Equational proofs for a theorem by Jacobson for a significant density of even exponents

Michael A. Daas, Universiteit Leiden

Abstract

For each positive integer $n \geq 2$, a purely equational proof must exist for the statement that a ring R in which $x^n = x$ holds for all $x \in R$, must be commutative. By elementary means, we find such equational proofs for a significant density of even exponents n by establishing a reduction step that is as strong as can reasonably be expected by decreasing the given exponent n in a way that is minimal in view of the finite fields satisfying the same equation.

Contents

1 Introduction

A classical result by Jacobson [Jac45] from 1945 states that if R is a ring with the property that for every $x \in R$, there exists some integer $n(x) \geq 2$ such that $x^{n(x)} = x$, then the ring R must be commutative. Here, R need not be unital. The standard proof can be found in §12 in Lam's *A First Course in Noncommutative Rings* [Lam91], in which the proof of Jacobson's result in its complete generality is reduced to little more than a single page of reasoning after applying Herstein's Lemma and subsequently appealing to various structure theorems for certain classes of rings.

However, various authors observed that to prove Jacobson's result, there is no need for such powerful tools, and more elementary proofs have since been found. Examples can be found in Herstein's paper [Her54], Rogers's work [Rog71] and [Rog72], and in Nagahara and Tominaga's very short paper [NT74]. These proofs are much simpler than Jacobson's original proof, but they do rely on various ring theoretic notions. In particular, they venture beyond the framework of pure equational logic.

In a first course on ring theory, it is not uncommon to challenge students to prove Jacobson's theorem in the special case that one can take $n(x) = 2$ for all $x \in R$. In other words, tasking them to show that all Boolean rings must be commutative, which follows from expanding the equation $(x + y)^2 = x + y$ and cancelling, combined with the observation that $x = (-x)^2 = -x$.

In various online spaces, numerous examples can be found of students tasked to prove Jacobson's theorem in the special case that one can take $n(x) = 3$ for all $x \in R$; a problem that is considerably less trivial but can still be done purely equationally with some patience. It is natural to consider the special case of Jacobson's theorem for an arbitrary fixed exponent $n(x) = n$; we call all such rings $J(n)$-rings. By Birkhoff's

completeness theorem, included as Theorem 14.19 in [SB81], proofs using purely equational logic must exist in each case, but finding them and writing them down is a separate challenge. For $n \leq 6$, such proofs are easily found on the internet. Many have wondered about a more general solution to this problem, but often with little success.

A great source for explicit equational proofs for small exponents is Morita's article [Mor78], which is notoriously difficult to obtain but contains proofs for all $n \leq 25$ and all even $n \leq 50$. In [Zha90], Zhang uses an idea similar to the one presented in the present note to obtain equational proofs for an *empirically* positive density, with the drawback that deciding whether or not their strategy works for a given n is computationally as expensive as finding the equational proof itself. Significant progress was made by Burris and Lawrence in [BL91] by describing explicitly a finite set of rewrite rules complete for the equational theory of finite fields. However, they rely on the general results from [Jac45] to relate the equational theory for $J(n)$-rings to that of all finite $J(n)$-fields to draw their conclusions.

In this short note we propose an elementary reduction step for general even exponents that yields equational proofs for Jacobson's commutativity theorem for a very significant positive density of even integers. This makes explicit the general reduction step from the equational theory for $J(n)$-rings to that of all finite $J(n)$-fields used in [BL91]. In this sense, our reduction step is as strong as one could expect.

2 The reduction step

To obtain our reduction, our strategy is as follows. Fix a positive even integer n and a $J(n)$-ring R. Note that we do not assume that R is unital. We may then notice that $x = (-x)^n = -x$ for all $x \in R$, and as such, the ring is of characteristic at most 2. For any $x \in R$ and any $h \in X\mathbb{F}_2[X]$, it must hold that $h(x)^n - h(x) = 0 \in R$. Let $I_n \subset \mathbb{F}_2[X]$ be the ideal spanned by all these relations. Then by construction, for any $f \in I_n$ and $x \in R$, we must have that $f(x) = 0 \in R$. Because $\mathbb{F}_2[X]$ is a principal ideal domain, it follows that $I_n = (g_n)$ for some $g_n \in \mathbb{F}_2[X]$. Our key result determines g_n exactly using only some very elementary algebra. We use the convention that $\mathbb{N} = \mathbb{Z}_{\geq 1}$.

Proposition 1. *With the definitions from above, define the set*

$$S_n = \{m \in \mathbb{N} : 2^m - 1 \mid n - 1\}.$$

Then we have

$$g_n = \operatorname{lcm}\big\{X^{2^m} - X \mid m \in S_n\big\}.$$

Proof. We use the principle that two squarefree polynomials over $\mathbb{F}_2$ are equal if and only if they have the same zeroes in an algebraic closure $\overline{\mathbb{F}}_2$ of $\mathbb{F}_2$. Indeed, both sides are squarefree because the polynomial $X^k - X$ is separable for any positive even integer k. The zeroes of the right hand side are easily determined; some $\alpha \in \overline{\mathbb{F}}_2$ is one of its zeroes if and only if it is a zero of $X^{2^m} - X$ for some $m \in S_n$, or equivalently, if and only if $\alpha \in \mathbb{F}_{2^m}$ for some $m \in S_n$. On the other hand, some $\alpha \in \overline{\mathbb{F}}_2$ is a zero of g_n if and only if it is a zero of all $h^n - h$ for $h \in X\mathbb{F}_2[X]$. We have thus reduced to showing that for $\alpha \in \overline{\mathbb{F}}_2$,

$$h(\alpha)^n = h(\alpha) \text{ for all } h \in X\mathbb{F}_2[X] \iff \alpha \in \mathbb{F}_{2^m} \text{ for some } m \in S_n.$$

If $\alpha \in \mathbb{F}_{2^m}$ for some $m \in S_n$ and $h(\alpha) = 0$, then we are done. If $h(\alpha) \in \mathbb{F}_{2^m}^\times$ instead, it holds that $h(\alpha)^{2^m - 1} = 1$. By definition of m, raising this expression to some power yields that $h(\alpha)^{n-1} = 1$, proving one direction.

Now let $\alpha \in \overline{\mathbb{F}}_2$ and suppose that $h(\alpha)^n = h(\alpha)$ for all $h \in X\mathbb{F}_2[X]$. If we write $\mathbb{F}_2[\alpha] = \mathbb{F}_{2^m}$ for some $m \in \mathbb{N}$, we must show that $m \in S_n$. Using that $X^{2^m - 1} \in X\mathbb{F}_2[X]$ is constantly equal to 1 on $\mathbb{F}_{2^m}^\times$, we observe that

$$\big\{h(\alpha) \mid h \in X\mathbb{F}_2[X]\big\} = \big\{h(\alpha) \mid h \in \mathbb{F}_2[X]\big\} = \mathbb{F}_2[\alpha] = \mathbb{F}_{2^m}.$$

In other words, we have shown that $\beta^n = \beta$ for all $\beta \in \mathbb{F}_{2^m}$. Since $\mathbb{F}_{2^m}^\times$ is cyclic of order $2^m - 1$, we may choose β to be a generator. It then follows immediately that $2^m - 1 \mid n - 1$, showing $m \in S_n$ and completing the proof. □

In our context, the above proposition tells us *precisely* how much we can deduce from examining *all* possible relations generated by looking at just a single element $x \in R$, the polynomial g_n being the *minimal* relation from which all others follow. Even though the proof uses some mild ring theory, it sets up equational proofs by generating relations using all $h \in X\mathbb{F}_2[X]$ of degree smaller than n and finding g_n by performing Euclid's algorithm. Any deductions beyond this must be made using at least two variables, as is exemplified by our brief sketch earlier of the proof for Boolean rings.

Further, for any positive integer m, there is a finite field $\mathbb{F}_{2^m}$, which is a $J(2^m)$-ring. It is easy to see that $\mathbb{F}_{2^m}$ is a $J(n)$-ring if and only if $m \in S_n$. Any attempt at a reduction to any smaller exponent finds an obvious obstruction in the existence of rings in which this reduction step would fail to hold. One way to interpret the proposition above is that, for any obstruction ring from the set $\{\mathbb{F}_{2^m} \mid m \in S_n\}$, we get a factor contributing to g_n and together these exactly form the minimal relation. In this sense, the obstructions coming from finite fields are really the only ones and our reduction step is optimal.

3 Densities for equational proofs

In order to compute densities of even numbers satisfying the condition that S_n is equal to a given set, we require the following elementary lemma.

Lemma 2. *Let $m, n \in \mathbb{N}$ and denote $d = \gcd(m, n)$. Then*

$$\gcd(2^m - 1, 2^n - 1) = 2^d - 1.$$

Proof. This is a restatement of the fact that $\mathbb{F}_{2^m}^\times \cap \mathbb{F}_{2^n}^\times = \mathbb{F}_{2^d}^\times$. □

Of particular interest to us is the case in which among all the finite fields which are $J(n)$-rings, there is one that contains all others. This allows us to explicitly reduce the problem to a smaller exponent.

Theorem 3. *Let n be an even positive integer with the property that there is some $m \in \mathbb{N}$ such that all finite $J(n)$-fields are $\mathbb{F}_{2^m}$ and its subfields. Then any $J(n)$-ring is also a $J(2^m)$-ring. The density of even n for which any $J(n)$-ring is necessarily Boolean is given by*

$$\alpha := \prod_{p \text{ prime}} \frac{2^p - 2}{2^p - 1} \approx 0.54830.$$

Proof. For the first claim, we are to show that $g_n = X^{2^m} - X$. Indeed, by Proposition 1, this is equivalent to showing that $X^{2^k} - X \mid X^{2^m} - X$ for any $k \in S_n$. But by assumption, $\mathbb{F}_{2^k} \subset \mathbb{F}_{2^m}$, proving the claim. From this it follows that for any even positive integer n, any $J(n)$-ring must be Boolean if and only if $m = 1$ in the previous claim. This happens if and only if $n - 1$ is divisible by no number of the form $2^k - 1$ for $k \geq 2$. Because for any prime $p \mid k$ we have $2^p - 1 \mid 2^k - 1$ by Lemma 2, it suffices for n to not be divisible by any number of the form $2^p - 1$. By the same lemma, all these numbers are pairwise coprime. Since the density of the numbers divisible by $2^p - 1$ is its reciprocal, an expansion using *inclusion-exclusion* yields that the set of numbers not divisible by any of the numbers $\{2^p - 1 \mid p \text{ is prime}\}$ has density

$$\prod_{p \text{ prime}} \left(1 - \frac{1}{2^p - 1}\right),$$

which precisely equals α. Because all the numbers $2^p - 1$ are odd, it does not matter for the density if we restrict to the odd numbers $n - 1$. □

Recall that for each even $n \leq 50$, Morita in [Mor78] found a purely equational proof for the commutativity of all $J(n)$-rings. If we assume these results, in particular their proofs for the even values $n \in \{8, 16, 32\}$, we may drastically increase the density of even n for which explicit equational proofs are known.

Theorem 4. *With the results from [Mor78], Theorem 3 yields equational proofs for the commutativity of all $J(n)$-rings for a density of even integers n equal to*

$$\left(\frac{127}{85}+\frac{12}{73}+\frac{36080}{1082401}\right)\alpha \approx 0.92763.$$

Proof. Using Theorem 3 for $m \leq 5$ in combination with [Mor78], we can find equational proofs whenever $S_n \subset \{1,2,4\}$, $S_n = \{1,3\}$ or $S_n = \{1,5\}$. For the first case, we replace the condition of not being divisible by $2^{2^1}-1=3$ by not being divisible by $2^{2^3}-1=255$, yielding a density of $127\alpha/85$. The other two densities are deduced by subtracting α, the density of numbers with $S_n = \{1\}$, from the densities for $S_n \subset \{1,3\}$ and $S_n \subset \{1,5\}$, which are obtained similarly. □

In other words, for about 92.76% of positive even exponents, we can find an explicit equational proof for the commutativity of all $J(n)$-rings. One may try to explore equational proofs for more families of conditions sufficient for commutativity, some of which are listed in Pinter-Lucke's paper [PL07]. One may further attempt to find equational proofs for odd exponents n, but the loss of the quick observation that $\mathrm{char}(R) = 2$ significantly complicates matters here. The author would welcome any ideas to expand upon these attempts further.

4 References

[BL91] Stanley Burris and John Lawrence. Term rewrite rules for finite fields. *International Journal of Algebra and Computation*, 1(03):353–369, 1991.

[Her54] I. N. Herstein. An elementary proof of a theorem of Jacobson. 1954.

[Jac45] Nathan Jacobson. Structure theory for algebraic algebras of bounded degree. *Annals of Mathematics*, 46(4):695–707, 1945.

[Lam91] Tsit-Yuen Lam. *A first course in noncommutative rings*, volume 131. Springer, 1991.

[Mor78] Y. Morita. Elementary proofs of the commutativity of rings satisfying $x^n = x$. *Memoirs of the Defense Academy. Mathematics, Physics, Chemistry and Engineering*, 18(1):1–24, 1978.

[NT74] Takasi Nagahara and Hisao Tominaga. Elementary proofs of a theorem of Wedderburn and a theorem of Jacobson. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, volume 41, pages 72–74. Springer, 1974.

[PL07] James Pinter-Lucke. Commutativity conditions for rings: 1950–2005. *Expositiones Mathematicae*, 25(2):165–174, 2007.

[Rog71] Kenneth Rogers. An elementary proof of a theorem of Jacobson. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, volume 35, pages 223–229. Springer, 1971.

[Rog72] Kenneth Rogers. Berichtigung zu der arbeit "An elementary proof of a theorem of Jacobson". In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, volume 37, pages 268–268. Springer, 1972.

[SB81] Hanamantagouda P. Sankappanavar and Stanley Burris. A course in universal algebra. *Graduate Texts Math*, 78:56, 1981.

[Zha90] Hantao Zhang. Automated proof of ring commutativity problems by algebraic methods. *Journal of symbolic computation*, 9(4):423–427, 1990.