Bulletin of the G.M.S., Vol. ??, No. ? (2002) ?–?
Printed in Greece

IDENTITIES WHICH IMPLY THAT A RING IS BOOLEAN

THEODOROS S. BOLIS AND ANDRZEJ SCHINZEL

The following theorem is proved: *In a unitary ring of characteristic 2 the identity $x^n = x$ implies that the ring is Boolean if and only if $n-1$ is not divisible by $2^p - 1$ for any prime p.*

Key words and phrases: Boolean ring, polynomial identity, finite field, prime number, asymptotic density, ℓ-ring

For some time problems of the sort "Show that in a unitary ring the identity $x^6 = x$, or the identity $x^{12} = x$ implies that $x^2 = x$" appeared in the literature (cf. Năstăsescu *et al.* [3], Problem A19, p. 88, Năstăsescu *et al.* [4], Problem 64, Capitolul XXI, p. 126). On the other hand, the identity $x^{10} = x$ does not imply that $x^2 = x$ as the example of the Galois field of four elements $\mathbb{F}_4$ readily shows.

This naturally gives rise to the question: In a unitary ring, for which n does the identity $x^{2n} = x$ imply that the ring is Boolean? More generally, which polynomial identities imply that a ring is Boolean?

The following results answer these questions, the second one for rings of characteristic 2, the first one completely.

Theorem 1. *In a unitary ring R of characteristic 2 the polynomial identity $f(x) = 0$ implies that the ring is Boolean if and only if $x^2 + x$ is the greatest common divisor of some polynomials $f(g_i(x))$, where $g_i \in \mathbb{F}_2[x]$ $(1 \le i \le k)$.*

Theorem 2. *In a unitary ring R of characteristic 2 the identity $x^n = x$ implies that the ring is Boolean if and only if $n - 1$ is not divisible by $2^p - 1$ for any prime p.*

Theorem 2 has already been proved by Hansen, Luh and Ye [1], as pointed out by an anonymous referee. Our proof, based on Theorem 1, is different.

Corollary 1. *In a unitary ring R the identity $x^{2n} = x$ implies that the ring is Boolean if and only if $2n - 1$ is not divisible by $2^p - 1$ for any prime p.*

Corollary 2. *The number $N(x)$ of integers $n \le x$ satisfying the conditions of Corollary 1 is*

$$C_2 x + O\left(e^{\frac{\log x}{\log\log x - 1}}\right),$$

where

$$C_2 = \prod_{p \in P}\left(1 - \frac{1}{2^p - 1}\right) \approx 0.548300831282098407677640491522 67,$$

and P denotes the set of (positive) primes.

Proof of Theorem 1. **Necessity.** Let us order all elements of $\mathbb{F}_2[x]$ in a sequence $g_1 = x, g_2, \ldots$ and put

$$d_k = GCD(f(g_1), \ldots, f(g_k)) \ (k = 1, 2, \ldots).$$

Since $d_{k+1}|d_k$ and d_1 has only finitely many divisors, there exists an integer n such that

$$d_n | f(g(x)) \quad \text{for all} \quad g \in \mathbb{F}_2[x]. \tag{1}$$

Since $f(g(0)) = f(g(1)) = 0$ for all $g \in \mathbb{F}_2[x]$, we have

$$x^2 + x | d_n.$$

If now $x^2 + x \neq d_n$, it follows that

$$x^2 + x \not\equiv 0 \mod d_n. \tag{2}$$

Take for R the residue ring of $\mathbb{F}_2[x]$ mod d_n. By (1) we have $f(a) = 0$ for every $a \in R$, while by (2) $x^2 + x \neq 0$ in R.

Sufficiency. By the Euclidean property of the g.c.d., there exist $u_i \in \mathbb{F}_2[x]$ such that

$$x^2 + x = \sum_i u_i(x) f(g_i(x)),$$

hence $f(x) = 0$ for every x in R implies $x^2 + x = 0$.

Proof of Theorem 2. **Necessity.** If $2^p - 1 | n - 1$ we have for every $g \in \mathbb{F}_2[x]$

$$g^{2^p} + g | g^n + g.$$

Since, by the property of $\mathbb{F}_{2^p}$,

$$h | g^{2^p} + g$$

for every irreducible polynomial $h \in \mathbb{F}_2[x]$ of degree p, it follows that

$$h | g^n + g$$

and, by Theorem 1, n has not the required property.

Sufficiency. Let

$$x^n + x = x(1+x)^m \prod_{i=1}^{k} f_i(x)$$

be the factorization of the polynomial $x^n + x$ into irreducible factors over $\mathbb{F}_2$, and let $d_i = \deg f_i \geq 2$ for $1 \leq i \leq k$ (k may be zero). Let p_i be a prime factor of d_i. Since the multiplicative group of $\mathbb{F}_{2^{d_i}}$ is cyclic, there exists a polynomial $g_i \in \mathbb{F}_{2^{d_i}}[x]$ such that

$$g_i \not\equiv 0 \mod f_i \tag{3}$$

and

$$g_i^e \equiv 1 \mod f_i \Rightarrow e \equiv 0 \mod d_i \tag{4}$$

Consider now the greatest common divisor d of the polynomials

$$x^n + x, (x+1)^n + x + 1, g_1^n + g_1, \dots, g_k^n + g_k.$$

Clearly $x^2 + x | d$. On the other hand

$$(x+1)^2 \not| (x+1)^n + x + 1$$

and, since $2^{p_i} - 1 | n - 1$, by (3) and (4) we obtain

$$f_i \not| g_i^n + g_i.$$

Hence $d = x^2 + x$ and, by Theorem 1, n has the required property.

Remark 1. Theorems 1 and 2 carry over to ℓ-rings (for definition see [2], p.144). The number 2 has to be replaced by ℓ and the polynomial $x^2 + x$ by $x^\ell - x$.

Proof of Corollary 1. Since $-x = (-x)^{2n} = x^{2n} = x$, the ring has characteristic 2 and the assertion follows at once from Theorem 2.

Proof of Corollary 2. Let p_i be the i-th prime and define k by the inequality

$$p_k \le \frac{log 2x}{log 2} < p_{k+1}. \tag{5}$$

For $n \le x$ we have

$$2n - 1 \le 2x - 1 < 2^{p_k+1} - 1 \tag{6}$$

and hence $2p_i - 1 \not| 2n - 1$ for $i > k$. Moreover $GCD(2^{p_i} - 1, 2^{q_j} - 1) = 1$, for $i \ne j$. Since for D odd, the number of $n \le x$ satisfying $D | 2n - 1$ is $\left\lfloor \frac{x + (D-1)/2}{D} \right\rfloor$, we have

$$N(x) = \sum_{d | p_1 \cdots p_k} \mu(d) \left\lfloor \frac{x + (\prod_{p|d}(2^p - 1) - 1)/2}{\prod_{p|d}(2^p - 1)} \right\rfloor = x \sum_{d | p_1 \cdots p_k} \frac{\mu(d)}{\prod_{p|d}(2^p - 1)} + O(2^k), \tag{7}$$

where μ is the Möbius function. Now,

$$\sum_{d | p_1 \cdots p_k} \frac{\mu(d)}{\prod_{p|d}(2^p - 1)} = \prod_{i=1}^{k} \left(1 - \frac{1}{2^{p_i} - 1}\right) = C_2 \prod_{i=k+1}^{\infty} \left(1 - \frac{1}{2^{p_i} - 1}\right)^{-1} \tag{8}$$

and by (6)

$$1 \le \prod_{i=k+1}^{\infty} \left(1 - \frac{1}{2^{p_i} - 1}\right)^{-1} = \exp\left(-\sum_{i=k+1}^{\infty} log\left(1 - \frac{1}{2^{p_i} - 1}\right)\right)$$

$$\le \exp \sum_{i=k+1}^{\infty} \frac{1}{2^{p_i} - 1} \le \exp \frac{2}{2^{p_{k+1}} - 2} \le \exp \frac{2}{2x - 2} = 1 + O\left(\frac{1}{x}\right). \tag{9}$$

On the other hand, by (5) and the strong form of the prime number theorem, we get that for every $\epsilon > 0$ and $x > x_0(\epsilon)$

$$k \leq \frac{p_k}{logp_k - 1 - \epsilon} \leq \frac{log2x/log2}{loglog2x - loglog2 - 1 - \epsilon}$$

and hence for $x > x_0(-loglog2)$

$$2^k \leq \exp\left(\frac{log2x}{loglog2x - 1}\right) = O\left(\exp\left(\frac{logx}{loglogx - 1}\right)\right). \tag{10}$$

Now the corollary follows from (7)-(10).

Remark 2. In the case of ℓ-rings the constant C_2 is replaced by

$$C_\ell = \frac{\ell - 2}{\ell - 1} + \frac{1}{\ell - 1}\prod_{p \in P}\left(1 - \frac{\ell - 1}{\ell^p - 1}\right).$$

It is easy to obtain numerical results about these constants, e.g. $C_3 \approx 0,842974678$, $C_5 \approx 0,951602563$, $C_7 \approx 0,976555991$, $C_{11} \approx 0,990971747$, ..., $C_{37} \approx 0,999249768$, *etc.* We thank a second anonymous referee for a question which led to the obtaining the asymptotic term of Corollary 2.

Examples. Some non trivial examples of polynomial identities which satisfy the conditions of Theorem 1 are

$$\begin{aligned} 1) \quad f(x) &= x + x^3 + x^9 + x^{12} + x^{18} + x^{20} \\ &= x(1+x)(1+x+x^9)(1+x^8+x^9) = 0 \end{aligned}$$

(use $g_1(x) = x$ and $g_2(x) = x^3$),

and

$$\begin{aligned} 2) \quad f(x) &= x + x^2 + x^3 + x^5 + x^6 + x^{10} + x^{13} + x^{14} + x^{17} + x^{21} + x^{22} \\ &\quad + x^{24} + x^{25} + x^{26} \\ &= x(1+x)(1+x+x^3+x^4+x^5+x^6+x^8)\times \\ &\quad \times(1+x^2+x^3+x^4+x^7+x^8)(1+x+x^2+x^4+x^6+x^7+x^8) = 0 \end{aligned}$$

(again use $g_1(x) = x$ and $g_2(x) = x^3$).

The fact that $GCD(f(x), f(x^3)) = x^2 + x$ is easily verified by using a Computer Algebra System (CAS).

References

1. Hansen D.J.,Luh J.,Ye Y.P. *J rings of characteristic two which are Boolean.* Internat. J. Math. Sci. **17**(1994), no.4, 807-811.
2. McCoy N.H. *Rings and Ideals.* Buffalo, NY, 1948.
3. Năstăsescu C., Andrei G., Ţena M., Otărăşanu I. *Probleme de Structuri Algebrice, Biblioteca Profesorului de Matematică.* Editura Academiei Republicii Socialiste România, Bucureşti 1988.

4. Năstăsescu C., Brandiburu M., Niţă C., Joiţa D. *Exerciţii şi Probleme de Algebră pentru clasele IX-XII.* Editura Didactică şi Pedagogică, Bucureşti 1983.

◇ Theodoros S. Bolis
Department of Mathematics
Univeristy of Ioannina
451 10 Ioannina, GREECE
`tbolis@cc.uoi.gr`

◇ Andrzej Schinzel
Institute of Mathematics
Polish Academy of Sciences
ul. Sniadeckich 8
00-950 Warsaw, POLAND
`schinzel@impan.gov.pl`