Matrix Berlekamp-Massey

July 8, 2017

1 Definition of recurrence relations

First issue: which definition to use for matrix generator? There is one in [1], and a different one in [2]; both are related as follows.

Definition 1 ([2]). *Let $\mathcal{S} = (S_k)_{k\in\mathbb{Z}_{\geqslant 0}} \subset \mathbb{K}^{m\times n}$ be a sequence of $m \times n$ matrices over $\mathbb{K}$. We define the power series matrix $\mathbf{S} = \sum_{k\geqslant 0} S_k X^k \in \mathbb{K}[\![X]\!]^{m\times n}$. Then, a vector $\mathbf{p} \in \mathbb{K}[X]^{n\times 1}$ is said to be a* (linear recurrence) relation for $\mathcal{S}$ *if the product* $\mathbf{Sp}$ *has polynomial entries, that is,* $\mathbf{Sp} \in \mathbb{K}[X]^{n\times 1}$.

For some reason (which is unclear to me), in [2] the word "generator" is used for such relations. Here we will reserve this word for sets of vectors that indeed generate the set of all relations.

Assume there exists a nonzero relation for $\mathcal{S}$, and let $\mathbf{p}$ be such a relation. Writing $\mathbf{p} = \sum_k p_k X^k$ for matrices $p_k \in \mathbb{K}^{n\times 1}$, then we have

$$\sum_{k=0}^{d} S_{\delta-k} p_k = 0 \quad \text{for all } d \geqslant \deg(\mathbf{p}) \text{ and } \delta \geqslant \max(d, \deg(\mathbf{Sp}) + 1). \tag{1}$$

One may have in mind that $\deg(\mathbf{Sp}) < \deg(\mathbf{p})$ since this typically holds for the output of existing algorithms; in general, this does not necessary hold. For example, if $\mathcal{S}$ has only finitely many nonzero terms, and thus $\mathbf{S}$ already has polynomial entries, any coordinate vector is a relation $\mathbf{p}$ such that $\mathbf{Sp}$ has degree larger than $\deg(\mathbf{p})$.

Definition 2 ([1]). *Let $\mathcal{S} = (S_k)_{k\in\mathbb{Z}_{\geqslant 0}} \subset \mathbb{K}^{m\times n}$ be a sequence of $m \times n$ matrices over $\mathbb{K}$. We define the power series matrix $\mathbf{S} = \sum_{k\geqslant 0} S_k X^k \in \mathbb{K}[\![X]\!]^{m\times n}$. Then, a vector $\mathbf{p} \in \mathbb{K}[X]^{n\times 1}$ of degree at most d is said to be a* (linear recurrence) relation for $\mathcal{S}$ *if*

$$\sum_{k=0}^{d} S_{\delta+k} p_k = 0 \quad \textit{for all } \delta \geqslant 0.$$

where $(p_k)_k$ are the matrices in $\mathbb{K}^{n\times 1}$ such that $\mathbf{p} = \sum_{0\leqslant k\leqslant d} p_k X^k$.

Lemma 3. *For a given sequence $\mathcal{S} \subset \mathbb{K}^{m\times n}$, a nonzero vector $\mathbf{p} \in \mathbb{K}[X]^{n\times 1}$ is a relation for Definition 1 if and only if there exists $d \geqslant \deg(\mathbf{p})$ such that the reverse $X^d\mathbf{p}(X^{-1})$ is a relation for Definition 2.*

Proof. First, we assume that $X^d\mathbf{p}(X^{-1}) = \sum_{k=0}^{d} p_{d-k}X^k$ is a relation for Definition 2, for some integer $d \geqslant \deg(\mathbf{p})$. This means that, for all $\delta \geqslant 0$, we have $0 = \sum_{k=0}^{d} S_{\delta+k}p_{d-k} = \sum_{k=0}^{d} S_{\delta+d-k}p_k$. This implies that $\mathbf{Sp}$ has polynomial entries (and $\deg(\mathbf{Sp}) \leqslant d$).

Now, we assume that $\mathbf{p}$ is a relation for Definition 1. Taking $d = \max(\deg(\mathbf{p}), \deg(\mathbf{Sp})+1)$ in Eq. (1), we obtain $\sum_{k=0}^{d} S_{\delta-k}p_k = 0$ for all $\delta \geqslant d$. This implies $\sum_{k=0}^{d} S_{\delta-d+k}p_{d-k} = 0$ for all $\delta \geqslant d$, or equivalently, $\sum_{k=0}^{d} S_{\delta+k}p_{d-k} = 0$ for all $\delta \geqslant 0$. Therefore the reverse $X^d\mathbf{p}(X^{-1})$ is a relation for Definition 2. □

References

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

[2] E. Thomé. Subquadratic computation of vector generating polynomials and improvement of the block Wiedemann algorithm. *J. Symbolic Comput.*, 33(5):757–775, 2002.