Matrix Berlekamp-Massey

November 3, 2017

1 Definitions

First thing: what are linearly recurrent sequences and minimal generators, when talking about matrix sequences? The definition is essentially the same as in the scalar case. There is a similar notion of generator of a sequence (which is a matrix): it is related to the denominator in some minimal fraction description of the generating series of the sequence.

We consider the following definition which extends the scalar case. It can be found in [2, Sec. 3], and in [6, Def. 4.2].

Definition 1.1. *Let* $\mathcal{S} = (S_k)_{k\in\mathbb{Z}_{\geqslant 0}} \subset \mathbb{K}^{m\times n}$. *A vector* $\mathbf{p} = \sum_{0\leqslant k\leqslant d} p_k X^k \in \mathbb{K}[X]^{1\times m}$ *of degree at most* d *is said to be a* (linear recurrence) relation for $\mathcal{S}$ *if* $\sum_{k=0}^{d} p_k S_{\delta+k} = 0$ *for all* $\delta \geqslant 0$. *Then,* $\mathcal{S}$ *is said to be linearly recurrent if there exists a nontrivial relation for* $\mathcal{S}$.

The set of relations for $\mathcal{S}$ is a $\mathbb{K}[X]$-submodule of $\mathbb{K}[X]^{1\times m}$, which has rank m if $\mathcal{S}$ is linearly recurrent. This is showed in [3, Fact 1] but only for sequences having a *scalar* recurrence relation. Let us now link this with the property of being linearly recurrent as in the above definition.

Lemma 1.2. *The sequence* $\mathcal{S}$ *is linearly recurrent if and only if there exists a polynomial* $P(X) = \sum_{0\leqslant k\leqslant d} p_k X^k \in \mathbb{K}[X]$ *such that* $\sum_{k=0}^{d} p_k S_{\delta+k} = 0$ *for all* $\delta \geqslant 0$.

Proof. I cannot find this result in the literature..! (but we don't care since in our case the sequence is obviously cancelled by a polynomial) □

Then, the fact that the relation module has rank m is straightforward: since the sequence is linearly recurrent, it has a scalar recurrence polynomial $P(X)$, hence for each i the vector $[0 \cdots 0\ P(X)\ 0 \cdots 0]$ with $P(X)$ at position i is a relation for $\mathcal{S}$.

A *generating matrix*, or *generator*, for the sequence is a matrix whose rows form a generating set for the module of relations; it is said to be

- *minimal* if the matrix is reduced [7, 1];
- *ordered weak Popov* if the matrix is in weak Popov form [4] with pivots on the diagonal;
- *canonical* if the matrix is in Popov form [5, 1].

In this context, an important quantity related to the sequence is the determinantal degree $\deg(\det(\mathbf{P}))$, invariant for all generators $\mathbf{P} \in \mathbb{K}[X]^{m\times m}$. Hereafter, we denote it by $\Delta(\mathcal{S})$.

Lemma 1.3. *Consider $\mathcal{S} = (S_k)_{k\in\mathbb{Z}_{\geqslant 0}} \subset \mathbb{K}^{m\times n}$ and its generating series $\mathbf{S} = \sum_{k\geqslant 0} S_k/X^{k+1} \in \mathbb{K}[\![X^{-1}]\!]^{m\times n}$.*

- *A vector $\mathbf{p} \in \mathbb{K}[X]^{1\times m}$ is a relation for $\mathcal{S}$ if and only if the entries of $\mathbf{q} = \mathbf{pS}$ are in $\mathbb{K}[X]$. Then, $\deg(\mathbf{q}) < \deg(\mathbf{p})$.*
- *A matrix $\mathbf{P} \in \mathbb{K}[X]^{m\times m}$ is a generator for $\mathcal{S}$ if and only if $\deg(\det(\mathbf{P})) = \Delta(\mathcal{S})$ and the entries of $\mathbf{Q} = \mathbf{PS}$ are in $\mathbb{K}[X]$. Then, $\operatorname{rdeg}(\mathbf{Q}) < \operatorname{rdeg}(\mathbf{P})$ componentwise.*

Proof. Let $\mathbf{p} = \sum_{0\leqslant k\leqslant d} p_k X^k$. For $\delta \geqslant 0$, the coefficient of $\mathbf{q}$ of degree $-\delta - 1 < 0$ is $\sum_{0\leqslant k\leqslant d} p_k S_{k+\delta}$. Hence the equivalence, by definition of a relation. The degree comparison is clear since $\mathbf{S}$ has only terms of (strictly) negative degree.

Concerning the second item, thanks to the first item applied to each row of $\mathbf{P}$, it is enough to assume that all the rows of $\mathbf{P}$ are relations for $\mathcal{S}$, and to prove that $\mathbf{P}$ is a generator if and only if $\deg(\det(\mathbf{P})) = \Delta(\mathcal{S})$. Our assumption implies that $\mathbf{P}$ is a left multiple $\mathbf{P} = \mathbf{UG}$ for some matrix $\mathbf{U}$ and some generator $\mathbf{G}$. Obviously if $\mathbf{P}$ is a generator then $\deg(\det(\mathbf{P})) = \Delta(\mathcal{S})$. Conversely, if $\deg(\det(\mathbf{P})) = \Delta(\mathcal{S})$ then $\mathbf{U}$ is unimodular. □

2 Computing a minimal matrix generators

We consider the following problem.

Problem 1 – *Minimal generator*

Input:

- sequence $\mathcal{S} = (S_k)_k \subset \mathbb{K}^{m\times n}$,
- degree bound $d \in \mathbb{Z}_{\geqslant 0}$.

Assumptions:

- the sequence $\mathcal{S}$ is linearly recurrent,
- the canonical generating matrix of $\mathcal{S}$ has degree at most $d \in \mathbb{Z}_{\geqslant 0}$.

Output: a minimal generating matrix for $\mathcal{S}$.

References

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

[2] E. Kaltofen and G. Villard. On the complexity of computing determinants. In *ISSAC'01*, pages 13–27. ACM, 2001.

[3] Erich Kaltofen and George Yuhasz. On the matrix Berlekamp-Massey algorithm. *ACM Trans. Algorithms*, 9(4):33:1–33:24, October 2013.

[4] T. Mulders and A. Storjohann. On lattice reduction for polynomial matrices. *J. Symbolic Comput.*, 35:377–401, 2003.

[5] V. M. Popov. Invariant description of linear, time-invariant controllable systems. *SIAM Journal on Control*, 10(2):252–264, 1972.

[6] W. J. Turner. *Black box linear algebra with the LINBOX library.* PhD thesis, North Carolina State University, 2002.

[7] W. A. Wolovich. *Linear Multivariable Systems*, volume 11 of *Applied Mathematical Sciences*. Springer-Verlag New-York, 1974.