PROJECTIVE P-ORDERINGS AND HOMOGENEOUS INTEGER-VALUED POLYNOMIALS

K. Johnson
Department of Mathematics, Dalhousie University, Halifax, Nova Scotia, Canada
johnson@mathstat.dal.ca

D. Patterson
Department of Mathematics, Dalhousie University, Halifax, Nova Scotia, Canada
donaldp@mathstat.dal.ca

Received: 7/22/10, Accepted: 1/16/11, Published: 3/18/11

Abstract

Bhargava defined p-orderings of subsets of Dedekind domains and with them studied polynomials which take integer values on those subsets. In analogy with this construction for subsets of $\mathbb{Z}_{(p)}$ and p-local integer-valued polynomials in one variable, we define projective p-orderings of subsets of $\mathbb{Z}^2_{(p)}$. With such a projective p-ordering for $\mathbb{Z}^2_{(p)}$ we construct a basis for the module of homogeneous, p-local integer-valued polynomials in two variables.

1. Introduction

Let p be a fixed prime and denote by ν_p the p-adic valuation with respect to p, i.e., $\nu_p(m)$ is the largest power of p dividing m. If S is a subset of $\mathbb{Z}$ or $\mathbb{Z}_{(p)}$ then a p-ordering of S, as defined by Bhargava in [2] and [3], is a sequence $\{a(i) : i = 0, 1, 2, \dots\}$ in S with the property that for each $n > 0$ the element $a(n)$ minimizes $\{\nu_p(\prod_{i=0}^{n-1}(s - a(i))) : s \in S\}$. The most important property of p-orderings is that the Lagrange interpolating polynomials based on them give a $\mathbb{Z}_{(p)}$-basis for the algebra $\mathrm{Int}(S, \mathbb{Z}_{(p)}) = \{f(x) \in \mathbb{Q}[x] : f(S) \subseteq \mathbb{Z}_{(p)}\}$, of p-local integer-valued polynomials on S. In this paper we will extend this idea to give p-orderings of certain subsets of $\mathbb{Z}^2$ or $\mathbb{Z}^2_{(p)}$ in such a way as to give a construction of a $\mathbb{Z}_{(p)}$-basis for the module of p-local integer-valued homogeneous polynomials in two variables.

One reason the algebra of homogeneous integer-valued polynomials is of interest is because of its occurence in algebraic topology as described in [1]. Let $\mathbb{C}P^\infty$ denote infinite complex projective space. Computing the homotopy groups of this space shows that it is an Eilenberg-Mac Lane space $K(\mathbb{Z}, 2)$ and so is the classifying space, BT^1, of the circle group. It follows that $(\mathbb{C}P^\infty)^n$ is the classifying space of the n-torus, BT^n. It was shown in [6] that the complex K-theory, $K_0(\mathbb{C}P^\infty)$, is isomorphic to $\mathrm{Int}(\mathbb{Z},\mathbb{Z})$ from which it follows that $K_0(BT^n) = \mathrm{Int}(\mathbb{Z}^n,\mathbb{Z}) = \{f(x_1,\ldots,x_n) \in \mathbb{Q}[x_1,\ldots,x_n] : f(\mathbb{Z}^n) \subseteq \mathbb{Z}\}$. For any space X the complex K-theory, $K_0(X)$, has the structure of a comodule with respect to the Hopf algebroid of stable cooperations for complex K-theory, K_0K. In [1] it was shown that the primitive elements in $K_0(BT^n)$ with respect to this coaction are the homogeneous polynomials and this was used to give an upper bound on the K-theory Hurewicz image of BU. Projective p-orderings give an alternative to the recursive construction used in Theorem 1.11 of that paper.

The paper is organized as follows: In Section 2 we recall some of the basic properties of p-orderings of subsets of $\mathbb{Z}_{(p)}$ which allow their computation in specific cases. Section 3 contains the definition of projective p-orderings for subsets of $\mathbb{Z}^2_{(p)}$ and the construction of a specific p-ordering of $\mathbb{Z}^2_{(p)}$ using the results of Section 2 and their extensions. Section 4 defines a sequence of homogeneous polynomials associated to a projective p-ordering and shows that in the case of p-orderings of $\mathbb{Z}^2_{(p)}$ these polynomials are $\mathbb{Z}_{(p)}$-valued when evaluated at points in $\mathbb{Z}^2_{(p)}$. From these a basis is constructed for the $\mathbb{Z}_{(p)}$-module of homogeneous p-local integer-valued polynomials in two variables of degree m for any nonnegative integer m.

2. p-Orderings in $\mathbb{Z}$ and $\mathbb{Z}_{(p)}$

As in the introduction we have the basic definitions:

Definition 1. [3] If p is a prime then a p-ordering of a subset S of $\mathbb{Z}_{(p)}$ is an ordered sequence $\{a_i, i = 0,1,2,\ldots |S|\}$ of elements of S with the property that for each $i > 0$ the element a_i minimizes $\nu_p(\prod_{j<i}(s - a_j))$ among all elements s of S.

and

Definition 2. [3] If $\{a_i\}_{i=0}^\infty$ is a p-ordering of a set $S \subseteq \mathbb{Z}_{(p)}$ then the p-sequence of S is the sequence of integers $D = \{d_i\}_{i=0}^\infty$ with $d_0 = 0$ and $d_i = \nu_p(\prod_{j<i}(a_i - a_j))$.

These objects have the following properties:

Proposition 3. (a) *The p-sequence of a set S is independent of the p-ordering used to compute it, i.e., any two p-orderings of S have the same p-sequence.*

(b) *The p-sequence of a set characterizes the p-orderings of S, i.e., if $\{d_i : i = 0,1,2,\ldots\}$ is the p-sequence of S and $\{a_i : i = 0,1,2,\ldots\}$ is a sequence in S with the property that $d_i = \nu_p(\prod_{j<i}(a_i - a_j))$ for all i, then $\{a_i : i = 0,1,2,\ldots\}$ is a p-ordering of S.*

(c) *The increasing order on the non-negative integers is a p-ordering of $\mathbb{Z}_{(p)}$ for any prime p, and the p-sequence of $\mathbb{Z}_{(p)}$ is given by $\{\nu_p(i!) : i = 0,1,2,\ldots\}$.*

(d) *The increasing order on the non-negative integers divisible by* p *is a* p*-ordering of* $p\mathbb{Z}_{(p)}$ *and the* p*-sequence of* $p\mathbb{Z}_{(p)}$ *is given by* $\{i + \nu_p(i!) : i = 0, 1, 2, \dots\}$.

(e) *If the set* S *is the disjoint union* $S = S_0 \cup S_1$ *of sets* S_0 *and* S_1 *with the property that if* $a \in S_0$ *and* $b \in S_1$ *then* $\nu_p(a - b) = 0$*, then the* p*-sequence of* S *is equal to the shuffle of those of* S_0 *and* S_1*, i.e., the disjoint union of the* p*-sequences of* S_0 *and* S_1 *sorted into nondecreasing order. Furthermore, the same shuffle applied to* p*-orderings of* S_0 *and* S_1 *will yield a* p*-ordering of* S *and any* p*-ordering of* S *occurs in this way.*

Proof. Statement (a) is Theorem 5 of citeB1. Statement(b) is Lemma 3.3(a) of [7]. Statement(c) follows from Proposition 6 of [2] and the observation that the minimum of $\nu_p(\prod_{j<i}(s - a_j))$ for $s \in \mathbb{Z}$ is equal to the minimum for $s \in \mathbb{Z}_{(p)}$. Statement (d) follows from Statement (c) by Lemma 3.3(c) of [7]. (e) is a generalization of Lemma 3.5 of [7] for which the same proof holds. □

In the next section, we define projective p-orderings for pairs in $\mathbb{Z}_{(p)}$ and show that there are analogs to some of the properties of p-orderings given above. Specifically, part (e) in Proposition 3 generalizes to projective p-orderings and allows $\mathbb{Z}^2_{(p)}$ to be divided into disjoint subsets whose p-orderings are obtained from parts (c) and (d) of Proposition 3. While there is no analog to part (a) in Proposition 3, we show that any projective p-ordering of all of $\mathbb{Z}^2_{(p)}$ (and some other specific subsets) will produce the same p-sequence, and so the p-sequence of $\mathbb{Z}^2_{(p)}$ is independent of the projective p-ordering used to compute it.

3. Projective p-Orderings in $\mathbb{Z}^2_{(p)}$

Definition 4. A projective p-ordering of a subset S of $\mathbb{Z}^2_{(p)}$ is a sequence $\{(a_i, b_i) : i = 0, 1, 2, \dots\}$ in S with the property that for each $i > 0$ the element (a_i, b_i) minimizes $\nu_p(\prod_{j<i}(sb_j - ta_j))$ over $(s, t) \in S$. The sequence $\{d_i : i = 0, 1, 2, \dots\}$ with $d_i = \nu_p(\prod_{j<i}(a_i b_j - b_i a_j))$ is the p-sequence of the p-ordering.

Lemma 5. a) *If* $\{(a_i, b_i) : i = 0, 1, 2, \dots\}$ *is a* p*-ordering of* $\mathbb{Z}^2_{(p)}$*, then for each* i *either* $\nu_p(a_i) = 0$ *or* $\nu_p(b_i) = 0$.

(b) *If* $\{(a_i, b_i) : i = 0, 1, 2, \dots\}$ *is a* p*-ordering of* $\mathbb{Z}^2_{(p)}$*, then there is another* p*-ordering* $\{(a'_i, b'_i) : i = 0, 1, 2, \dots\}$ *with the property that for each* i *either* $a'_i = 1$ *and* $p|b'_i$ *or* $b'_i = 1$ *and* $\{(a'_i, b'_i) : i = 0, 1, 2, \dots\}$ *has the same* p*-sequence as* $\{(a_i, b_i) : i = 0, 1, 2, \dots\}$.

Proof. (a) Since $\nu_p(psb_j - pta_j) = 1 + \nu_p(sb_j - ta_j)$, the pair (s, t) would always be chosen in place of the pair (ps, pt) in the construction of a p-ordering.

(b) By part (a) either a_i or b_i is a unit in $\mathbb{Z}_{(p)}$ for every i. Let $(a'_i, b'_i) = (1, b_i/a_i)$ if a_i is a unit and $p|b_i$, and $(a'_i, b'_i) = (a_i/b_i, 1)$ if b_i is a unit. In the first case we have $\nu_p(a_ib_j - b_ia_j) = \nu_p(b_j - b_ia_j/a_i) = \nu_p(a'_ib_j - b'_ia_j)$ for all j and similarly in the second case. Thus $\{(a'_i, b'_i) : i = 0, 1, 2, \dots\}$ is a p-ordering with the same p-sequence as $\{(a_i, b_i) : i = 0, 1, 2, \dots\}$. □

Definition 6. Let S denote the subset of $\mathbb{Z}^2_{(p)}$ consisting of pairs (a, b) with either $a = 1$ and $p|b$ or $b = 1$, and let $S_0 = \{(a, 1) : a \in \mathbb{Z}_{(p)}\}$ and $S_1 = \{(1, pb) : b \in \mathbb{Z}_{(p)}\}$.

Lemma 7. *The set S is the disjoint union of S_0 and S_1, and if $(a, b) \in S_0$ and $(c, d) \in S_1$ then $\nu_p(ad - bc) = 0$.*

Proof. The first assertion is obvious and the second follows from the observation that d is a multiple of p, and $b = c = 1$, so p does not divide $ad - 1$. □

Proposition 8. *Any p-ordering of S is the shuffle of p-orderings of S_0 and S_1 into nondecreasing order. The shuffle of any pair of p-sequences of S_0 and S_1 into nondecreasing order gives a p-sequence of S and the corresponding shuffle of the p-orderings of S_0 and S_1 that gave rise to these p-sequences gives a p-ordering of S.*

Proof. Let $\{(a_i, b_i) : i = 0, 1, 2, \dots\}$ be a p-ordering of S and $\{(a_{\sigma(i)}, b_{\sigma(i)}) : i = 0, 1, 2, \dots\}$ the subsequence of elements which are in S_0. The previous lemma implies that for any i, we have $\nu_p(\prod_{j<\sigma(i)}(a_{\sigma(i)}b_j - a_jb_{\sigma(i)})) = \nu_p(\prod_{j<i}(a_{\sigma(i)}b_{\sigma(j)} - a_{\sigma(j)}b_{\sigma(i)}))$, so that $\{(a_{\sigma(i)}, b_\sigma(i)) : i = 0, 1, 2, \dots\}$ is a p-ordering of S_0. A similar argument shows that the subsequence of elements in S_1 gives a p-ordering of S_1. Since S is the disjoint union of S_0 and S_1 it follows that $\{(a_i, b_i) : i = 0, 1, 2, \dots\}$ is the shuffle of these two subsequences.

Conversely, suppose that $\{(a'_i, b'_i) : i = 0, 1, 2, \dots\}$ is a p-ordering of S_0 with associated p-sequence $\{d'_i : i = 0, 1, 2, \dots\}$ and that $\{(a''_i, b'') : i = 0, 1, 2, \dots\}$ and $\{d''_i : i = 0, 1, 2, \dots\}$ are the corresponding objects for S_1. Assume as the induction hypothesis that the first $n+m+2$ terms in a p-sequence of S are the nondecreasing shuffle of $\{d'_i : i = 0, 1, 2, \dots, n\}$ and $\{d''_i : i = 0, 1, 2, \dots, m\}$ into nondecreasing order and that the corresponding shuffle of $\{(a'_i, b'_i) : i = 0, 1, 2, \dots, n\}$ and $\{(a''_i, b''_i) : i = 0, 1, 2, \dots, m\}$ is the first $n+m+2$ terms of a p-ordering of S. Since (a'_{n+1}, b'_{n+1}) minimizes $\nu_p(\prod_{j<n+1}(sb'_j - ta'_j))$ over S_0 and $\nu_p(a'_{n+1}b''_j - b'_{n+1}a''_j) = 0$, it also minimizes $\nu_p(\prod_{j<n+m+2}(sb_j - ta_j))$ over S_0. Similarly (a''_{m+1}, b''_{m+1}) minimizes this product over S_1. Since S is the union of these two sets, the minimum over S is realized by the one of these giving the smaller value. □

Lemma 9. (a) *the map $\phi : \mathbb{Z}_{(p)} \to S_0$ given by $\phi(x) = (x, 1)$ gives a 1 to 1 correspondence between p-orderings of $\mathbb{Z}$ and projective p-orderings of S_0 and preserves p-sequences.*

(b) *The map* $\psi : p\mathbb{Z}_{(p)} \to S_1$ *given by* $\psi(x) = (1, x)$ *gives a one-to-one correspondence between* p*-orderings of* $p\mathbb{Z}$ *and projective* p*-orderings of* S_1 *and preserves* p*-sequences.*

Proof. If (a, b) and (c, d) are in S_0 then $\nu_p(ad - bc) = \nu_p(a - c)$ since $b = d = 1$. Thus the map ϕ is a bijection, which preserves the p-adic norm and so preserves p-orderings and p-sequences. A similar argument applies to ψ. □

Proposition 10. (a) *A* p*-ordering of* $\mathbb{Z}^2_{(p)}$ *is given by the periodic shuffle of the sequences* $\{(i, 1) : i = 0, 1, 2, \dots\}$ *and* $\{(1, pi) : i = 0, 1, 2, \dots\}$ *which takes one element of the second sequence after each block of* p *elements of the first. The corresponding* p*-sequence is* $\{\nu_p(\lfloor pi/(p + 1)\rfloor)! : i = 0, 1, 2, \dots\}$.

(b) *The* p*-sequence of* $\mathbb{Z}^2_{(p)}$ *is independent of the choice of* p*-ordering used to compute it.*

Proof. p-orderings of $\mathbb{Z}_{(p)}$ and $p\mathbb{Z}_{(p)}$ are given in Proposition 3 and so, by Lemma 9, give p-orderings of S_0 and S_1 whose shuffle gives a p-ordering of S. The p-sequences of these two p-orderings are $\{\nu_p(i!) : i = 0, 1, 2, \dots\}$ and $\{\nu_p(pi!) : i = 0, 1, 2, \dots\}$, for which the nondecreasing shuffle is periodic taking one element of the second sequence after each p elements of the first. The result of this shuffle is the formula given.

Since the p-sequences of $\mathbb{Z}_{(p)}$ and $p\mathbb{Z}_{(p)}$ are independent of the choices of p-orderings, those of S_0 and S_1 are also. The p-sequence of S, being the shuffle of these two, is unique and so is independent of the chosen p-orderings. Finally, by Lemma 5 (b) any p-sequence of $\mathbb{Z}^2_{(p)}$ is equal to one of S, hence it is independent of the chosen p-ordering. □

4. Homogeneous Integer-Valued Polynomials in Two Variables

A p-ordering of a subset of $\mathbb{Z}$ or $\mathbb{Z}_{(p)}$ gives rise to a sequence of polynomials that are integer – or $\mathbb{Z}_{(p)}$ – valued on S. The analogous result for projective orderings is:

Proposition 11. *If* $\{(a_i, b_i) : i = 0, 1, 2, \dots\}$ *is a projective* p*-ordering of* $\mathbb{Z}^2_{(p)}$ *then the polynomials*

$$f_n(x, y) = \prod_{i=0}^{n-1} \frac{xb_i - ya_i}{a_nb_i - b_na_i}$$

are homogeneous and $\mathbb{Z}_{(p)}$*-valued on* $\mathbb{Z}^2_{(p)}$.

Proof. The minimality condition used to define projective p-orderings implies that for any $(a, b) \in \mathbb{Z}^2_{(p)}$, the p-adic value of $\prod_{i=0}^{n-1} a_nb_i - b_na_i$ is less than or equal to that of $\prod_{i=0}^{n-1} ab_i - ba_i$. □

For p-orderings of subsets of $\mathbb{Z}$ or $\mathbb{Z}_{(p)}$ we have the further result that the polynomials produced in this way give a regular basis for the module of integer-valued polynomials. To obtain an analogous result in the projective case we restrict our attention to the particular projective p-ordering of $\mathbb{Z}^2_{(p)}$ constructed in the previous section and, for a fixed nonnegative integer m, make the following definition:

Definition 12. For $0 \leq n \leq m$ and $\{(a_i, b_i) : i = 0, 1, 2, \dots\}$, the projective p-ordering of $\mathbb{Z}^2_{(p)}$ constructed in Proposition 10, let

$$g_n^m(x,y) = \begin{cases} y^{m-n} \displaystyle\prod_{i=0}^{n-1} \frac{xb_i - ya_i}{a_n b_i - b_n a_i} & \text{if} \quad (a_n, b_n) \in S_0 \\ x^{m-n} \displaystyle\prod_{i=0}^{n-1} \frac{xb_i - ya_i}{a_n b_i - b_n a_i} & \text{if} \quad (a_n, b_n) \in S_1. \end{cases}$$

Lemma 13. *The polynomials $g_n^m(x,y)$ have the properties*

$$g_n^m(a_i, b_i) = \begin{cases} 0 & \textit{if} \quad i < n \\ 1 & \textit{if} \quad i = n. \end{cases}$$

Proposition 14. *The set of polynomials $\{g_n^m(x,y) : n = 0, 1, 2, \dots, m\}$ forms a basis for the $\mathbb{Z}_{(p)}$-module of homogeneous polynomials in $\mathbb{Q}[x,y]$ of degree m which take values in $\mathbb{Z}_{(p)}$ when evaluated at points of $\mathbb{Z}^2_{(p)}$.*

Proof. First note that a homogeneous polynomial is $\mathbb{Z}_{(p)}$-valued on $\mathbb{Z}^2_{(p)}$ if and only if it is $\mathbb{Z}_{(p)}$-valued on S. To see this suppose that $g(x,y)$ is homogeneous of degree m and $\mathbb{Z}_{(p)}$-valued on S and that $(a,b) \in \mathbb{Z}^2_{(p)}$. If $(a,b) = (0,0)$ then $g(a,b) = 0$. If $(a,b) \neq (0,0)$ then $(a,b) = p^k(a',b')$ for some k with either a' or b' a unit in $\mathbb{Z}_{(p)}$. Since $g(x,y)$ is homogeneous, $g(a,b) = p^{km} g(a',b')$, and so if $g(a',b') \in \mathbb{Z}_{(p)}$ then $g(a,b) \in \mathbb{Z}_{(p)}$. If a' is a unit in $\mathbb{Z}_{(p)}$ and $p|b'$ then $(a',b') = a'(1, b'/a')$, and so $g(a',b') = (a')^m g(1, b'/a')$. Since $g(x,y)$ is $\mathbb{Z}_{(p)}$-valued on S_0 we have $g(1, b'/a') \in \mathbb{Z}_{(p)}$, and so $g(a',b') \in \mathbb{Z}_{(p)}$ since a' is a unit. A similar argument applies if b' is a unit.

Since no two of the elements of the p-ordering $\{(a_i, b_i) : i = 0, 1, 2, \dots\}$ are rational multiples of each other the previous lemma shows that the given set is rationally linearly independent and forms a basis for the rational vector space of homogeneous polynomials of degree m in $\mathbb{Q}[x,y]$. Let M be the $(m+1) \times (m+1)$ matrix whose (i,j)-th entry is $g_i^m(a_j, b_j)$. If $g(x,y) \in \mathbb{Q}[x,y]$ is homogeneous and of degree m, then there exists a unique vector on $A = (a_0, \dots, a_m) \in \mathbb{Q}^{m+1}$ such that $g(x,y) = \sum a_i g_i^m(x,y)$. Let V be the vector $V = (v_0, \dots, v_m) = (g(a_0, b_0), \dots, g(a_m, b_m))$ so that $V = AM$. If $g(x,y)$ is $\mathbb{Z}_{(p)}$-valued then $V \in \mathbb{Z}^{m+1}_{(p)}$. By the previous lemma, M is lower triangular with diagonal entries 1, and hence invertible over $\mathbb{Z}_{(p)}$. Thus $A \in \mathbb{Z}^{m+1}_{(p)}$ also, i.e., the set $\{g_n^m(x,y) : n = 0, 1, 2, \dots, m\}$ spans the $\mathbb{Z}_{(p)}$-module of homogeneous, $\mathbb{Z}_{(p)}$-valued polynomials of degree m and so forms a basis as required. □

Example 15. Let $p = 2$ and $m = 3$. By Proposition 10, the following is a projective 2-ordering of $\mathbb{Z}^2_{(2)}$:

$$\begin{array}{lll} (0,1), & (1,1), & (1,0), \\ (2,1), & (3,1), & (1,2), \\ (4,1), & (5,1), & \dots . \end{array}$$

With this projective 2-ordering, we construct $g^3_n(x,y)$ for $n = 0,1,2,3$:

$$\left\{ y^3, xy^2, x^2(x-y), \frac{xy(x-y)}{2} \right\}.$$

This set, by Proposition 14, forms a basis for the $\mathbb{Z}_{(2)}$-module of homogeneous polynomials in $\mathbb{Q}[x,y]$ of degree 3 which take values in $\mathbb{Z}_{(2)}$ when evaluated at points of $\mathbb{Z}^2_{(2)}$.

References

[1] A. Baker, F. Clarke, N. Ray, and L. Schwartz, On the Kummer congruences and the stable homotopy of BU, *Trans. Amer. Math. Soc.* **316** (1989), 385-432.

[2] M. Bhargava, P-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. Reine Angew. Math. (Crelle)* **490** (1997), 101-127.

[3] M. Bhargava, The factorial function and generalizations, *Amer. Math. Monthly* **107** (2000), 783-799.

[4] J. Boulanger, J.-L. Chabert, S. Evrard, and G. Gerboud, The characteristic sequence of integer-valued polynomials on a subset, *Lect. Notes in Pure and Appl. Math.* **205** (1999), 161-174.

[5] P.-J. Cahen and J.-L. Chabert, Integer Valued Polynomials, American Math. Society, Providence, R.I., 1997.

[6] F. Clarke, Self Maps of BU, *Math. Proc. Cam. Phil. Soc.* **89** (1981), 491-500.

[7] K. Johnson, P-orderings of Finite Subsets of Dedekind Domains, *J. Algebraic Combinatorics* **30** (2009), 233-253.

[8] G. Polya, Über ganzwertige Polynome in algebraischen Zahlkörper, *J. Reine Angew. Math. (Crelle)* **149** (1919), 97-116.