Lecture: 19 - 20

[Home][PDF]

Topics: Periodic sequences, Characteristic Polynomials

Periodic Sequences

Chapter 8 ,1 p.398 -399

Definition *ultimately periodic*

Let S be an arbitrary nonempty set, and let $s_0, s_1, ...$ be a asequqnce of elements of S. If there exisst integers $r > 0$ and $n_0 \geq 0$ s.t $s_{n+r} = s_n$ for all $n \geq n_0$, then the sequence is called ultimately periodic and r is vcalled a periode of the sequence. The samellest number amont all the possibel periods of an ultimately periodic sequcen is called the least perido of the sequence.

Lemma 8.4: Every period of an ultimately periodic sequence is divisible by the least period

Proof

Let r be an arbitraty period of the ultimatetly periodic sequence $s_0, s_1, ...$ and let r_1 be its least periode, so taht we have $s_{n+r} = s_n$ for all $n \geq 0$ and $s_{n+r_1} = s_n$ for all $n \geq n_1$ with suitable nonnegative integers n_0 and n_1. If r were not divisivble by r_1, we could use the division algorighm for integers to write $r = m \cdot r_1 + t$ with intergers $m \geq 1$ and $0 < t < r_1$. Then for all $n \geq \max(n_0, n_1)$ we get:

$$s_n = s_{n+r} = s_{n+mr_1+t} = s_{n+(m-1)r_1+t} = \cdots = s_{n+t}$$

and so t is a periode of the sequence, which contractids the difintion of the least period $\square$.

Theorem 8.7

Let $\mathbb{F}$ be any finite filed and k any positive integer. Then every k-th-order linear recurring sequence in $\mathbb{F}$ is ultimately periodic with least period r satisfying $r \leq q^k$ and $r \leq q^k - 1$ if the sequence is homogeneous.

Proof:

We note that there are exactly q^k distinct k-tuples of elements of $\mathbb{F}$. Therefore, by considering the state vectors $\vec{s}_j = \vec{s}_i$ for some i and j with $0 \leq i \leq j \leq q^k$. Using linear recurrence relation and induction, we arrive at $\vec{s}_{n+j-i} = \vec{s}_n$ for all $n \ geqi$ which showes that the linear roecurring sequence itself is ultimately periodic with least period $r \leq j - i \leq q^k$

In case the linera recurring sequene is homogeneous and no state vector is the zero vector ($\vec{0}$), then all subsequenct state vecctors are zero vecrtors, and so the sequence has least period $r = 1 \leq q^k - 1 \square$

Example 1 (8.8)

The first-order linear recurring sequence $s_0, s_1, \dots$ in $\mathbb{F}$, p prime, with $s_{n+1} = s_n + 1$ for $n = 0, 1, \dots$ and arbitratry $s_0 \in \mathbb{F}$ shows that the upper bound for r in Theorem 8.7 may be attaind.

If $\mathbb{F}$ is any finnite filed and g is a primitive element of $\mathbb{F}$, then the first-order homogeneous linear recurring sequence $s_0, s_1, \dots$ in $\mathbb{F}$ with $s_{n+1} = g \cdot s_n$ for $n = 0, 1, \dots$ and $s_0 \neq 0$ has period $r = q - 1$. Therefore the upper bound for r in the homogeneous case may also be attained.

We have $s_n = g^n \cdot s_0$ and then $s_{n+r} = s_n$ implies $g^{n+r} \cdot s_0 = g^n \cdot s_0$ We get $g^r = 1$ and since g is primiteve in $\mathbb{F}$ and r is the least period, then it gives $r = q - 1$.

Example 1 (8.9)

For a first-order homogeneoud linerar recurring sequcen in $\mathbb{F}$, it is easily seen taht the least period is the order og a_0 and hence divices $q - 1$. Indeed, we have $s_{n+1} = a_0 \cdot s_n$, $a_0 \in \mathbb{F}$, and with the same argument as above we see that $s_n = a_0^n \cdot s_0$ and then $s_{n+r} = s_n$ implies $a_0^{n+r} \cdot s_0 = a_0^n \cdot s_0$ giving us $g^r = 1$ which happens only if r is a multipøle of the order of a_0 which we know is a divisor og $q - 1$. Since r is the smallest number with this property then it is the order og a_0.

If $k \geq 2$, then the least periode of a k-th-order homogeneous linear recurring sequence does not necessarily divide $q^k - 1$. Consider for instance, the sequence $s_0, s_1, \dots$ in $\mathbb{F}_5$ with $s_0 = 0, s_1 = 1$ and $s_{n+2} = s_{n+1} + s_n$ for $n = 0, 1, \dots$. It can be easil verified that its least period is 20 which does not divide $5^2 - 1 = 24$.

Accordirng to Theorem 8.7, every linear recurring sequence in a finite filed is ultimately periodic. But it is not necessarliy periodic in genreal, as is illustrated by simple example of Example 8.10 in the book.

Theorem 8.11

If $s_0, s_1, \dots$ is a linear recurring sequence inf a finite filed satisfying the linear recurrence relation, and if the coefficient a_0 is nonzero, then the sequence $s_0, s_1, \dots$ is periodic.

Characteristic polynomial of a linear recurring sequence

Chapter 8, 2 , p 404-406,410

Let $s_0, s_1, \dots$ be a k-th order homogeneous linear recurring sequence in $\mathbb{F}$ satisfying the linear recurrence relation:

$$s_{n+k} = a_{k-1} \cdot s_{n+k-1} + a_{k-2} \cdot s_{n+k-2} + \dots + a_0 \cdot s_n$$

for $n = 0, 1, \dots,$ where $a_j \in \mathbb{F}$ for $0 \leq j \leq k - 1$.

The polynomial:

$$f(x) = x^k - a_{k-1} \cdot x^{k-1} - a_{k-2} \cdot x^{k-2} - \dots - a_0 \in \mathbb{F}[x]$$

is called the characteristic polynomial of the linear recurring sequence. It depends, of course, only on the linear recurrince relation. If A is the matrix, then it is easily seen that $f(x)$ is identical with the characteristics polynomial of A in the sens of linear algebra.

$$f(x) = det(xI - A)$$

with I being the $k \times k$ identity matric over $\mathbb{F}$. On the otherhand, then matrix A may be thought of as the comapion matrix of the monic polynomial $f(x)$.

Theorem 8.21

Let $s_0, s_1, \ldots$ be a k-th order homogeneous linear recurring sequence in $\mathbb{F}$ wiht characteristic polynomial $f(x)$. If the roots $\alpha_1, \ldots, \alpha_k$ of $f(x)$ are all distinct then:

$$s_n = \sum_{j=1}^{k} \beta_j \cdot \alpha_j^n \text{ for } n = 0, 1, \ldots$$

where $\beta_1, \ldots, \beta_k$ are elements that are uniquely determined by the inital values of the sequqnce and beling to the splitting field of $f(x)$ over $\mathbb{F}$

Proof in the book page 405

Example 8.22

Consider the linear recurring sequnce $s_0, s_1, \ldots$ in $\mathbb{F}_\mathbf{2}$ with $s_0 = s_1 = 1$ and $s_{n+2} = s_{n+1} + s_n$ for $n = 0, 1, \ldots$

The characteristic polynomial is $f(x) = x^2 - x - 1 \in \mathbb{F}_\mathbf{2}[x]$

If $\mathbb{F}_\mathbf{4} = \mathbb{F}_\mathbf{2}(\alpha)$, then the roots of $f(x)$ are $\alpha_1 = \alpha$ and $\alpha_2 = 1 + \alpha$.

Using inital values, we obtain $\beta_1 + \beta_2 = 1$ and $\beta_1 \alpha + \beta_2(1 + \alpha) = 1$.

Hence $\beta_1 = \alpha$ and $\beta_2 = 1 + \alpha$

By Theorem 8.21 it follows that $s_n = \alpha^{n+1} + (a + \alpha)^{n+1}$ for all $n \geq 0$.

Since $\beta^3 = 1$ for every nonzero $\beta \in \mathbb{F}_\mathbf{4}$, we deduce that $s_{n+3} = s_n$ for all $n \geq 0$ which is in accordence with the fact that the least period of the sequence is 3.

In case the characteristic polynomial is irreducible, the elements of the linear recurring sequence can be represented in terms of a suitable trace function.

Theorem 8.24

Let $s_0, s_1, \ldots$ be a k-th order homogeneous linear recurring sequence in $K = \mathbb{F}$ whose characteristic polynomial $f(x)$ is irreducible over K.

Let α be a root of $f(x)$ in the extension field $F = \mathbb{F}_\mathbb{k}$. Then there exists a uniquely determined $\theta \in F$ s.t

$$s_n = Tr_{F/K}(\theta \alpha^n)$$

for $n = 0, 1, \ldots$

Proof in the book at page 406.

A polynomial $f \in \mathbb{F}[x]$ of degree $m \geq 1$ is called a primitive polunomial over $\mathbb{F}$ if it is a monic polynomial that is irreducibel over $\mathbb{F}$ and has a root $a \in \mathbb{F}_\mathbb{m}$ that generates $\mathbb{F}_\mathbb{m}^*$

Definition 8.32 Maximal period sequence in $\mathbb{F}$

A homogeneous linera recurring sequence in $\mathbb{F}$ whose characteristic polynomial is a primitive polynomial over $\mathbb{F}$ and which has a nonzero initial state vector is called a maximal period sequcen in $\mathbb{F}$

Theorem 8.33 Period of a maximal period sequence in $\mathbb{F}$

Every k-th-order maximal period sequence in $\mathbb{F}$ is periodic and its least period is equal to the largest possible value for the least period of any kth-order homogeneous linear recurring sequence in $\mathbb{F}$ - namely $q^k - 1$.

Proof:

The fact that the sequence is periodic and that the least periodic is $q^k - 1$ is a consequence of Theorem 8.28 and 3.16. The remainin assertion f0llows from theorem 8.7. $\square$

Example

The characteristic polynomial of the sequence $s_{n+2} = s_{n+1} + s_n$ in $\mathbb{F}_\mathbf{2}$ is $f(x) = x^2 + x + 1$ which is monic and irreducible over $\mathbb{F}_\mathbf{2}$ (since neither 0 nor 1 can be a root).

Besides, $\mathbb{F}^*_{\mathbf{2}^2}$ that is f is a primitive polynomial over $\mathbb{F}_\mathbf{2}$.

Then the sequence given by $s_{n+2} = s_{n+1} + s_n$ in $\mathbb{F}_\mathbf{2}$ with initial state $s_0 = 1, s_1 = 0$ is a second-order maximal period sequence in $\mathbb{F}_\mathbf{2}$ and its period is $2^2 - 1 = 3$