Helleseth, Tor

Some results about the cross-correlation function between two maximal linear sequences. (English) Zbl 0348.94017

Discrete Math. 16, 209-232 (1976).

Let $\{a_j\}$ and $\{a_{dj}\}$ be two maximal linear sequences of period $p^n - 1$. The cross-correlation function is defined by

$$C_d(t) = \sum_{j=0}^{p^n-2} \zeta^{a_{j-t}-a_{dj}} \qquad \text{for } t = 0, 1, \ldots, p^n - 2$$

where $\zeta = \exp(2\pi i/p)$. Finding the values and the number of occurrences for each value of $C_d(t)$ is equivalent to finding the complete weight enumerator for the cyclic $(p^n - 1, 2n)$ code with parity-check polynomial which is the product of the recursion polynomials for the two maximal linear sequences. here properties of $C_d(t)$ are investigated. An expression for

$$\sum_{t=0}^{p^n-2} C_d(t)C_d(t+\tau_1)\ldots C_d(t+\tau_{n-1})$$

is derived. When $\tau_1 = \tau_2 = \ldots = \tau_{n-1} = 0$ this is an analogue to the Pless power moment identities which is often used in calculation of the Hamming weight enumerator. When $d \not\equiv p^i \pmod{p^n - 1}$ it is shown that $C_d(t)$ has at least three different values. We also provide an upper bound on the number of different values of $C_d(t)$ for some choices of d. Further, the values and number of occurrences of each value of $C_d(t)$ is determined completely for several new decimations d when $C_d(t)$ has less than or equal to six different values. Numerical results and some conjectures are given.

Reviewer: Tor Helleseth (Bergen)

For a scan of this review see the web version.

MSC:

94A55 Shift register sequences and sequences over finite alphabets in information and communication theory
94B15 Cyclic codes
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)

Full Text: DOI

References:

[1] Baumert, L.D.; McEliece, R.J., Weight of irreducible cyclic codes, Information and control, 20, 158-175, (1972) · Zbl 0239.94007

[2] Carlitz, I.; Uchiyama, S., Bounds for exponential sums, Duke math. J., 24, 37-41, (1957) · Zbl 0088.03901

[3] Gold, R., Maximal recursive sequences with 3-valued recursive cross-correlation functions, IEEE trans. information theory, 14, 154-156, (1967) · Zbl 0228.62040

[4] Golomb, S.W., Theory of transformation groups of polynomials over GF(2) with applications to linear shift register sequences, Information sci., 1, 87-109, (1968) · Zbl 0238.20060

[5] Kasami, T., Weight enumerators for several classes of subcodes of the second order binary Reed-muller codes, Information and control, 18, 369-394, (1971) · Zbl 0217.58802

[6] Kasami, T.; Lin, S.; Peterson, W.W., Some results on cyclic codes which are invariant under the affine group and their applications, Information and control, 11, 475-496, (1968) · Zbl 0169.51101

[7] Mattson, H.E.; Solomon, G., A new treatment of Bose-chaudhuri codes, J. SIAM, 9, 654-669, (1961) · Zbl 0137.13604

[8] McEliece, R.J.; Rumsey, H., Euler products, cyclotomy, and coding, J. number theory, 4, 302-311, (1972) · Zbl 0235.12014

[9] McEliece, R.J., Weight congruences for \textit{p}-ary cylic codes, Discrete math, 3, 177-192, (1972) · Zbl 0251.94008

[10] Niho, Y., Multi-valued cross-correlation function between two maximal linear recursive sequences, ()

[11] Pless, V., Power moment identities on weight distributions in error-correcting codes, Information and control, 6, 147-152, (1963) · Zbl 0149.37905

[12] Storer, T., Cyclotomy and difference sets, (1967), Markham Chicago · Zbl 0157.03301

[13] Trachtenberg, H.M., On the cross-correlation functions of maximal linear sequences, ()

[14] Lint, J.H.Van, Coding theory, (1971), Springer Berlin