Integer-Valued Polynomials over $p \times p$ Matrices

Asmita Sodhi

Dalhousie University

acsodhi@dal.ca

November 4, 2019

Overview

1. Intro to IVPs
   - The ring of integer-valued polynomials
   - p-orderings and p-sequences
2. IVPs over Matrix Rings
   - Moving the problem to maximal orders
   - An analogue to p-orderings
3. The $p \times p$ Case
   - Structure of Δ_p
   - Subsets of $T = \pi\Delta_p$
   - The ν-sequence of Δ_p
   - Characteristic Polynomials
   - Computing Minimal Polynomials

The Ring of Integer-Valued Polynomials

The set

$$\mathrm{Int}(\mathbb{Z}) = \{f \in \mathbb{Q}[x] : f(\mathbb{Z}) \subseteq \mathbb{Z}\}$$

of rational polynomials taking integer values over the integers forms a subring of $\mathbb{Q}[x]$ called the *ring of integer-valued polynomials* (IVPs).

$\mathrm{Int}(\mathbb{Z})$ is a polynomial ring and has basis $\left\{\binom{x}{k} : k \in \mathbb{Z}_{>0}\right\}$ as a $\mathbb{Z}$-module, with

$$\binom{x}{k} := \frac{x(x-1)\cdots(x-(k-1))}{k!}\,, \qquad \binom{x}{0} = 1\,, \qquad \binom{x}{1} = x\,.$$

This basis is a *regular basis*, meaning that the basis contains exactly one polynomial of degree k for $k \geq 1$.

p-orderings

The study of IVPs on subsets of the integers greatly benefited from the introduction of p-orderings by Bhargava [1].

Definition

Let S be a subset of $\mathbb{Z}$ and p be a fixed prime. A *p-ordering of S* is a sequence $\{a_i\}_{i=0}^{\infty} \subseteq S$ defined as follows: choose an element $a_0 \in S$ arbitrarily. Further elements are defined inductively where, given $a_0, a_1, \ldots, a_{k-1}$, the element $a_k \in S$ is chosen so as to minimize the highest power of p dividing

$$\prod_{i=0}^{k-1} (a_k - a_i) \ .$$

p-sequences

The choice of a p-ordering gives a corresponding sequence:

Definition

The *associated p-sequence of S*, denoted $\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$, is the sequence wherein the k^{th} term $\alpha_{S,p}(k)$ is the power of p minimized at the k^{th} step of the process defining a p-ordering. More explicitly, given a p-ordering $\{a_i\}_{i=0}^{\infty}$ of S,

$$\alpha_{S,p}(k) = \nu_p\left(\prod_{i=0}^{k-1}(a_k - a_i)\right) = \sum_{i=0}^{k-1}\nu_p(a_k - a_i)\ .$$

Though the choice of a p-ordering of S is not unique, the associated p-sequence of a subset $S \subseteq \mathbb{Z}$ is independent of the choice of p-ordering [1].

These p-sequences can be used to define a generalization of the binomial polynomials to a specific set $S \subseteq \mathbb{Z}$ which serve as a basis for the integer-valued polynomials of S over $\mathbb{Z}$,

$$\mathrm{Int}(S, \mathbb{Z}) = \{f \in \mathbb{Q}[x] : f(S) \subseteq \mathbb{Z}\} \ .$$

IVPs over Matrix Rings

We are interested in studying IVPs over matrix rings.

We denote the set of rational polynomials mapping integer matrices to integer matrices by

$$\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z})) = \{f \in \mathbb{Q}[x] : f(M) \in M_n(\mathbb{Z}) \text{ for all } M \in M_n(\mathbb{Z})\} .$$

We know from Cahen and Chabert [2] that $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ has a regular basis, but it is not easy to describe using a formula in closed form [3].

Link to Maximal Orders

Finding a regular basis for $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$ is related to finding a regular basis for its integral closure, and we understand the latter object through studying its localizations at rational primes.

If p is a fixed prime, D is a division algebra of degree n^2 over $K = \mathbb{Q}_p$, and Δ_n is its maximal order, then we obtain the following useful result:

Proposition ([3], 2.1)

The integral closure of $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z})_{(p)})$ is $\mathrm{Int}_{\mathbb{Q}}(\Delta_n)$.

Thus, the problem of describing the integral closure of $\mathrm{Int}_{\mathbb{Q}}(M_n(\mathbb{Z})_{(p)})$ is exactly that of describing $\mathrm{Int}_{\mathbb{Q}}(\Delta_n)$, and so we move our attention towards studying IVPs over maximal orders.

An Analogue to p-orderings

Definition-Proposition ([4], 1.1, 1.2)

Let K be a local field with valuation ν, D a division algebra over K to which ν extends, Δ the maximal order in D, and S a subset of Δ.

- A *ν-ordering* of S is a sequence $\{a_i\} \subseteq S$ such that for each $k > 0$, the element a_k minimizes the quantity $\nu(f_k(a_0, \ldots, a_{k-1})(a))$ over $a \in S$, where $f_k(a_0, \ldots, a_{k-1}(x))$ is the minimal polynomial of the set $\{a_0, a_1, \ldots, a_{k-1}\}$, with the convention that $f_0 = 1$. We call $\alpha_S = \{\alpha_S(k) = \nu(f_k(a_0, \ldots, a_{k-1})(a_k)) : k = 0, 1, \ldots\}$ the *ν-sequence* of S.
- Additionally, let $\pi \in \Delta$ be a uniformizing element. Then the ν-sequence α_S depends only on the set S, and not on the choice of ν-ordering. The sequence of polynomials

$$\{\pi^{-\alpha_S(k)} f_k(a_0, \ldots, a_{k-1})(x) : k = 0, 1, \ldots\}$$

forms a regular Δ-basis for the Δ-algebra of polynomials which are integer-valued on S.

In order to use this proposition, we need to be able to construct a ν-ordering for the maximal order Δ_n. A recursive method for constructing ν-orderings for elements of a maximal order is based on two lemmas.

Lemma (see [4], 6.2)

Let $\{a_i : i = 0, 1, 2, \dots\}$ be a ν-ordering of a subset S of Δ_n with associated ν-sequence $\{\alpha_S(i) : i = 0, 1, 2, \dots\}$ and let b be an element in the centre of Δ_n. Then:

i) $\{a_i + b : i = 0, 1, 2, \dots\}$ is a ν-ordering of $S + b$, and the ν-sequence of $S + b$ is the same as that of S

ii) If p is the characteristic of the residue field of K (so that $(p) = (\pi)^n$ in Δ_n), then $\{pa_i : i = 0, 1, 2, \dots\}$ is a ν-ordering for pS and the ν-sequence of pS is $\{\alpha_S(i) + in : i = 0, 1, 2, \dots\}$

Lemma ([4], 5.2)

Let S_1 and S_2 be disjoint subsets of S with the property that there is a non-negative integer k such that $\nu(s_1 - s_2) = k$ for any $s_1 \in S_1$ and $s_2 \in S_2$, and that S_1 and S_2 are each closed with respect to conjugation by elements of Δ_n. If $\{b_i\}$ and $\{c_i\}$ are ν-orderings of S_1 and S_2 respectively with associated ν-sequence $\{\alpha_{S_1}(i)\}$ and $\{\alpha_{S_2}(i)\}$, then the ν-sequence of $S_1 \cup S_2$ is the sum of the linear sequence $\{ki : i = 0, 1, 2, \dots\}$ with the shuffle $\{\alpha_{S_1}(i) - ki\} \wedge \{\alpha_{S_2}(i) - ki\}$, and this shuffle applied to $\{b_i\}$ and $\{c_i\}$ gives a ν-ordering of $S_1 \cup S_2$.

The theory presented in the previous slides is utilized by Evrard and Johnson [3] to construct a ν-order for Δ_2 and establish a ν-sequence and regular basis for the IVPs on Δ_2 when the division algebra D is over the local field $\mathbb{Q}_2$.

We would like to extend these results to the general case, in order to find a regular basis for the integer-valued polynomials on Δ_n over the local field $\mathbb{Q}_2$. In particular, this talk focuses on the question when n is a prime.

Constructing Δ_p

We can decompose Δ_p as a union of subsets to which the lemmas apply. Let $\mathbb{Q}_2$ denote the 2-adic numbers, and let ζ be a $(2^p - 1)^{\text{th}}$ root of unity. Let θ be the automorphism of $\mathbb{Q}_2(\zeta)$ that maps $\theta(\zeta) = \zeta^2$. Define $p \times p$ matrices ω_p and π_p as:

$$\omega_p = \begin{pmatrix} \zeta & 0 & \cdots & 0 \\ 0 & \theta(\zeta) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \theta^{p-1}(\zeta) \end{pmatrix} \qquad \pi_p = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ 2 & 0 & \cdots & 0 \end{pmatrix}$$

The maximal order Δ_p with which we concern ourselves can be represented by

$$\Delta_p = \mathbb{Z}_2[\omega_p, \pi_p]$$

where $\mathbb{Z}_2$ denotes the 2-adic integers.

$$\Delta_p = \mathbb{Z}_2[\omega_p, \pi_p]$$

$$\omega_p = \begin{pmatrix} \zeta & 0 & \cdots & 0 \\ 0 & \theta(\zeta) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \theta^{p-1}(\zeta) \end{pmatrix} \qquad \pi_p = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ 2 & 0 & \cdots & 0 \end{pmatrix}$$

The elements ω_p and π_p observe the commutativity relation $\pi_p\omega_p = \omega_p^2\pi_p$, and note also that $\pi_p^p = 2I_p$. An element $z \in \Delta_p$ can be expressed as a $\mathbb{Z}_2$-linear combination of the elements $\{\omega_p^i\pi_p^j : 0 \leq i, j \leq p-1\}$, or else uniquely in the form $z = \alpha_0 + \alpha_1\pi_p + \cdots + \alpha_{p-1}\pi_p^{p-1}$ with $\alpha_i \in \mathbb{Z}_2(\zeta)$.

Conjugacy Classes mod π

The maximal order $\Delta_p = \mathbb{Z}_2[\omega, \pi]$ can be divided into the following conjugacy classes modulo π:

$$T = \{z \in \Delta_p : z \equiv 0 \pmod{\pi}\}$$
$$T + 1 = \{z \in \Delta_p : z \equiv I_p \pmod{\pi}\}$$
$$S_i = \{z \in \Delta_p : z \equiv \omega^{2^k i} \pmod{\pi}, 0 \leq k \leq p-1\}$$

There are $\frac{1}{p}(2^p - 2)$ such sets S_i.

Subsets of $T = \pi\Delta_p$

The set $T = \pi\Delta_p$ can be broken up into further subsets that are closed under conjugation modulo powers of π.

Lemma

Let $\widetilde{T} = \{z \in \Delta_p : z \equiv 0 \pmod{\pi^j}\} = \pi^j\Delta_p$. Then $\widetilde{T}$ splits into the sets $\{z \in \Delta_p : z \equiv 0 \pmod{\pi^{j+1}}\} = \pi^{j+1}\Delta_p$ and $\{z \in \Delta_p : z \equiv \omega^i\pi^j \pmod{\pi^{j+1}}, 1 \leq i \leq 2^p - 1\} = \pi^j\Delta_p \setminus \pi^{j+1}\Delta_p$, which are each closed under conjugation.

Proof.

It is clear that $\{z \in \Delta_p : z \equiv 0 \pmod{\pi^{j+1}}\}$ is closed under conjugation. Conjugating $z \equiv \pi^j \pmod{\pi^{j+1}} \in \Delta_p$ by an element of the form $\omega^k \pi^\ell$ gives

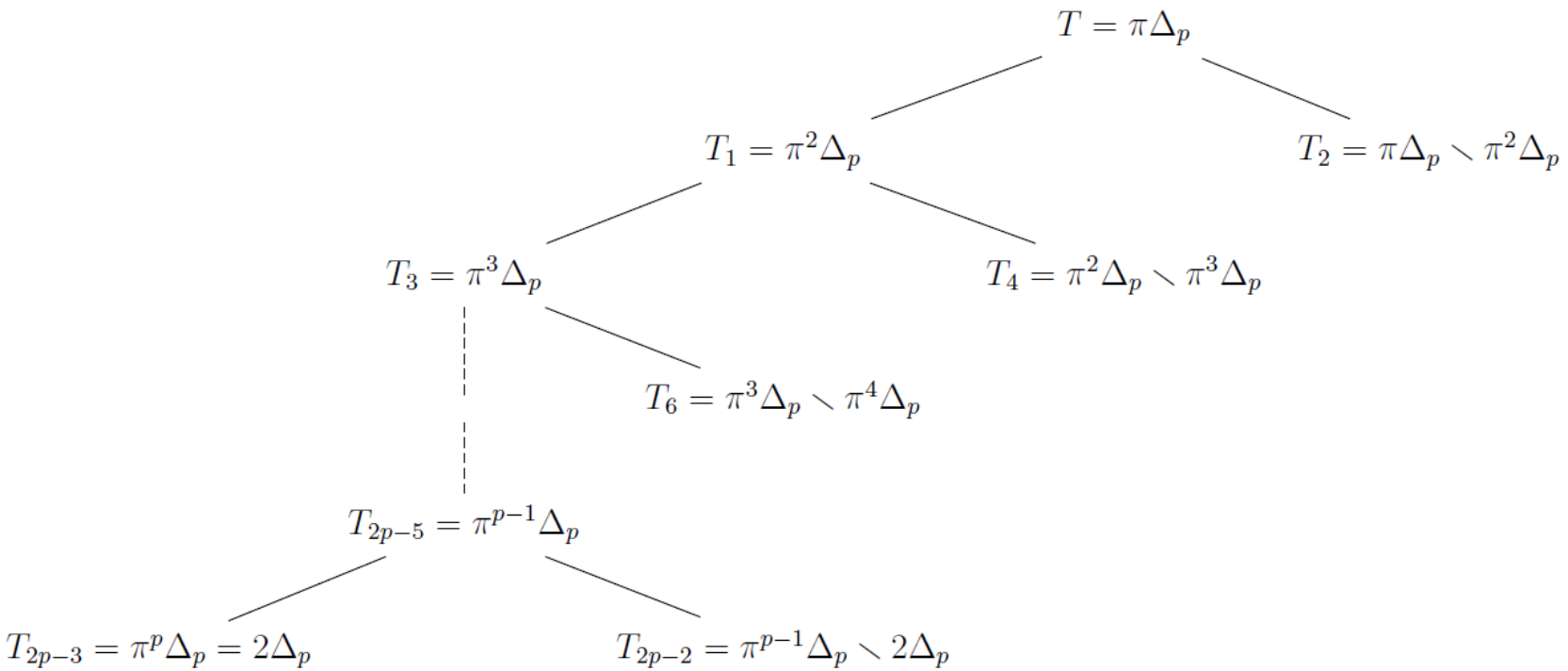
$$\omega^{k(1-2^j)}\pi^j$$

with j fixed such that $1 \leq j \leq p-1$ and $1 \leq \ell \leq p-1$, $1 \leq k \leq 2^p - 1$.

This set of elements will be all of $\pi^j \Delta_p \setminus \pi^{j+1}\Delta_p$ if and only if $k(1-2^j)$ forms a complete set of residues modulo $2^p - 1$, with j fixed and k variable.

This is indeed the case, and the result follows from a theorem about Mersenne numbers, from which it follows that since $\gcd(j, p) = 1$, we have $\gcd(1-2^j, 2^m - 1) = 1$. Therefore the set $\{\omega^{k(1-2^j)}\pi^j \pmod{\pi^{j+1}} : 1 \leq k \leq 2^p - 1\}$ is equivalent to the set $\{\omega^i \pi^j \pmod{\pi^{j+1}} : 1 \leq i \leq 2^p - 1\}$. □

Tree of Subsets of T



The ν-sequence of Δ_p

The subsets of Δ_p we have described will satisfy the earlier lemmas regarding constructing ν-sequences. We also note that the ν-sequence of each subset of the form S_i will be equal, so we will denote this sequence α_S.

From these lemmas, it is clear that the ν-sequence α_{Δ_p} of Δ_p will depend only on itself, α_S, and $\alpha_{T_{2k}}, 1 \leq k \leq p-1$.

The ν-sequence of Δ_p

Proposition

The ν-sequence α_{Δ_p} of the maximal order Δ_p is determined by the recursive formula

$$\begin{aligned}\alpha_{\Delta_p} = \Big[\Big[\cdots\Big[\Big[(\alpha_{\Delta_p} + (n)) \wedge \Big(\alpha_{T_{2(p-1)}} - ((p-1)n)\Big) + (n)\Big] \\ \wedge \Big(\alpha_{T_{2(p-2)}} - ((p-2)n)\Big) + (n)\Big] \wedge \cdots\Big] \\ \wedge (\alpha_{T_2} - (n)) + (n)]^{\wedge 2} \wedge \alpha_S^{\wedge \frac{1}{p}(2^p-2)}\end{aligned}$$

Characteristic Polynomials

To use a construction of IVPs analogous to that in [3], we would like to be able to describe subsets of Δ_p entirely in terms of their characteristic polynomials.

Lemma

Let $z \in \Delta_p$ be a non-constant element. The characteristic polynomial of z is irreducible over $\mathbb{Q}_2$.

Lemma ([5], 12.9 restated)

Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in K[x]$ be irreducible. Then

$$\nu(a_j) \geq \frac{n-j}{n}\nu(a_0) \ , \qquad 0 \leq j \leq n-1 \ .$$

Proposition

Let $T_{2k} = \pi^k \Delta_p \setminus \pi^{k+1} \Delta_p = \{z \in \Delta_p : z \equiv \omega^i \pi^k \pmod{\pi^{k+1}}, 1 \leq i \leq 2^p - 1\}$ for $k \geq 1$. Then for $z \in T_{2k}$, the coefficients of the characteristic polynomial $f_z(x) = a_0 + a_1 x + \cdots + a_{p-1} x^{p-1} + x^p$ satisfy

$$\begin{aligned} \nu_2(a_0) &= k \\ a_0 &\equiv 2^k \pmod{2^{k+1}} \\ \nu_2(a_j) &\geq k\left(\frac{p-j}{p}\right) = k\left(1 - \frac{j}{p}\right) \end{aligned}$$

and, conversely, any element $z \in \Delta_p$ with characteristic polynomial satisfying the above conditions is an element of T_{2k}.

Computing Minimal Polynomials

Consider the subset $T_{2k} = \pi^k \Delta_p \setminus \pi^{k+1} \Delta_p \subseteq \Delta_p$.

Let $\phi = (\phi_0, \phi_1, \ldots, \phi_{p-1})$ be defined on $\mathbb{Z}$ so that

$$\phi_0(b) = 2^k + 2^{k+1} \sum_{i \geq 0} b_{pi+p-1} 2^i$$

$$\phi_j(b) = 2^{\left\lceil \frac{(p-j)k}{p} \right\rceil} \sum_{i \geq 0} b_{pi+((jk-1) \pmod p)} 2^i$$

where $1 \leq j \leq p-1$ and $b = \sum_{i \geq 0} b_i 2^i$ is the expansion of $b \in \mathbb{Z}$ in base 2. Define a function

$$g_n(x) = \prod_{b=0}^{n-1} (x^p - \phi_{p-1}(b) x^{p-1} + \phi_{p-2}(b) x^{p-2} + \cdots + (-1)^p \phi_0(b)) \ .$$

Proposition

Let $z \in T_{2k}$, and let $m \in \mathbb{Z}$ be such that $\phi(m)$ gives a tuple consisting of the coefficients of the characteristic polynomial of z, with $\phi_j(m)$ being the coefficient of x^j, and let $0 \leq b \leq p$. Then

$$\begin{aligned}\nu(z^p - \phi_{p-1}(b)z^{p-1} + \phi_{p-2}(b)z^{p-2} + \cdots + (-1)^p\phi_0(b)) \\ = pk + 1 + \nu_2(m-b)\ .\end{aligned}$$

Lemma

If $z \in T_{2k}$ then

$$\nu(g_n(z)) \geq (pk+1)n + \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor$$

with equality if $\phi(n) = (\phi_0(n), \ldots, \phi_{p-1}(n))$ gives the tuple of coefficients $a_0, \ldots, a_{p-1}$ of the characteristic polynomial for $z \in T_{2k}$.

References

M. Bhargava.

The factorial function and generalizations.
The American Mathematical Monthly, 107(9):783–799, 2000.

P.-J. Cahen and J.-L. Chabert.

Integer-Valued Polynomials, volume 48 of *Mathematical Surveys and Monographs*.
American Mathematical Society, Providence, RI, USA, 1997.

S. Evrard and K. Johnson.

The ring of integer valued polynomials on 2×2 matrices and its integral closure.
Journal of Algebra, 441:660–677, 2015.

K. Johnson.

p-orderings of noncommutative rings.
Proceedings of the American Mathematical Society, 143(8):3265–3279, 2015.

I. Reiner.

Maximal Orders.
London Mathematical Society. Academic Press, London, 1975.