Matrix Berlekamp-Massey

November 4, 2017

1 Linearly recurrent matrix sequences

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 obviously admits a scalar relation) □

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 a matrix sequence $\mathcal{S} = (S_k)_{k\in\mathbb{Z}_{\geqslant 0}} \subset \mathbb{K}^{m\times n}$ and its generating series $\mathbf{S} = \sum_{k\geqslant 0} S_k/X^{k+1} \in \mathbb{K}[\![X^{-1}]\!]^{m\times n}$. Then, 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 $\mathbb{K}[X]$; furthermore, in this case, $\deg(\mathbf{q}) < \deg(\mathbf{p})$.*

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. □

Corollary 1.4. *A matrix sequence $\mathcal{S} = (S_k)_{k\in\mathbb{Z}_{\geqslant 0}} \subset \mathbb{K}^{m\times n}$ is linearly recurrent if and only if its generating series $\mathbf{S} = \sum_{k\geqslant 0} S_k/X^{k+1} \in \mathbb{K}[\![X^{-1}]\!]^{m\times n}$ can be written as a matrix fraction $\mathbf{S} = \mathbf{P}^{-1}\mathbf{Q}$ where $\mathbf{P} \in \mathbb{K}[X]^{m\times m}$ is nonsingular and $\mathbf{Q} \in \mathbb{K}[X]^{m\times n}$. In this case,*

- *we have* $\mathrm{rdeg}(\mathbf{Q}) < \mathrm{rdeg}(\mathbf{P})$ *and* $\deg(\det(\mathbf{P})) \geqslant \Delta(\mathcal{S})$,
- $\mathbf{P}$ *is a matrix generator of* $\mathcal{S}$ *if and only if the fraction is irreducible (i.e.* $\mathbf{UP}+\mathbf{VQ} = \mathbf{I}$ *for some* $\mathbf{U}$, $\mathbf{V}$*),*
- $\mathbf{P}$ *is a matrix generator of* $\mathcal{S}$ *if and only if* $\deg(\det(\mathbf{P})) = \Delta(\mathcal{S})$.

2 Computing minimal matrix generators

Now, we focus on the following algorithmic problem: we are given a linearly recurrent sequence and we want to find a matrix generator. If we want our algorithm to run efficiently (or simply, in finite time), we cannot access infinitely many terms of the sequence. We therefore ask for an additional input, which one often has when considering a sequence coming from some application: a (finite) bound on the degree of a minimal generating matrix. Note that a bound on the determinantal degree $\Delta(\mathcal{S})$ is sufficient since any minimal generating matrix will have degree less than this; yet better bounds can be available and will imply better efficiency.

In short, 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,
- any minimal matrix generator of $\mathcal{S}$ has degree at most d.

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

We now show how the additional information of d allows us to find a matrix generator by considering only a small chunk of the sequence, rather than all its terms.

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.