COMPUTING J-IDEALS OF A MATRIX OVER A PRINCIPAL IDEAL DOMAIN

CLEMENS HEUBERGER AND ROSWITHA RISSNER

Abstract. Given a square matrix $B$ over a principal ideal domain $D$ and an ideal $J$ of $D$, the $J$-ideal of $B$ consists of the polynomials $f \in D[X]$ such that all entries of $f(B)$ are in $J$. It has been shown that in order to determine all $J$-ideals of $B$ it suffices to compute a generating set of the $(p^t)$-ideal of $B$ for finitely many prime powers $p^t$. Moreover, it is known that a $(p^t)$-ideal is generated by a set of polynomials of the form $p^{t-s}f_s$ for certain $s \leq t$ where each $f_s$ is a monic polynomial of minimal degree in the $(p^s)$-ideal of $B$. However, except for the case of diagonal matrices, it was not known how to determine these polynomials explicitly. We present an algorithm which allows us to compute the polynomials $f_s$ for general square matrices. Exploiting one of McCoy’s theorems we first compute some set of generators of the $(p^n)$-ideals of $B$ for finitely many prime powers $p^n$. It is further known that these so-called $(p^n)$-minimal polynomials are strongly related to the decomposition of the modules

$$(D/p^n D) [B + M_n(p^n D)] = \{ f(B + M_n(p^n D)) \mid f \in (D/p^n D)[X] \}$$

into cyclic submodules with ascending annihilators, see Section 2.3. However, the characterization of these generating sets given in [9] is theoretic. Except for diagonal matrices, it was not known until now how to compute $(p^n)$-minimal polynomials. This paper is the algorithmic counterpart of [9]. Algorithm 5 determines these polynomials explicitly for general square matrices $B$ with entries in a principal ideal domain. The iterative computation consists of two main steps. Given a generating system of the $(p^{t-1})$-ideal of $B$, we first determine a set $F$ of polynomials such that $N_{(p^t)}(B) = (F) + pN_{(p^{t-1})}(B)$. We then perform a couple of carefully chosen polynomial long divisions to compute a $(p^n)$-minimal polynomial.

In order to determine the set $F$, we use a description of the null ideal of a matrix given by McCoy in [8, Theorem 54] (see Lemma 4.2). This result allows us to translate the question to that of solving a system of linear equations modulo $p^n$. In order to solve this linear system, we present a special lifting technique in Section 3. The application of this technique to the original question is considered in Section 4. The topic of Section 5 is then the computation of a $(p^n)$-minimal polynomial. Next, in Section 6 we explain why the minimal polynomial $\mu_B$ of $B$ is a $(p^n)$-minimal polynomial for all but finitely many prime elements $p$. Finally, in Section 7 we prove that for the
remaining prime elements \( p \) it suffices to determine a finite number of \((p')\)-minimal polynomials to describe the \((p')\)-ideals for all \( t \geq 0 \).

2. Results

All rings considered in this paper are assumed to be commutative with unity. For a ring \( R \) and positive integers \( r, s \), the set of \((r \times s)\)-matrices over \( R \) is denoted by \( M_{r,s}(R) \) or by \( M_r(R) \) if \( r = s \).

2.1. \((a)\)-ideals of matrices. Let \( D \) be a principal ideal domain with quotient field \( K \), \( B \in M_n(D) \) and \((a)\) be an ideal of \( D \). The aim is to describe the structure of the \((a)\)-ideal

\[
N_{(a)}(B) = \{ f \in D[X] \mid f(B) \equiv 0 \pmod{a} \}
\]

of \( B \).

If \( a = 0 \), then it is easily seen that

\[
N_{(0)}(B) = \mu_B D[X]
\]

where \( \mu_B \) is the minimal polynomial of \( B \) over the quotient field \( K \) of \( D \), cf. [3].

If \( 0 \neq a = bc \) for coprime elements \( b \) and \( c \), then \( N_a(B) = cN_b(B) + bN_c(B) \) according to [9, Lemma 2.9]. Since every element in \( D \) has a decomposition into primes, it suffices to consider the case \( a = p^t \) where \( p \) is a prime element and \( t \in \mathbb{N} \).

For almost all prime elements \( p \), we have

\[
N_{(p^t)}(B) = \mu_B D[X] + p^t D[X]
\]

for \( t \geq 1 \). More precisely, this is the case for all primes \( p \) which do not divide \( \det(T) \) where \( T \) is a matrix in \( M_n(D) \cap \text{GL}_n(K) \) such that \( TBT^{-1} \) is in rational canonical form, see Theorem 4. However, the transformation matrix \( T \) is not uniquely determined and the set of prime divisors \( \det(T) \) depends on the choice of \( T \), see Example 6.1.

Thus it is sufficient to determine \( N_{(p^t)}(B) \) for finitely many primes \( p \). The following result is a consequence of [9, Theorem 2.19, Corollary 2.23]. We give a proof below in Section 7.

**Theorem 1** ([9, Theorem 2.19, Corollary 2.23]). Let \( p \) be a prime element of \( D \). Then there is a finite set \( S_p \) of positive integers and monic polynomials \( \nu_{(p,s)} \) for \( s \in S_p \) such that for \( t \geq 1 \),

\[
N_{(p^t)}(B) = \mu_B D[X] + p^t D[X] + \sum_{s \in S_p, s \leq b(t)} p^{\max\{0,t-s\}} \nu_{(p,s)} D[X]
\]

holds where \( b(t) = \inf\{ r \in S_p \mid r \geq t \} \). The degree of \( \nu_{(p,s)} \) is strictly increasing in \( s \in S_p \) and \( \nu_{(p,s)} \) is a monic polynomial of minimal degree in \( N_{(p^t)}(B) \). If \( t \leq \max S_p \), then the summand \( \mu_B D[X] \) can be omitted.

Whereas [9] could only show the existence of these \( S_p \), and \( \nu_{(p,s)} \), \( s \in S_p \), the present paper presents an algorithm (Algorithm 5) to explicitly compute these quantities. Thus the structure of \( N_{(a)}(B) \) is completely understood.

For simplicity, we omit the indices \( p \) and write \( S \) and \( \nu_s \) instead of \( S_p \) and \( \nu_{(p,s)} \), respectively, when the prime \( p \) is clear from the context.

An implementation of Algorithm 5 has been included in the free open-source mathematics software system SageMath [10] as method \texttt{p_minimal_polynomials} of a matrix; the \((a)\)-ideal of \( B \) can be computed by the method \texttt{null_ideal} of \( B \).

2.2. Integer-valued polynomials. Let \( D \) be a principal ideal domain with quotient field \( K \) and \( B \in M_n(D) \). Then

\[
\text{Int}(B, M_n(D)) := \{ f \in K[X] \mid f(B) \in M_n(D) \}
\]

is called the ring of integer-valued polynomials on \( B \). As before, the minimal polynomial of \( B \) over \( K \) is denoted by \( \mu_B \).
If a polynomial \( f \in K[X] \) is written as \( f = g/d \) for some \( g \in D[X] \) and \( d \in D \), then \( f \in \text{Int}(B, M_n(D)) \) holds if and only if \( g \in N_{(d)}(B) \). Thus Theorem 1 translates into the following corollary proved in [9].

**Corollary 2.1 ([9] Theorem 4.3).** With the above notations, there is a finite set \( \mathcal{P} \) of prime elements such that

\[
\text{Int}(B, M_n(D)) = \mu_B K[X] + D[X] + \sum_{p \in \mathcal{P}} \sum_{s \in \mathcal{S}_p} \frac{1}{p^s} \nu(s, p) D[X]
\]

where \( \mathcal{S}_p \) and \( \nu(s, p) \), \( s \in \mathcal{S}_p \), are the set and polynomials from Theorem 1.

As a consequence, Algorithm 5 completely describes the structure of \( \text{Int}(B, M_n(D)) \).

An implementation has been submitted as method `integer_valued_polynomials` for inclusion in SageMath.

### 2.3. Module decompositions.

Again, let \( D \) be a principal ideal domain, \( B \in M_n(D) \) and \( p^t \) a prime power of \( D \). The \((D/p^tD)\)-module

\[
(D/p^tD)[B + M_n(p^tD)] = \{ f(B + M_n(p^tD)) \mid f \in (D/p^tD)[X] \}
\]

is a finitely generated module over a principal ideal ring. According to [9] Theorem 15.33 this module decomposes into a direct sum of cyclic submodules with uniquely determined annihilators (the invariant factors). As shown in [9], this decomposition is strongly related to the generating set described in Theorem 1 which is stated in the next theorem. This further implies that the set \( \mathcal{S}_p \) and the degrees of the polynomials \( \nu(s, p), s \in \mathcal{S}_p \) are uniquely determined.

**Theorem 2 ([9] Theorem 3.5).** Let \( B \in M_n(D) \) and for a prime \( p \) of \( D \), let \( \mathcal{S}_p \) and \( \nu(s, p) \), \( s \in \mathcal{S}_p \), the set and polynomials from Theorem 1. We order \( \{\nu(s, p) \mid s \in \mathcal{S}_p \} \cup \{\mu_B\} \) by ascending degree and define \( \text{succ}(\nu(s, p)) \) for \( s \in \mathcal{S}_p \) to be the successor of \( \nu(s, p) \) with respect to this ordering. Finally, let \( d = \min\{\deg(\nu(s, p)) \mid s \in \mathcal{S}_p\} \) and \( d_s = \deg(\text{succ}(\nu(s, p))) - \deg(\nu(s, p)) \). Then

\[
(D/p^tD)[B + M_n(p^tD)] = (D/p^tD)^d \oplus \bigoplus_{s \in \mathcal{S}_p, s \leq t} (D/p^{t-s}D)^{d_s}
\]

for \( t \geq 0 \).

As a consequence, Algorithm 5 completely determines the structure of \((D/p^tD)[B + M_n(p^tD)]\).

### 3. Lifting

In this section, we provide the lifting procedure which allows the recursive computation of the \((p^t)\)-minimal polynomials in Section 5.

Let \( D \) be a principal ideal domain, \( p \) be a prime element of \( D \) and \( d \geq c \geq 1 \). The projection of some \( z \in D \) to the field \( D/pD \) is denoted by \( \overline{z} \). We extend this notation to polynomials in \( D[X] \) and vectors in \( D[X]^d \) as well as matrices in \( M_{c,d}(D[X]) \). The identity matrix is denoted by \( I \).

Let \( A \in M_{c,d}(D[X]) \) be a matrix such that \( \overline{A} \) has rank \( c \). For \( t \geq 0 \), we consider the set

\[
\mathcal{O}_t := \mathcal{O}_t(A) := \{ f \in D[X]^d \mid \overline{A}f \equiv 0 \pmod{p^t} \}.
\]

This is clearly a \( D[X] \)-module. For \( t = 0 \), we obviously have \( \mathcal{O}_0 = D[X]^d \).

A recursive method for computing \( \mathcal{O}_t \) is given in Algorithm 1.

**Proposition 3.1.** Algorithm 1 is correct.

**Proof.** By hypothesis, an element \( f \in D[X]^d \) is in \( \mathcal{O}_{t-1} \) if and only if there exist \( h \in D[X]^d \) and \( q \in D[X]^d \) such that \( f = p^{t-1}h + Gq \).

Since \( \mathcal{O}_1 \subseteq \mathcal{O}_{t-1} \), it follows that \( f \in \mathcal{O}_1 \) if and only if \( f = p^{t-1}h + Gq \) for some \( h \in D[X]^d \) and \( q \in D[X]^d \) and \( p^{t-1}Ah + AGq \equiv 0 \pmod{p^t} \). As the columns of \( G \) are elements of \( \mathcal{O}_{t-1} \), the matrix \( R \) is indeed an element of \( M_{c,d}(D[X]) \) and \( f \in \mathcal{O}_t \) holds if and only if

\[
Ah + Rq \equiv 0 \pmod{p^t}.
\]
Thus we have for a suitable $\nu(t - 1) I \ G$ are generators of $O_t$.

Input: $t \geq 1$, $G \in M_{d,s}(D[X])$ such that the columns of $(p^{t-1} I \ G)$ are generators of $O_{t-1}$

Output: $F \in M_{d,d-c+s}(D[X])$ such that the columns of $(p^t I \ F \ pG)$ are generators of $O_t$

Let $S \in M_c(D[X])$ and $T \in M_{d+s}(D[X])$ such that $S$ and $T$ are invertible and $S(\overline{A} \overline{R})T = \text{diag}_{c \times (d+s)}(\overline{\alpha}_1, \ldots, \overline{\alpha}_c)$ with $\overline{\alpha}_1 | \overline{\alpha}_2 | \cdots | \overline{\alpha}_c$ (Smith normal form).

Let $F \in M_{d,d-c+s}(D[X])$ consist of the last $d - c + s$ columns of $(p^{t-1} I \ G)T$.

Projecting into $(D/pD)[X]$, $[1]$ is equivalent to

$$\left(\overline{A} \overline{R}\right) \begin{pmatrix} \overline{h} \\ \overline{q} \end{pmatrix} = 0.$$

As $\overline{A}$ has full row rank, so do $(\overline{A} \overline{R})$ and $\text{diag}_{c \times (d+s)}(\overline{\alpha}_1, \ldots, \overline{\alpha}_c)$.

Left-multiply $(2)$ by $S$ to obtain

$$S(\overline{A} \overline{R})TT^{-1} \begin{pmatrix} \overline{h} \\ \overline{q} \end{pmatrix} = \text{diag}_{c \times (d+s)}(\alpha_1, \ldots, \alpha_c)T^{-1} \begin{pmatrix} \overline{h} \\ \overline{q} \end{pmatrix} = 0.$$

This is equivalent to

$$\begin{pmatrix} \overline{h} \\ \overline{q} \end{pmatrix} = T \begin{pmatrix} 0 \\ y \end{pmatrix}$$

for a suitable $y \in D[X]^{d-c+s}$.

Thus $\overline{h} = \overline{h}_0 + \overline{p}\overline{h}_1$ and $\overline{q} = \overline{q}_0 + \overline{p}\overline{q}_1$ for some $\overline{h}_1 \in D[X]^d$, $\overline{q}_1 \in D[X]^s$ and

$$\begin{pmatrix} \overline{h}_0 \\ \overline{q}_0 \end{pmatrix} = T \begin{pmatrix} 0 \\ y \end{pmatrix}.$$

Thus we have

$$f = p^{t-1}\overline{h} + G\overline{q} = (p^{t-1} I \ G)T \begin{pmatrix} 0 \\ y \end{pmatrix} + p'\overline{h}_1 + G'\overline{q}_1 = Fy + p'\overline{h}_1 + G'\overline{q}_1,$$

as claimed. \qed

4. Generators of $(p^t)$-ideals

This section is dedicated to the computation of a generating set of the $(p^t)$-ideal of a matrix over a principal ideal domain. Before we go into details, let us recall the basic definitions.

**Definition 4.1.** Let $R$ be a commutative ring, $J$ an ideal and $B \in M_n(R)$ be a square matrix. The $J$-ideal of $B$ is defined as

$$N_J(B) = N_J^R(B) = \{ f \in R[X] \mid f(B) \in M_n(J) \}.$$  

A monic polynomial $\nu \in R[X]$ is called $J$-minimal polynomial of $B$ if

1. $\nu \in N_J(B)$ and
2. $\deg(g) \geq \deg(\nu)$ for all monic polynomials $g$ with $g \in N_J(B)$.

We omit the superscript in $N_J^R(B)$ if the underlying ring is clear from the context.

**Remark.** The $(0)$-ideal of $B$ is just the null ideal of $B$, that is, $N_{(0)}(B) = \{ f \in R[X] \mid f(B) = 0 \}$. In case that $R$ is a field, $N_{(0)}(B)$ is a principal ideal of $R[X]$. The minimal polynomial of $B$ is the (in this case) uniquely determined $(0)$-minimal polynomial of $B$. Over general commutative rings, a $(0)$-minimal polynomial of a matrix is not necessarily uniquely determined although its degree is.
Lemma 4.2. Note that every square matrix $B \in M_n(R)$ has a $J$-minimal polynomial for every ideal $J$ of $R$. This is due to the Cayley-Hamilton theorem; every matrix over a commutative ring is a root of its own characteristic polynomial which is monic, cf. [7, Theorem XIV.3.1]. Let $B + M_n(J) \in M_n(R/J)$ be the residue class of $B$ modulo $J$ and $\chi \in (R/J)[X]$ denote the characteristic polynomial of $B + M_n(J)$. Then every preimage $f \in R[X]$ of $\chi$ satisfies $f(B) \equiv \chi(B + M_n(J)) \equiv 0 \pmod{M_n(J)}$ and hence $f \in N_j(B)$. In particular, there exists a monic preimage of $\chi$ in $R[X]$.

From now on, let the underlying ring be the principal ideal domain $D$ and $B \in M_n(D)$ a square matrix. For any ideal $J$ of $D$ there exists $a \in D$ such that $J = (a)$. Following the convention in [9], we write $N_a(B)$ instead of $N_{(a)}(B)$.

Assume that $a = 0$ and let $K$ denote the quotient field of $D$. The null ideal of $B$ considered as a matrix over $K$ is generated by its minimal polynomial $\mu_B \in K[X]$. Since the characteristic polynomial $\chi \in D[X]$ of $B$ is in $N_0^0(B)$ it follows that $\mu_B$ divides $\chi$. However, $D$ is integrally closed and therefore every monic factor in $K[X]$ of a monic polynomial in $D[X]$ is already an element of $D[X]$ (see [2] Ch. 5, §1.3, Prop. 11)). Hence $\mu_B \in D[X]$ and 

$$N_0^0(B) = N_0^0(K) \cap D[X] = \mu_B K[X] \cap D[X] = \mu_B D[X].$$

In order to find a generating set of $N_{p^t}(B)$, we reformulate the problem in a form to which the approach of the previous section is applicable. For this purpose we use one of McCoy’s theorems.

Lemma 4.2 ([8, Theorem 54]). Let $R$ be a commutative ring and $C \in M_n(R)$ a square matrix. Then 

$$N_0(C) = \{ f \in R[X] \mid \exists Q \in M_n(R)[X] : \text{adj}(X-C)f(X) = Q(X)\chi_C(X) \}.$$

Here, $\text{adj}(X-C) \in M_n(R[X])$ is the adjugate (or classical adjoint) matrix of $X-C$ and $\chi_C \in R[X]$ denotes the characteristic polynomial of $C$.

Since this result is central to our work, we restate its proof here for the reader’s convenience.

Proof. We embed $R[X]$ in $M_n(R[X]) \cong M_n(R)[X]$ via $f \mapsto f(X)I$ where $I$ is the identity matrix and identify $f \in R[X]$ with its image. A straight-forward verification shows that $f(C) = 0$ if and only if $f(X) \in M_n(R)[X]|_{X = C}$.

Being a monic polynomial, $X - C$ is not a zero-divisor in $M_n(R)[X]$ and therefore 

$$\text{adj}(X-C)f(X) \in M_n(R)[X]C(X)$$

if and only if 

$$\chi_C(X)f(X) = \text{adj}(X-C)(X-C)f(X) \in M_n(R)[X]C(X)(X-C)$$

which is, in turn, equivalent to 

$$f(X) \in M_n(R)[X]|_{X = C}$$

since $\chi_C(X)$ is also not a zero-divisor in $M_n(R)[X]$. \hfill \Box

If $B + M_n(p^tD) \in M_n(D/p^tD)$ denotes the residue class of $B$ modulo $p^t$, then $N_{p^t}(B)$ is the preimage of $N_0^0(B + M_n(p^tD))$ under the projection modulo $p^t$. Hence we can write the $(p^t)$-ideal of our matrix $B \in M_n(D)$ in the following way.

Corollary 4.3. Let $D$ be a principal ideal domain, $p \in D$ a prime element, $B \in M_n(D)$ be a square matrix and $t \geq 0$. Then 

$$N_{p^t}(B) = \{ f \in D[X] \mid \exists Q \in M_n(D[X]) : \text{adj}(X-B)f(X) \equiv Q(X)\chi_B(X) \pmod{p^t} \}.$$

Note that if $t = 0$, then $(p^t) = D$ and $D/D$ is the zero ring which has no unity and we cannot apply McCoy’s theorem (Lemma 4.2). However, it is easily seen that the corollary still holds which is why we allow the case $t = 0$.

For $1 \leq i, j \leq n$, the congruence in Corollary 4.3 translates to 

$$\text{adj}(X-B)_{ij}f - \chi_BQ_{ij} \equiv 0 \pmod{p^t}.$$
Proposition 4.4. Let $D$ be a principal ideal domain, $p \in D$ a prime element, $B \in M_n(D)$ be a square matrix with characteristic polynomial $\chi_B$ and $t \geq 0$. Further, let $\mathbf{b} \in D[X]^{n^2}$ be the column vector containing all entries of $\text{adj}(X - B)$ in some fixed order, $A = (\mathbf{b} - \chi_B I) \in M_{n^2, n^2+1}(D)$ where $I$ denotes the $n^2 \times n^2$-identity matrix and 

$$O_t(A) = \{ f \in D[X]^{n^2+1} \mid A f \equiv 0 \pmod{p^t} \}.$$ 

For $g_{11}, \ldots, g_{1s} \in D[X]$ (with $s \in \mathbb{N}_0$), the following assertions are equivalent:

1. There is a matrix $G \in M_{n^2+1,s}(D[X])$ with first row $g_{11}, \ldots, g_{1s}$ such that the columns of $(p^t I \ G)$ form a generating set of $O_t(A)$.

2. $p^t, g_{11}, \ldots, g_{1s}$ form a generating set of $N_{p^t}(B)$.

Proof. The ideal $N_{p^t}(B)$ is the projection of $O_t(A)$ on the first component according to Corollary 4.3. It follows that (1) implies (2). For the reverse implication let $g_{11}, \ldots, g_{1s} \in D[X]$ such that $N_{p^t}(B) = (p^t, g_{11}, \ldots, g_{1s})$. Since $g_{11} \in N_{p^t}(G)$ for $1 \leq i \leq s$, there exist polynomials $g_{ij} \in D[X]$ for $2 \leq j \leq n^2 + 1$ such that $g_{ij} = (\chi_B g_{j+1,i}) \in O_t(A)$ according to Corollary 4.3. If $\mathbf{f} = (f_j)_{j} \in O_t(A)$ is an arbitrary element, then $f_1 \in N_{p^t}(A)$ and there exist $h_0, \ldots, h_s$ such that 

$$f_1 = p^t h_0 + \sum_{i=1}^{s} h_i g_{1i}. \tag{3}$$

If $b_j$ denotes the $j$-th coordinate of $\mathbf{b}$ then, by definition of $O_t(A)$,

$$f_1 b_j \equiv \chi_B f_{j+1} \pmod{p^t}$$

and

$$g_{1i} b_j \equiv \chi_B g_{j+1,i} \pmod{p^t}$$

hold for $1 \leq j \leq n^2$. Together with (3), we get

$$\chi_B f_{j+1} \equiv f_1 b_j \equiv \sum_{i=1}^{s} h_i g_{1i} b_j \equiv \sum_{i=1}^{s} h_i \chi_B g_{j+1,i} \pmod{p^t}. \tag{4}$$

Since $\chi_B$ is monic, its residue class modulo $p^t$ is no zero-divisor and we can cancel $\chi_B$ in the equation above to conclude that

$$f_{j+1} \equiv \sum_{i=1}^{s} h_i g_{j+1,i} \pmod{p^t}.$$ 

Therefore $\mathbf{f}$ is a $D[X]$-linear combination of the columns of $(p^t I \ \ G)$ where $G = (g_{ij})_{1 \leq j \leq n^2+1, 1 \leq i \leq s}$.

It follows from Proposition 4.4 that we can use Algorithm 1 to compute a generating system of $O_t(A)$ (with $c = n^2$ and $d = n^2 + 1$). Note that the residue class $\mathbf{A}$ of $A$ has full rank since $\chi_B$ is monic. Assume that we are given $G \in M_{n^2+1,s}(D[X])$ whose columns together with those of $p^{t-1}I$ generate $O_{t-1}(A)$, then Algorithm 1 computes a matrix $F \in M_{n^2+1,s+1}(D[X])$ such that the columns of $(p^t I \ F \ pG)$ generate $O_t(A)$. Then $p^t$, $f_{11}$, ..., $f_{1,s+1}$, $p g_{11}$, ..., $p g_{1s}$ generate $N_{p^t}(B)$, according to Proposition 4.4. In particular, the elements $f_{11}, \ldots, f_{1,s+1}$ satisfy a property which motivates the next definition.

Definition 4.5. Let $D$ be a principal ideal domain, $p \in D$ a prime element, $B \in M_n(D)$ be a square matrix and $t \geq 1$. We say that a finite subset $\mathcal{F}$ of $D[X]$ has the $(p^t)$-generating property w.r.t. $B$ if

$$N_{p^t}(B) = (\mathcal{F}) + p N_{p^{t-1}}(B).$$

As output of Algorithm 1, $\mathcal{F} = \{ f_{11}, \ldots, f_{1,s+1} \}$ has $s + 1$ elements. Applying the algorithm recursively leads to a huge set of generators.

Indeed, according to [9, Proposition 2.13], if $t \geq 1$ and $\nu_t$ is a $(p^t)$-minimal polynomial of $B$, then 

$$N_{p^t}(B) = (\nu_t) + p N_{p^{t-1}}(B). \tag{4}$$
This is also a consequence of Algorithm 5 below.

The next section is dedicated to the question how to compute \((p^t)\)-minimal polynomials given a set \(\mathcal{F}\) with the \((p^t)\)-generating property and a \((p^{t-1})\)-minimal polynomial. For now, we assume that we already know \((p^i)\)-minimal polynomials \(\nu_i\) for \(1 \leq i \leq t-1\). Then Equation 4 implies

\[
N_{p^t-1}(B) = \sum_{i=0}^{t-1} p^{t-1-i} \nu_i D[X]
\]

and according to Proposition 4.4 there exists a matrix \(G \in M_{n^2+1,t-1}(D)\) with \(g_{1i} = p^{t-1-i} \nu_i\) for \(1 \leq i \leq t-1\) such that \((p^{t-i} I - G)\) generates \(\mathcal{O}_{t-1}(A)\). With this choice, \(s = t - 1\) and hence Algorithm 4 produces a set \(\mathcal{F}\) with \(t\) elements.

Note that [9] Theorem 2.19 states that it suffices to sum over the \((t-1)\)-st index set in Equation 4 which may result in a smaller number of columns of \(G\). However, even this reduction technique does not yield \(|\mathcal{F}| = 1\) except in trivial cases. Therefore, reduction of \(|\mathcal{F}|\) in every step is essential.

5. Computing \((p^t)\)-minimal polynomials

This section considers the question how to compute a \((p^t)\)-minimal polynomial of a square matrix \(B \in M_n(D)\) over a principal ideal domain \(D\) for \(t \geq 1\). For this purpose, we assume throughout this section that we already determined a \((p^t)\)-minimal polynomial \(\nu_i\) for \(0 \leq i \leq t-1\) and a set \(\mathcal{F}\) with the \((p^t)\)-generating property. We start with a special case, namely the case where the set \(\mathcal{F}\) consists of a single monic polynomial \(f\).

**Proposition 5.1.** Let \(D\) be a principal ideal domain, \(p \in D\) a prime element, \(B \in M_n(D)\) be a square matrix, \(t \geq 1\) and \(\nu \in D[X]\) be a monic polynomial.

If \(N_{p^t}(B) = (\nu) + pN_{p^t-1}(B)\) then \(\nu\) is a \((p^t)\)-minimal polynomial.

**Proof.** Since \(\nu \in N_{p^t}(B)\) holds by hypothesis, it suffices to show that \(\deg(f) \geq \deg(\nu)\) for all monic polynomials \(f \in N_{p^t}(B)\). By assumption,

\[
N_{p^t}(B) = (\nu) + pN_{p^t-1}(B)
\]

holds, so for a monic polynomial \(f \in N_{p^t}(B)\) there exist \(g \in D[X]\) and \(h \in N_{p^t-1}(B)\) such that \(f = g\nu + ph\). Let \(g_1, g_2 \in D[X]\) be polynomials such that \(g = g_1 + pg_2\) and no non-zero coefficient of \(g_1\) is divisible by \(p\). Then \(f = g_1\nu + p(g_2\nu + h)\) and since \(f\) is monic and \(p\) does not divide \(\lc(g_1)\) it follows that \(\deg(f) = \deg(g_1\nu) + \deg(\nu) \geq \deg(\nu)\).

In order to apply Proposition 5.1, we have to reduce the output set \(\mathcal{F}\) of Algorithm 1 such that it only contains one monic polynomial.

As a first step, observe that

\[
N_{p^t}(B) \cap pD[X] = pN_{p^t-1}(B)
\]

holds and therefore \(\mathcal{F} \setminus pD[X]\) has the \((p^t)\)-generating property. From now on we can therefore assume that \(\mathcal{F} \cap pD[X] = \emptyset\). Since \(N_{p^t}(B)\) always contains a monic polynomial it follows that \(N_{p^t}(B) \neq pN_{p^t-1}(B)\) and hence \(\mathcal{F}\) is never empty.

In order to compute a \((p^t)\)-minimal polynomial from the polynomials in \(\mathcal{F}\) we need the following special case of [9] Corollary 2.14.

**Lemma 5.2** ([9]). Let \(\nu_i\) be a \((p^i)\)-minimal polynomial of \(B\) and \(f \in N_{p^t}(B)\).

If \(f \notin pD[X]\), then \(\deg(f) \geq \deg(\nu_i)\).

The idea is to start with \(\mathcal{F}_0 = \mathcal{F}\) and show (for \(i \geq 1\)) that if \(|\mathcal{F}_{i-1}| > 1\) then we can compute a set \(\mathcal{F}_i\) of monic polynomials with the \((p^i)\)-generating property with \(\mathcal{F}_i \cap pD[X] = \emptyset\) such that \((\min_{f \in \mathcal{F}} \deg f, |\mathcal{F}_i|)\) decreases lexicographically in each step.

Since the degree of monic polynomials in \(N_{p^t}(B)\) is clearly bounded from below, we end up with a singleton satisfying the \((p^t)\)-generating property. Hence, by Proposition 5.1 the singleton at the end contains a \((p^t)\)-minimal polynomial.
It turns out that polynomial division is a useful tool to compute $\mathcal{F}_t$. However, we are working in $D[X]$, so we cannot just divide some polynomial by another; we want to deal with monic polynomials to guarantee that polynomial division is applicable. Algorithms 2 and 3 provide the tools to replace a set with the $(p^t)$-generating property by another one which consists only of monic polynomials.

**Algorithm 2** Find monic polynomial

**Input:** $p \in D$ prime, $t \geq 1$, $\nu_{t-1}$ a $(p^{t-1})$-minimal polynomial of $B$ and $f \in \mathcal{N}_{p^t}(B) \setminus pD[X]$

**Output:** Monic polynomial $h \in \mathcal{N}_{p^t}(B)$ with $\deg(h) \leq \deg(f)$

Write $f = f_1 + pf_2$ such that all non-zero coefficients of $f_1$ are not divisible by $p$

Let $r$ be the remainder of $f_2$ modulo $\nu_{t-1}$ with $\deg r < \deg \nu_{t-1}$

Choose $u, v \in D$ with $u \deg(f_1) + vp = 1$

$h := u(f_1 + pr) + vX^{\deg(f_1) - \deg(\nu_{t-1})}p\nu_{t-1}$

**Lemma 5.3.** Algorithm 2 is correct.

**Proof.** Let $q \in D[X]$ such that $f_2 = q\nu_{t-1} + r$. We set

\[
\hat{h} = f_1 + pr = f - q(p\nu_{t-1}) \in \mathcal{N}_{p^t}(B).
\]

Since $p$ does not divide $\deg(f_1)$, the leading terms of $f_1$ and $pr$ cannot cancel each other out and $\deg(\hat{h}) = \max\{\deg(f_1), \deg(r)\}$. On the other hand, $\hat{h} \in \mathcal{N}_{p^t}(B) \setminus pD[X]$ and therefore $\deg(\hat{h}) \geq \deg(\nu_t)$ by Lemma 5.2. We conclude that

\[
\deg(\nu_{t-1}) \leq \deg(\nu_t) \leq \deg(\hat{h}) = \max\{\deg(f_1), \deg(r)\} = \max\{\deg(f_1), \deg(\nu_{t-1}) - 1\}
\]

and it follows that $\max\{\deg(f_1), \deg(\nu_{t-1}) - 1\} = \deg(f_1) = \deg(\hat{h})$ and therefore $p \nmid \deg(h)$. As $\deg(\hat{h}) \geq \deg(\nu_{t-1}) > \deg(r)$, we have $\deg(h) = \deg(f_1)$. Thus $h$ is monic.

**Algorithm 3** Replacing by monic polynomials

**Input:** $p \in D$ prime, $t \geq 1$, $f \in \mathcal{N}_{p^t}(B) \setminus pD[X]$

**Output:** Monic polynomials $h_1, \ldots, h_s \in \mathcal{N}_{p^t}(B)$ such that

1. $f \in (h_1, \ldots, h_s) + p\mathcal{N}_{p^{t-1}}(B)$ and
2. $\deg(f) \geq \deg(h_1) > \cdots > \deg(h_s)$.

$i := 0$, $f_i := f$

while $f_i \notin pD[X]$ do

$i := i + 1$

Determine monic $h_i \in \mathcal{N}_{p^t}(B)$ with $\deg(h_i) \leq \deg(f_{i-1})$ (Algorithm 2)

Let $f_i \in D[X]$ be the remainder of $f_{i-1}$ modulo $h_i$ with $\deg(f_i) < \deg(h_i)$.

end while

$s := i$

**Lemma 5.4.** Algorithm 3 terminates and is correct.

**Proof.** The construction implies that $f_i \in \mathcal{N}_{p^t}(B)$ and $f_{i-1} \in (h_i, f_i)$.

Further, $\deg(f_i) < \deg(f_{i-1})$ holds which implies that there exists $s \in \mathbb{N}$ such that $f_s \in pD[X]$. Hence $f_s \in p\mathcal{N}_{p^{t-1}}(B)$ and

\[
f = f_0 \in (h_1, f_1) \subseteq (h_1, h_2, f_2) \subseteq \cdots \subseteq (h_1, h_2, \ldots, h_s, f_s) \subseteq (h_1, \ldots, h_s) + p\mathcal{N}_{p^{t-1}}(B).
\]

We can now replace $\mathcal{F}$ by a set with the $(p^t)$-generating property which consists only of monic polynomials using Algorithm 3. Note that we need to know a $(p^{t-1})$-minimal polynomial to do the necessary computations. We are now ready to present Algorithm 4 to compute a $(p^t)$-minimal polynomial.
Algorithm 4 Computation of a \((p^l)\)-minimal polynomial

**Input:** \(t \geq 1, \mathcal{F} \subseteq D[X]\) with the \((p^l)\)-generating property, \(\nu_{t-1}\) a \((p^{l-1})\)-minimal polynomial

**Output:** \((p^l)\)-minimal polynomial \(\nu_t\)

Delete all elements in \(\mathcal{F} \cap pD[X]\) from \(\mathcal{F}\) and then replace non-monic polynomials in \(\mathcal{F}\) by monic polynomials using Algorithm [3]

Let \(g \in \mathcal{F}\) be of minimal degree.

**while** \(f \in \mathcal{F}\) with \(f \neq g\) do

\[\mathcal{F} := \mathcal{F} \setminus \{f\}\]

Let \(q, r \in D[X]\) such that \(f = qg + r\) and \(\deg(r) < \deg(g)\).

**if** \(r \notin pD[X]\) **then**

Let \(h_1, \ldots, h_s\) be monic polynomials with \(r \in (h_1, \ldots, h_s) + p\mathcal{N}_{p^{l-1}}(B)\) (Algorithm [3]).

Set \(g := h_s\) and \(\mathcal{F} := \mathcal{F} \cup \{h_1, \ldots, h_s\}\).

**end if**

**end while**

\[\nu_t := g\]

**Proposition 5.5.** Algorithm 4 terminates and is correct.

**Proof.** We will show that in every step, \(\mathcal{F}\) consists of monic polynomials and has the \((p^l)\)-generating property and \((\min_{f \in \mathcal{F}} \deg(f), |\mathcal{F}|)\) decreases lexicographically in each step.

This implies that the algorithm computes a singleton with the \((p^l)\)-generating property. According to Proposition 5.1, such a singleton contains a \((p^l)\)-minimal polynomial.

Removing all polynomials in \(\mathcal{F} \cap pD[X] \subseteq p\mathcal{N}_{p^{l-1}}(B)\) in the first step does not affect the \((p^l)\)-generating property. The same holds for replacing non-monic polynomials by Algorithm [3].

Now, let \(\mathcal{F}_0\) be the result of this first step in the algorithm and \(\mathcal{F}_i\) be the resulting set after \(i\) iterations of the while loop. Further, let \(g_i\) be a polynomial of minimal degree in \(\mathcal{F}_i\).

Now assume that \(|\mathcal{F}_{i-1}| > 1\) and let us have a closer look at the \(i\)-th iteration of the while loop. For a polynomial \(f \in \mathcal{F}_{i-1}\) with \(f \neq g_{i-1}\), the algorithm computes the remainder \(r\) of \(f\) modulo \(g_{i-1}\) with \(\deg(r) < \deg(g_{i-1})\). Then the following holds

\[\mathcal{N}_{p^l}(B) = (\mathcal{F}_{i-1} \setminus \{f\}) + (r) + p\mathcal{N}_{p^{l-1}}(B)\]

We split into two cases: \(r \in pD[X]\) and \(r \notin pD[X]\). If \(r \in pD[X]\), then \(r \in p\mathcal{N}_{p^{l-1}}(B)\) and hence \(\mathcal{F}_i = \mathcal{F}_{i-1} \setminus \{f\}\) has the \((p^l)\)-generating property. In this case, \(|\mathcal{F}_i| < |\mathcal{F}_{i-1}|\) holds and \(g_i = g_{i-1}\) is a polynomial of minimal degree in \(\mathcal{F}_i\).

If, however, \(r \notin pD[X]\), then the algorithm computes monic polynomials \(h_1, \ldots, h_s\) with \(\deg(r) \geq \deg(h_1) > \cdots > \deg(h_s)\) and \(r \in (h_1, \ldots, h_s) + p\mathcal{N}_{p^{l-1}}(B)\). Hence \(\mathcal{F}_i = \{h_1, \ldots, h_s\} \cup \mathcal{F}_{i-1} \setminus \{f\}\) has the \((p^l)\)-generating property and \(g_i = h_s\) is a polynomial of minimal degree in \(\mathcal{F}_i\). In this case, \(\deg(g_i) = \deg(h_s) \leq \deg(r) < \deg(g_{i-1})\).

We conclude this section with Algorithm 5 that computes the generators of \(\mathcal{N}_{p^l}(B)\) of a matrix \(B \in \mathcal{M}_n(D)\) and a prime element \(p \in D\) as stated in Theorem 5.4 that are \((p^s)\)-minimal polynomials \(\nu_s\) for indices \(s\) of a finite set \(\mathcal{S}\) such that for all \(t \geq 1\),

\[\mathcal{N}_{p^l}(B) = \mu_B D[X] + p^l D[X] + \sum_{s \in \mathcal{S}} p^{\max(0,t-s)} \nu_s D[X]\]

holds where \(b(t) = \inf\{r \in \mathcal{S} \mid r \geq t\}\).

**Theorem 3.** Algorithm 5 terminates and is correct.

**Proof.** By definition, \((\deg(\nu_s))_{s \geq 0}\) is a non-decreasing sequence which is bounded from above by \(\deg(\mu_B)\). Hence this sequence eventually stabilizes. Moreover, as shown in [3] Proposition 2.22, the sequence always stabilizes at the value \(\deg(\mu_B)\), that is, there exists \(s_0 \geq 0\) such that \(\deg(\nu_s) = \deg(\mu_B)\) for all \(s \geq s_0\). This implies that the algorithm terminates.
Algorithm 5 Computation of $S$ and minimal polynomials $\nu_s$ for $s \in S$

Input: $B \in M_n(D)$, $p \in D$ prime
Output: $S$, $\nu_s$ for $s \in S$ (Theorem \[1\]),

$\chi_B :=$ characteristic polynomial of $B$
$\mu_B :=$ minimal polynomial of $B$ over quotient field $K$
$b :=$ the entries of adj$(X - B)$ in some fixed order
$A := (b - \chi_B I)$
$t := 0, S := \emptyset, G :=$ the $((n^2 + 1) \times 0)$-matrix, $\nu_0 := 1$

while True do

\begin{itemize}
  \item $t := t + 1$
  \item (The columns of $(p^{t-1}I \ G)$ generate $O_{t-1}(A)$)
  \item Determine $F$ such that $(p^{t}I \ F \ pG)$ are generators of $O_t(A)$ by Algorithm \[1\]
  \item $F :=$ first row of $F$
  \item $\nu_t :=$ $(p^t)$-minimal polynomial of $B$ by Algorithm \[4\] (using $\nu_{t-1}$)
  \item if $\deg \nu_t \geq \deg \mu_B$ then
    \begin{itemize}
      \item return $S$, $\nu_s$ for $s \in S$
    \end{itemize}
  \item end if
  \item for $i = 1, \ldots, n^2$ do
    \begin{itemize}
      \item $\nu_i b_i = g_i \chi_B + r_i$ (long division)
    \end{itemize}
  \item end for
  \item $g := (g_i)_{1 \leq i \leq n^2}$
  \item if $\deg \nu_t = \deg \nu_{t-1}$ then
    \begin{itemize}
      \item Delete last column of $G$
      \item $S := S \setminus \{t - 1\}$
    \end{itemize}
  \item end if
  \item $G := \begin{pmatrix} pG & \nu_t \\ \nu_t & g \end{pmatrix}$
  \item $S := S \cup \{t\}$
\end{itemize}

end while

For the correctness, observe first that Algorithm \[1\] computes a $(p^t)$-minimal polynomial $\nu_t$ with the $(p^t)$-generating property. Next, we explain the choice of $g$. As $\nu_t \in N_{p^t}(B)$, there is some $g_t \in D[X]$ such that $\nu_t b_i \equiv \chi_B g_t \pmod{p^t}$ by Corollary \[4.3\]. Thus we have $r_i \equiv \chi_B (g_t - g_i) \pmod{p^t}$. As $\chi_B$ is monic, the degree of the right hand side modulo $p^t$ exceeds the degree of $r_i$ unless $g_t \equiv g_i$ (mod $p^t$).

If $\deg(\nu_t) = \deg(\nu_{t-1})$, then $\nu_t$ is a $(p^{t-1})$-minimal polynomial and $\nu_t - \nu_{t-1}$ is a polynomial in $N_{p^{t-1}}(B)$ with degree less than $\deg(\nu_{t-1})$. By Lemma \[5.2\] this implies that $\nu_t - \nu_{t-1} \in N_{p^{t-1}}(B) \cap pD[X] = pN_{p^{t-2}}(B)$. Hence

$$(\nu_t) + pN_{p^{t-2}}(B) = (\nu_{t-1}) + pN_{p^{t-2}}(B) = N_{p^{t-1}}(B)$$

and thus $\nu_t$ has the $(p^{t-1})$-generating property. Observe that this is in particular the case if the Algorithm reaches its stopping point, that is, if $\deg(\nu_t) = \deg(\mu_B)$. Then $\mu_B$ is a $(p^s)$-minimal polynomial for all $s \geq t$.

The remaining proof consists of repeated application of Proposition \[4.4\] in both directions. \[\Box\]

Remark. Gröbner bases provide an alternative to Algorithm \[4\]. Adams and Loustaunau describe in \[1\] Ch. 4.5] how to extend the theory of Gröbner bases to polynomial rings over principal ideal domains. If $G$ is a Gröbner basis of $N_p(B)$, we set $\widehat{G} = \{ g \in G \mid p \not| \ lc(g) \}$. One can show that $\widehat{G} \neq \emptyset$ and if $q$ is a polynomial of minimal degree in $\widehat{G}$, then $uq + vp^tX^{\deg(g)}$ is a $(p^t)$-minimal polynomial where $u, v \in D$ such that $u \lc(g) + vp^t = 1$. 


**Example 5.6.** We demonstrate Algorithm 5 and compute \((2^t)\)-minimal polynomials for the matrix

\[
B = \begin{pmatrix}
1 & 0 & 1 \\
1 & -2 & -1 \\
10 & 0 & 0
\end{pmatrix}
\]

for \(t \geq 1\). The minimal and characteristic polynomial of \(B\) is \(\mu_B = \chi_B = X^3 + X^2 - 12X - 20\). We skip the computation of \(\nu_1\) and claim that \(\nu_1 = X^2 + X\) is a \((2)\)-minimal polynomial (one can check that its residue class is the minimal polynomial of \(B\) over the field \(\mathbb{Z}/2\mathbb{Z}\)).

Hence \(N_1(B) = \nu_1\mathbb{Z}[X] + 2\mathbb{Z}[X]\) and there exists a vector \(g \in \mathbb{Z}[X]^9\) such that the columns of

\[
G_1 = \begin{pmatrix} 2I & \nu_1 \\ g \end{pmatrix}
\]

generate \(\mathcal{O}_1(A)\) where \(A = (b \quad -\chi_B I)\) with

\[
b = (X^2 + 2X, 0, X + 2, X - 10, X^2 - X - 10, -X + 2, 10X + 20, 0, X^2 + X - 2)^t
\]

(cf. Proposition 1.4). Algorithm 5 performs polynomial long divisions to determine

\[
g = (X + 2, 0, 1, 1, X - 1, -1, 10, 0, X + 1)^t
\]

Next, Algorithm 5 calls Algorithm 1 to compute a matrix \(F_2 \in \mathbb{M}_{10,2}(\mathbb{Z}[X])\) such that the columns of \((4I \quad F_2 \quad 2G_1)\) generate \(\mathcal{O}_2(A)\). Without giving details here, we claim that

\[
F_2 = \begin{pmatrix}
2X^2 + 2X & 2X & 0 & 2 & 2 & 2X + 2 & 2 & 0 & 0 & 2X + 2 \\
X^2 + 3X + 2 & X + 4 & 0 & 1 & 1 & X + 1 & -1 & 10 & 0 & X + 3
\end{pmatrix}^t
\]

is such a matrix. Hence \(\{2X^2 + 2X, X^2 + 3X + 2\}\) is a set with the \((4)\)-generating property. We can apply Algorithm 4 which removes the first polynomial as it is an element of \(2\mathbb{Z}[X] \cap N_2(B) = 2N_1(B)\). Hence \(\{X^2 + 3X + 2\}\) has the \((4)\)-generating property and by Proposition 5.1 \(\nu_2 = X^2 + 3X + 2\) is a \((4)\)-minimal polynomial.

If \(f\) denotes the second column of \(F_2\), then the columns of \(G_2 = (4I \quad f)\) generate \(\mathcal{O}_2(A)\). In the next step, we apply again Algorithm 1 to compute

\[
F_3 = \begin{pmatrix}
X^3 + 7X^2 + 6X & X^2 + 8X + 24 & 0 & X + 8 & \ldots \\
X^3 + 3X^2 + 2X & X^2 + 4X + 16 & 0 & X + 4 & \ldots
\end{pmatrix}^t
\]

such that the columns of \((8I \quad F_3 \quad 2G_2)\) generate \(\mathcal{O}_3(A)\). It follows that \(\{X^3 + 7X^2 + 6X, X^3 + 3X^2 + 2\}\) has the \((8)\)-generating property. Since

\[
X^3 + 7X^2 + 6X \in \langle X^3 + 3X^2 + 2X \rangle + 2N_4(B),
\]

it follows that \(\nu_3 = X^3 + 3X^2 + 2X\) is an \((8)\)-minimal polynomial. However, since the degree of \(\nu_3\) is equal to \(\deg(\mu_B)\), it follows that \(\mu_B\) is a \((2^3)\)-minimal polynomial for \(t \geq 3\). Note that \(S_2 = \{2\}\).

### 5.1 Run-time and memory usage in practice

Table 5.1 displays average run-time and memory usage for Algorithm 5 for a dense random integer matrix \(B\) of size \(n\) and a prime number \(p\). Note that only instances with non-trivial \((p^t)\)-minimal polynomials were taken into account, see Section 4 below. To find such instances, Theorem 4 below provides a strategy to test only a finite number of primes \(p\) for a given matrix \(B\). Table 5.1 also contains the total number of pairs \((B, p)\) to which we applied Algorithm 5 and the number of pairs \((B, p)\) among them with non-trivial \((p^t)\)-minimal polynomials.

All computations were done in the free open-source mathematics software system SageMath (Version 7.6.beta6) on a machine with an Intel(R) Core(TM) i5-4690S CPU @ 3.20GHz processor.

However, the current implementation of the Smith normal form in SageMath is designed to deal with matrices in general principal ideal domains and does not exploit the Euclidean structure of univariate polynomial rings over fields. We experienced memory issues using this implementation in Algorithm 1. For this reason we implemented the algorithm presented in [6] which is also applicable to matrices with entries in a univariate polynomial ring over a field.

In addition, it is worth mentioning that large prime numbers can cause a significant increase in run-time and memory usage. For example, for \(p = 366388788500439413183777\) Algorithm 5 takes
5006.08 seconds and 207.5 MB given the input matrix

\[ B = \begin{pmatrix}
-1 & -1 & 6 & 3 & 3 & -1 & 11 & -2 & -1 & -2 \\
-2 & -1 & 9 & -1 & -2 & 1 & 1 & 3 & -1 & -2 \\
-1 & -6 & -6 & -1 & -4 & 5 & 1 & 1 & -4 & 1 \\
1 & 1 & 1 & -2 & 1 & 2 & -1 & 1 & 1 & 13 \\
-1 & 1 & -1 & 3 & -2 & -4 & -1 & -1 & 4 & -4 \\
-4 & 1 & 1 & 2 & -1 & 2 & 5 & -2 & -1 & 1 \\
14 & 1 & 1 & -1 & 1 & 2 & 1 & 3 & 1 & -1 \\
-3 & 1 & -1 & 1 & -3 & 4 & -2 & 2 & 6 & 11 \\
-2 & 1 & -1 & 1 & 1 & 1 & 6 & -23 & -1 & 1 \\
-1 & -1 & -1 & 1 & 3 & -1 & -3 & 1 & 1 & -2 \\
\end{pmatrix} \in M_{10}(\mathbb{Z}).
\]

In this particular example however, it turns out that this value of \( p \) only occurs as a root of the determinant of the transformation matrix (see Theorem \[4\]). In fact, \( B \) has no non-trivial \((p')\)-minimal polynomial for any \( p \). As we decided to only include matrices with non-trivial \((p')\)-minimal polynomials, this matrix (along with many other examples) does not contribute to the timings.

| n     | 2     | 3     | 4     | 5     | 6     | 7     | 8     | 9     | 10    | 11    |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|--------|-------|
| sec   | 0.03  | 0.12  | 0.57  | 2.53  | 8.95  | 28.81 | 80.51 | 193.22 | 501.31 | 983.66 |
| MB    | 0.014 | 0.041 | 0.073 | 0.151 | 0.276 | 0.611 | 0.331 | 0.355  | 0.25   | 2.603  |
| non-trivial | 73   | 175   | 242   | 329   | 184   | 112   | 111   | 19     | 5      | 13     |
| total | 587   | 1624  | 2651  | 3571  | 2069  | 1389  | 1489  | 257    | 114    | 106    |

Table 1. Run-time in seconds and memory usage in megabytes of Algorithm \[5\] for primes \( p \) and integer matrix instances of size \( n \) with non-trivial \((p')\)-minimal polynomials.

6. PRIMES WITH TRIVIAL \((p')\)-MINIMAL POLYNOMIALS

In this section, we show that for all but finitely many prime elements \( p \) and all \( t \geq 1 \), \( \mu_B \) is a \((p')\)-minimal polynomial. This further implies that the \((p')\)-ideal \( N_{p^t}(B) \) of \( B \) is generated by \( \mu_B \) and the constant \( p^t \).

This assertion has been shown before as auxiliary result in the proof of \[3\] Theorem 4.3. In order to make it more accessible, we restate it here as proper theorem together with a proof.

**Theorem 4** (\[3\]). Let \( D \) be a principal ideal domain and \( B \in M_n(D) \) a square matrix with minimal polynomial \( \mu_B \). Then for all but finitely many prime elements \( p \in D \) and all \( t \geq 1 \)

\[ N_{p^t}(B) = \mu_B D[X] + p^t D[X]. \]

**Proof.** It suffice to show that \( \mu_B \) is a \((p)\)-minimal polynomial for all but finitely many prime elements \( p \in D \). If this is the case (for a fixed \( p \)), then Algorithm \[6\] stops in the first iteration of the while loop returning \( S = \emptyset \). Hence, \( N_{\mu_p}(B) = \mu_B D[X] + p^t D[X] \) for all \( t \geq 0 \) by Theorem \[3\].

Considered as a matrix over the quotient field \( K \) of \( D \), \( B \) is similar to its rational canonical form \( C \), that is, there exists a matrix \( T \in \text{GL}_n(K) \) such that

\[ TBT^{-1} = C = C_{\mu_1} \oplus \cdots \oplus C_{\mu_r} \]

where \( \mu_1 | \cdots | \mu_r = \mu_B \) are the invariant factors of \( B \) (in \( K[X] \)) and \( C_{\mu_i} \) denotes the companion matrix of the polynomial \( \mu_i \) for \( 1 \leq i \leq r \) (cf. [2] Theorem XIV.2.1)). Since \( D \) is integrally closed, every monic factor in \( K[X] \) of a monic polynomial in \( D[X] \) is already in \( D[X] \), cf. [2] Ch. 5, §1.3, Prop. 11. Therefore \( \mu_i \in D[X] \) for \( 1 \leq i \leq r \) because \( \mu_i | \mu_B \) and \( \mu_B \) divides the characteristic polynomial \( \chi_B \in D[X] \).

Hence the rational canonical form \( C \) of \( B \) is a matrix with entries in \( D \). Moreover, we can choose \( T \in M_n(D) \). However, in general, the similarity relation of \( B \) and \( C \) does not hold over the domain \( D \), that is, we cannot assume \( T \in \text{GL}_n(D) \).
Let \( p \) be a prime element that does not divide \( \det(T) \). Then \( \det(T) \) is invertible in the localization \( D_p(D) \) of \( D \) at \( p \) and \( T^{-1} = \det(T)^{-1} \text{adj}(T) \in GL_n(D_p(D)) \). This allows to reduce Equation (7) modulo \( p \)
\[
TBT^{-1} = TBT^{-1} = \overline{C} = c_{pT} \oplus \cdots \oplus c_{pT}
\]
(where we identify the residue fields of \( D \) and \( D_p(D) \) modulo \( p \)). Hence \( \overline{C} \) is the rational canonical form of \( B \) which implies that \( \overline{\mu}_B \) is the minimal polynomial of \( B \). Equivalently, \( \mu_B \) is a \((p)\)-minimal polynomial of \( B \). The assertion follows since \( \det(T) \) has only finitely many prime divisors. \( \square \)

The choice of the transformation matrix in the proof of Theorem 4 is not unique. Moreover, the prime divisors of different transformation matrices may not coincide as the following example demonstrates.

**Example 6.1.** Let \( B = \begin{pmatrix} 4 & 5 \\ 3 & 5 \end{pmatrix} \in M_2(\mathbb{Z}) \). The rational canonical form of \( B \) is \( C = \begin{pmatrix} 0 & -5 \\ 1 & 9 \end{pmatrix} \).

The matrices \( T = \begin{pmatrix} 3 & -4 \\ 0 & 1 \end{pmatrix} \) and \( S = \begin{pmatrix} 1 & 2 \\ -2 & -3 \end{pmatrix} \) both satisfy (over \( \mathbb{Q} \))
\[
TBT^{-1} = C = SBS^{-1}.
\]
Since \( \det(S) = 1 \), \( B \) is similar to \( C \) over \( \mathbb{Z} \). This implies that \( \mu_B \) is a \((p)\)-minimal polynomial for all primes \( p \) of \( \mathbb{Z} \). However, \( \det(T) = 3 \).

7. Finite description of \((p^t)\)-ideals for all \( t \)

Finally, we give a proof of Theorem 1 which has been stated above in Section 2. For the reader’s convenience we restate it at this point.

**Theorem 1 (9 Theorem 2.19, Corollary 2.23).** Let \( p \) be a prime element of \( D \). Then there is a finite set \( S_p \) of positive integers and monic polynomials \( \nu_{(p,s)} \) for \( s \in S_p \) such that for \( t \geq 1 \),
\[
N_{(p^t)}(B) = \mu_B D[X] + p^t D[X] + \sum_{s \in S_p} p^{\max\{0, t−s\}} \nu_{(p,s)} D[X]
\]
holds where \( b(t) = \inf \{r \in S_p \mid r \geq t \} \). The degree of \( \nu_{(p,s)} \) is strictly increasing in \( s \in S_p \) and \( \nu_{(p,s)} \) is a monic polynomial of minimal degree in \( N_{(p^t)}(B) \). If \( t \leq \max S_p \), then the summand \( \mu_B D[X] \) can be omitted.

**Proof.** It has been shown in (9) Theorem 2.19 that
\[
N_{(p^t)}(B) = \sum_{i \in \mathcal{I}_t} p^{t−i} \nu_{(p,i)} D[X]
\]
where \( \mathcal{I}_t \) denotes the \( t \)-th index set of \( B \) with respect to \( p \) and \( \nu_{(p,i)} \) are monic polynomials of minimal degree in \( N_{(p^t)}(B) \) whose degree is strictly increasing in \( i \in \mathcal{I}_t \). Moreover, it follows from (9) Corollary 2.23 that for every \( p \) there exists an integer \( m \) such that
\[
N_{(p^t)}(B) = \mu_B D[X] + p^{t−m} N_{(p^m)}(B)
\]
holds for all \( t \geq m \). We set \( S_p = \mathcal{I}_m \setminus \{0, m\} \). Note that \( \nu_{(p,0)} = 1 \) is a monic polynomial of minimal degree in \( N_{(p^t)}(B) = D[X] \). For \( t \geq m \), the assertion now follows from Equations (8) and (9).

If \( t < m \), it follows from (9) Definition 2.16, Remark 2.18) that \( \mathcal{I}_t \setminus \{0, t\} = S_p \cap \{1, \ldots, t−1\} \) and \( \nu_{(p,b(t))} \) is also a feasible choice for \( \nu_{(p,t)} \). Therefore, the assertion follows from Equation (8). \( \square \)
References

[1] W. W. Adams and P. Loustaunau. An introduction to Gröbner bases, volume 3 of Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 1994.

[2] N. Bourbaki. Commutative Algebra, Chapters 1–7. Springer, Berlin, 1989.

[3] W. C. Brown. Matrices over Commutative Rings. Monographs and Textbooks in Pure and Applied Mathematics. Marcel Dekker, Inc., New York, 1993.

[4] W. C. Brown. Null ideals and spanning ranks of matrices. Comm. Algebra, 26(8):2401–2417, 1998.

[5] C. Heuberger and R. Rissner. Compute J-ideal of a matrix. http://trac.sagemath.org/ticket/21992 2016.

[6] R. Kannan and A. Bachem. Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix. SIAM J. Comput., 8(4):499–507, 1979.

[7] S. Lang. Algebra, volume 211 of Graduate Texts in Mathematics. Springer-Verlag New York, 2002.

[8] N. H. McCoy. Rings and ideals. Carus Monograph Series, no. 8. The Open Court Publishing Company, LaSalle, Ill., 1948.

[9] R. Rissner. Null ideals of matrices over residue class rings of principal ideal domains. Linear Algebra Appl., 494:44–69, 2016.

[10] The SageMath Developers. SageMath Mathematics Software (Version 7.5), 2017. http://www.sagemath.org

Institut für Mathematik, Alpen-Adria-Universität Klagenfurt, Universitätsstrasse 65–67, 9020 Klagenfurt am Wörthersee, Austria
E-mail address: clemens.heuberger@aau.at

Institut für Analysis und Zahlentheorie, TU Graz, Kopernikusgasse 24, 8010 Graz, Austria
E-mail address: roswitha.rissner@tugraz.at