On the crosscorrelation of sequences over $GF(p)$ with shorter periods

Eva Nuria Müller[1]
Fachbereich Mathematik und Informatik, WE 02
FU Berlin
Arnimallee 3
D-14195 Berlin
e-mail: nuria@math.fu-berlin.de

[1]Supported by Deutsche Forschungsgemeinschaft, Graduiertenkolleg Algorithmische Diskrete Mathematik, Grant WE 1265

Maximal linear shift register sequences have been the object of extensive studies. In this note we present two results concerning the crosscorrelation of the sequences $(a_i)_{i\in\mathbb{N}}$ and $(a_{di})_{i\in\mathbb{N}}$ where $(a_i)_{i\in\mathbb{N}}$ is a maximal sequence and $\gcd(d, p^n-1) = 2$. For a more comprehensive introduction we refer the reader to [1] and [2]. More information about the trace-function and the theory of quadratic forms can be found in [3].

Let $c_1, \ldots, c_n$ be elements of $GF(p)$, $c_n \neq 0$. A sequence $(a_i)_{i\in\mathbb{N}}$ is called a linear shift register sequence if every element a_i obeys the linear recurrence relation

$$a_i = c_1 a_{i-1} + \ldots + c_n a_{i-n}. \tag{1}$$

Every sequence $(a_i)_{i\in\mathbb{N}}$ obtained in this way is periodic of period less or equal to p^n-1, depending on the values $c_1, \ldots, c_n$ and the starting-vector $(a_{-n}, \ldots, a_{-1})$. It is well-known that $(a_i)_{i\in\mathbb{N}}$ has maximal period p^n-1 if and only if the characteristic polynomial $f(x) = x^n + c_1x^{n-1} + \ldots + c_{n-1}x + c_n$ associated to recursion (1) is a primitive polynomial over $GF(p)$. In this case we call the sequence $(a_i)_{i\in\mathbb{N}}$ a maximal sequence.
We give a brief list of the most important properties:(c.f. [2])

(i) The number of maximal sequences which are different under cyclic shifts is $\frac{\varphi(p^n-1)}{n}$ where φ is the Eulerian function.

(ii) Let $(a_i)_{i\in\mathbb{N}}$ be a maximal sequence and α be a root of the characteristic polynomial $f(x)$, then α is a primitive element of $GF(p^n)$. Let Tr denote the Trace-function from $GF(p^n)$ onto $GF(p)$ where $Tr(y) = \sum_{i=0}^{n-1} y^{p^i}$ for every $y \in GF(p^n)$. Then there exists a $\beta \in GF(p^n)^*$ such that $a_i = Tr(\beta\alpha^i)$ for every $i \in \mathbb{N}$. Furthermore each choice of $\beta \in GF(p^n)^*$ gives a cyclic shift of $(a_i)_{i\in\mathbb{N}}$.

(iii) If $b_i = a_{di}$ for all $i \in \mathbb{N}$ we say the sequence $(b_i)_{i\in\mathbb{N}}$ is obtained by decimation from $(a_i)_{i\in\mathbb{N}}$ and d is the decimation-factor. The sequence $(b_i)_{i\in\mathbb{N}}$ has maximal period if and only if $\gcd(d, p^n-1) = 1$. Conversely, if $(b_i)_{i\in\mathbb{N}}$ is a maximal sequence, there exist natural numbers d and t such that $b_{i+t} = a_{di}$.

If $(a_i)_{i\in\mathbb{N}}$ is a maximal sequence these conditions ensure that there exists a cyclic shift $(a_j)_{j\in\mathbb{N}} = (a_{i+t})_{i\in\mathbb{N}}$ such that $a_j = Tr(\alpha^j)$ is true for every $j \in$

$\mathbb{N}$. Without loss of generality we assume from now on that every maximal sequence obeys $a_j = Tr(\alpha^j)$.

Definition 1 (Crosscorrelation)
Let $(a_i)_{i\in\mathbb{N}}$ and $(b_i)_{i\in\mathbb{N}}$ be linear shift register sequences over $GF(p)$ and $(a_i)_{i\in\mathbb{N}}$ a maximal sequence. For a (primitive) complex p-th root of unity $\zeta \neq 1$ the crosscorrelation $C_{ab}(t)$ of the sequences (a_i) and (b_i) with respect to t is defined by

$$C_{ab}(t) = \sum_{i=0}^{p^n-2} \zeta^{a_{i-t}} \cdot \overline{\zeta^{b_i}} \tag{2}$$

where $\overline{\zeta^{b_i}}$ denotes the complex conjugate of ζ^{b_i}.

We study the crosscorrelation function by comparing a cyclic shift of the sequence $(a_i)_{i\in\mathbb{N}}$ term by term with the sequence $(b_i)_{i\in\mathbb{N}}$. This has to be done for every shift of $(a_i)_{i\in\mathbb{N}}$. If the sequence $(b_i)_{i\in\mathbb{N}}$ is given by decimation d from the sequence $(a_i)_{i\in\mathbb{N}}$ we can simplify expression (2):

$$\begin{aligned}
C_{ab}(t) &= \sum_{i=0}^{p^n-2} \zeta^{a_{i-t}} \cdot \overline{\zeta^{b_i}} \\
&= \sum_{i=0}^{p^n-2} \zeta^{a_{i-t}} \cdot \zeta^{-b_i} \\
&= \sum_{i=0}^{p^n-2} \zeta^{a_{i-t}} \cdot \zeta^{-a_{di}} \\
&= \sum_{i=0}^{p^n-2} \zeta^{Tr(\alpha^{i-t})-Tr(\alpha^{di})} \\
&= \sum_{i=0}^{p^n-2} \zeta^{Tr(\alpha^{i-t}-\alpha^{di})} \\
&= \sum_{x\in GF(p^n)^*} \zeta^{Tr(\gamma x - x^d)} \\
&= -1 + \sum_{x\in GF(p^n)} \zeta^{Tr(\gamma x - x^d)} \qquad (3)
\end{aligned}$$

where we used $\gamma := \alpha^{-t}$ and $Tr(0) = 0$. We use the notation $C_d(t)$ instead of $C_{ab}(t)$.

Sometimes it will be more convenient to change the roles of the sequences and we will compare $(a_i)_{i\in\mathbb{N}}$ with all possible shifts of $(a_{di})_{i\in\mathbb{N}}$ termwise which leads to the same result regarding the set of values of $C_d(t)$. In this case we consider the expression

$$C_d(t) = -1 + \sum_{x\in GF(p^n} \zeta^{Tr(x-\gamma x^d)}$$

instead of (3).

Theorem 1
Let $p = 3$, n odd, $n \geq 3$ and $d = \frac{p^n+1}{4} + \frac{p^n-1}{2}$. Furthermore let $(a_i)_{i\in\mathbb{N}}$ be a maximal linear shift register sequence. Then the absolute value of the crosscorrelation of $(a_i)_{i\in\mathbb{N}}$ and $(a_{di})_{i\in\mathbb{N}}$ obeys the following inequality:

$$|1 + C_d(t)| \leq 2 \cdot \sqrt{p^n}.$$

Proof: [2]
We have to evaluate

$$1 + C_d(t) = \sum_{x\in GF(3^n)} \zeta^{Tr(x-\gamma x^d)} \tag{4}$$

for every $\gamma \in GF(3^n)$. This means we have to determine the number of solutions of

$$Tr(x - \gamma x^d) = c \tag{5}$$

in $GF(3^n)$ for each $c \in GF(3)$.

Each x in $GF(3^n)$ is either a square, a non-square or 0. But since n is odd $3^n \equiv (-1)^n \equiv -1$ $(mod\ 4)$ and we have: 2 divides $3^n - 1$ and 4 divides $3^n + 1$, thus $\frac{3^n+1}{4}$ is an integer. Using $x^{3^n} = x$ we get $(x^{\frac{3^n+1}{4}})^4 = x^{3^n+1} = x^2$ and conclude that every square can be written as a fourth power of some element in $GF(3^n)$:

$$\{x^2 | x \in GF(3^n)\} = \{x^4 | x \in GF(3^n)\}.$$

Let α be a primitive element of $GF(3^n)$, then $2 = -1 = \alpha^{\frac{3^n-1}{2}}$ and 4 does not divide $3^n - 1$, so -1 is a non-square in $GF(3^n)$. (A more general result

[2] I am grateful to Professor Helleseth for drawing my attention on this value of d.

can be found in [4] Lemma 3.4: The non-squares in $GF(p)$ are non-squares in $GF(p^n)$ if and only if n is odd.) Instead of dividing $GF(3^n)$ in squares and non-squares we can write:

$$GF(3^n) = \{y^4 | y \in GF(3^n)\} \cup \{2 \cdot y^4 | y \in GF(3^n)\}.$$

Let $x = y^4$, as y becomes each nonzero element in $GF(3^n)$, x becomes every square in $GF(3^n)$ twice and $x = 0$ iff $y^4 = 0$. In the same way $x = 2y^4$ becomes every non-square in $GF(3^n)$ twice as y runs through $GF(3^n)$ and $x = 0$ iff $2y^4 = 0$.

We look at the function in (5) if x is a square:

$$\begin{aligned} Tr(x - \gamma \cdot x^d) &= Tr\left(y^4 - \gamma \cdot (y^4)^{\frac{3^n+1}{4} + \frac{3^n-1}{2}}\right) \\ &= Tr\left(y^4 - \gamma \cdot y^{3^n+1} \cdot y^{2 \cdot (3^n-1)}\right) \\ &= Tr\left(y^4 - \gamma \cdot y^2 \cdot (y^{3^n-1})^2\right) \\ &= Tr(y^4 - \gamma \cdot y^2) \end{aligned}$$

and similarly if x is a non-square:

$$\begin{aligned} Tr(x - \gamma \cdot x^d) &= Tr\left(2y^4 - \gamma \cdot (2y^4)^{\frac{3^n+1}{4} + \frac{3^n-1}{2}}\right) \\ &= Tr\left(2y^4 - \gamma \cdot 2^{\frac{3^n+1}{4} + \frac{3^n-1}{2}} \cdot y^{3^n+1} \cdot y^{2 \cdot (3^n-1)}\right) \\ &= Tr(2y^4 - \gamma \cdot y^2). \end{aligned}$$

In the last equation we used the fact that $\frac{3^n+1}{4} + \frac{3^n-1}{2}$ is an even number (we have seen already that $\frac{3^n-1}{2}$ is odd, since n is odd $3^n \equiv 3 \ (mod\ 8)$, thus $3^n + 1 \equiv 4 \ (mod\ 8)$ and we see that $\frac{3^n+1}{4}$ is odd).

Instead of counting the number of solutions of equation (5) we determine the number of solutions of

$$Tr(y^4 - \gamma y^2) = c \quad \text{and} \quad Tr(-y^4 - \gamma y^2) = c \tag{6}$$

in $GF(3^n)$ and divide the sum by 2.

We have to show that both equations in (6) lead to quadratic forms. This is easily done like in [4]: Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of $GF(3^n)$ over $GF(3)$ and let $y = \sum_{i=1}^{n} y_i\alpha_i$ with $y_i \in GF(3)$. Using the Frobenius–property, $y_i^3 = y_i$ since $y_i \in GF(3)$ and the linearity of the Trace–function we get

$$\begin{aligned} Tr(y^4-\gamma y^2) &= Tr\left((\sum_{i=1}^{n} y_i\alpha_i)^3 \sum_{j=1}^{n} y_j\alpha_j - \gamma\cdot(\sum_{i=1}^{n} y_i\alpha_i \sum_{j=1}^{n} y_j\alpha_j)\right) \\ &= Tr\left((\sum_{i=1}^{n} y_i\alpha_i^3) \sum_{j=1}^{n} y_j\alpha_j - \gamma\cdot(\sum_{i=1}^{n} y_i\alpha_i \sum_{j=1}^{n} y_j\alpha_j)\right) \\ &= Tr\left(\sum_{i=1}^{n}\sum_{j=1}^{n} y_iy_j\alpha_i^3\alpha_j - \gamma\cdot\sum_{i=1}^{n}\sum_{j=1}^{n} y_iy_j\alpha_i\alpha_j\right) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} y_iy_jTr(\alpha_i^3\alpha_j) - \sum_{i=1}^{n}\sum_{j=1}^{n} y_iy_jTr(\gamma\cdot\alpha_i\alpha_j) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{n} y_iy_jTr(\alpha_i^3\alpha_j - \gamma\cdot\alpha_i\alpha_j) \end{aligned}$$

if x is a square. Since γ is fixed this is a quadratic form in y_i.
Similarly we get

$$Tr(-y^4-\gamma y^2) = \sum_{i=1}^{n}\sum_{j=1}^{n} y_iy_jTr(-\alpha_i^3\alpha_j - \gamma\alpha_i\alpha_j)$$

for every non–square x. Thus, we have two quadratic forms, namely

$$f_1(y) = Tr(y^4-\gamma y) \quad \text{and} \quad f_2(y) = Tr(-y^4-\gamma y^2) \tag{7}$$

both of them in n indeterminates.

If we know the rank of f_1 and f_2 we can determine the number of solutions of equation (6). To do this we have to find out for how many z's in $GF(3^n)$ the equation

$$f_i(y+z) - f_i(y) = 0 \qquad \text{for all } y \in GF(3^n) \tag{8}$$

holds. Again with the properties of the trace–function, especially

$$Tr(yz^3) = Tr\left((yz^3)^3\right) \tag{9}$$

we get:

$$\begin{aligned}
0 &= f_1(y+z) - f_1(y) = Tr\left((y+z)^4 - \gamma(y+z)^2 - y^4 + \gamma y^2\right) \\
&= Tr\left((y+z)^3(y+z) - \gamma(y+z)^2 - y^4 + \gamma y^2\right) \\
&= Tr\left(y^4 + y^3 z + y z^3 + z^4 - \gamma y^2 - 2\gamma y z - \gamma z^2 - y^4 + \gamma y^2\right) \\
&\overset{(9)}{=} Tr\left(y^3 z + (y z^3)^3 - (2\gamma)^3 y^3 z^3 + z^4 - \gamma z^2\right) \\
&= Tr\left(y^3(z + z^9 - 2^3\gamma^3 z^3) + z^4 - \gamma z^2\right)
\end{aligned}$$

But equation (8) has to be fulfilled for every y in $GF(3^n)$, so z must be a root of

$$g_1 := z^9 + \gamma^3 z^3 + z.$$

Similarly we get for f_2 that z has to be a root of

$$g_2 := z^9 - \gamma^3 z^3 + z.$$

Since both g_1 and g_2 are linearized polynomials[3] the set of roots forms a linear space and we conclude that the possible numbers of roots of g_1 and g_2 are 1, 3 and 9. Hence, the rank of f_1 and f_2 is either n, $n-1$ or $n-2$.

To exclude some of the possible combinations we look an g_1 and g_2 simultaneously:

$$\begin{aligned}
g_1 \cdot g_2 &= (z^9 + \gamma^3 z^3 + z) \cdot (z^9 - \gamma^3 z^3 + z) \\
&= z^{18} + 2 \cdot z^{10} - \gamma^6 z^6 + z^2 \\
&= z^2 \cdot (z^{16} + 2 \cdot z^8 - \gamma^6 z^4 + 1) \\
&= z^2 \cdot ((z^4)^4 + 2 \cdot (z^4)^2 - \gamma^6 z^4 + 1)
\end{aligned}$$

Let $u := z^4$, the polynomial $u^4 + 2 \cdot u^2 - \gamma^6 u + 1$ has at most four roots in $GF(3^n)$. If u_0 is one of these roots and ω is a primitive fourth root of unity then the corresponding roots of $g_1 \cdot g_2$ in the splitting field of $g_1 \cdot g_2$ over $GF(3^n)$ are $\sqrt[4]{u_0}$, $\omega\sqrt[4]{u_0}$, $2\sqrt[4]{u_0}$ and $2\omega\sqrt[4]{u_0}$. But ω is an element of $GF(3^2)$ and not contained in $GF(3^n)$ since n is odd by assumption.

Thus for each root u_0 of $u^4 + 2 \cdot u^2 - \gamma^6 u + 1$ only two of the four possible corresponding roots are elements of $GF(3^n)$ and we can conclude that $g_1 \cdot g_2$ has at most $2 + 2 \cdot 4 = 10$ roots in $GF(3^n)$.

The remaining cases we still have to consider are the following:

[3] i.e. the sum of two roots of g_i is again a root of g_i

1. Both g_1 and g_2 have one root in $GF(3^n)$, then $\text{rank}(f_1) = \text{rank}(f_2) = n$.
2. Both g_1 and g_2 have three roots in $GF(3^n)$, then $\text{rank}(f_1) = \text{rank}(f_2) = n-1$.
3. g_1 has one root and g_2 has three roots in $GF(3^n)$ or vice versa, without loss of generality we can assume $\text{rank}(f_1) = n$ and $\text{rank}(f_2) = n-1$.
4. g_1 has one root and g_2 has nine roots in $GF(3^n)$ or vice versa, then we have $\text{rank}(f_1) = n$ and $\text{rank}(f_2) = n-2$.

Now we can calculate the upper bound for the absolute value of the crosscorrelation: Theorem 4 of the appendix gives us the number of solutions of the non-degenerate quadratic form in $\text{rank}(f_i)$ many indeterminates. Since we are interested in the number of solutions of $f_i(y) = c$ we must multiply the numbers of solutions given by theorem 4 of the appendix with $3^{n-\text{rank}(f_i)}$.

Let $\lambda_i := \left(\frac{\mu_i\cdot(-1)^{\frac{k-1}{2}}}{3}\right)$ where μ_i is the determinant of the non–degenerate quadratic form belonging to f_i, $k = \text{rank}(f_i)$ and $\left(\frac{c}{3}\right)$ denotes the Legendre symbol.

The sign "$*$" indicates that we collect multiples of $1 + \zeta + \ldots + \zeta^{p-1} = 0$.

Case 1: $\text{rank}(f_1) = \text{rank}(f_2) = n$
According to equation (4) we get:

$$\begin{aligned}
2\cdot(1+C_d(t)) &= \underbrace{3^{n-1} + \zeta\cdot(3^{n-1} + \lambda_1\cdot 3^{\frac{n-1}{2}}) + \zeta^2\cdot(3^{n-1} - \lambda_1\cdot 3^{\frac{n-1}{2}})}_{f_1} \\
&\quad + \underbrace{3^{n-1} + \zeta\cdot(3^{n-1} + \lambda_2\cdot 3^{\frac{n-1}{2}}) + \zeta^2\cdot(3^{n-1} - \lambda_2\cdot 3^{\frac{n-1}{2}})}_{f_2} \\
&\overset{*}{=} 3^{\frac{n-1}{2}}\cdot(\lambda_1\cdot\zeta - \lambda_1\cdot\zeta^2 + \lambda_2\cdot\zeta - \lambda_2\cdot\zeta^2) \\
&= 3^{\frac{n-1}{2}}\cdot(\lambda_1+\lambda_2)\cdot(\zeta-\zeta^2).
\end{aligned}$$

Squaring both sides and using $|1-\zeta|^2 = 3$ we get

$$\begin{aligned}
4\cdot|(1+C_d(t))|^2 &= 3^{n-1}\cdot|\lambda_1+\lambda_2|^2\cdot 3 \\
&= \begin{cases} 0 & if \quad \lambda_1 \neq \lambda_2 \\ 4\cdot p^n & if \quad \lambda_1 = \lambda_2. \end{cases}
\end{aligned}$$

In this case $|1+C_d(t)| \leq \sqrt{3^n}$.

Case 2: $\mathrm{rank}(f_1) = \mathrm{rank}(f_2) = n-1$

$2 \cdot (1+C_d(t))$

$= 3 \cdot (3^{n-2} + 2 \cdot 3^{\frac{n-3}{2}} \cdot \lambda_1 + \zeta \cdot (3^{n-2} - 3^{\frac{n-3}{2}} \cdot \lambda_1) + \zeta^2 \cdot (3^{n-2} - 3^{\frac{n-3}{2}} \cdot \lambda_1))$

$\; + 3 \cdot (3^{n-2} + 2 \cdot 3^{\frac{n-3}{2}} \cdot \lambda_2 + \zeta \cdot (3^{n-2} - 3^{\frac{n-3}{2}} \cdot \lambda_2) + \zeta^2 \cdot (3^{n-2} - 3^{\frac{n-3}{2}} \cdot \lambda_2))$

$\stackrel{\star}{=} 3^{\frac{n-1}{2}} \cdot (2 \cdot (\lambda_1 + \lambda_2) - \zeta \cdot (\lambda_1 + \lambda_2) - \zeta^2 \cdot (\lambda_1 + \lambda_2))$

$\stackrel{\star}{=} 3^{\frac{n-1}{2}} \cdot 3 \cdot (\lambda_1 + \lambda_2)$

Squaring leads to

$$\begin{aligned} 4 \cdot |1+C_d(t)|^2 &= 3^{n-1} \cdot 3^2 \cdot |\lambda_1 + \lambda_2|^2 \\ &= \begin{cases} 0 & if \quad \lambda_1 \neq \lambda_2 \\ 4 \cdot p^{n+1} & if \quad \lambda_1 = \lambda_2 \end{cases} \end{aligned}$$

In this case $|1+C_d(t)| \leq \sqrt{3} \cdot \sqrt{3^n} \leq 2 \cdot \sqrt{3^n}$.

Case 3: $\mathrm{rank}(f_1) = n$, $\mathrm{rank}(f_2) = n-1$

$2 \cdot (1+C_d(t))$

$= 3^{n-1} + \zeta \cdot (3^{n-1} + \lambda_1 \cdot 3^{\frac{n-1}{2}}) + \zeta^2 \cdot (3^{n-1} - \lambda_1 \cdot 3^{\frac{n-1}{2}})$

$\; + 3 \cdot (3^{n-2} + 2 \cdot 3^{\frac{n-3}{2}} \cdot \lambda_2 + \zeta \cdot (3^{n-2} - 3^{\frac{n-3}{2}} \cdot \lambda_2) + \zeta^2 \cdot (3^{n-2} - 3^{\frac{n-3}{2}} \cdot \lambda_2))$

$\stackrel{\star}{=} 3^{\frac{n-1}{2}} \cdot (\zeta \cdot \lambda_1 - \zeta^2 \cdot \lambda_1 + 2 \cdot \lambda_2 - \zeta \cdot \lambda_2 - \zeta^2 \cdot \lambda_2)$

$= 3^{\frac{n-1}{2}} \cdot (\lambda_1 \cdot (\zeta - \zeta^2) + 3 \cdot \lambda_2)$

$= 3^{\frac{n-1}{2}} \cdot (\zeta \cdot (\lambda_1 - 3\lambda_2) - \zeta^2 \cdot (\lambda_1 + 3\lambda_2))$.

If we square we get

$$4 \cdot |1+C_d(t)|^2 \;=\; 3^{n-1} \cdot (3\lambda_1^2 + 9\lambda_2^2) = 3^n \cdot 4$$

In this case we get again $|1+C_d(t)| = \sqrt{3^n}$.

Case 4: $\mathrm{rank}(f_1) = n$, $\mathrm{rank}(f_2) = n-2$

$$\begin{aligned} 2 \cdot (1+C_d(t)) &= 3^{n-1} + \zeta \cdot (3^{n-1} + \lambda_1 \cdot 3^{\frac{n-1}{2}}) + \zeta^2 \cdot (3^{n-1} - \lambda_1 \cdot 3^{\frac{n-1}{2}}) \\ &\quad +3^2 \cdot (3^{n-3} + \zeta \cdot (3^{n-3} + \lambda_1 \cdot 3^{\frac{n-3}{2}}) + \zeta^2 \cdot (3^{n-3} - \lambda_1 \cdot 3^{\frac{n-3}{2}})) \\ &\stackrel{\star}{=} \zeta \cdot (\lambda_1 \cdot 3^{\frac{n-1}{2}} + \lambda_2 \cdot 3^{\frac{n+1}{2}}) - \zeta^2 \cdot (\lambda_1 \cdot 3^{\frac{n-1}{2}} + \lambda_2 \cdot 3^{\frac{n+1}{2}}) \\ &= 3^{\frac{n-1}{2}} \cdot (\zeta \cdot (\lambda_1 + 3 \cdot \lambda_2) - \zeta^2 \cdot (\lambda_1 + 3 \cdot \lambda_2)). \end{aligned}$$

Similarly, it follows:

$$\begin{aligned} 4 \cdot |1 + C_d(t)|^2 &= 3^{n-1} \cdot (|\zeta - \zeta^2|^2 \cdot |\lambda_1 + 3\lambda_2|) \\ &= \begin{cases} 3^n \cdot 4^2 & if \quad \lambda_1 = \lambda_2 \\ 3^n \cdot 4 & if \quad \lambda_1 \neq \lambda_2. \end{cases} \end{aligned}$$

Here we have $|1 + C_d(t)| \leq 2 \cdot \sqrt{3^n}$.

In the following theorem we consider a class of values for the decimation factor d. Due to [4] we know $\gcd(p^k + 1, p^n - 1) = 2$ if p is an odd prime and n is odd.

Theorem 2
Let p be an odd prime, n odd, $n \neq 1$, $k \in \{1, \ldots, n\}$, $(a_i)_{i \in \mathbb{N}}$ a maximal linear shift register sequence and $d = p^k + 1$. Then the crosscorrelation $C_d(t)$ of the sequences $(a_i)_{i \in \mathbb{N}}$ and $(a_{di})_{i \in \mathbb{N}}$ is p-valued and $\frac{|1+C_d(t)|}{\sqrt{p^n}} = 1$.

Proof:
We prove the propositions in four steps:

1. We show that it is sufficient to determine the number of solutions of an equation
$$f_\gamma(x_1, \ldots, x_n) = c$$
where f_γ is a polynomial in $GF(p)[x_1, \ldots, x_n]$ and $deg(f_\gamma) = 2$.

2. In two steps we transform the polynomial $f_\gamma(x_1, \ldots, x_n)$ to a diagonal quadratic form $h(z_1, \ldots, z_n)$ and investigate in which way the solutions of $f_\gamma(\mathbf{x}) = c$ and $h_\gamma(\mathbf{z}) = c$ correspond.

3. We show that the crosscorrelation-function $C_d(t)$ takes on exactly p values if $n \geq 3$.

4. We prove that $|1 + C_d(t)| = \sqrt{p^n}$ which is optimal.

ad 1: According to equation (3) we can write

$$1 + C_d(t) = \sum_{x \in GF(p^n)} \zeta^{Tr(\gamma x - x^d)}. \tag{10}$$

Let $\{\alpha_1, \ldots, \alpha_n\}$ be a basis of $GF(p^n)$ over $GF(p)$ and $x = \sum_{i=1}^n x_i\alpha_i$ with $x_i \in GF(p)$. Like in theorem 1 we have

$$\begin{aligned}
Tr(\gamma x - x^d) &= Tr\left(\gamma \cdot \sum_{i=1}^n x_i\alpha_i - (\sum_{i=1}^n x_i\alpha_i)^{p^k} \cdot \sum_{j=1}^n x_j\alpha_j\right) \\
&= Tr\left(\gamma \cdot \sum_{i=1}^n x_i\alpha_i - \sum_{i=1}^n\sum_{j=1}^n x_i x_j \alpha_i^{p^k}\alpha_j\right) \\
&= \sum_{i=1}^n x_i \cdot Tr(\gamma \cdot \alpha_i) - \sum_{i=1}^n\sum_{j=1}^n x_i x_j Tr(\alpha_i^{p^k}\alpha_j)
\end{aligned}$$

which is a polynomial in $GF(p)[x_1, \ldots, x_n]$ of degree 2. It consists of a linear part $\sum_{i=1}^n x_i \cdot Tr(\gamma \cdot \alpha_i)$ and a quadratic form $\sum_{i=1}^n \sum_{j=1}^n x_i x_j Tr(-\alpha_i^{p^k}\alpha_j)$.

We have to determine the number of solutions of

$$Tr(\gamma x - x^d) = \sum_{i=1}^n x_i \cdot Tr(\gamma \cdot \alpha_i) - \sum_{i=1}^n\sum_{j=1}^n x_i x_j Tr(\alpha_i^{p^k}\alpha_j) = c \qquad (11)$$

for each c in $GF(p)$.

ad 2: Let A be the symmetric coefficient matrix of the quadratic form given by (11), with this notation we can write

$$f_\gamma(x_1, \ldots, x_n) = (x_1, \ldots, x_n) \cdot A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

According to [3] there exists a non-singular transformation-matrix T such that $T^T \cdot A \cdot T$ is a diagonal matrix. Performing the non-singular transformation

$$(x_1, \ldots, x_n) = T \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

we get

$$g_\gamma(y_1, \ldots, y_n) = \sum_{i=1}^n b_i y_i + \sum_{i=1}^n a_i y_i^2$$

for some elements [4] $a_1, \ldots, a_n$ in $GF(p)$. The coefficients $b_1, \ldots, b_n$ are obtained by

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = T^T \cdot \begin{pmatrix} Tr(\gamma \cdot \alpha_1) \\ \vdots \\ Tr(\gamma \cdot \alpha_n) \end{pmatrix}$$

and we know that this transformation preserves the number of solutions of the quadratic forms associated to f_γ and g_γ. Since T is a regular matrix this transformation does not affect the linear parts of f_γ and g_γ and we get:

$$f_\gamma(x_1, \ldots, x_n) = c \quad \Leftrightarrow \quad g_\gamma(y_1, \ldots, y_n) = c. \tag{12}$$

To determine the number of solutions of equation (12) we must know the rank of the quadratic form of g_γ. Since this quadratic form is equivalent to the quadratic form of f_γ we consider $Tr(-x^{p^k+1})$. To prove that this quadratic form is non-degenerate we show that

$$Tr\left((x+y)^{p^k+1}\right) - Tr\left(x^{p^k+1}\right) = 0 \quad \text{for all } x \in GF(p^n) \tag{13}$$

has no solution exept $y = 0$:

$$\begin{aligned}
0 &= Tr\left((x+y)^{p^k+1}\right) - Tr\left(x^{p^k+1}\right) \\
&= Tr\left((x+y)^{p^k}(x+y)\right) - Tr\left(x^{p^k+1}\right) \\
&= Tr\left((x^{p^k} + y^{p^k})(x+y) - x^{p^k+1}\right) \\
&= Tr\left(x^{p^k+1} + x^{p^k}y + xy^{p^k} + y^{p^k+1} - x^{p^k+1}\right) \\
&= Tr\left(x^{p^k}y + xy^{p^k} + y^{p^k+1}\right) \\
&= Tr\left(x^{p^k}(y + y^{p^{2k}}) + y^{p^k+1}\right).
\end{aligned}$$

We used again the linearity of the trace function and $Tr\left(xy^{p^k}\right) = Tr\left(x^{p^k}y^{p^{2k}}\right)$ in the last equation. Since this equation has to hold for every x in $GF(p^n)$ we conclude that y has to fulfill

$$y + y^{p^{2k}} = 0 \quad \Leftrightarrow \quad y^{p^{2k}} = -y. \tag{14}$$

[4] The coefficients $a_1, \ldots, a_n$ of the diagonalized quadratic form have nothing in common with the members a_i of the maximal sequence in the statement of the theorem.

Squaring leads to

$$y^{p^{4k}} = \left(y^{p^{2k}}\right)^{p^{2k}} = (-1)^{p^{2k}} \cdot y^{p^{2k}} = -(-y) = y,$$

so y is an element of $GF(p^{4k})$. But y is an element of $GF(p^n)$ at the same time and we get

$$y \in GF(p^{4k}) \cap GF(p^n) = GF(p^{\gcd(4k,n)}) \subseteq GF(p^k), \tag{15}$$

where we used $\gcd(4k,n)|k$ which is true since n is odd by assumption. This implies

$$y^{p^{2k}} = \left(y^{p^k}\right)^{p^k} = y^{p^k} = y,$$

going back to equation (14) we get $y^{p^{2k}} = y = -y$ and since p is odd, $y = 0$ is the only solution of equation (13).

We have shown that the quadratic form belonging to f_γ is non-degenerate which implies that the quadratic form belonging to g_γ has full rank and every coefficient a_i in

$$g_\gamma(y_1, \ldots, y_n) = \sum_{i=1}^{n} a_i y_i^2 + b_i y_i$$

a nonzero element of $GF(p^n)$.

Let us now consider the mapping $h_\gamma(z_1, \ldots, z_n)$ that we get from g_γ via the transformation

$$y_i = z_i - \frac{b_i^2}{2 \cdot a_i}.$$

A simple calculation leads to

$$\sum_{i=1}^{n} a_i y_i^2 + \sum_{i=1}^{n} b_i y_i = c \quad \Leftrightarrow \quad \sum_{i=1}^{n} a_i z_i^2 - \sum_{i=1}^{n} \frac{b_i^2}{2^2 a_i} = c \tag{16}$$

If we set

$$h(z_1, \ldots, z_n) = \sum_{i=1}^{n} a_i z_i^2 \quad \text{and} \quad c_\gamma = \sum_{i=1}^{n} \frac{b_i^2}{2^2 a_i} \tag{17}$$

and write $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ instead of $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_n)$ and $(z_1, \ldots, z_n)$ respectively equation (16) becomes

$$g_\gamma(\mathbf{y}) = \sum_{i=1}^{n} \left(a_i y_i^2 + b_i y_i\right) = c \quad \Leftrightarrow \quad h(\mathbf{z}) = \sum_{i=1}^{n} a_i z_i^2 = c + c_\gamma. \tag{18}$$

Since h is a (diagonal) quadratic form we can determine the number of solutions of $h(\mathbf{z})$ which is identical with the quadratic form associated to g_γ and therefore non-degenerate. Equations (12) and (16) show the relations of the numbers of solutions of $f_\gamma(\mathbf{x}) = c$ and $h(\mathbf{z}) = c$.

ad 3: Let $k_h(i)$ denote the number of solutions of $h(z_1, \ldots, z_n) = i$ given by theorem 4 of the appendix and let

$$\mathbf{v}_h := (k_h(0), \ldots, k_h(p-1)) \tag{19}$$

denote the "coefficient-vector" of $h(\mathbf{z})$ which belongs to the distribution of values of $h(\mathbf{z})$. If $\mathbf{v}_{f_\gamma}$ is the corresponding "coefficient-vector" of f_γ we have

$$1 + C_d(t) = \sum_{i=1}^{p-1} k_{f_\gamma}(i) \cdot \zeta^i$$

according to equation (10). Let σ denote the cyclic-shift-operator on $\mathbb{N}^p$

$$\sigma(v_0, \ldots, v_{p-1}) := (v_1, \ldots, v_{p-1}, v_0).$$

From equations (12) and (18) we get:

$$f_\gamma(\mathbf{x}) = i \quad \Leftrightarrow \quad h(\mathbf{z}) = i + c_\gamma, \tag{20}$$

or, more detailed:

$$\Big(k_{f_\gamma}(0), \ldots, k_{f_\gamma}(p-1)\Big) = (k_h(c_\gamma), \ldots, k_h(c_\gamma - 1)) \quad \Leftrightarrow \quad \mathbf{v}_{f_\gamma} = \sigma^{c_\gamma}(\mathbf{v}_h). \tag{21}$$

Since this property holds for every $\gamma \in GF(p^n)^*$ we have as a first result: each "coefficient-vector" of f_γ is nothing but a cyclic shift of the "coefficient-vector" $\mathbf{v}_h$ of h.

As $\mathbf{v}_h$ is a vector in $\mathbb{N}^p$ there exists at most p different cyclic shifts of $\mathbf{v}_h$ so $C_d(t)$ takes on at most p different values. To prove that the crosscorrelation-function takes on exactly p values it remains to show the following statements:

(a) Each cyclic shift of $\mathbf{v}_h$ is a coefficient-vector of f_γ for an appropriate γ in $GF(p^n)^*$.

(b) The p possible cyclic shifts of $\mathbf{v}_h$ are mutually different.

(c) Different coefficient-vectors of $\mathbf{v}_h$ lead to different values of $C_d(t)$.

ad (a): It is sufficient to show that c_γ from equation (17) attains each value in $GF(p)$ as γ runs through $GF(p^n)^*$. To do this we have to go back a bit: if $\gamma \in GF(p^n)^*$ is given,

$$(Tr(\gamma \cdot \alpha_1), \ldots, Tr(\gamma \cdot \alpha_n))$$

are the coefficients of the linear part of f_γ where $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of $GF(p^n)$ over $GF(p)$. The first transformation led us to

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = T^T \cdot \begin{pmatrix} Tr(\gamma \cdot \alpha_1) \\ \vdots \\ Tr(\gamma \cdot \alpha_n) \end{pmatrix}$$

where $b_1, \ldots, b_n$ are the coefficients of the linear part of g_γ. Since T is a regular matrix, every non-zero vector in $(GF(p))^n$ is a coefficient-vector.

Consider the mapping

$$r : \left\{ \begin{array}{ccc} (GF(p))^n & \rightarrow & GF(p) \\ (b_1, \ldots, b_n) & \mapsto & \frac{1}{2^2 a_1} b_1^2 + \cdots + \frac{1}{2^2 a_n} b_n^2. \end{array} \right. ,$$

given $b_1, \ldots, b_n$ this function returns the appropriate value such that equation (20) holds. Obviously r is a non-degenerate quadratic form, according to theorem 4 each value in $GF(p)$ is attained at least

$$p^{n-1} - p^{\frac{n-1}{2}} = p^{\frac{n-1}{2}} \cdot \left(p^{\frac{n-1}{2}} - 1\right) \geq 3^{\frac{3-1}{2}} \cdot \left(3^{\frac{n-1}{2}} - 1\right) = 6$$

times (remember that $n \geq 3$). So r is a mapping onto $GF(p)$ and we are finished.

ad (b): The entries of the coefficient vectors $\mathbf{v}_h$ in equation (19) are given by:

$$k_h(0) = p^{n-1} \quad \text{and} \quad k_h(i) = p^{n-1} \pm p^{\frac{n-1}{2}}. \tag{22}$$

Suppose $i \geq j$ and $\sigma^i(\mathbf{v}_h) = \sigma^j(\mathbf{v}_h)$, this implies $\sigma^{i-j}(\mathbf{v}_h) = \mathbf{v}_h$. But there is exactly one position in each cyclic shift of $\mathbf{v}_h$ with the entry p^{n-1}, comparing the first positions of the two vectors we get $i = j$.

ad (c): Given a coefficient-vector $(k_s, \ldots, k_{s+p-1})$ we compute the value of the crosscorrelation in the following way:

$$1 + C_d(t) = \sum_{i=0}^{p-1} k_{s+i}\zeta^i = \zeta^{-s} \cdot \sum_{i=0}^{p-1} k_i \zeta^i. \tag{23}$$

Suppose two coefficient-vectors would lead to the same value of $C_d(t)$. This would mean there exist $s, t \in \{0, \ldots, p-1\}$ such that:

$$\zeta^{-t} \cdot \sum_{i=0}^{p-1} k_i\zeta^i = \zeta^{-s} \cdot \sum_{i=0}^{p-1} k_i\zeta^i \quad \Leftrightarrow \quad (\zeta^{-s} - \zeta^{-t}) \cdot \sum_{i=0}^{p-1} k_i\zeta^i = 0,$$

so one of the factors has to be 0. If $(\zeta^{-s} - \zeta^{-t}) = 0$ we get $s = t$ and we are finished. It remains to show that $\sum_{i=0}^{p-1} k_i\zeta^i = 0$ can not happen. As a p-th root of unity ζ obeys $\zeta^{p-1} = -1 - \zeta - \zeta^2 - \ldots - \zeta^{p-2}$ and we conclude:

$$\sum_{i=0}^{p-1} k_i\zeta^i = 0 \quad \Leftrightarrow \quad \sum_{i=0}^{p-2} (k_i - k_{p-1})\zeta^i.$$

But $\{1, \ldots, \zeta^{p-2}\}$ is a linear independent set over $\mathbb{Q}$, thus $k_i = k_{p-1}$ for every i, which is a contradiction to equation (22).

Finally we will calculate the values of $C_d(t)$ and determine the absolute values.

Let $\lambda := \left(\frac{\det h \cdot (-1)^{\frac{n-1}{2}}}{p}\right)$, note that λ is either 1 or -1. Equation (23) and theorem 4 of the appendix give us for an appropriate $s \in \{1, \ldots, p-1\}$:

$$\begin{aligned}
1 + C_d(t) &= \zeta^s \cdot \sum_{i=0}^{p-1} k_i \cdot \zeta^i \\
&= \zeta^s \cdot \sum_{i=0}^{p-1} \left[p^{n-1} + \lambda \cdot \left(\frac{i}{p}\right) \cdot p^{\frac{n-1}{2}} \right] \cdot \zeta^i \\
&= \zeta^s \cdot \left(\sum_{i=0}^{p-1} p^{n-1} \cdot \zeta^i + \sum_{i=0}^{p-1} \lambda \cdot \left(\frac{i}{p}\right) \cdot p^{\frac{n-1}{2}} \cdot \zeta^i \right) \\
&= \zeta^s \cdot \pm \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \cdot p^{\frac{n-1}{2}} \cdot \zeta^i
\end{aligned}$$

ad 4: It remains to show that $|\sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \cdot \zeta^i| = \sqrt{p}$ holds. But this expression can be regarded as a Gaussian sum $\sum_{i\in GF(p)^*} \chi(i) \cdot \Psi(i)$ where $\left(\frac{i}{p}\right)$ is a nontrivial multiplicative character and ζ^i is a nontrivial additive character. According to theorem 5.11 in [3] the absolute value of a nontrivial Gaussian sum is $\sqrt{p}$.

We can generalize the result of theorem 2 for the case when n is even and get similar results. But the condition $\gcd(p^k+1, p^n-1) = 2$ is in general only true for $k = n$, for other values of k the greatest common divisor gets much bigger.

Theorem 3

Let p be an odd prime, n even, $n \neq 2$, $k \in \{1, \ldots, n-1\}$ $(a_i)_{i\in\mathbb{N}}$ a maximal linear shift register sequence, $\frac{n}{\gcd(k,n)}$ not divisible by 4 and $d = p^k + 1$. Then the crosscorrelation $C_d(t)$ of the sequences $(a_i)_{i\in\mathbb{N}}$ and $(a_{di})_{i\in\mathbb{N}}$ is p-valued and $\frac{|1+C_d(t)|}{\sqrt{p^n}} = 1$.

Proof:

We proceed like in the proof of theorem 2, only a few changes will have to be made. We have to show that the quadratic form

$$f_\gamma(x_1, \ldots, x_n) = Tr(\gamma x - x^d)$$

is non-degenerate for every $\gamma \in GF(p^n)^*$. Like above in equations (13) and (14) we get

$$Tr\left((x+y)^{p^k+1}\right) - Tr\left(x^{p^k+1}\right) = 0 \quad \Leftrightarrow \quad y^{p^{2k}} = -y \tag{24}$$

so y must be in $GF(p^{\gcd(n,4k)})$. But $\frac{n}{\gcd(n,k)}$ is not divisible by 4 by assumption and we can conclude

$$\frac{n}{\gcd(n,k)} = m \quad \text{or} \quad \frac{n}{\gcd(n,k)} = 2\cdot m \tag{25}$$

for an odd integer m. Thus we have

$$\gcd(n,4k) = \gcd(n,k) \qquad \text{or} \qquad \gcd(n,4k) = \gcd(n,2k) \tag{26}$$

respectively. In both cases $\gcd(n,4k)$ divides $2k$ so $y^{p^{2k}} = y$ for every y and together with equation (24) again $y = 0$ is the only solution of

$$Tr\left((x+y)^{p^k+1}\right) - Tr\left(x^{p^k+1}\right) = 0 \quad \text{for every } x \in GF(p^n).$$

To continue we can go on like in the case when n is odd. There is a little difference in the third part of the proof because the number of solutions of a quadratic form in an even number of indeterminates is given by a different formula then in the proof of theorem 2. But still the number of solutions of $f_\gamma(\mathbf{x}) = c$ is greater then 0 for every $c \in GF(p)$ since $n \geq 2$ which is the crucial property to make sure that we get at most p different values of $C_d(t)$. Similarly the number of solutions of $f_\gamma(\mathbf{x}) = 0$ is different from the number of solutions of $f_\gamma(\mathbf{x}) = c$ for $c \neq 0$ which guarantees that we get exactly p different values of $C_d(t)$.

The last part of the proof has to be adjusted a bit because the values of k_i are again different. We compute the values of the crosscorrelation: Let $\lambda := \left(\frac{\det h \cdot (-1)^{\frac{n}{2}}}{p}\right)$, note that λ is either 1 or -1. Equation (23) gives us for an appropriate $s \in \{1, \ldots, p-1\}$:

$$1 + C_d(t) = \zeta^s \cdot \sum_{i=0}^{p-1} k_i \zeta^i.$$

Theorem 4 of the appendix and $1 + \ldots + \zeta^{p-1} = 0$, which is indicated by $*$ leads to

$$\begin{aligned}
\sum_{i=0}^{p-1} k_i \zeta^i &= \underbrace{p^{n-1} + \lambda \cdot (p-1) \cdot p^{\frac{n-2}{2}}}_{i=0} + \sum_{i=1}^{p-1} \left(p^{n-1} - \lambda \cdot p^{\frac{n-2}{2}}\right) \cdot \zeta^i \\
&= p^{n-1} + \lambda \cdot (p^{\frac{n}{2}} - p^{\frac{n-2}{2}}) + \sum_{i=1}^{p-1} p^{n-1} \zeta^i - \sum_{i=1}^{p-1} \lambda \cdot p^{\frac{n-2}{2}} \cdot \zeta^i \\
&= p^{n-1} + \sum_{i=1}^{p-1} p^{n-1} \zeta^i + \lambda \cdot (p^{\frac{n}{2}} - p^{\frac{n-2}{2}}) - \sum_{i=1}^{p-1} \lambda \cdot p^{\frac{n-2}{2}} \cdot \zeta^i \\
&= p^{n-1} \cdot \sum_{i=0}^{p-1} \zeta^i + \lambda \cdot (p^{\frac{n}{2}} - p^{\frac{n-2}{2}}) - \sum_{i=1}^{p-1} \lambda \cdot p^{\frac{n-2}{2}} \cdot \zeta^i \\
&\stackrel{*}{=} \lambda \cdot p^{\frac{n}{2}} - \lambda \cdot p^{\frac{n-2}{2}} - \lambda \cdot p^{\frac{n-2}{2}} \cdot \sum_{i=1}^{p-1} \zeta^i \\
&= \lambda \cdot p^{\frac{n}{2}} - \lambda \cdot p^{\frac{n-2}{2}} \cdot \sum_{i=0}^{p-1} \zeta^i \\
&\stackrel{*}{=} \lambda \cdot p^{\frac{n}{2}}. \qquad (27)
\end{aligned}$$

Without any further calculations we see that $|1 + C_d(t)| = \sqrt{p^n}$.

Appendix

Theorem 4 (Number of solutions of a quadratic form) *(c.f. theorems 6.26 and 6.27 in [3])*
Let f be a non-degenerate quadratic form over $GF(p)$, p odd, in k indeterminates, $\Delta = \det(f)$, $c \in GF(p)$ and $\left(\frac{a}{p}\right)$ is the Legendre–symbol.

- *If k is even then the number of solutions of $f(x_1, \ldots, x_k) = c$ is*

$$\begin{cases} p^{k-1} - \left(\frac{(-1)^{\frac{k}{2}} \cdot \Delta}{p}\right) \cdot p^{\frac{k-2}{2}}, & \text{if} \quad c \neq 0 \\ p^{k-1} + (p-1) \cdot \left(\frac{(-1)^{\frac{k}{2}} \cdot \Delta}{p}\right) \cdot p^{\frac{k-2}{2}} & \text{if} \quad c = 0. \end{cases}.$$

- *If k is odd then the number of solutions of $f(x_1, \ldots, x_k) = c$ is*

$$\begin{cases} p^{k-1} + \left(\frac{\Delta \cdot (-1)^{\frac{k-1}{2}} \cdot c}{p}\right) \cdot p^{\frac{k-1}{2}}, & \text{if} \quad c \neq 0 \\ p^{k-1}, & \text{if} \quad c = 0. \end{cases}$$

References

[1] S. W. Golomb: *Shift register sequences.* Laguna Hills 1982

[2] T. Helleseth: *Some results about the crosscorrelation between two maximal linear sequences.* Discrete Mathematics **16** (1976), p.209-232

[3] R. Lidl, H. Niederreiter: *Finite Fields.* Encyclopedia of mathematics and its applications **20**, Reading 1980

[4] H. M. Trachtenberg: *On the cross-correlation functions of maximal linear recurring sequences.* Dissertation, Faculty of the Graduate School, University of Southern California, Los Angeles, California, 1970