On the Canonical Decomposition of Sequences Satisfying Recursions which are Powers of Irreducible Polynomials

ABSTRACT

Let \( u(t) \) be a linear recursive sequence over \( \mathbb{F}_2 \) satisfying a polynomial which is the \( r \)th power, \( f(x)^r \), of an irreducible polynomial \( f(x) \). Then there are \( r \) linear recursive sequences \( u_0(t), \ldots, u_{r-1}(t) \), each satisfying \( f(x) \), such that

\[
 u(t) = \sum_{i=0}^{r-1} \delta_i(t) \, u_i(t),
\]

where \( \delta_i(t) \) is \( \binom{t}{i} \) modulo 2.

A new derivation in terms of matrix theory offers further insight into this decomposition.
On the Canonical Decomposition of Sequences Satisfying
Recursions which are Powers of Irreducible Polynomials

J. P. Fillmore
March 1966

Let $u(t)$ be a linear recursive sequence in $F_2$, the field of two
elements, satisfying the polynomial

$$x^N - c_1 x^{N-1} - \ldots - c_N,$$

that is,

$$u(t+N) - c_1 u(t+N-1) - \ldots - c_N u(t) = 0$$

for all $t = 0, 1, 2, \ldots$. Suppose that the polynomial $x^N - c_1 x^{N-1} - \ldots - c_N$ is the power $f(x)^r$ of an irreducible polynomial $f(x)$. Then there are $r$
linear recursive sequences $u_0(t), u_1(t), \ldots, u_{r-1}(t)$, each satisfying
$f(x)$, such that

$$u(t) = \sum_{i=0}^{r-1} \delta_i(t) u_i(t)$$

where $\delta_i(t)$ is the binomial coefficient $\binom{t}{i}$ taken modulo 2. The
sequences $u_i(t)$ are unique, and $\delta_i(t) u_i(t)$ satisfies $f(x)^{i+1}$.

This decomposition appears in Blankinship [2], where it is derived
in terms of field theory, and in Benson, Fillmore, Marx [1] where it
is derived by elementary considerations. Using matrix theory, we
give a new derivation which offers further insight into this theorem.
We refer the reader to [1] for applications.
Let
\[
v(t) = \begin{pmatrix}
  u(t) \\
  u(t+1) \\
  \vdots \\
  \vdots \\
  u(t+N-1)
\end{pmatrix}.
\]

Then \( v(t+1) = A v(t) \) where \( A \) is the companion matrix

\[
A = \begin{bmatrix}
  0 & 1 & 0 & \cdots & 0 \\
  0 & 0 & 1 & \cdots & 0 \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  0 & 0 & 0 & \cdots & 1 \\
  c_N & c_{N-1} & c_{N-2} & \cdots & c_1
\end{bmatrix}.
\]

If we obtain a decomposition

\[
v(t) = \sum_{i=0}^{r-1} \delta_i(t) v_i(t),
\]

the decomposition for \( u(t) \) follows by looking at the first component of \( v(t) \).

Put \( A \) into Jordan canonical form:

\[
A = T J T^{-1}
\]
where

\[
J = \begin{pmatrix}
B_1 & & \\
& B_2 & \\
& & \ddots \\
& & & B_n \\
\end{pmatrix},
\]

\[
B_j = \begin{pmatrix}
\lambda_j & 1 & 0 & \cdots & 0 \\
0 & \lambda_j & 1 & \cdots & \vdots \\
\vdots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & 0 & \cdots & \lambda_j \\
\end{pmatrix} 
\]

and \( \lambda_1, \ldots, \lambda_n \) are the roots of \( f(x) \).

The matrix \( T \) has the form

\[
T = \begin{pmatrix}
1 & 0 & 0 & \cdots & 0 \\
\lambda_1 & 1 & 0 & \cdots & \vdots \\
\lambda_1^2 & 2\lambda_1 & 1 & \cdots & \vdots \\
\lambda_1^3 & 3\lambda_1^2 & 3\lambda_1 & \cdots & \vdots \\
\lambda_1^4 & 4\lambda_1^3 & 6\lambda_1^2 & \cdots & \vdots \\
\vdots & \cdots & \cdots & \cdots & \vdots \\
\lambda_1^{N-1} & (N-1)\lambda_1^{N-2} & \binom{N-1}{2} \lambda_1^{N-2} & \cdots & \lambda_1^{N-2}
\end{pmatrix}
\]

\( n-1 \) similar such

\( N \times r \) blocks with

\( \lambda_2, \ldots, \lambda_n \) replacing

\( \lambda_1 \).
which we write

\[ T = (K_1, K_2, \ldots, K_n) \]

with \( K_j \) an \( N \times r \) matrix whose \( \mu \nu^{th} \) entry is

\[ (\nu - 1)^{\frac{\mu - 1}{\lambda_j}} \]

See [3], Ch. VI, p. 60.

Since \( v(t+1) = A^t v(t) \), we have

\[ v(t) = A^t v(0) = T J^t T^{-1} v(0) \]

\[
\begin{pmatrix}
B_1^t \\
\cdot \\
\cdot \\
\cdot \\
B_n^t
\end{pmatrix}
\]

\[ = T 
\begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & \cdots & \cdots & \cdots & 1 \\
0 & \cdots & \cdots & \cdots & 0
\end{pmatrix} T^{-1} v(0). \]

Put \( B_j = \lambda_j E + F \) where

\[ E = r \times r \text{ identity matrix}, \]

\[ F = \begin{pmatrix}
0 & 1 & 0 & \cdots & 0 \\
0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & \cdots & \cdots & \cdots & 1 \\
0 & \cdots & \cdots & \cdots & 0
\end{pmatrix} \]

\( (r \times r) \).
Then

\[ B_j^t = (\lambda_j E + F)^t = \sum_{i=0}^{r-1} \lambda_j^{t-i} \binom{t}{i} F^i \]

\[ = \sum_{i=0}^{r-1} \delta_i(t) \lambda_j^{t-i} F^i \]

where \( \delta_i(t) \) is the integer \( \binom{t}{i} \) modulo 2. Thus

\[ v(t) = \sum_{i=0}^{r-1} \delta_i(t) v_i(t) \]

where

\[ v_i(t) = T \begin{pmatrix} \lambda_1^{t-i} F_i \\ \lambda_2^{t-i} F_i \\ \vdots \\ \lambda_n^{t-i} F_i \end{pmatrix} \]

\[ T^{-1} v(0) \]

We claim this is the desired decomposition.

Each \( v_i(t), i = 0, 1, \ldots, r-1 \) satisfies the linear recursion \( f(x) \) since \( \lambda_1, \ldots, \lambda_n \) are the roots of \( f(x) \).

Each \( v_i(t) \) has its components in the ground field \( \mathbb{F}_2 \). Let \( \sigma \) be the automorphism \( \sigma (\lambda_i) = \lambda_{i+1} \). \( \sigma \) is applied to vectors and matrices component-wise. We must show \( v_i(t)^\sigma = v_i(t) \). We have
\[ T^\sigma = (K_1, K_2, \ldots, K_n)^\sigma \]

\[ = (K_2, K_3, \ldots, K_n, K_1) \]

\[ = (K_1, K_2, \ldots, K_n) D \]

\[ = T D \]

where

\[
D = \begin{pmatrix}
0_{(r \times r)} & 0_{(r \times r)} & \cdots & 0 \\
E_{(r \times r)} & 0 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 0 & 0 \\
0 & 0 & \cdots & E & 0 \\
\end{pmatrix}_{(N \times N)}
\]

Put

\[ G_i = \text{diag.} \left( \lambda_1^{t-i} F_i, \lambda_2^{t-i} F_i, \ldots, \lambda_n^{t-i} F_i \right) \]

so that \( v_i(t) = T G_i T^{-1} v(0) \). Then

\[ G_i^\sigma = \text{diag.} \left( \lambda_2^{t-i} F_i, \lambda_3^{t-i} F_i, \ldots, \lambda_n^{t-i} F_i, \lambda_1^{t-i} F_i \right) \]

\[ = D^{-1} G_i D . \]
and

\[ v_i(t)^{\sigma} = (T G_i T^{-1})^{\sigma} v(0)^{\sigma} = T^{\sigma} G_i^{\sigma} (T^{\sigma})^{-1} v(0) \]

\[ = (T D) (D^{-1} G_i D) (T D)^{-1} v(0) \]

\[ = T G_i T^{-1} v(0) \]

\[ = v_i(t). \]

Hence \( v_i(t) \) is in the ground field.

Finally, we show that \( \delta_i(t) v_i(t) \) satisfies the recursion \( f(x)^{i+1} \), \( i = 0, 1, \ldots, r-1 \). It suffices to check one component \( x(t) \) of \( v_i(t) \).

Using the relation \( \delta_i(t+1) - \delta_i(t) = \delta_{i-1}(t) \) and an induction on \( i \), we have

\[ \sum_{\alpha=0}^{i+1} (-1)^\alpha \binom{i+1}{\alpha} \delta_i(t+\alpha) = 0 \]

for \( t = 0, 1, 2, \ldots \), and \( i = 0, 1, \ldots, r-1 \). That is, \( \delta_i(t) \) satisfies the recursion \( (x-1)^{i+1} \).

The companion matrix of \( (x-1)^{i+1} \) is similar over \( F_2 \) to

\[
E + F = \begin{pmatrix}
1 & 1 & 0 & \ldots & 0 & 0 \\
0 & 1 & 1 & \ldots & 0 & 0 \\
& & & & & \\
& & & & & \\
& & & & & \\
0 & 0 & 0 & \ldots & 1 & 1 \\
0 & 0 & 0 & \ldots & 0 & 1 \\
\end{pmatrix}_{(i+1) \times (i+1)}
\]
where \( E \) is the \((i+1) \times (i+1)\) identity matrix, since the companion matrix of \((x-1)^{i+1}\) is the rational canonical form of \( E + F \).

There is a matrix \( C \) such that

\[
\delta_i(t) = \text{trace} \ (C (E+F)^t).
\]

Let \( \Lambda \) be the companion matrix of \( f(x) \). Then there is a matrix \( C' \) such that

\[
x(t) = \text{trace} \ (C' \Lambda^t).
\]

Since the trace is multiplicative for Kronecker products, we have

\[
\delta_i(t) \ x(t) = \text{trace} \ (C (E+F)^t) \ \text{trace} \ (C' \Lambda^t)
\]

\[
= \text{trace} \ ((C \otimes C') (E \otimes \Lambda + F \otimes \Lambda)^t).
\]

The \((n(i+1)) \times (n(i+1))\) square matrix \( E \otimes \Lambda + F \otimes \Lambda \) is similar to

\[
\begin{pmatrix}
\Lambda & \Lambda & 0 & \ldots & 0 \\
0 & \Lambda & \Lambda & \ldots & 0 \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & \ldots & \Lambda
\end{pmatrix}
\]

Thus

\[
f (E \otimes \Lambda + F \otimes \Lambda)
\]

is similar to
where $g_1(\Lambda), \ldots, g_i(\Lambda)$ are polynomials in $\Lambda$. Since $f(\Lambda) = 0$, clearly

$$f (E \otimes \Lambda + F \otimes \Lambda)^{i+1} = 0.$$ 

Thus $\delta_i(t) x(t)$ satisfies the recursion $f(x)^{i+1}$.

An easy dimension counting argument gives the corollary: The vector space of all sequences satisfying $f(x)^T$ has dimension $nr$, where $n = \deg. f(x)$, and has as a basis the $nr$ product $\delta_i(t) u_j(t)$, where $u_1(t), \ldots, u_n(t)$ is a basis for the vector space of sequences satisfying $f(x)$.

Clearly these proofs are valid when $F_2$ is replaced by an arbitrary field $K$, $\delta_i(t)$ is $\binom{t}{i}$ modulo the characteristic of $K$, and the polynomial $f(x)$ is irreducible and separable over $K$. 
References

