\mathcal{R}$ is Boolean. ∎

Remark 16. It is easily seen that all the numbers p which are determined by Theorem 15 are just the numbers of the form $p = 6 \cdot 2^{k-1}$ where k is an arbitrary natural number.

REFERENCES

[1] I.T. Adamson, Rings, modules and algebras (Oliver&Boyd, Edinburgh, 1971).

[2] G. Birkhoff, Lattice Theory, 3rd edition (AMS Colloq. Publ. 25, Providence, RI, 1979).

[3] I. Chajda and F. Švrček, *Lattice-like structures derived from rings*, Contributions to General Algebra, Proc. of Salzburg Conference (AAA81), J. Hayn, Klagenfurt **20** (2011), 11–18.

[4] N. Jacobson, Structure of Rings (Amer. Math. Soc., Colloq. Publ. 36 (rev. ed.), Providence, RI, 1964).

[5] J. Lambek, Lectures on Rings and Modules (Blaisdell Publ. Comp., Waltham, Massachusetts, Toronto, London, 1966).

[6] N.H. McCoy, Theory of Rings (Mainillan Comp., New York, 1964).

Received 17 February 2011
Revised 22 June 2011