Implementations of efficient univariate polynomial matrix algorithms and application to bivariate resultants
Seung Gyu Hyun, Vincent Neiger, Éric Schost

To cite this version:
Seung Gyu Hyun, Vincent Neiger, Éric Schost. Implementations of efficient univariate polynomial matrix algorithms and application to bivariate resultants. 2019. hal-01995873v2

HAL Id: hal-01995873
https://hal-unilim.archives-ouvertes.fr/hal-01995873v2
Preprint submitted on 10 May 2019

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Implementations of efficient univariate polynomial matrix algorithms and application to bivariate resultants

Seung Gyu Hyun  
University of Waterloo  
Waterloo, ON, Canada

Vincent Neiger  
Univ. Limoges, CNRS, XLIM, UMR 7252  
F-87000 Limoges, France

Éric Schost  
University of Waterloo  
Waterloo, ON, Canada

Abstract

Complexity bounds for many problems on matrices with univariate polynomial entries have been improved in the last few years. Still, for most related algorithms, efficient implementations are not available, which leaves open the question of the practical impact of these algorithms, e.g. on applications such as decoding some error-correcting codes and solving polynomial systems or structured linear systems. In this paper, we discuss implementation aspects for most fundamental operations: multiplication, truncated inversion, approximants, interpolants, kernels, linear system solving, determinant, and basis reduction. We focus on prime fields with a word-size modulus, relying on Shoup’s C++ library NTL. Combining these new tools to implement variants of Villard’s algorithm for the resultant of generic bivariate polynomials (ISSAC 2018), we get better performance than the state of the art for large parameters.

Keywords

Polynomial matrices, algorithms, implementation, resultant.

ACM Reference Format:


1 Introduction

Hereafter, \( \mathbb{K} \) is a field and \( \mathbb{K}[x] \) is the algebra of univariate polynomials over \( \mathbb{K} \). Recent years have witnessed a host of activity on fast algorithms for polynomial matrices and their applications:

- Minimal approximant bases \([15, 53]\) were used to compute kernel bases \([54]\), giving the first efficient deterministic algorithm for linear system solving over \( \mathbb{K}[x] \).
- Basis reduction \([15, 16]\) played a key role in accelerating the decoding of one-point Hermitian codes \([35]\) and in designing deterministic determinant and Hermite form algorithms \([29]\).
- Progress on minimal interpolant bases \([23, 24]\) led to the best known complexity bound for list-decoding Reed-Solomon codes and folded Reed-Solomon codes \([24, Sec. 2.4 to 2.7]\).
- Coppersmith’s block Wiedemann algorithm and its extensions \([7, 26, 48]\) were used in a variety of contexts, from integer factorization \([44]\) to polynomial system solving \([22, 49]\).

At the core of these improvements, one also finds techniques such as high-order lifting \([41]\) and partial linearization \([42],[16, Sec. 6]\).

For many of these operations, no implementation of the latest algorithms is available and no experimental evidence has been given regarding their practical behavior. Our goal is to partly remedy this issue, by providing and discussing implementations for a core of fundamental algorithms such as multiplication, approximant and interpolant bases, etc., upon which one may implement higher level algorithms. As an illustration, we describe the performance of slightly modified versions of Villard’s recent breakthroughs on bivariate resultant and characteristic polynomial computation \([49]\).

Our implementation is based on Shoup’s Number Theory Library (NTL) \([40]\), and is dedicated to polynomial matrix arithmetic over \( \mathbb{K} = \mathbb{F}_p \) for a word-size prime \( p \). Particular attention was paid to performance issues, so that our library compares favorably with previous work for those operations where comparisons were possible. Our code is available at https://github.com/vneiger/pml.

Overview. Polynomial matrix algorithms rely on efficient arithmetic in \( \mathbb{K}[x] \) and for matrices over \( \mathbb{K} \); in Section 2, we review some related algorithms and their NTL implementations. Then, we describe our implementation of a key building block: multiplication.

Section 3 presents the next major part of our work, concerning algorithms for approximant bases \([2, 15, 25, 53]\) and interpolant bases \([3, 23, 24, 47]\). We focus on a version of interpolants which is less general than in these references but allows for a more efficient algorithm. In particular, we show that with this version, both interpolant and approximant bases can be used interchangeably in several contexts, with interpolants sometimes achieving better performance than approximants. In Section 4, we discuss algorithms for minimal kernel bases, linear system solving, determinant, and basis reduction. Finally, using these tools, we study the practical behavior of the bivariate resultant algorithm of \([49]\) (Section 5).

Below, cost bounds are given in an algebraic complexity model, counting all operations in the base field at unit cost. While standard, this point of view fails to describe parts of the implementation (CRT-based algorithms, such as the 3-primes FFT, cannot be described in such a manner), but we believe that this is a minor issue.

Implementation choices. NTL is a C++ library for polynomial and matrix arithmetic over rings such as \( \mathbb{Z}, \mathbb{Z}/n\mathbb{Z} \), etc., and is often seen as a reference point for fast implementations in such contexts. Other libraries for these operations include for example FLINT \([18]\) as well as FFLAS-FFPACK and LinBox \([45, 46]\). Currently, our implementation relies solely on NTL; this choice was based on comparisons of performance for the functionalities we need.

In our implementation, the base field is a prime finite field \( \mathbb{F}_p \); we rely on NTL’s \( \mathbb{Z}/p \) class. At the time of writing, on standard x86_64 platforms, NTL v11.3.1 uses unsigned long’s as its primary data type for \( \mathbb{Z}/p \), supporting moduli up to 60 bits long.
2. Basic polynomial and matrix arithmetic

We review basic algorithms for polynomials and matrices, and related complexity results that hold over an abstract field $\mathbb{K}$, and we describe how we implemented these operations. Hereafter, for $d \geq 0$, $\mathbb{K}[x]_d$ is the set of elements of $\mathbb{K}[x]$ of degree less than $d$.

2.1. Polynomial multiplication. Multiplication in $\mathbb{K}[x]$ and Fast Fourier Transform (FFT) are cornerstones of most algorithms in this paper. Let $M : \mathbb{N} \to \mathbb{N}$ be a function such that polynomials of degree at most $d$ in $\mathbb{K}[x]_d$ can be multiplied in $\mathbb{M}(d)$ operations in $\mathbb{K}$. If $\mathbb{K}$ supports FFT, we can take $M(d) \in O(d \log d)$, and otherwise, $M(d) \in O(d \log d \log \log d)$ [11, Chapter 8]; as in this reference, we assume that $d \mapsto M(d)/d$ is increasing. A useful variant of multiplication is the middle product [5, 17]: for integers $c$ and $d$, and $F \in \mathbb{K}[x]_c$, and $G \in \mathbb{K}[x]_{c+d}$, MiddleProduct($F, G, c, d$) returns the slice of the product $FG$ with coefficients of degrees $c, \ldots, c+d-1$; a common case is with $c = d$. The direct approach computes the whole product and extracts the slice. Yet, the transposition principle [27] yields a more efficient approach, saving a constant factor (roughly a factor 2 when $c = d$, if FFT multiplication is used).

Polynomial matrix algorithms frequently use fast evaluation and interpolation at multiple points. In general, subproduct tree techniques [11, Chapter 10] allow one to do evaluation and interpolation of polynomials in $\mathbb{K}[x]_d$ at $d$ points in $\mathbb{O}(M(d) \log d)$ operations. For special sets of points, one can do better: if we know $\alpha$ in $\mathbb{K}$ of order at least $d$, then evaluation and interpolation at the geometric progression $(1, \alpha, \ldots, \alpha^{d-1})$ can both be done in time $O(M(d))$ [6].

In NTL, multiplication in $\mathbb{F}_p[x]$ uses either naive, Karatsuba, or FFT techniques, depending on $p$ and on the degree (NTL provides FFT primes with roots of unity of order $2^{25}$, and supports arbitrary user-chosen FFT primes). FFT multiplication uses the TFFT algorithm of [19] and Harvey’s improvements on arithmetic mod $p$ [20]. For primes $p$ that do not support Fourier transforms, multiplication is done by means of either 3-primes FFT techniques [11, Chapter 8] or Schönhage and Strassen’s algorithm. We implemented middle products for naive, Karatsuba and FFT multiplication, closely following [5, 17], as well as evaluation/interpolation algorithms for general sets of points and for geometric progressions.

2.2. Matrix multiplication. Let $\omega$ be such that $n \times n$ matrices over any ring can be multiplied by a bilinear algorithm doing $O(n^\omega)$ ring operations. The naïve algorithm does exactly $n^3$ multiplications. First improvements due to Winograd and Waksman [50, 51] reduced the number of operations to $n^3/2 + O(n^2)$ if $2$ is a unit. Strassen’s and Winograd’s recursive algorithms [43, 52] have $\omega = \log_2(7)$; the best known bound is $\omega \leq 2.373$ [8, 30]. Note that, using blocking, rectangular matrices of sizes $(m \times n)$ and $(n \times p)$ can be multiplied in $O(mnp \min(m,n,p)^{\omega-1})$ ring operations. NTL implements its own arithmetic for matrices over $\mathbb{F}_p$, and chooses one of several implementations depending on the bit size of $p$, the matrix dimensions, the available processor instructions, etc.

2.3. Polynomial matrix multiplication. In what follows, we write $\mathbb{M}(n, d)$ for a function such that two $n \times n$ matrices of degree at most $d$ can be multiplied in $\mathbb{M}(n, d)$ operations in $\mathbb{K}$; we make the assumption that $d \mapsto \mathbb{M}(n, d)/d$ is increasing for all $n$.

From the definitions above we obtain $\mathbb{M}(n, d) \in O(n^\omega \mathbb{M}(d))$, which is in $O(n^\omega d)$ using evaluation/interpolation at $1, \alpha, \ldots, \alpha^2d$ or at roots of unity, one obtains the following bounds on $\mathbb{M}(n, d)$:

- $O(n^{\omega} d + n^2 \mathbb{M}(d))$ if an element $\alpha$ in $\mathbb{K}$ of order more than 2 is known [6, Thm. 2.4].
- $O(n^{\omega} d + n^{2d} \log d)$ if $\mathbb{K}$ supports FFT in degree $2d$.

We also mention a polynomial analogue of an integer matrix multiplication algorithm from [10] which uses evaluation/interpolation, done plainly via multiplication by (inverse) Vandermonde matrices.

When the corresponding part of the cost (e.g. $O(n^2 \mathbb{M}(d))$ for geometric progressions) is replaced by the cost of multiplying matrices over $\mathbb{K}$ in sizes roughly $(d \times d)$ by $(d \times d^2)$, this is in $O(n^2 \mathbb{M}(d^{d-1}))$ if $d \leq n^2$. For moderate values of $d$, where $\mathbb{M}(d)$ is not in the FFT regime, this allows us to leverage fast matrix multiplication over $\mathbb{K}$.

We implemented and compared various algorithms for matrix multiplication over $\mathbb{F}_p[x]$. For matrices of degree less than 5, we used dedicated routines based on Karatsuba’s and Montgomery’s formulas [32]; for matrices of small size (up to 10, depending on $p$), we use Waksman’s algorithm. For other inputs, most of our efforts were spent on variants of the evaluation/interpolation scheme.

For FFT primes, we use evaluation/interpolation at roots of unity. For general primes, we use either evaluation/interpolation at geometric progressions (if such points exist in $\mathbb{F}_p$), or our adaptation of the algorithm of [10], or 3-primes multiplication (as for polynomials, we lift the product from $\mathbb{F}_p[x]$ to $\mathbb{Z}[x]$, where it is done modulo up to 3 FFT primes). No single variant outperformed or underperformed all others for all sizes and degrees, so thresholds were experimentally determined to switch between these options, with different values for small (less than 23 bits) and for large primes.

Middle product versions of these algorithms were implemented, and are used in approximant basis algorithms (Section 3.1) and Newton iteration (Section 4.3). Multiplier classes are available: they
do precomputations on a matrix $A$ to accelerate repeated multiplications by $A$; they are used in Dixon’s algorithm (Section 4.3).

The table below shows timings for our multiplication and LinBox’ one, for random $m \times m$ matrices of degree $d$ and two choices of prime $p$. The global comparison showed running times that are either similar or in favor of our implementation.

<table>
<thead>
<tr>
<th>$m$</th>
<th>$d$</th>
<th>20 bit FFT prime</th>
<th>60 bit prime</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ours</td>
<td>LinBox ratio</td>
</tr>
<tr>
<td>8</td>
<td>131072</td>
<td>1.1198</td>
<td>1.5930</td>
</tr>
<tr>
<td>32</td>
<td>4906</td>
<td>0.4283</td>
<td>0.5092</td>
</tr>
<tr>
<td>128</td>
<td>1024</td>
<td>1.7292</td>
<td>2.1126</td>
</tr>
<tr>
<td>512</td>
<td>128</td>
<td>4.3533</td>
<td>4.3837</td>
</tr>
</tbody>
</table>

3 Approximant bases and interpolant bases

These bases are matrix generalizations of Padé approximation and play an important role in many higher-level algorithms. For $F$ in $\mathbb{K}[x]^{m \times n}$ and $M$ non-constant in $\mathbb{K}[x]$, they are bases of the $\mathbb{K}[x]$-module $\mathcal{A}_M(F)$ of all $p \in \mathbb{K}[x]^n$ such that $F \equiv 0 \mod M$. Specifically, approximant bases are for $M = x^d$ and interpolant bases for $M = [1, (x-a_1), \ldots, (x-a_d)]$ in $\mathbb{K}$. (Here, we do not consider more general cases from the literature, for example with several moduli $M_1, \ldots, M_n$, one for each column of $pF$.)

Since $\mathcal{A}_M(F)$ is free of rank $m$, such a basis is represented row-wise by a nonsingular $P$ in $\mathbb{K}[x]^{m \times m}$. The algorithms below return $P$ in $s$-ordered weak Popov form (also known as $s$-quasi Popov form [4]), for a given shift $s = (s_1, \ldots, s_m)$ in $\mathbb{Z}^m$. Shifts allow us to set degree constraints on the sought basis $P$, and they inherently occur in a general approach for finding bases of solutions to equations (approximants, interpolants, kernels, etc.). Approximant basis algorithms often require $P$ to be in a $s$-reduced form [47]; although the $s$-ordered weak Popov form is stronger, obtaining it involves minor changes in these algorithms, without impact on performance according to our experiments. Recent literature shows that this stronger form reveals valuable information for further computations with $P$ [23, 25], in particular for finding $s$-Popov bases [4].

From the shift $s$, the $s$-degree of $p = [p_1]; \in \mathbb{K}[x]^{1 \times m}$ is defined as $\text{red}_s(p) = \max_{1 \leq i \leq m}(\text{deg}(p_i) + s_i)$, which extends to matrices: $\text{red}_s(P)$ is the list of $s$-degrees of the rows of $P$. Then, the $s$-pivot of $p$ is its rightmost entry $p_i$ such that $\text{red}_s(p) = \text{deg}(p_i) + s_i$, and a nonsingular matrix $P$ is in an $s$-ordered weak Popov form if the $s$-pivots of its rows are located on the diagonal.

To simplify cost bounds below, we make use of the function $\text{MM}^s(m, d) = \sum_{i=0}^{\lfloor \log_2(d) \rfloor} 2^i \text{MM}(m, d, 2^i) \in O(\text{MM}(m, d) \log(d))$.

3.1. Approximant bases. For $F$ in $\mathbb{K}[x]^{m \times n}$ and $d$ in $\mathbb{Z}_{>0}$, an approximant basis for $(F, d)$ is a nonsingular $m \times m$ matrix whose rows form a basis of $\mathcal{A}_d(F)$. We implemented minor variants of the algorithms M-Basis (iterative, via matrix multiplication) and PM-Basis (divide and conquer, via polynomial matrix multiplication) from [15]. The lowest-level function (M-Basis-1 with the signature in Algorithm 1), handles order $d = 1$ in time $O(\text{rank}(F^{\leq 2} m n))$; here, working modulo $X$, the matrix $F$ is over $\mathbb{K}$. Our implementation follows [25, Algo. 1], which returns an $s$-Popov basis, using only an additional row permutation compared to the algorithm in [15].

Algorithm 1: M-Basis-1($F, s$)

Input: matrix $F$ in $\mathbb{K}[x]^{m \times n}$, shift $s$ in $\mathbb{Z}^m$

Output: the $s$-Popov approximant basis for $(F, 1)$

with $d$ iterations, each computing the residual $R$ and updating $P$ via multiplication by a basis $Q$ obtained by M-Basis-1 on $R$. We also follow [15] for PM-Basis, using a threshold $T$ such that M-Basis is called if $d \leq T$. Building PM-Basis directly upon M-Basis-1, i.e., choosing $T = 1$, has the same cost bound but is slower in practice.

Algorithm 2: M-Basis($F, d, s$)

Input: matrix $F$ in $\mathbb{K}[x]^{m \times n}$, order $d$ in $\mathbb{Z}_{>0}$, shift $s$ in $\mathbb{Z}^m$

Output: an $s$-ordered weak Popov approximant basis for $(F, d)$

Algorithm 3: PM-Basis($F, d, s$)

Input: $F$ in $\mathbb{K}[x]^{m \times n}$, order $d$ in $\mathbb{Z}_{>0}$, shift $s$ in $\mathbb{Z}^m$

Output: an $s$-ordered weak Popov approximant basis for $(F, d)$

These algorithms use $O((m^{\omega} + m^{\omega-1} n) d^2)$ and $O((1 + \frac{n}{m}) \text{MM}(m, d))$, respectively [15]. Some implementation details are discussed in Section 3.2. The next table compares timings for LinBox’ and our implementations of PM-Basis for a 20 bit FFT prime (LinBox’ implementation is not optimized for large primes and general primes).

<table>
<thead>
<tr>
<th>$m$</th>
<th>$n$</th>
<th>$d$</th>
<th>ours</th>
<th>LinBox ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>4</td>
<td>131072</td>
<td>6.6754</td>
<td>15.5743</td>
</tr>
<tr>
<td>32</td>
<td>16</td>
<td>8192</td>
<td>4.1185</td>
<td>7.1150</td>
</tr>
<tr>
<td>128</td>
<td>64</td>
<td>2048</td>
<td>18.0030</td>
<td>28.7113</td>
</tr>
<tr>
<td>512</td>
<td>256</td>
<td>256</td>
<td>39.6255</td>
<td>42.4051</td>
</tr>
</tbody>
</table>

We also implemented [25, Algo. 3] which returns $s$-Popov bases and is about twice slower than PM-Basis; making this overhead negligible for some usual cases is future work. For completeness, we handle general approximants (with one modulus per column of $F$) by an iterative approach from [2, 47]; faster algorithms are more complex [23–25] and use partial linearization techniques.

These techniques from [42, 53] yield cost bounds in $O(n^{\omega-1} m^2 d)$, which is a $\Theta \left( \frac{n^2}{m} \right)$ speedup compared to PM-Basis. Implementing them is work in progress. Experimental code, which focuses for simplicity on $n = 1$ and “generic” inputs for which the degrees in $P$ can be predicted, revealed significant speedups:

<table>
<thead>
<tr>
<th>$m$</th>
<th>$n$</th>
<th>$d$</th>
<th>PM-Basis</th>
<th>PM-Basis with linearization</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>1</td>
<td>65356</td>
<td>1.6693</td>
<td>1.26891</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>16384</td>
<td>1.8535</td>
<td>0.89652</td>
</tr>
<tr>
<td>64</td>
<td>1</td>
<td>2048</td>
<td>2.2865</td>
<td>0.14362</td>
</tr>
<tr>
<td>256</td>
<td>1</td>
<td>1024</td>
<td>36.620</td>
<td>0.20660</td>
</tr>
</tbody>
</table>

Approximant bases are often applied to solve block-Hankel systems [28]. In two specific settings, we have compared this approach.
An \( \alpha \)-cients (and \( M \)-IntBasis mat\( \langle \mathbb{V}_{\mathbb{Z}, \mathbb{P}}, \mathbb{M} \rangle \) stand for the sublist \( I \langle \mathbb{V}, \mathbb{P}, \mathbb{M} \rangle \) of \( \mathbb{V} \times \mathbb{P} \times \mathbb{M} \) matrix of degree \( d \times 1 \), and we solve a block system with \( 1 \times m \) Hankel blocks of size \( m \times d \). The cost bounds are \( O(m^{d+1}d) \) and \( O(m^{d}d) \), respectively. Approximants are faster up to dimension 15, which is explained by the arguments in the previous paragraph. For larger dimensions, as predicted by the cost estimates, the block-Hankel solver is more efficient.

### 3.2. Interpolant bases

For matrices \( E = (E_1, \ldots, E_d) \) in \( \mathbb{K}^{m \times n} \) and pairwise distinct points \( \alpha = (\alpha_1, \ldots, \alpha_d) \) in \( \mathbb{K} \), consider

\[
I_\alpha(E) = \{ p \in \mathbb{K}[x]^{1 \times m} \mid p(\alpha_i)E_i = 0 \text{ for } 1 \leq i \leq d \}.
\]

An interpolant basis for \( (E, \alpha) \) is a matrix whose rows form a basis of the \( \mathbb{K}[x] \)-module \( I_\alpha(E) \). Note that \( I_\alpha(E(\alpha_1), \ldots, E(\alpha_d)) \) coincides with \( A_M(F) \), for \( F \) in \( \mathbb{K}[x]^{m \times n} \) and \( M = \Pi_{i=1}^{d}(x - \alpha_i) \).

This definition is a specialization of those in [3, 24], which consider \( n \) sets of points, one for each of the \( n \) columns of \( E_1, \ldots, E_d \); here, these sets are all equal. This more restrictive problem allows us to give faster algorithms than those in these references, by direct adaptations of the approximant basis algorithms presented above. Besides, Sections 4.1 and 4.2 will show that interpolant bases can often play the same role as approximant bases in applications.

These adaptations are described in Algorithms 4 and 5, where \( \alpha_{1, \ldots, j} \) stands for the sublist \( (\alpha_1, \alpha_{1, \ldots, j}) \). In the next proposition, we assume that \( MM(n, d) \) is in \( \Omega(n^2M(d)) \) (instead, one may add an extra term \( O(n^2M(d) \log(d)) \) in the cost).

**Proposition 3.1.** Algorithm 5 is correct. For input evaluation points in geometric progression, it costs \( O(MM(m, d)) \) if \( n \leq m \) and \( O(MM(m, d) + m^{d-1}n \log(d)) \) otherwise. For general evaluation points, an extra cost \( O(M^2M(d) \log^2(d)) \) is incurred.

(Correctness follows from Items (i) and (iii) of [25, Lem. 2.4]; the cost analysis is standard for such divide and conquer algorithms.)

Our current code uses the threshold \( T = 32 \) in the divide and conquer \( M \)-BP and \( M \)-IntBasis: beyond this point, they are faster than the iterative \( M \)-Basis and \( M \)-IntBasis. Unlike in most other functions, where elements of \( \mathbb{K}[x]^{m \times n} \) are represented as matrices of polynomials \( \langle \text{Mat}<\text{Vec}<\mathbb{V}_{\mathbb{Z}, \mathbb{P}}> \rangle \) in \( \mathbb{N} \), in \( \mathbb{N} \)-Basis and \( \mathbb{N} \)-IntBasis we see them as polynomials with matrix coefficients \( \langle \text{Vec}<\text{Mat}<\mathbb{V}_{\mathbb{Z}, \mathbb{P}}> \rangle \rangle \). Indeed, since these algorithms involve only matrix arithmetic over \( \mathbb{K} \) (recall that \( \deg(Q) \leq 1 \)), this turns out to be more cache-friendly and faster.

We implemented two variants for approximant bases: either the residual \( R \) is computed from \( P \) and \( F \) at each iteration, or we initialize a list of residuals with a copy of \( F \) and update the whole list at each iteration using \( Q \). The second variant improves the error before the first \( \alpha_1 = m/2 \), with significant savings when \( n \) is close to \( m \). For interpolant bases, this does not lead to any gain.

TIMINGS are shown in the next table, for Algorithms \( M \)-Basis (M), \( M \)-IntBasis (M-I), \( M \)-BP (M-1), \( M \)-IntBasis for general points (PM-I) and for geometric points (PM-lg). For approximants, we take a random input in \( \mathbb{K}[x]^{m \times n} \) of degree \( d \); for interpolants, we take \( d \) random matrices in \( \mathbb{K}^{m \times n} \). We focus on the common case \( m = 2n \), which arises for example in kernel algorithms (Section 4.2) and in fraction reconstruction, itself used in basis reduction (Section 4.5) and in the resultant algorithm of [49] (Section 5).

### Input: matrices \( E = (E_1, \ldots, E_d) \) in \( \mathbb{K}^{m \times n} \), evaluation points \( \alpha = (\alpha_1, \ldots, \alpha_d) \) in \( \mathbb{K} \), shift \( s \in \mathbb{Z}^m \)

### Output: an \( s \)-ordered weak Popov interpolant basis for \( (E, \alpha) \)

**Algorithm 4: M-IntBasis((E, \alpha), s)**

1. \( P \leftarrow \text{id} \text{ matrix}_{\mathbb{K}[x]^{m \times m}} \)
2. For \( k = 0, \ldots, d - 1 \):
   a. \( R \in \mathbb{K}^{m \times n} \leftarrow \text{P}(\alpha_1)E_1 \)
   b. \( Q \in \mathbb{K}[x]^{m \times m} \leftarrow \text{M-Basis-1}(R, t) \)
   c. \( P \leftarrow Q \), and then \( t \leftarrow \deg_q(P) \)
3. Return \( P \)

**Algorithm 5: M-IntBasis((E, \alpha), s)**

1. If \( d \leq T \) return \( M \)-IntBasis((E, \alpha), s)\)
2. \( P_1 \leftarrow \text{M-IntBasis}(E_{1 \ldots [d/2]}, \alpha_{1 \ldots [d/2]}, s) \)
3. \( R \leftarrow (P_1(\alpha_{[d/2]+1}E_{[d/2]+1} \ldots P_1(\alpha_d)E_d) \)
4. \( t \leftarrow \deg_q(P_1) \)
5. \( P_2 \leftarrow \text{M-IntBasis}(R, \alpha_{[d/2]+1 \ldots d}, t) \)
6. Return \( P_2P_1 \)

Concerning iterative algorithms, we observe that interpolants are slightly faster than approximants, which is explained by the cost of computing the residual \( R \); it uses one Horner evaluation of \( P \) and one matrix product for interpolants, whereas for approximants it uses about \( \min(k, \deg(P)) \) matrix products at iteration \( k \).

As for the divide and conquer algorithms, interpolant bases with general points are slower, in some cases significantly, than the other two algorithms: although the complexity analysis predicted a disadvantage, we believe that our implementation of multipoint evaluation at general points could be improved to reduce this gap.

For the other two algorithms, the comparison is less clear. There could be many factors at play here, but the main differences lie in the base case (Step 1) which calls the iterative algorithm, and in the
computation of residuals (Step 3) which uses either middle products or geometric evaluation. It seems that FFT-based polynomial multiplication performs slightly better than geometric evaluation for small matrices and slightly worse for large matrices.

4 Higher-level algorithms

In this section we consider kernel bases, system solving, determinants, and basis reduction; we discuss algorithms which rely on multiplication, through approximant/interpolant bases and lifting techniques. For many of these algorithms, we are not aware of previous implementations or experimental comparisons.

4.1. A note on matrix fraction reconstruction. Given \( H \) in \( \mathbb{K}(x)^{m \times n} \), a left fraction description of \( H \) is a pair of polynomial matrices \((Q, R)\) in \( \mathbb{K}(x)^{m \times n} \) such that \( H = Q^{-1}R \). It is minimal if \( Q \) and \( R \) have unimodular left matrix GCD and \( Q \) is in reduced form (right fraction descriptions are defined similarly). Besides, \( H \) is said to be strictly proper if the numerator of each of its entries has degree less than the corresponding denominator.

Such a description of \( H \) is often computed from the power series expansion of \( H \) at sufficient precision, using an approximant basis. Yet, for resultant computations in Section 5.2, we would like to use an interpolant basis to obtain this description from sufficiently many values of \( H \). We now state the validity of this approach; this is a matrix version of rational function reconstruction [11, Chap. 5.7].

**Proposition 4.1.** Let \( H \) be in \( \mathbb{K}(x)^{m \times n} \) be strictly proper and suppose \( H \) admits left and right fraction descriptions of degrees at most \( D \), for some \( D \in \mathbb{N}_0 \). For \( M \) in \( \mathbb{K}(x) \) of degree at least \( 2D \) and such that all denominators in \( H \) are invertible modulo \( M \), define the matrix \( F = [H \bmod M - I_n]^T \in \mathbb{K}(x)^{2n \times n} \). Then, if \( P \in \mathbb{K}(x)^{2n \times n} \) is a \( 0 \)-order weak Popov basis of \( \mathcal{A}_M(F) \), the first \( n \) rows of \( P \) form a matrix \((Q, R)\) such that \((Q, R)\) is a minimal left fraction description of \( H \), with \( Q \) in \( 0 \)-order weak Popov form.

The proof given in [15, Lem.3.7] for the specific \( M = x^{2D+1} \) extends to any modulus \( M \); using an ordered weak Popov form (rather than a reduced form) allows us both to know a priori that the first \( n \) rows are of degree at most \( D \), and to use degree \( 2D \) instead of \( 2D + 1 \) (since \( \text{deg}(R) < \text{deg}(Q) \) is ensured by this form).

In particular, if \( M = \prod_{i=1}^{2D} (x - \alpha_i) \) for pairwise distinct points \((\alpha_1, \ldots , \alpha_{2D})\), the interpolant basis algorithms in Section 3.2 give a minimal left fraction description of \( H \) from \( H(\alpha_1), \ldots , H(\alpha_{2D}) \).

4.2. Kernel basis. We implemented two kernel basis algorithms: the first one, based on Lemma 4.2, finds the kernel basis from a single approximant basis at sufficiently large order; the second one, from [54], uses several approximant bases at small order and combines recursively obtained kernel bases via multiplication. With a minor modification and no performance impact, the latter returns an \( s \)-ordered weak Popov basis. In both cases, we designed variants which rely on interpolant bases instead of approximant bases.

**Lemma 4.2.** Let \( F \) be in \( \mathbb{K}(x)^{m \times n} \) of degree \( d \geq 0 \), let \( s \) be in \( \mathbb{N}^m \), and let \( \delta \in \mathbb{N}_0 \) be an upper bound on the \( s \)-degree of any \( s \)-reduced left kernel basis of \( F \); for example, \( \delta = nd + \max(s) - \min(s) + 1 \).

Let \( M \) be in \( \mathbb{K}(x) \) of degree at least \( \delta + d \), and \( P \in \mathbb{K}(x)^{m \times n} \) be an \( s \)-reduced basis of \( \mathcal{A}_M(F) \). Then, the submatrix of \( P \) formed by its rows of \( s \)-degree less than \( \delta \) is an \( s \)-reduced left kernel basis of \( F \).

For a proof, see https://hal.archives-ouvertes.fr/hal-01995873v1/document.

In particular, one may find \( P \) via \( \text{PM-IntBasis} \) at \( d + \delta \) points or via \( \text{PM-Basis} \) at order \( d + \delta \); for \( n \leq m \), this costs \( \mathcal{O}(\text{MM}(m, d + \delta)) \). The approximant-based direct approach is folklore [54, Sec. 2.3], yet explicit statements in the literature focus on shifts linked to the degrees in \( F \), with better bounds \( \delta \) (see [54, Lem. 3.3],[33, Lem. 4.3]).

The algorithm of [54] is more efficient, at least when the entries of \( s \) are close to the corresponding row degrees of \( F \); for a uniform shift, it costs \( \mathcal{O}(m\delta^2 \left\lfloor nd/m \right\rfloor) \) operations. We obtained significant practical improvements over the plain implementation of [54, Algo. 1] thanks to the following observation: if \( n \leq m/2 \), for a vast majority of input \( F \), the approximant basis at Step 2 of [54, Algo. 1], computed at order more than \( 2s \), contains the sought kernel basis. Furthermore, this can be easily tested by checking well-chosen degrees, and then the algorithm can exit early, avoiding the further recursive calls. We took advantage of this via the following modifications: we use order \( 2s + 1 \) rather than \( 3s \) (see [54, Rmk. 3.5] for a discussion on this point), and when \( n > m/2 \) we directly reduce the number of columns via the divide and conquer scheme in [54, Thm. 3.15].

The use of approximants here follows the idea in Lemma 4.2: row vectors of small degree which are in \( \mathcal{A}_M(F) \) for a large degree \( M \) must be in the kernel of \( F \). Thus, one can directly replace approximant bases with interpolant bases in [54, Algo. 1], up to modifying Step 8 accordingly (dividing by the appropriate polynomial \( M \)).

Timings for both approaches are showed in the next table, for a random \( F \) of degree \( d \). Except for the last row, the shift is uniform and, as expected, [54, Algo. 1] is faster than the direct approach; the differences between interpolant and approximant variants follow those observed in Section 3. The last row corresponds to a shift yielding the kernel basis in Hermite form and shows, as expected, that the direct approach is faster for shifts that are far from uniform.

We note that [54, Algo. 1] may use partial linearization if it computes matrix products with unbalanced degrees or approximant bases with \( n < m \). We have not yet implemented this part of the algorithm, which may lead to slowdowns for some rare inputs.

<table>
<thead>
<tr>
<th>( m )</th>
<th>( n )</th>
<th>( d )</th>
<th>( \text{approx.} )</th>
<th>( \text{int.} )</th>
<th>( [54, \text{Algo. 1}] )</th>
<th>( \text{approx.} )</th>
<th>( \text{int.} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>4</td>
<td>1892</td>
<td>7.22</td>
<td>6.60</td>
<td>2.16</td>
<td>2.16</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>7</td>
<td>1892</td>
<td>14.1</td>
<td>14.4</td>
<td>4.64</td>
<td>4.64</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>16</td>
<td>1024</td>
<td>86.3</td>
<td>63.1</td>
<td>3.75</td>
<td>3.75</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>31</td>
<td>1024</td>
<td>142</td>
<td>118</td>
<td>8.27</td>
<td>8.27</td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>64</td>
<td>256</td>
<td>2720</td>
<td>1827</td>
<td>16.8</td>
<td>16.8</td>
<td></td>
</tr>
<tr>
<td>128</td>
<td>127</td>
<td>256</td>
<td>&gt;1h</td>
<td>&gt;1h</td>
<td>43.8</td>
<td>43.8</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>512</td>
<td>5.68</td>
<td>5.31</td>
<td>11.5</td>
<td>11.5</td>
<td></td>
</tr>
</tbody>
</table>

4.3. Linear system solving. For systems \( Av = b \), with \( A \) in \( \mathbb{K}(x)^{m \times n} \), \( b \) in \( \mathbb{K}(x)^{n \times 1} \) and \( v \) in \( \mathbb{K}(x)^{n \times 1} \), we implemented two families of algorithms. The first one uses lifting techniques, assuming \( A \) is square, nonsingular, with \( A(0) \) invertible; the algorithm returns a pair \((u, f)\) in \( \mathbb{K}(x)^{n \times 1} \times \mathbb{K}(x)^{n \times 1} \) such that \( Au = fb \) and \( f \) has minimal degree. The second one uses a kernel basis and works for any input \( A \); under the assumptions above, it has a similar output.

**Lifting techniques.** Under the above assumptions, our lifting algorithm is standard: if \( A \) and \( b \) have degree at most \( d \), we first compute the truncated inverse \( S = A^{-1} \bmod x^{d+1} \) by matrix Newton iteration [38]. Then, we use Dixon’s algorithm [9] to compute \( v \bmod x^{2nd} = A^{-1}b \bmod x^{2nd} \); it consists of roughly \( 2n \) steps, each involving a matrix-vector product using either \( A \) or \( S \). Then, vector
To exploit it best, we choose the input shift $20$, this is the fastest method (assuming that $d$). We implemented four algorithms, taking as input $\mathbf{b}$, compute $\mathbf{a} \bmod x^{2md}$, are cheaper, so the runtime is $O(\text{MM}(n,d) \log(n)) < O(n^2 d)$. 

Using kernel bases. For this second approach, let $\mathbf{A}$ be any matrix in $\mathbb{K}[x]^{m \times n}$ and $\mathbf{b}$ be in $\mathbb{K}[x]^{n \times 1}$. The algorithm simply computes $\mathbf{K} \in \mathbb{K}[x]^{(n+1) \times k}$, a right kernel basis of the augmented matrix $[\mathbf{A} | \mathbf{b}] \in \mathbb{K}[x]^{m \times (n+1)}$. The matrix $\mathbf{K}$ generates, via $\mathbb{K}(x)$-linear combinations of its columns, all solutions $\mathbf{v} \in \mathbb{K}(x)^{n \times 1}$ to $\mathbf{A}\mathbf{v} = \mathbf{b}$.

In particular, if $\mathbf{K}$ is empty (i.e., $\mathbf{k} = 0$, which requires $m \geq n$), or if the last row of $\mathbf{K}$ is zero, then the algorithm is unable to find a solution. Furthermore, if $\mathbf{A}$ is square and nonsingular, $\mathbf{K}$ has a single column $[\mathbf{u}^T | f]^T$, where $\mathbf{u} \in \mathbb{K}(x)^{n \times 1}$ and $f \in \mathbb{K}[x]$, with $f$ of minimal degree (otherwise, $\mathbf{K}$ would not be a basis).

In this context, the fastest known kernel algorithm is [54, Algo. 1]. To exploit it best, we choose the input shift $s = (d,d)$, where $d = \deg(b)$ and $d \in \mathbb{N}^m$ is the tuple of column degrees of $\mathbf{A}$ (zero columns of $\mathbf{A}$ are discarded while computing $\mathbf{d}$).

Implementation. We implemented the approaches described above: lifting with Dixon’s algorithm, high-order lifting, and via kernel. The table below shows timings for randomly chosen $m \times m$ matrix $\mathbf{A}$ and $m \times 1$ vector $\mathbf{b}$, both of degree $d$. In this case the lifting algorithms apply (with high probability). On such inputs, Dixon’s algorithm usually does best. High-order lifting, although theoretically faster, is outperformed, mainly because it performs $O(\log(n))$ matrix products (we will however see that this algorithm still plays an important role for basis reduction). The kernel based approach is moderately slower than Dixon’s algorithm, but has the advantage of working without any assumption on $\mathbf{A}$.

<table>
<thead>
<tr>
<th>$m$</th>
<th>$d$</th>
<th>Dixon</th>
<th>high-order lifting</th>
<th>kernel</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>1024</td>
<td>1.13</td>
<td>2.39</td>
<td>2.07</td>
</tr>
<tr>
<td>32</td>
<td>1024</td>
<td>4.94</td>
<td>13.8</td>
<td>9.45</td>
</tr>
<tr>
<td>64</td>
<td>1024</td>
<td>19.5</td>
<td>94.7</td>
<td>46.5</td>
</tr>
<tr>
<td>128</td>
<td>512</td>
<td>55.2</td>
<td>266</td>
<td>108</td>
</tr>
</tbody>
</table>

4.4. Determinant. We implemented four algorithms, taking as input a square $m \times m$ matrix $\mathbf{A}$.

The most basic one uses expansion by minors, which turns out to be the fastest option up to dimension about 6.

The second one assumes that we have an element $\alpha$ in $\mathbb{K}$ of order at least $2md + 1$, and uses evaluation/interpolation at the geometric progression $1, a^2, \ldots, a^{2md};$ this costs $O(m^3 M(d) + m^{w+1}d)$ operations in $\mathbb{K}$. For dimensions between 7 and about 20, it is often the fastest variant, sometimes competing with the third.

The third one consists in solving a linear system with random right-hand side of degree $d$; this yields a solution $(u, f)$ with $f$ the sought determinant up to a constant [36]. For dimensions exceeding 20, this is the fastest method (assuming that $A(0)$ is invertible).

5 Applications to bivariate resultants

We conclude this paper with algorithms originating from Villard’s recent breakthrough on computing the determinant of structured polynomial matrices [49]. Fix a field $\mathbb{K}$ and consider the two following questions: computing the resultant of two polynomials $F, G$ in $\mathbb{K}[x, z]$ with respect to $\mathbf{z}$, and computing the characteristic polynomial of an element $A$ in $\mathbb{K}[z]/(P)$, for some $P$ in $\mathbb{K}[z]$. 

The last one, from [29], is based on triangularization and runs in $O(m^d d)$. Our implementation currently only supports the generic case where the Hermite form of $A$ has diagonal $(1, \ldots, 1, \det(A))$, or in other words, all so-called row bases computed in that algorithm are the identity. This allows us to circumvent the temporary lack of a row basis implementation, while still being able to observe meaningful timings. Indeed, we believe that timings for a complete implementation called on such “generic” input will be similar to the timings presented here in many cases of interest, where one can easily detect whether the algorithm has made a wrong prediction about the row basis being identity (for example if the input matrix is reduced, which is the case if it is the denominator of a minimal fraction description). This recursive determinant algorithm calls expansion by minors as a base case for small dimensions; for larger dimensions, it is generally slightly slower than the third method.

The timings below are for a random $m \times m$ matrix $\mathbf{A}$ of degree $d$.

<table>
<thead>
<tr>
<th>$m$</th>
<th>$d$</th>
<th>minors</th>
<th>evaluation</th>
<th>invariable</th>
<th>triangular</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>65536</td>
<td>0.7571</td>
<td>2.014</td>
<td>8.460</td>
<td>0.7826</td>
</tr>
<tr>
<td>16</td>
<td>4096</td>
<td>$\infty$</td>
<td>4.14</td>
<td>5.023</td>
<td>7.38</td>
</tr>
<tr>
<td>32</td>
<td>4096</td>
<td>$\infty$</td>
<td>34.5</td>
<td>25.4</td>
<td>41.6</td>
</tr>
<tr>
<td>64</td>
<td>2048</td>
<td>$\infty$</td>
<td>127</td>
<td>68.6</td>
<td>100</td>
</tr>
<tr>
<td>128</td>
<td>512</td>
<td>$\infty$</td>
<td>244</td>
<td>96.6</td>
<td>99.0</td>
</tr>
</tbody>
</table>

4.5. Basis reduction. Our implementation of the algorithm of [15] takes as input a nonsingular matrix $\mathbf{A} \in \mathbb{K}[x]^{m \times m}$ of degree $d$ such that $A(0)$ is invertible, and returns a reduced form of $\mathbf{A}$. The algorithm first computes a slice $S$ of $2d$ consecutive coefficients of degree about $md$ in the power series expansion of $\mathbf{A}^{-1}$; then uses PM-Basis to reconstruct a fraction description $S^{-1} = R^{-1} Q$, and then returns $R$. A Las Vegas randomized version is mentioned in [15], to remove the assumption on $A(0)$: we will implement it for large enough $\mathbb{K}$, but for smaller fields this requires to work in an extension of $\mathbb{K}$, which is currently beyond the scope of our work.

In our experiments, to create the input $\mathbf{A}$, we started from a random $m \times m$ matrix of degree $d/3$ (which is reduced with high probability), and we left-multiplied it by a lower unit triangular matrix and then by an upper one, both chosen at random of degree $d/3$. The following table shows timings for both steps, with the first step either based on Newton iteration or on high-order lifting; the displayed total time is when using the faster of the two. We conclude that for reduction, as opposed to the above observations for system solving, it is crucial to rely on high-order lifting. Indeed, it improves over Newton iteration already for dimension $8$, and the gap becomes quite significant when the dimension grows.

<table>
<thead>
<tr>
<th>$m$</th>
<th>$d$</th>
<th>Newton</th>
<th>high-order</th>
<th>reconstruct</th>
<th>total</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>24574</td>
<td>1.251</td>
<td>1.688</td>
<td>8.772</td>
<td>10.02</td>
</tr>
<tr>
<td>8</td>
<td>16274</td>
<td>2.617</td>
<td>2.244</td>
<td>8.851</td>
<td>11.09</td>
</tr>
<tr>
<td>16</td>
<td>1534</td>
<td>4.457</td>
<td>3.044</td>
<td>8.506</td>
<td>11.55</td>
</tr>
<tr>
<td>32</td>
<td>382</td>
<td>11.147</td>
<td>4.858</td>
<td>7.977</td>
<td>12.83</td>
</tr>
<tr>
<td>64</td>
<td>94</td>
<td>30.62</td>
<td>5.509</td>
<td>5.833</td>
<td>11.48</td>
</tr>
</tbody>
</table>
The second problem is a particular case of the former, since the characteristic polynomial of \( A \) modulo \( P \) is the resultant of \( x - A(z) \) and \( P(z) \) with respect to \( z \), up to a nonzero constant. Let \( n \) be an upper bound on the degree in \( z \) of the polynomials we consider, and \( d \) be a bound on their degree in \( x \) (so in the second problem, \( d = 1 \)). Villard proved that for generic inputs, both problems can be solved in \( O(n^{2\omega/2}d) \) \( \subset O(n^{1.58}d) \) operations in \( \mathbb{K} \). For the first problem, the best previous bound is \( O(n^2d) \), obtained either by evaluation/interpolation techniques or Reischert’s algorithm [37]. For the second problem, the previous record was \( O(n^\omega \log n) \), where \( \omega \) is the exponent of matrix multiplication in size \( \mathbb{K}[x] \times \mathbb{K}[x] \) in \( \mathbb{K} \).

The correctness of the algorithm follows from the next properties, (for the second case, using an algorithm from [34]).

### 5.1. Overview of the approach

In [49], Villard designed the following algorithm to find the determinant of a matrix \( P \) over \( \mathbb{K}[x] \).

#### Algorithm 6: Determinant(P, m)

**Input:** nonsingular \( P \) in \( \mathbb{K}[x]^{n \times n} \); parameter \( m \in \{1, \ldots, v\} \)

**Output:** \( \det(P) \)

1. compute \( H = H \mod x^2[v/m]d+1 \), where \( d \) is the degree of \( P \) and \( H \) is the \( m \times m \) top-right quadrant of \( P^{-1} \in \mathbb{K}[x]^{v \times v} \)
2. from \( H \), find a minimal left fraction description \( (Q, R) \) of \( H \)
3. return \( \det(Q) \)

The parameter \( m \) is chosen so as to minimize the theoretical cost. The correctness of the algorithm follows from the next properties, which do not hold for an arbitrary nonsingular \( P \): the matrix \( H \) is strictly proper and admits a left fraction description \( H = Q^{-1}R \) such that \( \det(P) = \det(Q) \), for \( Q \) and \( R \) in \( \mathbb{K}[x]^{m \times m} \) of degree at most \( [v/m]d \) (see Section 4.1 for definitions). In [49], they are proved to hold for generic instances of the problems discussed here.

Once sufficiently many terms of the expansion of \( H \) have been obtained in Step 1, the denominator \( Q \) is recovered by an approximant basis algorithm and its determinant is computed by a general algorithm in Steps 2 and 3, which cost \( O(m^{\nu}vd/m) \).

While the algorithm applies to any nonsingular matrix \( P \) satisfying the properties above, in general it does not improve over previously known methods (see Section 4.4). Indeed, the fastest known algorithm for obtaining \( H \) costs \( O(v^{2d}/d) \) operations via high-order lifting (see for example [16, Thm. 1]).

However, sometimes \( P \) has some structure which helps to speed up the first step. Villard pointed out that when \( P \) is the Sylvester matrix of two bivariate polynomials, then \( P^{-1} \) is a Toeplitz-like matrix which can be described succinctly as \( P^{-1} = L_1U_1 + L_2U_2 \); here, \( L_1, L_2 \) (resp. \( U_1, U_2 \)) are lower (resp. upper) triangular Toeplitz matrices with entries in \( \mathbb{K}[x] \). Hence, we start by computing the first columns \( c_1 \) of \( L_1 \) and \( c_2 \) of \( L_2 \) as well as the first rows \( r_1 \) of \( U_1 \) and \( r_2 \) of \( U_2 \), all of them modulo \( x^2[v/m]d+1 \); then, \( H \) is directly obtained via the above formula for \( P^{-1} \), using \( O(mvd) \) operations. Computing these rows and columns is done by solving systems with matrices \( P \) and \( P^t \) and very simple right-hand sides [49, Prop. 5.1], with power series coefficients, in time \( O(v^{2d}/d) \).

Altogether, taking \( m = \sqrt{v^2} \) minimizes the cost, yielding the runtime \( O(v^{2-1/\omega}) \). In the case of bivariate resultants described above, the Sylvester matrix of \( F \) and \( G \) has size \( v = 2n \), hence the cost bound \( O((n^{2-1/\omega}) \).

#### 5.2. Resultant of generic bivariate polynomials

We implemented the algorithm described in the previous section to compute the resultant of generic \( F, G \) in \( \mathbb{K}[x, z] \); first experiments showed that obtaining \( e_1, e_2, r_1, r_2 \) was a bottleneck. These vectors have power series entries and are solutions of linear systems whose matrix is the Sylvester matrix of \( F \) and \( G \) or its transpose: they were obtained via Hensel lifting techniques, following [11, Ch. 15.4].

To get better performance, we designed a minor variant of Villard’s algorithm: instead of computing the power series expansion of \( H \) modulo \( x^3 \), where \( \delta = 2[v/m]d+1 \), we compute values of \( H \) at \( \delta \) points. We choose these points in geometric progression and use the interpolant basis algorithm of Section 3.2 to recover \( Q \) and \( N \), as detailed in Section 4.1. The value of \( H \) at \( x = \alpha \) is computed following the same approach as above, but over \( \mathbb{K} \) instead of \( \mathbb{K}[x] \).

In particular, our implementation directly relies on NTL’s extended GCD algorithm over \( \mathbb{K} \times \mathbb{P} \) to compute the vectors \( e_1, e_2, r_1, r_2 \).

The next table compares our implementation to the direct approach via evaluation/interpolation; note that the latter approach, while straightforward conceptually, is the state of the art.

<table>
<thead>
<tr>
<th>( n = d )</th>
<th>Direct</th>
<th>Algo. 6</th>
<th>( n = d )</th>
<th>Direct</th>
<th>Algo. 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>1.75</td>
<td>3.48</td>
<td>600</td>
<td>797</td>
<td>653</td>
</tr>
<tr>
<td>200</td>
<td>17.4</td>
<td>29.30</td>
<td>700</td>
<td>1343</td>
<td>1081</td>
</tr>
<tr>
<td>300</td>
<td>72.3</td>
<td>106.80</td>
<td>800</td>
<td>2121</td>
<td>1388</td>
</tr>
<tr>
<td>400</td>
<td>182</td>
<td>182</td>
<td>900</td>
<td>3203</td>
<td>1760</td>
</tr>
</tbody>
</table>

For these running times, input polynomials were chosen at random with partial degree \( n \) both in \( x \) and in \( z \); such polynomials have total degree \( 2n \), and their resultant has degree \( 2n^2 \). The largest examples have quite significant sizes, but such degrees are not unheard-of in applications, as for instance in the genus-2 point counting algorithms of [1, 12–14]. Overall, with \( n = d \), we observe a crossover point around \( n = 400 \). Besides, in a close match with the analysis above, the parameter \( m \) was set to \([n^{\nu}d] \) since this gave us the best runtimes. As an example, for \( d = 300 \), the cost of each individual steps were 65s for computing structured inversions, and 40s for obtaining \( Q \) and its determinant, which is a good balance.

#### 5.3. Characteristic polynomial

We consider the computation of the characteristic polynomial of an element \( A \) in \( \mathbb{K}[z]/(P) \), for some monic \( P \) in \( \mathbb{K}[z] \) of degree \( n \). The algorithm we implemented, and which we sketch below, is from [34] and assumes that \( A \) and \( P \) are generic.

As explained previously, this problem is a particular case of a bivariate resultant, but we rely on another point of view that allows for a better asymptotic cost. Indeed, the characteristic polynomial of \( A \) modulo \( P \) is by definition the characteristic polynomial of the matrix \( M \) of multiplication by \( A \) modulo \( P \). In other words, it is the determinant of the degree-1 matrix \( P = xI - M \in \mathbb{K}[x]^{n \times n} \).

The genericity assumption ensures that \( M \) is invertible, hence the power series expansion of \( P^{-1} \) is \( \sum_{k \geq 0} -M^{-k}x^k \). Here, we use the top-left \( m \times m \) quadrant \( H \) of \( P^{-1} \); it has entries \( h_{i,j} \in \mathbb{K}[\mathbb{K}[x]] \), where

\[
h_{i,j,k} := \text{coeff}(h_{i,j,k}, x^k) = \text{coeff}((-z^i)A^{-k-1} \mod P, z^j),
\]

for \( 0 \leq i, j < m \) and for all \( k \geq 0 \).
A direct implementation of this idea does not improve on the runtime given in Section 5.1, since it computes $A^{-k-1}$ mod $P$ for all $0 \leq k < \delta = 2[m/n]$ and therefore costs $\Omega(n^2)$. It turns out that baby-steps giant-steps techniques allow one to compute $h_{i,j,k}$ for $0 \leq i, j < m$ and $0 \leq k < \delta$ in $O((\delta + 1/2) \cdot m + m)$ operations in $\mathbb{K}$. Taking $m = \lceil n/3 \rceil$ minimizes the overall cost, resulting in the runtime $O((n^{(2+\epsilon)}+2)/3) \subset O(n^{1.46})$.

The following table compares our implementation to NTL’s built-in characteristic polynomial algorithm, with random inputs $A$ and $P$. For such inputs, NTL uses Shoup’s algorithm for power projection [39], which runs in time $O((n^{(2+\epsilon)}+2)/3)$.  

<table>
<thead>
<tr>
<th>n</th>
<th>m</th>
<th>NTL</th>
<th>New</th>
<th>n</th>
<th>m</th>
<th>NTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>5000</td>
<td>5</td>
<td>0.143</td>
<td>0.225</td>
<td>60000</td>
<td>10</td>
<td>8.45</td>
</tr>
<tr>
<td>20000</td>
<td>8</td>
<td>1.43</td>
<td>1.62</td>
<td>80000</td>
<td>10</td>
<td>16.6</td>
</tr>
<tr>
<td>40000</td>
<td>8</td>
<td>4.69</td>
<td>4.42</td>
<td>100000</td>
<td>10</td>
<td>23.1</td>
</tr>
</tbody>
</table>

Acknowledgements. Hyun was supported by a Mitacs Globalink award; Neiger was supported by CNRS/INS2I’s program for young researchers; Schost was supported by an NSERC Discovery Grant.

References


[13] P. Gaudry and É. Schost. 2004. Construction of secure random curves of genus 2 in characteristic polynomial algorithm, with random inputs $A$ and $P$. For such inputs, NTL uses Shoup’s algorithm for power projection [39], which runs in time $O((n^{(2+\epsilon)}+2)/3)$.  

[14] P. Gaudry and É. Schost. 2004. Construction of secure random curves of genus 2 in characteristic polynomial algorithm, with random inputs $A$ and $P$. For such inputs, NTL uses Shoup’s algorithm for power projection [39], which runs in time $O((n^{(2+\epsilon)}+2)/3)$.  

[15] P. Gaudry and É. Schost. 2004. Construction of secure random curves of genus 2 in characteristic polynomial algorithm, with random inputs $A$ and $P$. For such inputs, NTL uses Shoup’s algorithm for power projection [39], which runs in time $O((n^{(2+\epsilon)}+2)/3)$.  

[16] P. Gaudry and É. Schost. 2004. Construction of secure random curves of genus 2 in characteristic polynomial algorithm, with random inputs $A$ and $P$. For such inputs, NTL uses Shoup’s algorithm for power projection [39], which runs in time $O((n^{(2+\epsilon)}+2)/3)$.  

[17] P. Gaudry and É. Schost. 2004. Construction of secure random curves of genus 2 in characteristic polynomial algorithm, with random inputs $A$ and $P$. For such inputs, NTL uses Shoup’s algorithm for power projection [39], which runs in time $O((n^{(2+\epsilon)}+2)/3)$.  

[18] P. Gaudry and É. Schost. 2004. Construction of secure random curves of genus 2 in characteristic polynomial algorithm, with random inputs $A$ and $P$. For such inputs, NTL uses Shoup’s algorithm for power projection [39], which runs in time $O((n^{(2+\epsilon)}+2)/3)$.  

[19] P. Gaudry and É. Schost. 2004. Construction of secure random curves of genus 2 in characteristic polynomial algorithm, with random inputs $A$ and $P$. For such inputs, NTL uses Shoup’s algorithm for power projection [39], which runs in time $O((n^{(2+\epsilon)}+2)/3)$.  

[20] P. Gaudry and É. Schost. 2004. Construction of secure random curves of genus 2 in characteristic polynomial algorithm, with random inputs $A$ and $P$. For such inputs, NTL uses Shoup’s algorithm for power projection [39], which runs in time $O((n^{(2+\epsilon)}+2)/3)$.  

[21] P. Gaudry and É. Schost. 2004. Construction of secure random curves of genus 2 in characteristic polynomial algorithm, with random inputs $A$ and $P$. For such inputs, NTL uses Shoup’s algorithm for power projection [39], which runs in time $O((n^{(2+\epsilon)}+2)/3)$.  

[22] P. Gaudry and É. Schost. 2004. Construction of secure random curves of genus 2 in characteristic polynomial algorithm, with random inputs $A$ and $P$. For such inputs, NTL uses Shoup’s algorithm for power projection [39], which runs in time $O((n^{(2+\epsilon)}+2)/3)$.  


