The Popov Forms of Ore Matrices

Mark Giesbrecht **George Labahn** **Yang Zhang**
Symbolic Computation Group
University of Waterloo

May 18, 2002

Definition. Let $D[x;\sigma,\delta]$ be an Ore domain. An $m \times m$ non-singular Ore matrix $T(x) \in D[x;\sigma,\delta]^{m\times m}$ is in *Popov form* (with column degree $\vec{\alpha}$) if there exists a multi-index $\vec{\alpha}$ such that $T(x)$ satisfies the degree constraints

$$T(x)\cdot x^{-\vec{\alpha}} = T' + O(x^{-1})_{x\to\infty}, \quad T' \in D^{m\times m} \text{ is upper triangular.} \tag{1}$$

$$x^{-\vec{\alpha}}\cdot T(x) = I_m + O(x^{-1})_{x\to\infty}. \tag{2}$$

- Popov forms of polynomial matrices can be found in Kailath [3] with many applications to linear system theory.
- Advantages: The degrees of entries don't increase. Hermite forms and Smith forms don't have this property.

- **Example:** Let $M(x) \in \mathbb{Q}(t)[x;\sigma,\delta]^{m\times m}$, and

$$M(x) = \begin{bmatrix} x^2+1 & tx^2+x+1 & x-1 \\ x+1 & x^3+2x-1 & x+1 \\ x+1 & x-2 & x^4 \end{bmatrix}$$

Then we can write

$$M(x) = \begin{bmatrix} x^2 & 0 & 0 \\ 0 & x^3 & 0 \\ 0 & 0 & x^4 \end{bmatrix} + \begin{bmatrix} 1 & tx^2+x+1 & x-1 \\ x+1 & 2x-1 & x+1 \\ x+1 & x-2 & 0 \end{bmatrix}$$

and

$$M(x) = \begin{bmatrix} 1 & t & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} x^2 & 0 & 0 \\ 0 & x^3 & 0 \\ 0 & 0 & x^4 \end{bmatrix} + \begin{bmatrix} 1 & x+1 & x-1 \\ x+1 & 2x-1 & x+1 \\ x+1 & x-2 & 0 \end{bmatrix}$$

Popov forms of matrices over valuation rings

Popov forms of polynomial matrices and Ore matrices can be obtained as special cases of valuation Popov forms.

Definition. An *ordered group* Γ is a group with a total ordering $\geq$, which is preserved by the group operation:

$$\alpha \geq \beta, \alpha' \geq \beta' \;\Rightarrow\; \alpha + \alpha' \geq \beta + \beta' \quad \text{for all } \alpha, \alpha', \beta, \beta' \in \Gamma.$$

Usually, Γ will be augmented by a symbol ∞ to form a monoid with the operation

$$\alpha + \infty = \infty + \alpha = \infty + \infty = \infty \qquad \text{for all } \alpha \in \Gamma,$$

and the ordering $\infty > \alpha$ for all Γ.

Definition. Let R be a ring. By a *valuation* on R with values in an ordered group Γ, the *value group*, we mean a function v on R with values in $\Gamma \cup \{\infty\}$ subject to the conditions:

(V.1) $v(a) \in \Gamma \cup \{\infty\}$ and v assumes at least two values,

(V.2) $v(ab) = v(a) + v(b)$, and

(V.3) $v(a+b) \geq min\{v(a), v(b)\}$, for every pair of elements $a, b \in R$.

Example: Let D be a skew field with valuation v and an automorphism σ of D such that $v(a^\sigma) = v(a)$ for all $a \in D$. Now select an element μ in the value group Γ (or in an ordered extensions of Γ) and define a valuation on he skew polynomial $D[x;\sigma]$ by the rule

$$w(\sum a_i x^i) = min_i\{i\mu + v(a_i)\}.$$

and then w can be uniquely extended to the functional field $D(x;\sigma)$. If the residue-class skew field of D under v is k and the automorphism induced on k by σ is $\overline{\sigma}$, then the residue-class field of $D(x;\sigma)$ is $k(x;\sigma^{-i})$ if $i\mu$ is the least multiple of μ which

lies in Γ, and k if no multiple of μ lies in Γ.

Definition. Given an Ore domain D with quotient ring Q and valuation v. For $a, b \in D$, we say that $v(b)$ *divides* $v(a)$ with respect to v, denoted $v(b)|_v v(a)$, if there exists $d \in D$ such that $v(a) = v(db)$. d is called an *valuation quotient* of a by b with respect to v if $a = db$, or if $a \neq db$ and $v(a - db) < v(a)$.

Lemma. $v(b)|_v v(a)$ if and only if there exists an valuation quotient c of a by b.

Definition. Let $A \in D^{n \times m}$. For $1 \leq i \leq n$, the *ith pivot index* $piv(i)$ *of* A is defined as:

1. $piv(i) = 0$, if $a_{i,j} = 0$, for any $1 \leq j \leq m$.
2. $v(a_{i,j}) \leq v(a_{i,piv(i)})$ for $1 \leq j \leq piv(i)$.
3. $v(a_{i,j}) \leq v(a_{i,piv(i)})$ for $piv(i) \leq j \leq m$.

That is, a pivot element is the rightmost element with maximum value in value group Γ in its row.

Definition. The *pivot support set of* A is defined as $PivS(A) = \{1 \leq i \leq n | piv(i) \neq 0\}$.
$A \in D^{n\times m}$ is said to be in *weak popov form* if its pivot support set are all different.

• Define the row transformation:
Let $i \in PivS(A)$. For $1 \leq j \leq n$, if $v(a_{j,piv(i)})|_v v(a_{i,piv(i)})$, then there exists $s \in D$ such that $a_{i,piv(i)} = sa_{j,piv(i)}$ or $v(a_{i,piv(i)} - sa_{j,piv(i)}) < v(a_{j,piv(i)})$. Then we reduce $(j, piv(i))$-entry to zero or to small values by subtracting s times row i from row j the *simple transformation* of row i on row j. If $piv(i) = piv(j)$, the transformation is called of the *first kind*, otherwise it is called of the *second kind*.

Algorithm: `WeakPopovForm(Valuation form)`

Input: ▸ $A \in D^{n\times m}$;

Output: ▸ $P \in D^{n\times m}$ in weak Popov form with respect to a valuation v, obtained by applying first kind simple transformation on A;

While A is not in weak Popov form do

Apply a first kind simple transformation on A;

End do

- If $v(D)$ is well-ordered, the algorithm will termite.

Definition. A is said to be in *ascending order* if for $1 \leq i < j \leq n$, we have $v(a_{i,piv(i)}) < v(a_{j,piv(j)})$ or $v(a_{i,piv(i)}) = v(a_{j,piv(j)})$ but $piv(i) < piv(j)$, for any nonzero entries.

Definition. $A \in D^{n\times m}$ is said to be in *Popov form* with respect to the valuation v if

1. A is in weak popov form;
2. A is in ascending order with respect values;
3. $v(a_{i,piv(j)}) < v(a_{j,piv(j)})$ for $i \neq j$ and $j \in \mathrm{PivS}(A)$.

Algorithm: `PopovForm for the matrix over valuation domains`

Input: ▸ $A \in D^{n\times m}$; D: valuation domain wrt v.

Output: ▸ P in Popov form, left equivalent to A.

W := WeakPopovForm(A);

Permute rows of W s.t. W is in ascending order wrt v;

For k to n do

  if kth row is not the zero row then

    Let $\delta := max_{i<k, i\in PicS(W)}\{v(a_{k,piv(i,W)}) - v(w_{i,piv(i,W)})\}$;

    if $\delta < \infty$ then break;

    Let $l < k, l \in PivS(W)$ such that

$$v(a_{k,piv(l,W)}) - v(w_{l,piv(l,W)}) = \delta;$$

    Apply simple transformation of row l on row k;

  End if;

End do;

return $P := copy(W)$

- Corollary: (weak) Popov forms of polynomial matrices (Mulders and Storjohann [4]) and Ore matrices can be obtained by using degree valuations.
- Notice that different valuations induce different Popov forms.

References

[1] B. Beckermann, G. Labahn and G. Villard, Shifted Normal Forms of Polynomial Matrices, *Proceedings of ISSAC'99*, Vancouver, ACM Press, (1999) 189-196.

[2] B. Beckermann and G. Labahn, Fraction-free Computation of Matrix Rational Interpolants and Matrix GCD's. To appear in *SIAM J. Matrix Analysis and Applications*.

[3] T. Kailath, *Linear Systems*, Prentice Hall, 1980.

[4] T. Mulders and A. Storjohann, *On lattice reduction for polynomial matrices*, to appear in J. Sym. Computation.

[5] J. von zur Gathen, *Hensel and Newton methods in valuation rings*, Mathematics of Computation, vol.42(1984), 637-661.