

## A Composite Problem

Asmita Sodhi

Dalhousie University

*acsodhi@dal.ca*

November 2, 2018

# 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
  - The Maximal Order  $\Delta_n$
- 3 The  $3 \times 3$  Case
  - Subsets of  $\Delta_3$
  - Characteristic polynomials
  - Towards computing  $\nu$ -sequences
- 4 The  $4 \times 4$  Case
  - Structure of  $\Delta_4$
  - Determining the  $\nu$ -sequence of  $\Delta_4$

# The Ring of Integer-Valued Polynomials

The set

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

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

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

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

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  $a_0, a_1, \dots, a_{k-1}$ , 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  $k^{\text{th}}$  term  $\alpha_{S,p}(k)$  is the power of  $p$  minimized at the  $k^{\text{th}}$  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  $p$ -orderings 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  $\mathbb{Z}$ ,

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

# IVPs over Matrix Rings

We are particularly interested in studying IVPs over matrix rings.

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

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

We know from Cahen and Chabert [2] that  $\text{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$  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  $\text{Int}_{\mathbb{Q}}(M_n(\mathbb{Z}))$  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  $\Delta_n$  is its maximal order, then we obtain the following useful result:

**Proposition ([3], 2.1)**

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

Thus, the problem of describing the integral closure of  $\text{Int}_{\mathbb{Q}}(M_n(\mathbb{Z})_{(p)})$  is exactly that of describing  $\text{Int}_{\mathbb{Q}}(\Delta_n)$ , 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  $\nu$ ,  $D$  a division algebra over  $K$  to which  $\nu$  extends,  $\Delta$  the maximal order in  $D$ , and  $S$  a subset of  $\Delta$ .

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

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

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

In order to use this proposition, we need to be able to construct a  $\nu$ -ordering for the maximal order  $\Delta_n$ . A recursive method for constructing  $\nu$ -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  $\nu$ -ordering of a subset  $S$  of  $\Delta_n$  with associated  $\nu$ -sequence  $\{\alpha_S(i) : i = 0, 1, 2, \dots\}$  and let  $b$  be an element in the centre of  $\Delta_n$ . Then:

- i)  $\{a_i + b : i = 0, 1, 2, \dots\}$  is a  $\nu$ -ordering of  $S + b$ , and the  $\nu$ -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  $\Delta_n$ ), then  $\{pa_i : i = 0, 1, 2, \dots\}$  is a  $\nu$ -ordering for  $pS$  and the  $\nu$ -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  $\Delta_n$ . If  $\{b_i\}$  and  $\{c_i\}$  are  $\nu$ -orderings of  $S_1$  and  $S_2$  respectively with associated  $\nu$ -sequence  $\{\alpha_{S_1}(i)\}$  and  $\{\alpha_{S_2}(i)\}$ , then the  $\nu$ -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  $\nu$ -ordering of  $S_1 \cup S_2$ .

The theory presented in the previous slides is utilized by Evrard and Johnson [3] to construct a  $\nu$ -order for  $\Delta_2$  and establish a  $\nu$ -sequence and regular basis for the IVPs on  $\Delta_2$  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  $\Delta_n$  over the local field  $\mathbb{Q}_2$ .

# Constructing $\Delta_n$

We can use these lemmas by decomposing  $\Delta_n$  as a union of subsets to which the lemmas apply. Let  $\mathbb{Q}_2$  denote the 2-adic numbers, and let  $\zeta$  be a  $(2^n - 1)^{\text{th}}$  root of unity. Let  $\theta$  be the automorphism of  $\mathbb{Q}_2(\zeta)$  that maps  $\theta(\zeta) = \zeta^2$ . Define  $n \times n$  matrices  $\omega_n$  and  $\pi_n$  as:

$$\omega_n = \begin{pmatrix} \zeta & 0 & \cdots & 0 \\ 0 & \theta(\zeta) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \theta^{n-1}(\zeta) \end{pmatrix} \quad \pi_n = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ 2 & 0 & \cdots & 0 \end{pmatrix}$$

The maximal order  $\Delta_n$  with which we concern ourselves is

$$\Delta_n = \mathbb{Z}_2[\omega_n, \pi_n]$$

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

$$\Delta_n = \mathbb{Z}_2[\omega_n, \pi_n]$$

$$\omega_n = \begin{pmatrix} \zeta & 0 & \cdots & 0 \\ 0 & \theta(\zeta) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \theta^{n-1}(\zeta) \end{pmatrix} \quad \pi_n = \begin{pmatrix} 0 & 1 & \cdots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \\ 2 & 0 & \cdots & 0 \end{pmatrix}$$

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

# The Maximal Order

We present in particular some results for  $\Delta_3 = \mathbb{Z}_2[\omega, \pi]$  with

$$\omega = \begin{pmatrix} \zeta & 0 & 0 \\ 0 & \zeta^2 & 0 \\ 0 & 0 & \zeta^4 \end{pmatrix} \quad \pi = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$$

where  $\zeta$  is a 7<sup>th</sup> root of unity.

In addition to the relations  $\pi\omega = \omega^2\pi$  and  $\pi^3 = 2I_3$ , we also work with the convention that

$$\zeta + \zeta^2 + \zeta^4 \equiv 0 \pmod{2} \quad \text{and} \quad \zeta^3 + \zeta^5 + \zeta^6 \equiv 1 \pmod{2} .$$

The valuation in  $\Delta_3$  is described by  $\nu(z) = \nu_2(\det(z))$  for  $z \in \Delta_3$  realized as a matrix, where  $\nu_2$  denotes the 2-adic valuation.

# Conjugacy Classes mod $\pi$

Looking at all elements of  $\Delta_3 = \mathbb{Z}_2[\omega, \pi]$  modulo  $\pi$ , we obtain four conjugacy classes:

$$T = \{z \in \Delta_3 : z \equiv 0 \pmod{\pi}\}$$

$$T + 1 = \{z \in \Delta_3 : z \equiv I_3 \pmod{\pi}\}$$

$$S = \{z \in \Delta_3 : z \equiv \omega \text{ or } \omega^2 \text{ or } \omega^4 \pmod{\pi}\}$$

$$S + 1 = \{z \in \Delta_3 : z \equiv \omega^3 \text{ or } \omega^6 \text{ or } \omega^5 \pmod{\pi}\}$$

$$= \{z \in \Delta_3 : z \equiv \omega + I_3 \text{ or } \omega^2 + I_3 \text{ or } \omega^4 + I_3 \pmod{\pi}\}$$



# Conjugacy Classes mod $\pi^2$

We can break the set  $T$  down further by considering conjugacy classes modulo  $\pi^2$ :

$$T_1 = \{z \in \Delta_3 : z \equiv 0 \pmod{\pi^2}\} = \pi^2 \Delta$$

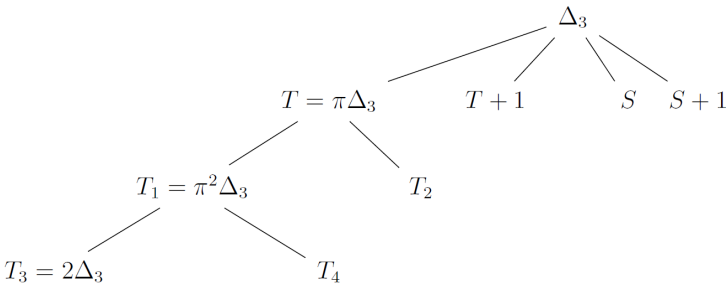
$$T_2 = \{z \in \Delta_3 : z \equiv \omega^i \pi \pmod{\pi^2} \text{ for some } 0 \leq i \leq 6\}$$

The set  $T_1$  can be broken down further still by looking at conjugacy classes modulo  $\pi^3 = 2$ :

$$T_3 = \{z \in \Delta_3 : z \equiv 0 \pmod{\pi^3}\} = 2\Delta$$

$$T_4 = \{z \in \Delta_3 : z \equiv \omega^i \pi^2 \pmod{\pi^3} \text{ for some } 0 \leq i \leq 6\}$$

From this analysis, we obtain the following tree of subsets of  $\Delta_3$ :



These sets all satisfy the necessary lemmas pertaining to shuffles of  $\nu$ -sequences, and so we can derive a formula for  $\alpha_{\Delta_3}$  that depends only on itself,  $\alpha_S$ ,  $\alpha_{T_2}$ , and  $\alpha_{T_4}$ .

# Characteristic Polynomials

The tree of subsets and the lemmas show us that the  $\nu$ -sequence of  $\Delta_3$  is recursively defined and also depends on the  $\nu$ -sequences of  $S, T_2, T_4$ .

It remains to determine the  $\nu$ -sequences for these sets, and to do so, it is useful to describe them in terms of their characteristic polynomials.

Given a  $3 \times 3$  matrix  $A$ , we define the characteristic polynomial of  $A$  to be

$$x^3 - \text{Tr}(A)x^2 + \beta(A)x - \det(A)$$

where  $\text{Tr}(A)$  and  $\det(A)$  are the usual trace and determinant of a  $3 \times 3$  matrix, and  $\beta(A)$  is defined in terms of the  $2 \times 2$  minors of  $A$ .

## Lemma

$$S = \{z \in \Delta_3 : \text{Tr}(z) \equiv 0 \pmod{2}, \beta(z) \equiv 1 \pmod{2}, \det(z) \equiv 1 \pmod{2}\}$$

$$T_2 = \{z \in \Delta_3 : \text{Tr}(z) \equiv 0 \pmod{2}, \beta(z) \equiv 0 \pmod{2}, \det(z) \equiv 2 \pmod{4}\}$$

$$T_4 = \{z \in \Delta_3 : \text{Tr}(z) \equiv 0 \pmod{2}, \beta(z) \equiv 0 \pmod{4}, \det(z) \equiv 4 \pmod{8}\}$$

We can determine some useful facts about the valuation of certain polynomials within  $S$ ,  $T_2$ , and  $T_4$ , with the goal of establishing these as the minimal polynomials within their respective sets. This process is analogous to the one presented in Evrard and Johnson [3] and Johnson [4].

# A Polynomial in $T_2$

Recall that

$$T_2 = \{z \in \Delta_3 : \text{Tr}(z) \equiv 0 \pmod{2}, \beta(z) \equiv 0 \pmod{2}, \det(z) \equiv 2 \pmod{4}\}.$$

Let us define the function

$$\psi = (\psi_1, \psi_2, \psi_3) : \mathbb{Z}_{\geq 0} \rightarrow 2\mathbb{Z}_{\geq 0} \times 2\mathbb{Z}_{\geq 0} \times (2 + 4\mathbb{Z}_{\geq 0})$$

$$\psi(n) = \left( 2 \sum_{i \geq 0} n_{3i+1} 2^i, 2 \sum_{i \geq 0} n_{3i} 2^i, 2 + 4 \sum_{i \geq 0} n_{3i+2} 2^i \right)$$

where  $n = \sum_{i \geq 0} n_i 2^i$  is the expansion of  $n$  in base 2. Let

$$g_n(x) = \prod_{k=0}^{n-1} (x^3 - \psi_1(k)x^2 + \psi_2(k)x - \psi_3(k)).$$

**Lemma**

If  $z \in T_2$  then

$$\nu(g_n(z)) \geq 4n + \sum_{i>0} \left\lfloor \frac{n}{2^i} \right\rfloor.$$

The polynomials constructed in the previous slide will be the minimal polynomial of a sequence of elements in  $T_2$ , which then suggests that this sequence extends to a  $\nu$ -ordering. The associated  $\nu$ -sequence will be the valuation of these polynomials, which we have calculated.

This method of creating minimal polynomials based on the characteristic polynomial that defines a conjugacy class within  $\Delta_3$  can be extended to any subset  $S$  of a maximal order  $\Delta_n$  sitting in  $M_n(\mathbb{Q}_2)$  that is closed under conjugation. However, the practical use of the construction comes from the fact that it is possible to achieve a known minimum when taking the valuation of the polynomials generated.

## Extension to General $n$

For any valuation  $\nu$ , if the valuation of  $n$  terms  $a_1, \dots, a_n$  produces a complete set of residues modulo  $n$ , then it must be the case that  $\nu(a_1 + \dots + a_n) = \min_{1 \leq i \leq n} \nu(a_i)$ . This fact is applied in the valuation of the polynomial

$$f(z) = z^n - \phi_1(k)z^{n-1} + \phi_2(k)z^{n-2} + \dots + (-1)^n \phi_n(k)$$

with  $z \in S \subseteq \Delta_n$  to show that a minimum for  $\nu(f)$  can be determined with certainty only when  $\gcd(n, \nu(z)) = 1$ .

In particular, if  $n = q$  is a prime, then a polynomial construction such as that of  $T_2$  in the  $3 \times 3$  case (given in detail for the  $2 \times 2$  case in [3] and [4]) will be possible for all conjugacy classes in the maximal order  $\Delta_q$ .

The construction will also work for some subsets of  $\Delta_n$  when  $n$  is composite, in particular for conjugacy classes modulo  $\pi^j$  where  $\gcd(j, n) = 1$ . It remains to see what adjustments must be made to this construction in the case where  $n$  is composite, and if there is any difference between the case where  $n$  is a power of a prime or  $n$  is squarefree.



# Structure of $\Delta_4$

We now consider  $\Delta_4 = \mathbb{Z}_2[\omega, \pi]$  with

$$\omega = \begin{pmatrix} \zeta & 0 & 0 & 0 \\ 0 & \zeta^2 & 0 & 0 \\ 0 & 0 & \zeta^4 & 0 \\ 0 & 0 & 0 & \zeta^8 \end{pmatrix} \quad \pi = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 \end{pmatrix}$$

where  $\zeta$  is a 15<sup>th</sup> root of unity.

In addition to the relations  $\pi\omega = \omega^2\pi$  and  $\pi^4 = 2I_4$ , we also work with the convention that

$$\zeta^3 + \zeta^4 + \zeta^7 \equiv 0 \pmod{2} \quad \text{and} \quad \zeta + \zeta^5 + \zeta^8 \equiv 1 \pmod{2} .$$

As previously, the valuation in  $\Delta_4$  is described by  $\nu(z) = \nu_2(\det(z))$  for  $z \in \Delta_4$  realized as a matrix, where  $\nu_2$  denotes the 2-adic valuation.

# Conjugacy Classes modulo $\pi$

Looking at all elements of  $\Delta_4 = \mathbb{Z}_2[\omega, \pi]$  modulo  $\pi$ , we obtain six conjugacy classes:

$$T = \{z \in \Delta_4 : z \equiv 0 \pmod{\pi}\} = \pi\Delta$$

$$T + 1 = \{z \in \Delta_4 : z \equiv I_4 \pmod{\pi}\}$$

$$S_1 = \{z \in \Delta_4 : z \equiv \omega \text{ or } \omega^2 \text{ or } \omega^4 \text{ or } \omega^8 \pmod{\pi}\}$$

$$S_2 = \{z \in \Delta_4 : z \equiv \omega^7 \text{ or } \omega^{11} \text{ or } \omega^{13} \text{ or } \omega^{14} \pmod{\pi}\}$$

$$S_3 = \{z \in \Delta_4 : z \equiv \omega^3 \text{ or } \omega^6 \text{ or } \omega^9 \text{ or } \omega^{12} \pmod{\pi}\}$$

$$S_4 = \{z \in \Delta_4 : z \equiv \omega^5 \text{ or } \omega^{10} \pmod{\pi}\}$$

We can break down the set  $T$  further into subsets:

$$T_1 = \{z \in \Delta_4 : z \equiv 0 \pmod{\pi^2}\} = \pi^2 \Delta_4$$

$$T_2 = \{z \in \Delta_4 : z \equiv \omega^i \pi \pmod{\pi^2} \text{ for some } 0 \leq i \leq 14\}$$

$$T_3 = \{z \in \Delta_4 : z \equiv 0 \pmod{\pi^3}\} = \pi^3 \Delta_4$$

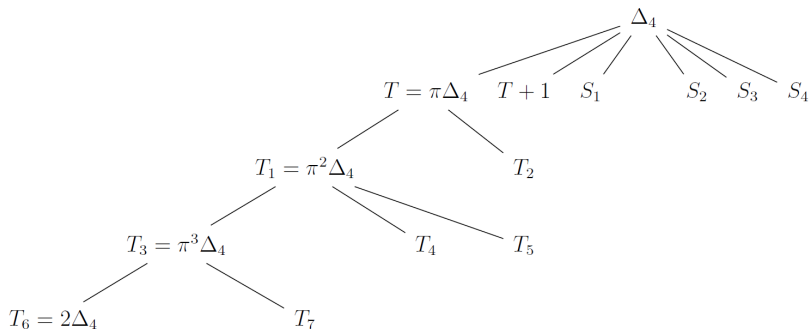
$$T_4 = \{z \in \Delta_4 : z \equiv \omega^i \pi^2 \pmod{\pi^3} \text{ for some } i \equiv 0 \pmod{3}\}$$

$$T_5 = \{z \in \Delta_4 : z \equiv \omega^i \pi^2 \pmod{\pi^3} \text{ for some } i \not\equiv 0 \pmod{3}\}$$

$$T_6 = \{z \in \Delta_4 : z \equiv 0 \pmod{\pi^4}\} = \{z \in \Delta_4 : z \equiv 0 \pmod{2}\} = 2\Delta_4$$

$$T_7 = \{z \in \Delta_4 : z \equiv \omega^i \pi^3 \pmod{\pi^4} \text{ for some } 0 \leq i \leq 14\}$$

From this analysis, we obtain the following tree of subsets of  $\Delta_4$ :



## $\nu$ -sequence of $\Delta_4$

The  $\nu$ -sequence of  $\Delta_4$  will be recursively defined, and will also depend on the  $\nu$ -sequences of the  $S_i$ ,  $T_2$ ,  $T_4$ ,  $T_5$ , and  $T_7$ .

For each  $z \in S_i$  we have  $\nu(z) = 0$ , for  $z \in T_2$  we have  $\nu(z) = 1$ , for  $z \in T_4$  and  $z \in T_5$  we have  $\nu(z) = 2$ , and for  $z \in T_7$  we have  $\nu(z) = 3$ . Since our aforementioned construction involving taking the valuation of products of characteristic polynomials works when  $\gcd(n, \nu(z)) = 1$ , we will be able to use this method for computing the  $\nu$ -sequences of the  $S_i$  for  $i = 1, 2, 3$ ,  $T_2$ , and  $T_7$ .

We will encounter problems for  $S_4$  since the characteristic polynomial of its elements modulo 2 is reducible, and for  $T_4$  and  $T_5$  because the valuation of elements in the set are not relatively prime to the dimension.

# A Potential Polynomial in $T_5$

Let us define the function

$$\phi = (\phi_1, \phi_2, \phi_3, \phi_4) : \mathbb{Z}_{\geq 0} \rightarrow 2\mathbb{Z}_{\geq 0} \times (2 + 4\mathbb{Z}_{\geq 0}) \times 4\mathbb{Z}_{\geq 0} \times (4 + 8\mathbb{Z}_{\geq 0})$$

$$\phi(n) = \left( 2 \sum_{i \geq 0} n_{4i} 2^i, 2 + 4 \sum_{i \geq 0} n_{4i+2} 2^i, 4 \sum_{i \geq 0} n_{4i+1} 2^i, 4 + 8 \sum_{i \geq 0} n_{4i+3} 2^i \right)$$

where  $n = \sum_{i \geq 0} n_i 2^i$  is the expansion of  $n$  in base 2. Let  $z \in T_5$ , let  $k \geq 0$ , and let

$$f_z(k) = z^4 - \phi_1(k)z^3 + \phi_2(k)z^2 - \phi_3(k)z + \phi_4(k).$$

Then

$$\nu(f_z(k)) \geq \begin{cases} 10 + \nu_2(m - k) & \text{if } \nu_2(m - k) \equiv 0 \pmod{2} \\ 9 + \nu_2(m - k) & \text{if } \nu_2(m - k) \equiv 1 \pmod{2} \end{cases}$$

where  $m \in \mathbb{Z}$  is chosen so that  $f(m)$  is the characteristic polynomial of  $z \in T_5$ .

$$\nu(f_z(k)) \geq \begin{cases} 10 + \nu_2(m - k) & \text{if } \nu_2(m - k) \equiv 0 \pmod{2} \\ 9 + \nu_2(m - k) & \text{if } \nu_2(m - k) \equiv 1 \pmod{2} \end{cases}$$

Note that due to the nature of the set  $T_5$ , we will not have any cancellation of terms when evaluating  $\nu(f_z(k))$ . This means that equality can be achieved in the expression above, and so too is the case for products of such polynomials  $f_z(k)$ , as we saw in the  $3 \times 3$  case. Therefore, we are still able to use this construction to establish a  $\nu$ -sequence for  $T_5$ .

# The Case of $T_4$

For  $z \in T_4$ , the result in constructing potential minimal polynomials is the same as for  $T_5$ :

$$\nu(f_z(k)) \geq \begin{cases} 10 + \nu_2(m - k) & \text{if } \nu_2(m - k) \equiv 0 \pmod{2} \\ 9 + \nu_2(m - k) & \text{if } \nu_2(m - k) \equiv 1 \pmod{2} \end{cases}$$

However, in the case of  $T_4$ , it is possible to choose elements in the set such that elements cancel when computing the valuation of a polynomial  $f_z(k)$ .

This means that we *cannot* guarantee equality in the above expression, and our inequality becomes strict when we consider products of such polynomials  $f_z(k)$ . A different method of approach is necessary for  $T_4$ .



## Next Steps

We can view  $\Delta_2$  as being embedded in  $\Delta_4$ . In  $\Delta_2$ , the subset denoted  $T_1$  is defined by

$$T_1 = \{z \in \Delta_2 : \text{Tr}(z) \equiv 0 \pmod{2}, N(z) \equiv 2 \pmod{4}\}$$

where characteristic polynomials are denoted as  $x^2 - \text{Tr}(z)x + N(z)$ . The characteristic polynomial of an element of  $T_1 \subseteq \Delta_2$ , when squared, has the same form as expected for the characteristic polynomial of an element in  $T_4 \subseteq \Delta_4$ .

We may be able to learn more about the  $\nu$ -sequence of  $T_4$  by looking at the squares of polynomials in  $\Delta_2$  and noting the relationship with the denominator.

# 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  $2 \times 2$  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.