Relaxing order basis computation
Pascal Giorgi, Romain Lebreton

To cite this version:


HAL Id: lirmm-01372532
https://hal-lirmm.ccsd.cnrs.fr/lirmm-01372532
Submitted on 27 Sep 2016

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.
Let $K$ be a field, $F = \sum_{i=0}^{m} F_i x^i \in K[x]_{m \times m}$ a matrix of power series, $\sigma$ a positive integer and $(F, \sigma)$ be the $K[x]$-module defined by the set of $v \in K[x]_{m \times m}$ such that $v F \equiv 0 \mod x^\sigma$.

**Definition of Order basis:** $P \in K[x]_{m \times m}$ is a (left) $(\sigma, \tilde{\sigma})$-order basis of $F$ if the rows of $P$ form a $\tilde{\sigma}$-row reduced basis of $(F, \sigma)$ (see [1]).

**Order basis are used in:** column reduction [2]; minimal nullspace basis [3]; block Wiedemann algorithm [4];...

### Two existing algorithms

**Input:** $F \in K[x]_{m \times m}, \sigma \in \mathbb{N}$ and $\tilde{\sigma} \in \mathbb{Z}^n$

**Output:** $P \in K[x]_{m \times m}$ a $(\sigma, \tilde{\sigma})$-order basis of $F$ and

$\vec{u} \in \mathbb{Z}^n$ the shifted $\tilde{\sigma}$-row degree of $P$.

To simplify the presentation, let us assume w.l.o.g. that:

1. the procedure Basis$(F, \tilde{\sigma})$ handles the $(1, \tilde{\sigma})$-order basis case
2. $n = \mathcal{O}(m)$ and the shift $\tilde{\sigma}$ is balanced, as in [2]

#### M-Basis

**Naive algorithm, iterative on the order $\sigma$, which costs $O(m^\sigma n^2)$ op. in $\mathbb{K}$:**

- Quadratic complexity in the precision $\sigma$
- Not convenient at any intermediate step
- Minimal knowledge on $F$, only coefficients $F_0, \ldots, F_k$ at step $k$

**Algorithm 1: M-Basis($F, \sigma$)**

```plaintext
1. $P_0, \vec{u} := \text{Basis}(F \mod x, \vec{u})$
2. for $k = 1$ to $\sigma - 1$
3. $P_k' := x^\sigma - P \mod x^{k+1}$
4. $P_k, \vec{u} := \text{Basis}(F', \vec{u})$
5. $P := P_k' \cdot P$
6. return $P, \vec{u}$
```

#### PM-Basis

**Recursive variant using a divide and conquer strategy on the order $\sigma$ which costs $O(m^\sigma M(\sigma) \log (\sigma)) = O(m^\sigma \log (\sigma))$ operations in $\mathbb{K}$:**

- Quasi-linear complexity in the precision $\sigma$
- Not convenient for early termination
- Often requires to know coefficients of $F$ in advance

**Algorithm 2: PM-Basis($F, \sigma$)**

```plaintext
1. if $\sigma = 1$
2. return Basis($F \mod x, \vec{u}$)
3. else
4. $P_1, \vec{u} := \text{PM-Basis}(F, \sigma/2, \vec{u})$
5. $P_2' := (x^{\sigma/2} P_1 \cdot F) \mod x^{\sigma/2}$
6. $P_2, \vec{u} := \text{PM-Basis}(F', \sigma/2, \vec{u})$
7. return $P_1 + P_2$
```

### Our contribution

1. Give an algorithm for order basis with the following properties:
   - Quasi-optimality: it takes a quasi-linear time in the precision $\sigma$
   - Early termination: easy to stop at any intermediate step
   - Relaxed algorithm: minimal knowledge on the input $F$ at each step.
2. Use 1 to improve the complexity of block Wiedemann approach.

### Fast iterative algorithm

**Iterative-PM-Basis**

Iterative version of PM-Basis that regroups computations step by step

- Quasi-linear complexity in the precision $\sigma$
- Convenient for early termination
- Often requires to know coefficients of $F$ in advance

**Algorithm 3: Iterative-PM-Basis($F, \sigma$)**

```plaintext
1. $P_0, \vec{u} := \text{Basis}(F \mod x, \vec{u})$
2. $P := [P_0 \text{ and } S = [0, \ldots, 0, F] \text{ with } \log_2(\sigma)]$ zeros
3. for $k = 1$ to $\sigma - 1$
4. $t := \nu_2(k)$ and $t' := \left\lceil \log_2(\sigma) \right\rceil$ if $k = 2^t$
5. $\nu(k - 2^t)$ otherwise
6. Merge first $k + 1$ elements of $P$ by multiplication
7. $S[t + 1] := (x^2 F[1] \cdot S[t + 1] \mod x^2)$ middle product step 7
8. $P_k, \vec{u} := \text{Basis}((S[t + 1] \mod x, \vec{u})$
9. Insert $P_0$ at the beginning of $P$
10. return $P, \vec{u}$
```

### Relaxed middle product

**Two methods for a relaxed middle product algorithm:**

1. Compute a full $2n \times n$ product using a relaxed multiplication algorithm on polynomial of matrices ([5])
2. Compute just the middle product as in Figure 1 to gain asymptotically a factor 2 compared to method 1.

**Relaxed-PM-Basis**

Using this relaxed middle product within Iterative-PM-Basis, we obtain a new order basis algorithm relaxed w.r.t. $F$, which costs $O(k M(\sigma) \log(\sigma))$

- Quasi-linear complexity in the precision $\sigma$ (with an extra $\log_2(\sigma)$)
- Convenient for early termination
- Requires minimal knowledge on $F$

### Application to block Wiedemann algorithm

Let $A \in GL_n(K)$ with $O(N)$ non-zero elements and $S = \sum_{i=0}^{N-1} U A V x^i$ for random $U, V \in K^{n \times n}$. The block Wiedemann approach uses a $(\sigma, \tilde{\sigma})$-order basis of $F = [S^t | I_n] \in K[x]_{m \times m}$ to solve sparse linear systems $A y = b$.

**Current approach:**

Computing $S$ at precision $\sigma$ costs $O(m^{\sigma} \cdot N \cdot \sigma)$ operations in $\mathbb{K}$, which is dominant since $n \ll N$. An a priori bound $\sigma$ on the order $\sigma$ is hard to find or may be loose. To circumvent this the paper [6] proposes a stopping criteria which has to be integrated into an iterative algorithm.

**Benefits of our approach:**

- Iterative-PM-Basis provides the first iterative algorithm with quasi-linear time complexity that can use stopping criteria from [6].
- Relaxed-PM-Basis improves the complexity of 1 on average by a constant factor because less coefficients of $S$ need to be computed.

### References


