m-Sequences with Good Cross Correlation for Communications and Cryptography

Tor Helleseth and Alexander Kholosha

9th Central European Conference on Cryptography:
Třebíč, June 26, 2009

Outline

- m-sequences and their properties
- Correlation of sequences
- Cross correlation of m-sequences and its properties
- Application of sequences with good correlation properties
- Orthogonal sequences and their use
- m-Sequences of different lengths and their cross correlation

m-Sequences and their Properties

Linear recurrence $s_{t+m} + c_{m-1}s_{t+m-1} + \cdots + c_0 s_t = 0$.

Characteristic polynomial $f(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_0$.

Select $f(x)$ such that

- $f(x)$ is irreducible of degree m so $f(x)$ divides $x^{2^m-1} - 1$
- $\gcd(f(x), x^r - 1) = 1$ for any $r = \{1, \ldots, 2^m - 1\}$ (primitiveness criterion)

Then $f(x)$ generates an m-sequence of period $2^m - 1$.

Properties of m-sequences

- Period $p = 2^m - 1$
- Balancedness (except for a missing 0) and run property
- Any decimation by d with $\gcd(d, 2^m - 1) = 1$ gives an m-sequence and all m-sequences of this period can be obtained this way
- $\{s_t\} + \{s_{t+\tau}\} = \{s_{t+\gamma}\}$ and $\{s_{2t}\} = \{s_{t+\delta}\}$

Correlation of Sequences

$\{a_t\}$ and $\{b_t\}$ – binary sequences of length p

$$C_{a,b}(\tau) = \sum_{t=0}^{p-1} (-1)^{a_t + b_{t+\tau}} \quad \text{and} \quad A_a(\tau) = \sum_{t=0}^{p-1} (-1)^{a_t + a_{t+\tau}} \quad \text{for} \quad 0 \leq \tau < p$$

are respectively *cross-correlation* and *auto-correlation* functions of shift τ.

If $\{s_t\}$ is an m-sequence of period $p = 2^m - 1$ then

$$A_s(\tau) = \begin{cases} 2^m - 1, & \text{if } \tau \equiv 0 \pmod{p} \\ -1, & \text{otherwise} \end{cases}$$

since $A_s(\tau) = \Sigma_{t=0}^{p-1} (-1)^{s_t + s_{t+\tau}} = \Sigma_{t=0}^{p-1} (-1)^{s_{t+\gamma}} = -1$ for $\tau \neq 0 \pmod{p}$.

Typical problems

- Find the *distribution* of cross- or auto-correlation values for all shifts.
- Find the *exact value* of these functions for each shift.

Cross Correlation of m-Sequences, Properties

$\{s_t\}$ binary m-sequence of length $p = 2^m - 1$,

$\{s_{dt}\}$ decimated m-sequence when $\gcd(d, p) = 1$.

$$C_d(\tau) = \sum_{t=0}^{p-1} (-1)^{s_{t+\tau} + s_{dt}} \quad \text{for} \quad 0 \le \tau < p$$

is the cross correlation between two m-sequences.

- $C_d(\tau)$ is 2-*valued* if and only if $d \equiv 2^i \pmod p$, at least 3-valued otherwise;
- $C_d(\tau)$ and $C_d(\tau')$ have the same distribution when $dd' \equiv 1 \pmod p$ or $d' \equiv 2^i d \pmod p$;
- $\Sigma_\tau (C_d(\tau) + 1) = 2^m$;
- $\Sigma_\tau (C_d(\tau) + 1)^2 = 2^{2m}$;
- $\Sigma_\tau \, C_d(\tau)^k = -(2^m - 1)^{k-1} + 2(-1)^{k-1} + a_k 2^{2m}$, where a_k is the number of solutions in $\mathrm{GF}(2^m)^*$ of $x_1 + \cdots + x_{k-1} + 1 = 0$ and $x_1^d + \cdots + x_{k-1}^d + 1 = 0$.

Binary 3-Valued Cross Correlation

$C_d(\tau)$ takes on exactly three values in the following cases:

- Gold: $d = 2^k + 1$, where $m/\gcd(m,k)$ is odd;
- Kasami: $d = 2^{2k} - 2^k + 1$, where $m/\gcd(m,k)$ is odd;
- Welch's conjecture: (Canteaut, Charpin, Dobbertin) $d = 2^k + 3$, where $m = 2k + 1$;
- Niho's conjecture: (Dobbertin, Charpin, Hollman, Xiang)

$$d = \begin{cases} 2^{(m-1)/2} + 2^{(m-1)/4} - 1, & \text{if } m \equiv 1 \pmod 4 \\ 2^{(m-1)/2} + 2^{(3m-1)/4} - 1, & \text{if } m \equiv 3 \pmod 4; \end{cases}$$

- Cusick and Dobbertin: $m \equiv 2 \pmod 4$

$$d = 2^{m/2} + 2^{(m+2)/4} + 1 \quad \text{and} \quad d = 2^{(m+2)/2} + 3 \ .$$

Application of Sequences with Good Correlation

- Synchronization
- Radar and sonar applications
- Generation of pseudo random sequences
- Stream ciphers in cryptography
- CDMA applications for mobile and wireless (all standards for 3G telephony are based on CDMA)
- many other

Orthogonal Sequences and their Use

Take an m-sequence 1001011 and construct the following set of sequences

$$
\begin{array}{cccccccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\
1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\
1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\
1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\
1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\
1 & -1 & -1 & 1 & 1 & -1 & 1 & -1
\end{array}
$$

Each pair of these sequences has zero inner product (orthogonal) because the cross correlation at shift 0 is zero.

Orthogonal Sequences and their Use (2)

- each user $i = \{1, \ldots, M\}$ has the sequence $p^i = \{p_0^i, \ldots, p_{n-1}^i\}$
- if user i wants to send data $d_i \in \{1, -1\}$ he transmits

$$d_i p^i = \{d_i p_0^i, \ldots, d_i p_{n-1}^i\}$$

- when many users transmit simultaneously (say, i and j) $s = d_i p^i + d_j p^j$
- data d_i is recovered by computing inner product

$$s \cdot p^i = (d_i p^i + d_j p^j) \cdot p^i = n d_i + 0 d_j = n d_i$$

Using threshold detectors data can be recovered if user sequences have low cross-correlation values even when synchronization is lost (sequences are shifted). To ease synchronization and minimize interference between users, we need *large* families (to support many users) of sequences with *small*

$$C_{\max} = \max\{C_{a,b}(\tau) \ : \ \text{either } a \neq b \text{ or } \tau \neq 0\}$$

m-Sequences of Different Lengths

$\{a_t\}$ and $\{b_t\}$ – binary sequences of length p

$$C(\tau) = \sum_{t=0}^{p-1} (-1)^{a_t + b_{t+\tau}} \quad \text{for} \quad 0 \le \tau < p \ .$$

the *cross-correlation function* of shift τ. Well studied for a pair of m-sequences of the same length.

α	primitive element in $\mathrm{GF}(2^m)$, m even, and $\beta = \alpha^{2^{m/2}+1}$;
$s_t = \mathrm{Tr}_m(\alpha^t)$	binary m-sequence of length $p = 2^m - 1$;
$u_t = \mathrm{Tr}_{m/2}(\beta^t)$	binary m-sequence of length $2^{m/2} - 1$ (Kasami family);
$v_t = u_{dt}$	m-sequence of length $2^{m/2} - 1$ if $\gcd(d, 2^{m/2} - 1) = 1$;

$$C_d(\tau) = \sum_{t=0}^{p-1} (-1)^{s_t + v_{t+\tau}} \ ,$$

where $\tau = 0, \ldots, 2^{m/2} - 2$.

m-Sequences of Different Lengths (2)

Crosscorrelation $C_d(\tau)$ between $\{s_t\}$ and $\{v_t\}$ is at most 4-valued if $m = 2k$ and $d(2^l + 1) \equiv 2^i \pmod{2^k - 1}$ for an integer l with $0 \leq l < k$ and $i \geq 0$. The following distribution holds

$$\begin{array}{lll} -1 - 2^{k+e} & \text{occurs} & \frac{2^{k-e}-1}{2^{2e}-1} \text{ times} \\ -1 - 2^k & \text{occurs} & \frac{(2^k-1)(2^{e-1}-1)}{2^e-1} \text{ times} \\ -1 & \text{occurs} & 2^{k-e} - 1 \text{ times} \\ -1 + 2^k & \text{occurs} & \frac{(2^k+1)2^{e-1}}{2^e+1} \text{ times} \end{array},$$

where $e = \gcd(l, k)$.

- If $k > 1$ and $e = 1$ then $C_d(\tau)$ is 3-valued ($C_d(\tau) \neq -1 - 2^k$).
- If $d = 1$ (Kasami family) then $C_d(\tau)$ is 2-valued (-1 and $-1 - 2^{k+e}$).

Conjecture 1 *Except for the case when $m = 8$ and $d = 7$, all decimations leading to at most four-valued cross correlation between two m-sequences of different lengths $2^{2k} - 1$ and $2^k - 1$ are described above.*

Computationally checked for $m \leq 32$.

Distribution of Cross Correlation

The set of values of $C_d(\tau)+1$ for $\tau = 0, \ldots, 2^k-2$ is equal to the set

$$\begin{aligned} S(a) &= \sum_{x \in \mathrm{GF}(2^m)} (-1)^{\mathrm{Tr}_m(ax)+\mathrm{Tr}_k(x^{d(2^k+1)})} \\ &= \sum_{y \in \mathrm{GF}(2^m)} (-1)^{\mathrm{Tr}_m(ay^{2^l+1})+\mathrm{Tr}_k(y^{2^k+1})} = S_0(a) \end{aligned}$$

when $a \in \mathrm{GF}(2^k)^*$ taking $m = 2k$ and assuming l/e being even.

Proposition 2 *Take integers l and k with $0 \le l < k$ such that k/e is odd. Then*

$$S_0(a) = 2^k \sum_{v \in \mathrm{GF}(2^k),\, F_a(v)=0} (-1)^{\mathrm{Tr}_k\left(a(l/e+1)c^{-2}v^{2^l+1}+v\right)} \ ,$$

where $F_a(x) = a^{2^l}x^{2^{2l}} + x^{2^l} + ax + c$ with $c^{-1} = \delta + \delta^{-1} \in \mathrm{GF}(2^e)$ for δ being a primitive $(2^e+1)^{\mathrm{th}}$ root of unity over $\mathrm{GF}(2)$, and $\mathrm{Tr}_e(c) = 1$. Moreover, $S_0(a)^2$ taken for all $a \in \mathrm{GF}(2^k)^*$ has the following distribution for l/e even:

0	*occurs*	$2^{k-e}-1$	*times*
2^{2k}	*occurs*	$\frac{2^{k+2e}-2^{k+e}-2^k+1}{2^{2e}-1}$	*times*
$2^{2(k+e)}$	*occurs*	$\frac{2^{k-e}-1}{2^{2e}-1}$	*times* .

Distribution of Cross Correlation (2)

Lemma 3 *For any decimation d with $\gcd(d, 2^k - 1) = 1$ the exponential sum $S(a)$ satisfies the following moment identities*

$$\begin{aligned}
\sum_{a \in \mathrm{GF}(2^k)^*} S(a) &= 2^k \\
\sum_{a \in \mathrm{GF}(2^k)^*} S(a)^2 &= 2^{2k}(2^k - 1) \\
\sum_{a \in \mathrm{GF}(2^k)^*} S(a)^3 &= -2^{4k} + (\lambda + 3)2^{m+k} \quad ,
\end{aligned}$$

where λ is the number of solutions for $x_1, x_2 \in \mathrm{GF}(2^m)^*$ of the equation system

$$\begin{aligned}
1 + x_1 + x_2 &= 0 \\
1 + x_1^{d(2^k+1)} + x_2^{d(2^k+1)} &= 0 \quad .
\end{aligned}$$

For the values of d that we consider it is easy to show that $\lambda = 2^{\gcd(l,k)} - 2$.

Permutation Polynomials by Dobbertin

$$
\begin{aligned}
A_1(x) &= x\ , \\
A_2(x) &= x^{2^l+1}\ , \\
A_{i+2}(x) &= x^{2^{(i+1)l}} A_{i+1}(x) + x^{2^{(i+1)l}-2^{il}} A_i(x) \quad \text{for} \quad i \geq 1\ , \\
B_1(x) &= 0\ , \\
B_2(x) &= x^{2^l-1}\ , \\
B_{i+2}(x) &= x^{2^{(i+1)l}} B_{i+1}(x) + x^{2^{(i+1)l}-2^{il}} B_i(x) \quad \text{for} \quad i \geq 1\ .
\end{aligned}
$$

Let $\gcd(l,k) = 1$ and $l' = l^{-1} \pmod{k}$ and define the polynomials

$$
R(x) = \sum_{i=1}^{l'} A_i(x) + B_{l'}(x) \quad \text{and} \quad S(x) = \frac{\sum_{i=1}^{l'} x^{2^{il}} + l' + 1}{x^{2^l+1}}\ .
$$

Theorem 4 (Dobbertin) *$S(x)$ is a permutation polynomial on $\mathrm{GF}(2^k)^*$. (To be formally more precise, we get a* polynomial *$S(x)$ if $x^{-(2^l+1)}$ is substituted by $x^{(2^k-1)-(2^l+1)}$.) Moreover, $S(x)$ and $R(x^{-1})$ are inverses of each other, i.e., for any nonzero $u, v \in \mathrm{GF}(2^k)$ with $S(u) = v^{-1}$ it always holds that $R(v) = u$.*

Polynomial $F_a(x) = a^{2^l} x^{2^{2l}} + x^{2^l} + ax + 1$

Lemma 5 *$R(a^{-1})$ is a zero of $F_a(x)$ in $\mathrm{GF}(2^k)$ for any $a \in \mathrm{GF}(2^k)^*$.*

Thus, it suffices to analyze the number of zeros of the linearized homogeneous part of $F_a(x)$ which, after dividing by $a^{-1}x$, then raising to power 2^{k-1} and replacing $(ax^{2^l-1})^{2^{k-1}}$ by z (one-to-one), takes on the form of

$$P_a(z) = z^{2^l+1} + z + a \ .$$

M_i is $\#a \in \mathrm{GF}(2^k)^*$ such that $P_a(z)$ has exactly i zeros in $\mathrm{GF}(2^k)$

Theorem 6 *For any $a \in \mathrm{GF}(2^k)^*$ and a positive integer $l < k$ with $\gcd(l,k) = 1$ polynomial $P_a(x)$ has either none, one, or three zeros in $\mathrm{GF}(2^k)$. Further, $P_a(x)$ has exactly one zero in $\mathrm{GF}(2^k)$ if and only if $\mathrm{Tr}_k(R(a^{-1}) + 1) = 1$. Finally, the following distribution holds for k odd (respectively, k even)*

$$\begin{array}{ll} M_0 = \frac{2^k+1}{3} & (\textit{resp.}\ \frac{2^k-1}{3}) \\ M_1 = 2^{k-1} - 1 & (\textit{resp.}\ 2^{k-1}) \\ M_3 = \frac{2^{k-1}-1}{3} & (\textit{resp.}\ \frac{2^{k-1}-2}{3}) \ . \end{array}$$

Polynomials $C_i(x)$ and $Z_n(x)$ over $\mathrm{GF}(2^k)$

Take integer $l < k$ and let $e = \gcd(l, k)$ so that $k = ne$.
Denoting $v_i = v^{2^{il}}$ ($i = 0, \ldots, n-1$) for any $v \in \mathrm{GF}(2^k)$, let

$$\begin{aligned} C_1(x) &= 1 \\ C_2(x) &= 1 \\ C_{i+2}(x) &= C_{i+1}(x) + x_i C_i(x) \quad \text{for} \quad 1 \le i \le n-1 \\ Z_n(x) &= C_{n+1}(x) + x C_{n-1}^{2^l}(x) \end{aligned}$$

$$D = \begin{pmatrix} 1 & x_j & \cdots & 0 & 0 \\ x_j & \ddots & \ddots & & 0 \\ \vdots & \ddots & & \ddots & \vdots \\ 0 & & \ddots & \ddots & x_i \\ 0 & \cdots & 0 & x_i & 1 \end{pmatrix} \quad \text{for} \quad j \le i \quad \text{and} \quad x \in \mathrm{GF}(2^k)$$

$$\begin{aligned} \Delta_x(1, i) &= C_{i+2}^2(x) \\ \Delta_x(1, i)^{2^{tl}} &= \Delta_x(1+t, i+t) \quad \text{for} \quad 0 \le t \le n-1 \ , \end{aligned}$$

where $\Delta_x(j, i) = \det D$.

Polynomials $C_i(x)$ and $Z_n(x)$ (2)

Proposition 7 *Take any $v \in \mathrm{GF}(2^{ne}) \setminus \mathrm{GF}(2^e)$ with $n > 1$ and let*

$$V = \frac{v_0^{2^{2l}+1}}{(v_0+v_1)^{2^l+1}} \quad . \tag{1}$$

Then

$$C_n(V) = \frac{\mathrm{Tr}_e^{ne}(v_0)}{(v_1+v_2)} \prod_{j=2}^{n-1} \left(\frac{v_0}{v_0+v_1}\right)^{2^{jl}} \quad .$$

If n is odd (respectively, n is even) then the total number of distinct zeros of $C_n(x)$ in $\mathrm{GF}(2^{ne})$ is equal to $\frac{2^{(n-1)e}-1}{2^{2e}-1}$ (respectively, $\frac{2^{(n-1)e}-2^e}{2^{2e}-1}$). All zeros have the form of (1) with $\mathrm{Tr}_e^{ne}(v_0) = 0$ and occur with multiplicity 2^l. Moreover, polynomial $C_n(x)$ splits in $\mathrm{GF}(2^{ne})$ if and only if $e = l$ or $n < 4$.

Corollary 8 *If n is odd (respectively, n is even) then the total number of distinct zeros of $Z_n(x)$ in $\mathrm{GF}(2^{ne})$ is equal to $\frac{2^{(n+1)e}-2^{2e}}{2^{2e}-1}$ (respectively, $\frac{2^{(n+1)e}-2^e}{2^{2e}-1}$). All zeros have the form of (1) and occur with multiplicity one. Moreover, polynomial $Z_n(x)$ splits in $\mathrm{GF}(2^{ne})$ if and only if $e = l$ or $n = 1$.*

Polynomial $P_a(x) = x^{2^l+1} + x + a$

For any $a \in \mathrm{GF}(2^k)^*$, polynomial $P_a(x)$ has

- none or exactly two zeros in $\mathrm{GF}(2^k)$ iff $Z_n(a) \neq 0$;
- exactly two zeros in $\mathrm{GF}(2^k)$ iff $Z_n(a) \neq 0$ and $\mathrm{Tr}_e\left(\mathrm{N}_e^k(a)/Z_n^2(a)\right) = 0$;
- exactly one zero in $\mathrm{GF}(2^k)$ iff $Z_n(a) = 0$ and $C_n(a) \neq 0$, this zero is equal to $\left(aC_n^{2^l-1}(a)\right)^{2^{k-1}}$;
- exactly $2^e + 1$ zeros in $\mathrm{GF}(2^k)$ iff $C_n(a) = 0$.

$$M_i = \#\{a \mid a \neq 0, P_a(x) \text{ has exactly } i \text{ zeros in } \mathrm{GF}(2^k)\}$$

If n is odd (resp. n is even) then

$$\begin{array}{lcll} M_0 & = & \frac{(2^k+1)2^{e-1}}{2^e+1} & (\text{resp. } \frac{(2^k-1)2^{e-1}}{2^e+1}) \,, \\ M_1 & = & 2^{k-e} - 1 & (\text{resp. } 2^{k-e}) \,, \\ M_2 & = & \frac{(2^k-1)(2^{e-1}-1)}{2^e-1} & (\text{in both cases}) \,, \\ M_{2^e+1} & = & \frac{2^{k-e}-1}{2^{2e}-1} & (\text{resp. } \frac{2^{k-e}-2^e}{2^{2e}-1}) \,. \end{array}$$

If $\gcd(l,k) = 1$ then $\mathrm{Tr}_k(R(a^{-1}) + 1) = 1$ iff $Z_k(a) = 0$ and $C_k(a) \neq 0$.

Polynomials $l_a(x) = a^{2^l} x^{2^{2l}} + x^{2^l} + ax$ and $P_a(x)$

Theorem 9 (Bluher) *For any $b \in \mathrm{GF}(2^k)^*$, take polynomials*

$$f(x) = x^{2^{l}+1} + b^2 x + b^2 \quad \textit{and} \quad g(x) = b^{-1} f(b x^{2^l-1}) = b^{2^l} x^{2^{2l}-1} + b^2 x^{2^l-1} + b$$

over $\mathrm{GF}(2^k)$ and let $\gcd(l, k) = e$. Then exactly one of the following holds

(i) $f(x)$ has none or two zeros in $\mathrm{GF}(2^k)$ and g(x) has none zeros in $\mathrm{GF}(2^k)$;

(ii) $f(x)$ has one zero in $\mathrm{GF}(2^k)$ and g(x) has $2^e - 1$ zeros in $\mathrm{GF}(2^k)$;

(iii) $f(x)$ has $2^e + 1$ zeros in $\mathrm{GF}(2^k)$ and g(x) has $2^{2e} - 1$ zeros in $\mathrm{GF}(2^k)$.

Let N_i denote the number of $b \in \mathrm{GF}(2^k)^*$ such that $f(x) = 0$ has exactly i roots in $\mathrm{GF}(2^k)$. Then the following distribution holds for k/e odd (resp., k/e even)

$$\begin{array}{lcll} N_0 & = & \frac{(2^k+1)2^{e-1}}{2^e+1} & (resp.\ \frac{(2^k-1)2^{e-1}}{2^e+1}) \,, \\ N_1 & = & 2^{k-e} - 1 & (resp.\ 2^{k-e}) \,, \\ N_2 & = & \frac{(2^k-1)(2^{e-1}-1)}{2^e-1} & (in\ both\ cases) \,, \\ N_{2^e+1} & = & \frac{2^{k-e}-1}{2^{2e}-1} & (resp.\ \frac{2^{k-e}-2^e}{2^{2e}-1}) \ . \end{array}$$

Polynomial $F_a(x) = a^{2^l} x^{2^{2l}} + x^{2^l} + ax + c$

Here $c \in \mathrm{GF}(2^e)$, and let
$N_i = \#\{a \mid a \neq 0, F_a(x) \text{ has exactly } i \text{ zeros in } \mathrm{GF}(2^k)\}$

Proposition 10 *Take any $a \in \mathrm{GF}(2^k)$. Then polynomial $F_a(x)$ has exactly one zero in $\mathrm{GF}(2^k)$ if and only if $Z_n(a) \neq 0$. Moreover, this zero is equal to $\mathcal{V}_a = cC_n(a)/Z_n(a)$ and $\mathrm{Tr}_e^k(\mathcal{V}_a) = nc$. Also if n is odd (resp. n is even) then*

$$|N_1| = \frac{2^{k+2e} - 2^{k+e} - 2^k + 1}{2^{2e} - 1} \text{ (resp. } \frac{2^{k+2e} - 2^{k+e} - 2^k - 2^{2e} + 2^e + 1}{2^{2e} - 1}) .$$

Proposition 11 *Take any $a \in \mathrm{GF}(2^k)^*$. Then polynomial $F_a(x)$ has exactly 2^e zeros in $\mathrm{GF}(2^k)$ if and only if $Z_n(a) = 0$ and $C_n(a) \neq 0$. In this case, $\mathrm{Tr}_e^k(v) = (n-1)c$ for any $v \in \mathrm{GF}(2^k)$ with $F_a(v) = 0$. Moreover, if n is odd then these zeros are the following*

$$v_\mu = c \sum_{i=0}^{\frac{n-1}{2}} \frac{C_{n-1}^{2^{(2i+1)l}}(a)}{C_n^{2^{(2i+1)l}+2^{2il}-1}(a)} + \mu C_n(a)$$

for every $\mu \in \mathrm{GF}(2^e)$. Also if n is odd (resp. n is even) then $|N_{2^e}| = 2^{k-e} - 1$ (resp. 2^{k-e}).

The Affine Polynomial $F_a(x)$ and $S_0(a)$

Proposition 12 *Take any $a \in \mathrm{GF}(2^k)^*$. Then polynomial $F_a(x)$ has exactly 2^{2e} zeros in $\mathrm{GF}(2^k)$ if and only if $C_n(a) = 0$. In this case, $\mathrm{Tr}_e^k(v) = nc$ for any $v \in \mathrm{GF}(2^k)$ with $F_a(v) = 0$. Moreover, if n is odd (resp. n is even) then*

$$M_{2^{2e}} = \frac{2^{k-e}-1}{2^{2e}-1} \ (\textit{resp.}\ \frac{2^{k-e}-2^e}{2^{2e}-1}) \ .$$

Proposition 13 *Take integers l and k with $0 \le l < k$ such that $n = k/e$ is odd, where $e = \gcd(l,k)$. For any $a \in \mathrm{GF}(2^k)$ the distribution of $S_0(a)$ for l/e being even is as follows:*

$$\begin{array}{lll} - \ 2^k(-1)^{\mathrm{Tr}_e\left(\mathrm{N}_e^k(a)/Z_n^2(a)\right)} & \textit{if} & Z_n(a) \neq 0 \\ \quad 0 & \textit{if} & Z_n(a) = 0 \textit{ and } C_n(a) \neq 0 \\ - \ 2^{k+e} & \textit{if} & C_n(a) = 0 \end{array}$$

and for l/e being odd

$$\begin{array}{lll} - \ 2^k & \textit{if} & Z_n(a) \neq 0 \\ \quad 2^{k+e} & \textit{if} & Z_n(a) = 0 \textit{ and } C_n(a) \neq 0 \\ - \ 2^{k+2e} & \textit{if} & C_n(a) = 0 \ . \end{array}$$

Remarkable Connections

Take k odd, $\gcd(l,k)=1$ and let A_1 be the number of solutions of

$$\begin{array}{ccccccc} x & + & y & + & z & + & u & = & 1 \\ x^{2^l+1} & + & y^{2^l+1} & + & z^{2^l+1} & + & u^{2^l+1} & = & 0 \\ x^{2^{2l}+1} & + & y^{2^{2l}+1} & + & z^{2^{2l}+1} & + & u^{2^{2l}+1} & = & 0 \end{array}$$

where $x,y,z,u \in \mathrm{GF}(2^k)$ are pairwise distinct. Then

$$A_1 = 2^k + 1 + 3G_k^{(l)} - 2C_k - 2K_k^{(l)} \ ,$$

where

$$G_k^{(l)} = \sum_{x\in \mathrm{GF}(2^k)^*} (-1)^{\mathrm{Tr}_k(x^{2^l+1}+x^{-1})} \stackrel{?}{=} \sum_{x\in \mathrm{GF}(2^k)^*} (-1)^{\mathrm{Tr}_k(x^3+x^{-1})} \ ,$$

$$C_k = \sum_{x\in \mathrm{GF}(2^k)} (-1)^{\mathrm{Tr}_k(x^{2^l+1}+x)} = \begin{cases} 2^{(k+1)/2} & \text{if } \ k=\pm 1 \pmod 8 \\ -2^{(k+1)/2} & \text{if } \ k=\pm 3 \pmod 8 \end{cases} \ ,$$

$$K_k^{(l)} = 2\sum_{\mathrm{Tr}_k(x)=1} (-1)^{\mathrm{Tr}_k\left(\frac{x^{2^{2l}+1}}{(x+x^{2^l})^{2^l+1}}\right)} \stackrel{?}{=} \sum_{x\in \mathrm{GF}(2^k)^*} (-1)^{\mathrm{Tr}_k(x+x^{-1})}$$

Dickson Polynomials

$$
\begin{aligned}
D_0(x) &= 0\ , \\
D_1(x) &= x\ , \\
D_{i+2}(x) &= xD_{i+1}(x) + D_i(x)
\end{aligned}
$$

$$
\begin{aligned}
D_{2^l+1} &= x^{2^l+1} + D_{2^k-1}(x) \\
D_{2^l-1} &= \sum_{i=0}^{l-1} x^{2^l+1-2^{l-i}} \\
D_i(x + x^{-1}) &= x^i + x^{-i}
\end{aligned}
$$

Theorem 14 *$D_i(x)$ is a permutation polynomial on $\mathrm{GF}(2^k)$ iff $\gcd(i, k^2-1) = 1$. In particular, if $\gcd(l, k) = 1$ then D_{2^l-1} is a permutation polynomial on $\mathrm{GF}(2^k)$ iff l is odd and D_{2^l+1} is a permutation polynomial on $\mathrm{GF}(2^k)$ iff l is even. Moreover $L_{D_{2^l+1}} = L_{D_3}$ if l is odd and $L_{D_{2^l-1}} = L_{D_3}$ if l is even, where*

$$L_\eta(v) := \#\{x \in \mathrm{GF}(2^k) : \eta(x) = v\}\ .$$

Idea of the Proof

Take equation $F_a(x) = 0$ and all its 2^{il} powers to obtain n equations

$$F_a^{2^{il}}(x) = a_{i+1}x_{i+2} + x_{i+1} + a_i x_i + c = 0 \quad \text{for} \quad i = 0, \ldots, n-1 \ .$$

$$\mathcal{M}_n = \begin{pmatrix} 0 & 0 & \cdots & a_1 & 1 & a_0 \\ 0 & & \iddots & 1 & a_1 & 0 \\ \vdots & \iddots & \iddots & \iddots & \iddots & \vdots \\ a_{n-2} & 1 & \iddots & & & 0 \\ 1 & a_{n-2} & \iddots & & 0 & a_{n-1} \\ a_{n-1} & 0 & \cdots & 0 & a_0 & 1 \end{pmatrix}$$

$\det \mathcal{M}_n = Z_n^2(a)$

Idea of the Proof (2)

If $Z_n(a) = 0$ and $B_n(a) \neq 0$ then $\mu B_n(a)$ (for all $\mu \in \mathrm{GF}(2^e)$) are zeros of

$$l_a(x) = a_1 x^{2^{2l}} + x^{2^l} + a_0 x$$

being the linearized homogeneous part of $A_a(x)$ and these are all the roots.

Substitute $x = B_n(a)v$. All zeros of $A_a(x)$ are also roots of

$$v^{2^l} + v = \frac{cB_{n-1}^{2^l}(a)}{B_n^{2^l+1}(a)} = cD \ ,$$

which is solvable if and only if $\mathrm{Tr}_e^{ne}\left(\frac{B_{n-1}^{2^l}(a)}{B_n^{2^l+1}(a)}\right) = 0$ (we know that if $Z_n(a) = 0$ and $B_n(a) \neq 0$ then $a = \frac{v_0^{2^{2l}+1}}{(v_0+v_1)^{2^l+1}}$ with $\mathrm{Tr}_e^{ne}(v_0) \neq 0$). If n is **odd** then

$$v = c(D + D^{2^{2l}} + \cdots + D^{2^{(n-1)l}}) \ .$$

What is the explicit solution if n is **even**?