

An application of the Rational Canonical Form

Steve Cheng

February 10, 2006

Copyright matters

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, with no Front-Cover Texts, and with no Back-Cover Texts.

The problem

Ever thought the rational canonical form that you studied in linear algebra was useless? Well, here is an application of it to something practical, that I stumbled upon when answering a question on the PlanetMath forums.

Let V be the vector space \mathbb{Z}_2^m , where \mathbb{Z}_2 denotes the field consisting of the elements 0 and 1. Given coefficients $a_1, \dots, a_m \in \mathbb{Z}_2$, we form the companion matrix

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & \vdots \\ & & & \ddots & \ddots & 0 \\ a_1 & a_2 & a_3 & \dots & \dots & a_m \end{bmatrix}$$

We can generate successive vectors $x_n \in V$ by the recurrence

$$x_{n+1} = Ax_n.$$

This procedure is one of the basic ones used for the generation of pseudo-random numbers on computers. In this application, we regard the vectors x_n as binary numbers with m bits, and the internal state of the pseudo-random generator x_n always moves to the next state x_{n+1} by applying the transformation A .

We consider an important question: what is the largest period of the pseudo-random generator A ?

In other words, we are to find the largest positive integer p such that p is the period for some vector $x \in V$. The period of a vector $y \in V$ is the smallest positive integer q such that $A^q y = y$ but $A^r y \neq y$ for $1 < r < q$.

Solution

Assume A is invertible. This means A is a permutation of the vectors in V , and hence ensures that every element $y \in V$ has a period $\leq 2^m$. (If A is not invertible, some vectors may have an infinite period.)

Suppose that the *minimal polynomial* of the matrix A is

$$g(t) = \phi_1(t)^{m_1} \phi_2(t)^{m_2} \dots \phi_k(t)^{m_k},$$

where m_j are positive integers, and $\phi_j(t)$ are distinct monic irreducible polynomial factors. To each ϕ_j there corresponds a vector space

$$N_j = \{y \in V : \phi_j(A)^q y = 0 \text{ for some } q \in \mathbb{N}\}.$$

Moreover, $N_1 \oplus N_2 \oplus \dots \oplus N_k = V$. Each N_j has a basis formed by taking the union of some cyclic bases. The combined basis for V from all N_j , is of course, the *rational canonical basis*.

Suppose that rational canonical basis for (A restricted to) N_j consists of the A -cycles:

$$\begin{array}{ccccccc} v_{j,1}, & A v_{j,1}, & \dots, & A^{s_{j,1}-1} v_{j,1}, \\ v_{j,2}, & A v_{j,2}, & \dots, & A^{s_{j,2}-1} v_{j,2}, \\ & & \dots, & \\ v_{j,s_j}, & A v_{j,s_j}, & \dots, & A^{s_{j,s_j}-1} v_{j,s_j}. \end{array}$$

Let $p_{j,i}$ be the period of $v_{j,i}$, and p be the least common multiple of all the $p_{j,i}$. Then $A^p y = y$ for all $y \in V$. This follows since y can be written as a linear combination of the $A^r v_{j,i}$ for $1 \leq r \leq s_{j,i}$, $1 \leq i \leq s_j$, $1 \leq j \leq k$, and each $A^r v_{j,i}$ has period $p_{j,i}$, which divides p .

In fact, there exists an element $x \in V$ that has period exactly equal to p . For instance,

$$x = \sum_{j,i} v_{j,i}.$$

Note that $N_{j,i} = \text{span}\{A^r v_{j,i} : 1 \leq r \leq s_{j,i}\}$ are all *disjoint* vector subspaces of V (they intersect at only the zero element). In fact, each cyclic subspace $N_{j,i}$ corresponds to a companion matrix block in the rational canonical form of A . Therefore $A^r x = x$ if and only if A^r brings every $v_{j,i}$ back to itself, and this occurs if and only if r divides each period $p_{j,i}$. So the smallest r possible for x must be the least common multiple p of all the $p_{j,i}$. Since we know $A^p y = y$ for all $y \in V$, the smallest period for x must be p .

Recall that if $h(t)$ is any polynomial such that $h(A) = 0$, then the minimal polynomial $g(t)$ must divide $h(t)$. In particular we can set $h(t) = t^p - 1$.

So we arrive at this conclusion: the maximum period p for A is the smallest positive integer p such that its minimal polynomial $g(t)$ divides $h(t) = t^p - 1$.

Moreover, since A is a companion matrix, its minimal polynomial is simply

$$g(t) = -a_1 - a_2 t - \dots - a_m t^{m-1} + t^m.$$

So we have given a complete procedure to solve this practical problem of (linear feedback) pseudo-random generators.

References

- [FIS] Stephen H. Friedberg, Arnold J. Insel, Lawrence E. Spence. *Linear Algebra*, 3rd ed. Prentice-Hall, 1997.