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, $F = \sum_{i=0}^{n} F_i x^i \in K[x]^{m \times n}$ 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 $vF \equiv 0 \mod x^\sigma$.

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

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

To simplify the presentation, let us assume w.l.o.g. that:
- the procedure Basis($F, \bar{u}$) handles the $(1, \beta)$-order basis case
- $n = O(m)$ and the shift $\beta$ is balanced, as in [2]

**M-Basis**

**Naive algorithm,** iterative on the order $\sigma$, which costs $O(m^2 \sigma^2)$ 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($F, \sigma, \beta$)**

```plaintext
1: $P, \bar{u} := \text{Basis}(F \mod x, \bar{u})$
2: for $k = 1$ to $\sigma - 1$ do
3: \hspace{1em} $P' := \sigma \cdot P \mod x^\beta$
4: \hspace{1em} $P_{\beta} := \text{Basis}(P', \bar{u})$
5: \hspace{1em} $P := P_{\beta} \cdot P$
6: return $P, \bar{u}$
```

**PM-Basis**

**Recursive variant using a divide and conquer strategy on the order $\sigma$ which costs** $O(m^2 M(\sigma) \log(\sigma)) = O(m^2 \sigma^2)$ 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($F, \sigma, \beta$)**

```plaintext
1: if $\sigma = 1$ then
2: return Basis($F \mod x, \bar{u}$)
3: else
4: $P_{\beta}, \bar{u} := \text{PM-Basis}(F, \sigma/2, \beta)$
5: $P' := (x^{\sigma/2} P_{\beta} \cdot F) \mod x^{\beta/2}$
6: $P_{\beta}, \bar{u} := \text{PM-Basis}(F', \sigma/2, \bar{u})$
7: return $P_{\beta}, P_{\beta}$
```

**Our contribution**

- 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.
- 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($F, \sigma, \bar{u}$)**

```plaintext
1: $P_{0}, \bar{u} := \text{Basis}(F \mod x, \bar{u})$
2: $P = [P_{0}]$ and $S = [0, \ldots, 0, F]$ with $|\log_{2}(\sigma)|$ zeros
3: for $k = 1$ to $\sigma - 1$ do
4: \hspace{1em} $t = 2 \cdot (k \mod 2)$
5: \hspace{1em} $t' = 2 \cdot (k \mod 2)$
6: \hspace{1em} $t'', t''' \in \mathbb{N}$
7: \hspace{1em} Merge first $t'' + 1$ elements of $P$ by multiplication product tree step 7
8: \hspace{1em} $S(k + 1) := (x^{-2} P[1] \cdot S(k + 1)) \mod x^{2}$ \hspace{1em} middle product step 5
9: \hspace{1em} $P_{k}, \bar{u} := \text{Basis}(S(k + 1) \mod x, \bar{u})$
10: return $P_{\beta}$
```

**Relaxing the order basis algorithm**

**Problem:** At step $k = 2^i$, Iterative-PM-Basis requires $S[|\log_{2}(\sigma)|] + 1 \mod x^{2^{i+1}}$, that is $F \mod x^{2^{i+1}}$, to perform the middle product of step 6. However, we only need the middle product modulo $x$ at step $k$, and therefore $F \mod x^{2^{i+2}}$. The other coefficients of the middle product will be used in the next steps.

**Solution:**
- Compute the middle products gradually with the additional constraint of not using any coefficient of the input before necessary, i.e. using a relaxed algorithm.

**Definition of relaxed (or on-line) algorithm**

When computing the coefficient in $x^i$ of the output, a relaxed algorithm can read at most the coefficients in $1, \ldots, x^{i}$ of the input.

**References**