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

**Definition of basis**: $P \in K[x]^{m \times n}$ is a (left) $(\sigma, \delta)$-order basis of $F$ if the rows of $P$ form a $\delta$-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**: $F \in K[x]^{m \times n}$, $\sigma \in \mathbb{N}$ and $\delta \in \mathbb{Z}^n$

**Output**: $P \in K[x]^{m \times n}$ a $(\sigma, \delta)$-order basis of $F$ and $\bar{u} \in \mathbb{Z}^n$ the shifted $\delta$-row degree of $P$.

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

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

### M-Basis

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

- Quadratic complexity in the precision $\sigma$
- Easy to stop at any intermediate step
- Minimal knowledge on $F$, only coefficients $F_0 \ldots F_k$ at step $k$

**Algorithm 1: M-Basis**

1: $P, \bar{u} \leftarrow$ Basis$(F \bmod x, \delta)$
2: for $k = 1$ to $\sigma - 1$
3: \hspace{2em} $P' \leftarrow x^\sigma P \prod x^\delta + 1$
4: \hspace{2em} $P_k, \bar{u} \leftarrow$ Basis$(P', \bar{u})$
5: \hspace{2em} $P \leftarrow P_k P$
6: return $P, \bar{u}$

### PM-Basis

**Recursive variant using a divide and conquer strategy on the order $\sigma$ which costs $O(m^{2}\log(\sigma)) + O(m\sigma^2)$ operations in $K$.**

- 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**

1: if $\sigma = 1$
2: return Basis$(F \bmod x, \delta)$
3: else
4: \hspace{2em} $P_1, \bar{u}_1 \leftarrow$ PM-Basis$(F, \sigma/2, \delta)$
5: \hspace{2em} $P' \leftarrow x^{\sigma/2} P_1 F \bmod x^{\sigma/2}$
6: \hspace{2em} $P_2, \bar{u}_2 \leftarrow$ PM-Basis$(F', \sigma/2, \bar{u}_1)$
7: return $P_2 P_1 P_2$

### Relaxed middle product

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

- Compute a full $2n \times n$ product as in [1].
- Use relaxed multiplication algorithm on polynomial of matrices ([5])

**Application to block Wiedemann algorithm**

Let $A \in \text{GL}_n(K)$ with $O(N)$ non-zero elements and $S = \sum_{k=0}^{\nu} V_k W_k$ for random $U, V, W \in K^{n \times n}$.

The block Wiedemann approach uses a $(\sigma, \delta)$-order basis of $F = [S^T] [I_N] \in K[x]^{m \times n}$ to solve sparse linear systems $Ay = b$.

**Current approach**: Computing $S$ at precision $\sigma$ costs $O(n^{2+\epsilon}N)$ operations in $K$, which is dominant since $\sigma \ll N$.

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**


