A characterisation of commutator-forcing polynomials

S.M. BUCKLEY AND D. MACHALE

ABSTRACT. We characterise those polynomials g such that a ring R is commutative whenever $g(c) = 0$ for all commutators c in R. We then discuss situations in which the more general condition $g_c(c) = 0$ implies commutativity, and also discuss the situation in unital rings.

1. INTRODUCTION

Jacobson [8] proved that a ring R satisfying an identity of the form $x^{n(x)+1} = x$, $n(x) \in \mathbb{N}$, is commutative. Such rings are rather special, but Herstein then showed that commutativity is equivalent to a weaker condition involving the *commutator* $[x, y] = xy - yx$.

Theorem A (Herstein [6])**.** *A ring R is commutative if and only if for each $x, y \in R$ there exists $n(x, y) \in \mathbb{N}$ such $[x, y]^{n(x,y)+1} = [x, y]$.*

Here we characterise the set of all *commutator-forcing polynomials*, by which we mean those polynomials $g(X) \in X\mathbb{Z}[X]$ such that a ring R is necessarily commutative if $g([x, y]) = 0$ for all $x, y \in R$. Thus Theorem A says in particular that all polynomials of the form $X^{n+1} - X$, $n \in \mathbb{N}$, are commutator-forcing polynomials. Note that every commutator-forcing polynomial provides a necessary and sufficient condition for commutativity.

Theorem 1. *The following conditions are equivalent for a polynomial $g(X) \in X\mathbb{Z}[X]$.*

(a) *A ring R is necessarily commutative if $g([x, y]) = 0$ for all $x, y \in R$.*
(b) *$g(X)$ has the form $f(X) \pm X$, where $f(X) \in X^2\mathbb{Z}[X]$.*

Characterisations of polynomials that force a ring to be commutative in other senses have been considered in [9], [2], and [3], but commutator-forcing polynomials do not appear to have been considered previously. We prove the main result in Section 2, and consider related results in Section 3.

We wish to thank the referee for pointing out an alternative approach to the proof of Theorem 1.

2010 *Mathematics Subject Classification.* 16R50.

Key words and phrases. rings, commutativity conditions, commutator.

2. Proof of Theorem 1

Let us begin by discussing some notation. If $f(X) \in X\mathbb{Z}[X]$, then f can naturally be interpreted as a function on a ring R. We must assume that $f(X) \in X\mathbb{Z}[X]$, rather than merely $f(X) \in \mathbb{Z}[X]$, because we do not assume that rings are unital. We always use X for the indeterminate of a formal polynomial, so if the argument of $f(*)$ involves X (e.g. $f(2X)$ or $f(f(X))$), then this is a formal polynomial, but in all other cases (e.g. $f(x)$), $f(*)$ is a value of $f : R \to R$ for some ring R. As usual, $Z(R)$ denotes the centre of a ring R.

The following result shows that (a) implies (b) in Theorem 1, and gives a special case of the converse.

Theorem B ([4, Theorem 3(c)])**.** *The following conditions are equivalent for a polynomial $g(X) \in X\mathbb{Z}[X]$.*

(a) *A ring R whose centre is an ideal is necessarily commutative if $g([x, y]) = 0$ for all $x, y \in R$.*
(b) *$g(X)$ has the form $f(X) \pm X$, where $f(X) \in X^2\mathbb{Z}[X]$.*

The results of [4] and [5] suggest that perhaps the centres of most finite indecomposable non-unital rings are ideals, and this in turn suggests that perhaps the ideal centre assumption in Theorem B could be dropped, leading to Theorem 1. Note however that the ideal centre assumption allows for an easy proof of equivalence in Theorem B, but this method is of no use when attempting to prove Theorem 1.

Before proving Theorem 1, we first give a couple of lemmas.

Lemma 2. *Suppose R is a ring, and that $f(x) = x$ for some $x \in R$ and $f(X) \in X^2\mathbb{Z}[X]$. Then for each $n \in \mathbb{N}$, there exists $f_n(X) \in X\mathbb{Z}[X]$, depending only on n and f, such that $x = x^n f_n(x)$.*

Proof. Since $x = f(x)$, we have $x = (f^k)(x)$ for all $k \in \mathbb{N}$, where $f^k(X)$ denotes the k-fold formal composition of f, i.e. $f^1(X) := f(X)$, $f^2(X) := f(f(X))$, etc. Note also that $f^k(X)$ can be written as $X^{2^k-1}h_k(X)$ for some $h_k(X) \in X\mathbb{Z}[X]$ so the equation $x = (f^k)(x)$ immediately implies that if $n < 2^k$ then $x = x^n f_{k,n}(x)$ where $f_{k,n}(X) = X^{2^k-1-n}h_k(X)$. We can therefore define $f_n(X)$ to be, for instance, $f_{k,n}(X)$, where k is the smallest integer such that $2^k > n$. □

Lemma 3. *Let R be a ring and $k > 1$ a fixed integer. Suppose that*

(i) *S is a subset of R such that $kx \in S$ whenever $x \in S$;*
(ii) *there exists $f(X) \in X^2\mathbb{Z}[X]$ such that $f(s) = s$ for all $s \in S$.*

Then there exists a square-free integer m, depending only on $\deg(f)$, such that $mx = 0$ for all $x \in S$.

Proof. We may assume that f is non-zero since otherwise the result is trivially true. Let d be the degree of $f(X)$. Expanding the formal polynomial $f_1(X) := k^d f(X) - f(kX)$, we see that it has degree at most $d-1$. Furthermore it has nonzero terms only for the same powers of X as f. In particular, $f_1(X) \in X^2\mathbb{Z}[X]$. Moreover, $f_1(s) = (k^d - k)s$ for $s \in S$.

Since the properties of f_1 are similar to those of f, we can repeatedly lower the degree of the polynomial under consideration by continuing this process. For instance, $f_2(X) := k^{d-1}f_1(X) - f_1(kX)$ has degree at most $d-2$, and $f_2(s) = (k^d - k)(k^{d-1} - k)s$ for $s \in S$. We eventually get that $f_{d-1}(X)$ is the zero polynomial and that $Mx = 0$ for all $x \in S$, where $M = \prod_{i=0}^{d-2}(k^{d-i} - k)$.

Let m be the product of the distinct prime factors of M, and let $n \in \mathbb{N}$ be such that m^n is divisible by M. Appealing to Lemma 2, the equation $ms = m^n s^n f_n(ms)$ readily implies that $ms = 0$, so we are done. □

We now prove Theorem 1 using Jacobson's structure theory, a well-known technique for proving commutativity theorems: see, for instance, the proof of Jacobson's theorem in [7, Theorem 3.1.2].

Proof of Theorem 1. The proof that (a) implies (b) follows a fortiori from the corresponding implication in Theorem B, but we include the short proof for completeness. Suppose $g(X) = f(X) + a_1X$, where $f(X) \in X^2\mathbb{Z}[X]$ and $a_1 \notin \{1, -1\}$. Thus a_1 has a prime factor p. Consider the ring R of 3×3 matrices over $\mathbb{Z}_p$ of the form

$$\begin{pmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{pmatrix}$$

The set of commutators C consists of all matrices of the above form with $a = c = 0$, and it follows from the equations $R \cdot C = C \cdot R = \{0\}$ that $g(c) = 0$ for all $c \in C$. However, R is not commutative: in fact, $Z(R) = C$.

We now prove that (b) implies (a). Assume first for the sake of contradiction that $g(X)$ satisfies (b) and that R is a noncommutative division ring R such that $g([R, R]) = 0$; this last equation is to be interpreted as meaning that $g([x, y]) = 0$ for all $x, y \in R$. Thus there is a nonzero commutator c in R. By Lemma 3, $mc = 0$ for some nonzero integer m, and so R has characteristic p for some prime p. It follows from the equation $f(c) = \pm c$ that the ring generated by c is finite. Consequently there exists distinct integers $m > m' > 0$ such that $c^m = c^{m'}$, and so $c^n = c$, where $n = m - m' + 1 > 1$. Since we have such an equation for all commutators c, it follows from Theorem A that R is commutative, contradicting our assumption.

Suppose next that R is primitive and that $g([R,R]) = 0$ for some $g(X)$ satisfying (b). The Jacobson density theorem tells us that R is a dense subring of the endomorphism ring of a vector space V over a division ring D. If R has finite dimension $k > 1$, then it follows that $R = V$ must equal the ring $M_k(D)$ of all $k \times k$ matrices over D. But if $k > 1$, and we define $A_{ij} \in M_k(D)$ to be the matrix that has 1 as its (i,j)th entry and has zeros everywhere else, then $c := A_{21}A_{11} - A_{11}A_{21} = A_{21} \neq 0$ and c^2 is the zero matrix, which is incompatible with the equation $g(c) = 0$.

Alternatively, if R is infinite dimensional, it follows that a quotient of a subalgebra of R is isomorphic to $M_k(D)$, for each $k \in \mathbb{N}$. Polynomial commutator identities are inherited by such subquotients, so it follows that every $M_k(D)$ satisfies the same polynomial commutator identity as R. Taking $k > 1$, we get a contradiction as before. The only remaining possibility is that $R = V$ has dimension 1. But then, R is itself a division ring, and so necessarily commutative by a previous argument.

Suppose now that R is a general ring such that $g([R,R]) = 0$ for some $g(X)$ satisfying (b). It is clear that R/I inherits the commutator identity of R, whenever I is an ideal in R. In particular, this holds when $I = J$ is the Jacobson radical of R. Since R/J is semiprimitive, it is a subdirect product of primitive rings P, and these rings P in turn inherit the commutator identity $g(c) = 0$. Thus each such P is commutative, and so R/J is also commutative.

We have proved that $c := [x,y] \in J$ for all $x, y \in R$. Writing our commutator identity in the form $c = c \cdot h(c)$, where $h(X) \in X\mathbb{Z}[X]$, we have an equation $cd = c$, where c and $d := h(c)$ lie in J. As is well known, an equation of the form $yx = y$ for fixed $x \in J(R)$ and $y \in R$ implies that $y = 0$, so the equation $cd = c$ forces c to be 0. Since c is an arbitrary commutator, R is commutative. □

3. Related results

Since the exponent $n(x,y)$ depends on the commutator in Theorem A, it seems plausible that a ring R might necessarily be commutative if it satisfies a condition of the form $f_c(c) = c$ for all commutators $c \in R$, where $f_c(X) \in X^2\mathbb{Z}[X]$ is allowed to depend on c. Adding to the plausibility of this result is that such an implication holds in the class of rings R in which $Z(R)$ is an ideal [4, Theorem 2]. We do not know if such an implication holds in the class of general rings, but we now consider some weaker results in this direction.

In our first such result, we add the auxiliary assumption that all commutators are of finite order.

Theorem 4. *Suppose R is a ring, and that for every commutator $c \in R$, there exists a positive integer m_c and a polynomial $g_c(X) \in X\mathbb{Z}[X]$ such that*

(i) *$g_c(X)$ has the form $f_c(X) \pm X$, where $f_c(X) \in X^2\mathbb{Z}[X]$,*

(ii) $g_c(c) = 0$, *and*
(iii) $m_c c = 0$.

Then R is commutative.

Proof. The proof is more or less the same as that of (b) $\Rightarrow$ (a) in Theorem 1: the only change is that condition (iii) replaces the appeal to Lemma 3 when we are proving that a division ring R with the hypothesised properties must have positive characteristic, and so the subring generated by a given nonzero commutator must be of finite order. □

What was above described as a *plausible result* was that Theorem 4 remains true if condition (iii) is dropped. But (iii) was used in the proof of Theorem 4 only to deduce that a division ring R must be commutative under conditions (i)–(iii). Thus we have reduced this result to a result for division rings. However, we do not know if assuming (i) and (ii) for all commutators c in a division ring R imply that R is commutative.

Note though that auxiliary condition (iii) follows from Lemma 3 if $g_c = g_{kc}$ for some fixed $k > 1$, and all commutators c in R. Thus we have the following variant of Theorem 4.

Theorem 5. *Suppose R is a ring, $k > 1$ is an integer, and that for every commutator $c \in R$, there exists a polynomial $g_c(X) \in X\mathbb{Z}[X]$ such that*

(i) *$g_c(X)$ has the form $f_c(X) \pm X$, where $f_c(X) \in X^2\mathbb{Z}[X]$,*
(ii) *$g_c(c) = 0$, and*
(iii) *$g_c = g_{kc}$.*

Then R is commutative.

For the next variant, we define R_0 to be R and, for all $n \in \mathbb{N}$, we inductively define $C_n(R)$ to be the set of commutators of R_{n-1}, and R_n to be the subring of R generated by $C_n(R)$. In particular, $C_1(R)$ is the set of commutators of R.

This next variant implies Theorem 4, and also shows that to deduce commutativity, we do not need g_c to be independent of c for all $c \in C_1(R)$: it suffices that it is independent of $c \in C_n(R)$ for some $n \in \mathbb{N}$.

Theorem 6. *Suppose R is a ring such that for every $c \in C_1(R)$ there exists a polynomial $g_c(X) \in X\mathbb{Z}[X]$ such that*

(i) *$g_c(X)$ has the form $f_c(X) \pm X$, where $f_c(X) \in X^2\mathbb{Z}[X]$, and*
(ii) *$g_c(c) = 0$.*

Then the following conditions are equivalent.

(a) *R is commutative.*
(b) *There exists $n \in \mathbb{N}$ such that $g_c(X)$ can be taken to be independent of c for all $c \in C_n(R)$.*
(c) *There exists $n \in \mathbb{N}$ such that every $c \in C_n(R)$ is of finite order.*

In order to prove Theorem 6, we first state a part of [1, Theorem 19].

Theorem C. *If $[x,z]$ and $[y,z]$ commute for all x,y,z in a ring R, then $[x,y]^4 = 0$ for all $x,y \in R$.*

Proof of Theorem 6. It is clear that (a) implies (b) and (c). Suppose therefore that (b) holds. Since $C_n(R) = C_1(R_{n-1})$, it follows from Theorem 1 that R_{n-1} is commutative. Once we know that R_{n-1} is commutative, we can use Theorem C and Lemma 2 to deduce by a backward induction process that R is commutative. The proof that (c) implies (a) is similar, except that we initially appeal to Theorem 4 instead of Theorem 1. □

We finish by considering *u-commutator-forcing polynomials*, meaning those polynomials $g(X) \in \mathbb{Z}[X]$ such that a unital ring R is necessarily commutative if $g([x,y]) = 0$ for all $x,y \in R$. For some other forcing problems, the set of polynomials that force commutativity for unital rings is much larger and quite different in nature than the corresponding set for all rings: see [9], [2], and [3]. However, in the case of our problem, there is no difference for polynomials $g(X) \in X\mathbb{Z}[X]$.

To see this, let us first recall the well-known Dorroh extension R' of a general ring R. Here $R' := \mathbb{Z} \times R$ is a unital ring, where addition is componentwise and multiplication is given by $(m,x)(n,y) = (mn, my + nx + xy)$. Then R is isomorphic to a subring of R' via the identification of $x \in R$ with $(0,x) \in R'$. Under this identification, it is clear that the commutator set of R coincides with that of R'. Moreover, R is commutative if and only if R' is commutative. It follows that a u-commutator-forcing polynomial is also commutator-forcing, and of course the converse implication is trivial. This does not quite finish the job of characterising u-commutator-forcing polynomials because polynomials in $\mathbb{Z}[X] \setminus X\mathbb{Z}[X]$ can be interpreted as functions on unital rings even though they cannot be so interpreted on non-unital rings. We have the following characterisation.

Theorem 7. *The following conditions are equivalent for a polynomial $g(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$.*

(a) *A unital ring R is necessarily commutative if $g([x,y]) = 0$ for all $x,y \in R$.*
(b) *a_0 and a_1 are coprime.*

Proof. We first prove that (b) implies (a). In the case $a_0 = 0$, (b) says that $a_1 = \pm 1$, and this is equivalent to (a), as discussed above. Suppose instead that $a_0 \neq 0$. Since $0 = [1,1]$ is a commutator, the commutator identity $g(c) = 0$ splits into the equation $a_0 \cdot 1 = 0$ and the commutator identity $f(c) = 0$ where $f(X) = g(X) - a_0$. If $a_0 = \pm 1$, it is therefore trivial that R is commutative, so suppose that $|a_0| > 1$. As is well known, a ring satisfying $a_0 R = 0$ is a direct sum of rings R_p satisfying $p^k R_p = 0$, where p^k is the highest positive integer power of a prime p

that divides a_0. Consider such a prime power p^k and associated direct summand R_p. Since multiples of p^k make no difference when g is viewed as a function on R_p, we can discard the a_0 term. Since a_1 is coprime to p^k, some multiple of it is equivalent to 1 mod p^k. By taking the same multiple of $g(X) - a_0$ and discarding a multiple of $p^k X$, it follows that there is a polynomial $G(x) = X + F(x)$, with $F(X) \in X^2\mathbb{Z}[X]$, such that $G(c) = 0$ for all commutators $c \in R_p$, and so R_p must be commutative by Theorem 1. Thus all direct summands R_p of R are commutative, and so R is commutative.

For the converse, it suffices to show that $g(X)$ is not u-commutator-forcing if both a_0 and a_1 are divisible by a prime p. To see this, let R be the ring of matrices of the form

$$\begin{pmatrix} d & a & b \\ 0 & d & c \\ 0 & 0 & d \end{pmatrix}, \qquad a, b, c, d \in \mathbb{Z}_p\,. \qquad \square$$

The commutators $[x, y]$ in R consist of all matrices with $a = c = d = 0$, so $[x, y]^2 = 0$, and thus $g([x, y]) = 0$ for any such $g(X)$.

References

[1] S.M. Buckley, D. MacHale, Variations on a theme: rings satisfying $x^3 = x$ are commutative, Amer. Math. Monthly **120** (2013), 430–440.

[2] S.M. Buckley, D. MacHale, Polynomials that force a unital ring to be commutative, Results Math. **64** (2013), 59–65.

[3] S.M. Buckley, D. MacHale, Z-polynomials and ring commutativity, Math. Proc. R. Ir. Acad. **112** (2012), 51–57.

[4] S.M. Buckley, D. MacHale, Rings with ideal centres, preprint. (Available at `http://www.maths.nuim.ie/staff/sbuckley/Papers/bm_ideal.pdf`)

[5] S.M. Buckley, D. MacHale, Small rings without ideal centres, Bull. Irish. Math. Soc. **70** (2012), 41–49.

[6] I.N. Herstein, A condition for the commutativity of rings, Canad. J. Math. 9 (1957) 583–586.

[7] ———, *Noncommutative Rings*, Carus Mathematical Monographs, Mathematical Association of America, Washington, DC, 1968.

[8] N. Jacobson, Structure theory for algebraic algebras of bounded degree, Ann. Math. 46 (1945) 695–707.

[9] T.J. Laffey, D. MacHale, Polynomials that force a ring to be commutative, Proc. R. Ir. Acad. 92A (1992) 277–280.

S.M. Buckley:

Department of Mathematics and Statistics, National University of Ireland Maynooth, Maynooth, Co. Kildare, Ireland.

E-mail address: `stephen.buckley@maths.nuim.ie`

D. MacHale:
School of Mathematical Sciences, University College Cork, Cork, Ireland.

E-mail address: d.machale@ucc.ie