
Volume 348, Issue 1, December 15, 2011 ISSN 0021-8693
ELSEVIER
JOURNAL OF
ALGEBRA
Editor-in-Chief
Michel Broué
Editor of the section on Computational Algebra
Gerhard Hiss
Founding Editor
G. Higman, 1964–1984
Editor-in-Chief
W. Feit, 1985–2000
Editorial Board
Nicolás Andruskiewitsch
Luchezar L. Avramov
Eva Bayer-Fluckiger
Steven Dale Cutkosky
Dihua Jiang
Masaki Kashiwara
E.I. Khukhro
Shrawan Kumar
Kazuhiko Kurano
Gus I. Lehrer
Martin Liebeck
Peter Littelmann
Laurent Moret-Bailly
Leonard L. Scott, Jr.
Vera Serganova
Aner Shalev
Ronald Solomon
V. Srinivas
J.T. Stafford
Gernot Stroth
Bernd Ulrich
Michel Van den Bergh
Changchang Xi
Efim Zelmanov
Section on Computational Algebra
Jon Carlson
John Cremona
Patrick Dehornoy
Harm Derksen
Derek Holt
William M. Kantor
Reinhard Laubenbacher
Gunter Malle
Eamonn O'Brien
Bruno Salvy
Seth Sullivant
Jean-Yves Thibon

Journal of Algebra 348 (2011) 350–353

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

On image sets of integer-valued polynomials

Scott T. Chapman [a,*], Vadim Ponomarenko [b]

[a] Sam Houston State University, Department of Mathematics and Statistics, Huntsville, TX 77341-2206, United States
[b] San Diego State University, Department of Mathematics and Statistics, San Diego, CA 92182-7720, United States

ARTICLE INFO

Article history:
Received 15 November 2010
Available online 13 October 2011
Communicated by Luchezar L. Avramov

MSC:
13F05
11C08
13F20
13G05
13B25

Keywords:
Integer-valued polynomial

ABSTRACT

Let $\text{Int}(\mathbb{Z})$ represent the ring of polynomials with rational coefficients which are integer-valued at integers. We determine criteria for two such polynomials to have the same image set on $\mathbb{Z}$.

If $\mathbb{Z}$ represents the integers and $\mathbb{Q}$ the rationals, then let

$$\text{Int}(\mathbb{Z}) = \{ f(X) \mid f(X) \in \mathbb{Q}[X] \text{ with } f(z) \in \mathbb{Z} \text{ for all } z \in \mathbb{Z} \}$$

represent the much studied ring of integer-valued polynomials. Given $f \in \text{Int}(\mathbb{Z})$, we denote the image set of f on $\mathbb{Z}$ as $f(\mathbb{Z}) = \{f(x) \mid x \in \mathbb{Z}\}$, the leading coefficient of f as $\text{lc}(f)$ and the degree of $f(X)$ as $\deg(f(X))$. We also denote the set of nonnegative integers as $\mathbb{N}_0$ and the set of positive integers as $\mathbb{N}$. For $n \in \mathbb{N}_0$, let $\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!}$ represent the nth element of the well-known binomial basis of $\text{Int}(\mathbb{Z})$ over $\mathbb{Z}$. The purpose of this note is to characterize the pairs of polynomials (f, g) in $\text{Int}(\mathbb{Z})$ such that $f(\mathbb{Z}) = g(\mathbb{Z})$. Clearly, if $f(X) = z_1$ and $g(X) = z_2$ in $\text{Int}(\mathbb{Z})$ are constant polynomials, then $f(\mathbb{Z}) = g(\mathbb{Z})$ if and only if $z_1 = z_2$. If $f(X)$ in $\text{Int}(\mathbb{Z})$ is not constant, then the image set $f(\mathbb{Z})$ is unbounded. Moreover, if $\deg(f(X))$ and $\deg(g(X))$ have opposite parity (i.e., one even and the other odd), then $f(\mathbb{Z}) \neq g(\mathbb{Z})$.

* Corresponding author.
E-mail addresses: scott.chapman@shsu.edu (S.T. Chapman), vadim123@gmail.com (V. Ponomarenko).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2011.10.003

Our work is motivated by several papers by McQuillan [8,9] and Gilmer [7] which explore properties related to the rings

$$\mathrm{Int}(S,D)=\bigl\{f(X)\bigm| f(X)\in K[X] \text{ with } f(s)\in D \text{ for all } s\in S\bigr\}$$

where D is an integral domain with quotient field K. Particular interest in $\mathrm{Int}(S,D)$ has appeared in the recent literature for the case where $D=\mathbb{Z}$ and $S=\mathbb{P}$ is the set of prime numbers in $\mathbb{Z}$ (see [4,5]). Good general references for rings of integer-valued polynomials determined by subsets are the monograph of Cahen and Chabert [1] or their succeeding survey paper [2]. There is also a connection between the question we explore here and the notions of an interpolation domain (considered in [6,3]) and the parameterization of integral values of polynomials (considered in [10]).

We begin by defining an equivalence relation on $\mathrm{Int}(\mathbb{Z})$, setting $f\sim g$ (for $f,g\in\mathrm{Int}(\mathbb{Z})$) if there is some $n\in\mathbb{Z}$ such that for all $X\in\mathbb{Z}$ either $f(X)=g(X-n)$ or $f(X)=g(-X-n)$. Certainly if $f\sim g$ then $f(\mathbb{Z})=g(\mathbb{Z})$. The converse does not hold, as demonstrated by Lemma 1.

Lemma 1. *Let $f\in\mathrm{Int}(\mathbb{Z})$ be such that $f(-X)=f(X-k)$ for some odd integer k, and set $h(X)=f(2X)$. Then $h(\mathbb{Z})=f(\mathbb{Z})$.*

Proof. Let $x\in\mathbb{Z}$. Then

$$f(x)=\begin{cases} h(\frac{x}{2}) & \text{if } x \text{ is even},\\ h(\frac{-x-k}{2}) & \text{if } x \text{ is odd}\end{cases}$$

and hence $f(x)\in h(\mathbb{Z})$ so $f(\mathbb{Z})\subseteq h(\mathbb{Z})$. The reverse containment is trivial. □

Note that the condition $f(-X)=f(X-k)$ in Lemma 1 is equivalent to the condition that $f(X-\frac{k}{2})$ be an even function, which in turn implies that $\deg(f)$ is even. This condition applies to all even binomial polynomials $\binom{X}{2n}=\frac{x(x-1)(x-2)\cdots(x-2n+1)}{(2n)!}$.

Our main result is that the equivalence relation $\sim$ together with the phenomenon from Lemma 1 suffice to provide a converse.

Theorem 2. *Let $f,g\in\mathrm{Int}(\mathbb{Z})$, with $|\mathrm{lc}(f)|\leqslant|\mathrm{lc}(g)|$. Then $f(\mathbb{Z})=g(\mathbb{Z})$ if and only if one of the following holds*:

(1) *$f\sim g$, or*
(2) *$f(-X)=f(X-k)$ for some odd integer k, and $g\sim h$ where $h(X)=f(2X)$.*

The remainder of this note is dedicated to the proof of this theorem. In both cases above, $\deg(f)=\deg(g)$. By the comments following Lemma 1, in case (2) this degree must be even. Further, in case (1), $|\mathrm{lc}(f)|=|\mathrm{lc}(g)|$; whereas in case (2), $|\mathrm{lc}(f)|<|\mathrm{lc}(g)|$ (provided $\deg(f)>0$).

We assume henceforth that $f(\mathbb{Z})$, for $f(X)\in\mathrm{Int}(\mathbb{Z})$, is unbounded above. In particular we exclude constant polynomials f. If $\deg(f)>0$, then $|f(\mathbb{Z})|$ is infinite. If $f(\mathbb{Z})$ were bounded above, then it must be unbounded below, so to compare $\{f,g\}$ we instead compare $\{-f,-g\}$, because $(-f)(\mathbb{Z})=(-g)(\mathbb{Z})$ is unbounded above. Hence the function

$$\sigma(x)=\min\bigl\{y\colon\ y\in f(\mathbb{Z}),\ y>x\bigr\}$$

is well defined. By taking $f(-X)\sim f(X)$ if necessary, we may also assume that $\mathrm{lc}(f)>0$. With this notation and assumptions, we make the following definitions.

Definition 3. Let $f \in \mathrm{Int}(\mathbb{Z})$.

(a) If there exists an $A \in \mathbb{R}$ such that $f(x+1) = \sigma(f(x))$ for all $x \in \mathbb{Z}$ with $x > A$, then f is of *type* 1.
(b) If there exists an $A \in \mathbb{R}$ such that $f(x+1) = \sigma^2(f(x))$ for all $x \in \mathbb{Z}$ with $x > A$, then f is of *type* 2.

Before proceeding to a proof of Theorem 2, Lemmas 5 and 6 will offer a proof of the following (under the above assumptions).

Proposition 4. *Each $f \in \mathrm{Int}(\mathbb{Z})$ is of type* 1 *or* 2.

Because the conditions of Definition 3 are mutually exclusive, no $f \in \mathrm{Int}(\mathbb{Z})$ can be of both type 1 and type 2. Note that if $f \sim g$, then f, g are of the same type. Our first lemma considers polynomials of odd degree.

Lemma 5. *Let $f \in \mathrm{Int}(\mathbb{Z})$ be of odd degree. Then f is of type* 1.

Proof. Recall that we assume $\mathrm{lc}(f) > 0$, and hence $\lim_{x\to+\infty} f'(x) = +\infty$. We choose $B > 0$ with $f'(x) > 0$ for all $x \geqslant B$. Because $\lim_{x\to+\infty} f(x) = +\infty$ and $\lim_{x\to-\infty} f(x) = -\infty$, we may choose $A > B$ satisfying $f(x) < f(A)$ for all $x < A$ and $f(x) > f(A)$ for all $x > A$. Let $x \in \mathbb{Z}$ with $x > A$. Because $f' > 0$ on $[B, +\infty) \supseteq [A, +\infty)$, $f(x+1) > f(x)$. If there were some $y \in \mathbb{Z}$ with $f(x+1) > f(y) > f(x)$, then $y > A$ by choice of A, but then $x < y < x+1$ by choice of B, which is impossible as $x, y \in \mathbb{Z}$. Hence $f(x+1) = \sigma(f(x))$ and f is of type 1. $\square$

We now consider polynomials of even degree.

Lemma 6. *Let $f \in \mathrm{Int}(\mathbb{Z})$ be of even degree. Then f is of type* 1 *or* 2. *It is of type* 1 *if and only if there is some $k \in \mathbb{Z}$ with $f(X-k) = f(-X)$. Lastly, if f is of type* 2 *then there is some $k \in \mathbb{Z}$ with $f(x+1) = \sigma(f(-x-k)) = \sigma^2(f(x))$ for all $x > A - k$.*

Proof. Let f be of even degree. As in Lemma 5, there is a constant B so that for all $x > B$, $f(x) < f(x+1)$. However, these might not be consecutive in $f(\mathbb{Z})$.

Suppose first that for some $k \in \mathbb{Z}$, $f(-X) = f(X-k)$. Then $f([B-k, +\infty)) = f((-\infty, -B])$. Thus the only values that can be between $f(x)$ and $f(x+1)$ for $x > N$ are $f((-B, B-k))$. As this set of potential exceptions is finite and $\lim_{x\to+\infty} f(x) = +\infty$, there is some $A > B$ such that, for all $x > A$, $f(x+1) = \sigma(f(x))$. Hence f is of type 1.

Suppose on the other hand that there is no $k \in \mathbb{Z}$ such that $f(-X) = f(X-k)$. We will show that f is of type 2 (and hence not of type 1). Write $f = aX^n + bX^{n-1} + O(X^{n-2})$, with n even. We set $g_t(X) = f(X-t) - f(-X) = (2b - ant)X^{n-1} + O(X^{n-2})$, and set $c = \frac{2b}{an}$. For $t \neq c$, we have $\mathrm{lc}(g_t) = 2b - ant$. Hence $\mathrm{lc}(g_t) > 0$ for $t < c$ and $\mathrm{lc}(g_t) < 0$ for $t > c$. We claim there exists $k \in \mathbb{Z}$ such that $\mathrm{lc}(g_{k-1}) > 0$ and $\mathrm{lc}(g_k) < 0$. If $c \notin \mathbb{Z}$, then choose $k = 1 + \lfloor c \rfloor$. If $c \in \mathbb{Z}$, then by our hypothesis g_c is not the zero polynomial so $\mathrm{lc}(g_c) \neq 0$. If $\mathrm{lc}(g_c) < 0$ choose $k = c$, otherwise choose $k = c+1$.

It follows that there is an integer constant $C > B$ so that, for all $x \geqslant C$, $g_{k-1}(x) > 0$ and $g_k(x) < 0$, that is $f(x-k+1) > f(-x) > f(x-k)$. Applying these inequalities repeatedly yields $f(C-k) < f(-C) < f(C-k+1) < f(-C-1) < f(C-k+2) < \cdots$. Only $f((-C, C-k))$ does not appear here. As this list is finite, there is some constant $A > C$ so that for all $x > A$, $f(x+1) = \sigma^2(f(x))$. Hence f is of type 2. $\square$

We are now ready to consider the case of $f, g \in \mathrm{Int}(\mathbb{Z})$ with $f(\mathbb{Z}) = g(\mathbb{Z})$. In Lemma 7 we will show that if f, g are of the same type then $f \sim g$. We will then show in Lemma 8 that if f is of type 1 and g is of type 2, then $f \nsim g$ and in fact $g(X) \sim f(2X)$.

Lemma 7. *Let $f, g \in \mathrm{Int}(\mathbb{Z})$ be of the same type with $f(\mathbb{Z}) = g(\mathbb{Z})$. Then $f \sim g$.*

Proof. Suppose first that f, g are of type 1, with corresponding constants A_f, A_g. Let $x \in \mathbb{Z}$ be chosen with $x > \max(A_f, A_g)$. Assume without loss that $f(x) \geqslant g(x)$. Since $x > A_g$ and $f(x) \in g(\mathbb{Z})$, it follows that $f(x) = \sigma^n(g(x)) = g(x+n)$ for some $n \in \mathbb{N}_0$. But now $f(x+j) = \sigma^j(f(x)) = \sigma^{n+j}(g(x)) = g(x+n+j)$ for all $j \in \mathbb{N}_0$. Hence $f(X) = g(X+n)$ and thus $f \sim g$.

Suppose now that f, g are of type 2, with corresponding constants A_f, A_g. There are integers $x, k, y, h \in \mathbb{Z}$ so that $f(x) < f(-x-k) < f(x+1) < f(-x-k-1) < \cdots$, these being consecutive values of f, and $g(y) < g(-y-h) < g(y+1) < g(-y-h-1) < \cdots$, these being consecutive values of g. As $f(\mathbb{Z}) = g(\mathbb{Z})$, we can arrange x and y to be such that either $f(x) = g(y)$ or $f(x) = g(-y-h)$, the values of both lists agreeing from then on. In the first case, let $n = y - x$. Then, $f(X)$ and $g(X+n)$ agree on $x, x+1, \ldots$ and thus $f(X) = g(X+n)$. In the second case, let $n = y + h - x$. Then $f(X)$ and $g(-X-n)$ agree on $x, x+1, \ldots$ and thus $f(X) = g(-X-n)$. In both cases $f \sim g$. $\square$

Lemma 8. *Let $f, g \in \mathrm{Int}(\mathbb{Z})$ with $f(\mathbb{Z}) = g(\mathbb{Z})$. Suppose that f is of type 1 and g is of type 2. Then $f(-X) = f(X-k)$ for some odd integer k, and $g \sim h$ where $h(X) = f(2X)$.*

Proof. Let $x, y, k \in \mathbb{Z}$ be such that $f(x) < f(x+1) < f(x+2) < \cdots$, these being consecutive values of f, and $g(y) < g(-y-k) < g(y+1) < g(-y-k-1) < \cdots$, these being consecutive values of g. Let $h(X) = f(2X)$. We arrange the lists so that either $h(x) = g(y)$ or $h(x) = g(-y-k)$. In the first case, for all $j \in \mathbb{N}_0$ we have that $h(x+j) = f(2x+2j) = \sigma^{2j}(f(2x)) = \sigma^{2j}(h(x)) = \sigma^{2j}(g(y)) = g(y+j)$ and hence $h(X) = g(Y)$. In the second case, for all $j \in \mathbb{N}_0$, $h(x+j) = f(2x+2j) = \sigma^{2j}(f(2x)) = \sigma^{2j}(h(x)) = \sigma^{2j}(g(-y-k)) = g(-y-k-j)$ and hence $h(X) = g(-Y-k)$. In either case, $h \sim g$.

As g is of type 2, $\deg(g)$ is even. Since $h \sim g$, $\deg(h)$ must be even. Finally $\deg(f) = \deg(h)$, so $\deg(f)$ is even. As f is of type 1, by Lemma 6 there is some $k \in \mathbb{Z}$ with $f(X-k) = f(-X)$. Now h satisfies $h(-X) = h(X - \frac{k}{2})$. But h is of type 2 since $h \sim g$. Hence, by Lemma 6, $\frac{k}{2}$ is not an integer and hence k is odd. $\square$

By Lemma 6 we know that all type 1 even-degree polynomials f satisfy $f(X-k) = f(-X)$ for some $k \in \mathbb{Z}$. By Lemma 8 we know that if such a polynomial shares an image set with a type 2 polynomial, then k must be odd. Lemma 1 gives the converse of this statement and completes the proof of Theorem 2.

We note that our proofs did not use the full power of $f(\mathbb{Z}) = g(\mathbb{Z})$, rather the intersection of each image set with some ray $[C, +\infty)$. This raises the question of what other infinite subsets of $\mathbb{Z}$ might be used instead of such a ray. Also, if we replace $(\mathbb{Z}, \mathbb{Q})$ with some other pair of domains, a natural question is to characterize when f, g have the same image on the subdomain.

Acknowledgments

The authors would like to thank Barbara McClain and Todor Kitchev for their helpful polynomial examples, and an anonymous referee for suggestions that improved the exposition of this note.

References

[1] P.-J. Cahen, J.-L. Chabert, Integer Valued-Polynomials, Amer. Math. Soc. Surveys Monogr., vol. 58, Amer. Math. Soc., Providence, 1997.
[2] P.-J. Cahen, J.-L. Chabert, What's new about integer-valued polynomials on a subset?, in: Non-Noetherian Commutative Ring Theory, Kluwer Academic Publishers, Boston, 2000, pp. 75–96.
[3] P.-J. Cahen, J.-L. Chabert, S. Frisch, Interpolation domains, J. Algebra 225 (2000) 794–803.
[4] J.-L. Chabert, Une caractérisation des polynômes prenant des valeurs entieres sur tous les nombres premiers, Canad. Math. Bull. 99 (1996) 273–282.
[5] J.-L. Chabert, S.T. Chapman, W.W. Smith, A basis for the ring of polynomials integer-valued on prime numbers, Lect. Notes Pure Appl. Math. 189 (1997) 271–284.
[6] S. Frisch, Interpolation by integer-valued polynomials, J. Algebra 211 (1999) 562–577.
[7] R. Gilmer, Sets that determine integer-valued polynomials, J. Number Theory 33 (1989) 95–100.
[8] D.L. McQuillan, Rings of integer-valued polynomials determined by finite sets, Math. Proc. R. Ir. Acad. 85 (1985) 177–184.
[9] D.L. McQuillan, On a theorem of R. Gilmer, J. Number Theory 39 (1991) 245–250.
[10] G. Peruginelli, U. Zannier, Parameterizing over $\mathbb{Z}$ integral values of polynomials over $\mathbb{Q}$, Comm. Algebra 38 (2010) 119–130.