BINARY PERIODIC SEQUENCES WITH LOW SIDELOBE SUPPRESSION LOSS

V. P. Ipatov

Izvestiya VUZ. Radioelektronika,
Vol. 23, No. 1, pp. 20-25, 1980

UDC 621.391.2

The properties of binary signals obtained by coding elements of q-ary M-sequences by symbols ±1 are considered. Coding rules are synthesized with respect to the criterion of minimum loss in threshold signal accompanying linear sidelobe suppression. Examples are quoted of new families of sequences which are better than the familiar sequences from the point of view of the minimum loss criterion.

To resolve a periodic discrete signal (PDS) in a reflection-type noise background, a linear sidelobe suppression filter (SLSF) can be successfully used [1]; the response of this filter to the input PDS has zero sidelobes throughout the signal period, thereby enabling efficient protection to be obtained against reflections of theoretically unlimited intensity. It was shown in [1] that an SLSF exists and is uniquely defined for any PDS with linearly independent cyclical shifts, its disadvantage in output signal/fluctuation noise ratio to the matched filter (MF) being solely determined by the type of periodic autocorrelation function (PACF) of the signal.

When choosing the signal for a radio channel with SLSF at the receiver end, it is natural to try to minimize this disadvantage; in this sense, PDS with PACF having zero sidelobes would be best, since the SLSF and MF are then identical. However, there are no signals of practical interest with such PACF among the PDS based on binary sequences consisting of ±1 [2]. In view of the obvious technical merits of binary PDS, it is clearly worth seeking coding rules whereby the sidelobes of the binary PDC can be completely suppressed at the cost of minimum energy loss. Below, we describe the synthesis of such rules, based on the mapping of the elements of q-ary M-sequences onto the set $\sigma=\{-1, 1\}$.

M-sequences over GF(q). Consider the finite field GF(q), where $q = p^w$, p is prime and w an integer. Let $g(x)=x^n+g_{n-1}x^{n-1}+g_{n-2}x^{n-2}+\ldots+g_0$, where $g_i\in GF(q)$, $i=\overline{0, n-1}$ is the normalized primitive polynomial of degree n over GF(q). Then, the recurrent sequence $\{c_i\}$ of elements of GF(q), generated by the rule

$$c_i=-g_{n-1}c_{i-1}-g_{n-2}c_{i-2}-\ldots-g_0c_{i-n},\ i=\ldots,-1,0,1,\ldots, \qquad (1)$$

is called an M-sequence over GF(q). A detailed theory of such sequences is given in [3]. Let us recall the following properties of $\{c_i\}$ [3,4]:

1) the period of $\{c_i\}$ is $M = q^n - 1$ bits;

2) in one period of the M-sequence, the zero element of GF(q) appears $q^{n-1} - 1$ times, and any other element q^{n-1} times;

3) let $m\not\equiv 0 \pmod h$, where $h=(q^n-1)/(q-1)$; then, among all the M pairs $\{c_i, c_{i+m}\}$, $i=\overline{0, M-1}$, the pair {0, 0}, where 0 is the zero element of GF(q), is encountered $q^{n-2} - 1$ times, and any other pair q^{n-2} times;

4) with $m=lh$, $l=\ldots,-1, 0, 1, \ldots$ $c_{i+m}=\mu^l c_i$, $i=\ldots,-1, 0, 1, \ldots$, where μ is the primitive element of field GF(q).

Binary sequences based on M-sequences. Let f be a mapping of elements of GF(q) into set $\sigma=\{-1, 1\}$ $(f: GF(q)\to\sigma)$, mapping M-sequence $\{c_i\}$ into binary sequence $\{a_i\}$, where $a_i=f(c_i)=\pm 1$, $i=\ldots,-1, 0, 1\ldots$. We can assume without loss of generality that $f(0) = 1$. Writing the nonzero

elements of GF(q) as μ^s and denoting their images in σ by $u_s = f(\mu^s)$, $s = \overline{0, q-2}$, consider the periodic sequence $\{u_s\} = \ldots, u_{q-2}, u_0, u_1, \ldots, u_{q-2}, \ldots$. Let t be the minimum positive number for which $u_s = u_{s+t}$, where the sum in the subscript is taken mod q - 1. Clearly, t is the period of sequence $\{u_s\}$ and hence divides into q - 1. Let r be the number of bits "-1" in the period t of sequence $\{u_s\}$; then, the number of elements of the multiplicative group of GF(q), mapped by mapping f into "-1," is (q - 1)r/t.

Now consider how the PACF of sequence $\{a_i\}$ is connected with mapping f:

$$R(m) = \sum_{i=0}^{M-1} a_i a_{((i+m,M))} = \sum_{i=0}^{M-1} f(c_i) f(c_{((i+m,M))}), \tag{2}$$

where ((x, y)) denotes the remainder of division of x by y:

$$((x, y)) \equiv x \pmod{y}, \quad 0 \leqslant ((x, y)) \leqslant y - 1.$$

We first put $m \not\equiv 0 \pmod{h}$. Using property 3 above, we obtain from (2):

$$R(m) = (q^{n-2} - 1) + 2q^{n-2} \sum_{s=0}^{q-2} f(\mu^s) + q^{n-2} \sum_{s=0}^{q-2} \sum_{v=0}^{q-2} f(\mu^s) f(\mu^v) = \tag{3}$$

$$= q^{n-2}\left(q - 2\frac{q-1}{t} r\right)^2 - 1, \quad m \not\equiv 0 \pmod{h}.$$

Hence, for all m which are not multiples of h, the values of the PACF of $\{a_i\}$: R(m) = R, are the same, and are entirely determined by the parameters t and r of mapping f.

Now let m = lh. Then, using the M-sequence properties 2 and 4, we obtain from (2):

$$R(lh) = (q^{n-1} - 1) + q^{n-1} \sum_{s=0}^{q-2} f(\mu^s) f(\mu^{s+l}) = q^{n-1} - 1 + q^{n-1} \frac{q-1}{t} \rho(l), \tag{4}$$

where

$$\rho(l) = \sum_{s=0}^{t-1} u_s u_{(s+l,t)} \tag{5}$$

is the PACF of sequence $\{u_s\}$. Since $\rho(t) = \rho(0)$, and hence R(th) = R(0), the period of sequence $\{a_i\}$ is $N = th = (q^n - 1)t/(q-1)$. Combining (3) and (4), we have

$$R(m) = R + (A + B\rho(l) - R)\delta_{m,lh}, \tag{6}$$

where δ_{ij} is Kronecker delta:

$$A = q^{n-1} - 1, \quad B = q^{n-1}\frac{q-1}{t}. \tag{7}$$

Sidelobe suppression loss. It was shown in [5] that the loss in signal/noise ratio accompanying complete suppression of the sidelobes of sequence $\{a_i\}$ in period N = th, is characterized by the factor

$$\gamma = \frac{q_{MF}}{q} = \frac{E}{N} \sum_{k=0}^{N-1} \xi_k^{-1} \geqslant 1, \tag{8}$$

where q_{MF} and q are the main signal peak to noise power ratios at MF and SLSF outputs, respectively, E = R(0), and

$$\xi_k = \sum_{m=0}^{N-1} R(m) \exp\left(-j\frac{2\pi}{N} km\right), \quad k = 0, 1, \ldots \tag{9}$$

are the components of the discrete Fourier transform (DFT) of PACF of $\{a_i\}$.

Using (6) in (9), we arrive at the result

$$\xi_k = \begin{cases} t(R(h-1)+A) + B\zeta_0, & k \equiv 0 \pmod N, \\ (A-R)t + B\zeta_0, & k \equiv 0 \pmod t,\ k \not\equiv 0 \pmod N, \\ B\zeta_k, & k \not\equiv 0 \pmod t. \end{cases} \tag{10}$$

In these last expressions,

$$\zeta_k = \sum_{l=0}^{t-1} \rho(l) \exp\left(-j\frac{2\pi kl}{t}\right),\ k = 0, 1, \ldots \tag{11}$$

are the components of the DFT of PACF of sequence $\{u_s\}$, while

$$\zeta_0 = \left(\sum_{s=0}^{t-1} u_s\right)^2 = (t-2r)^2.$$

Now, writing (8) in the form

$$\gamma = \frac{(q-1)^2}{(q^{n-1}(q(t-2r)+2r)-t)^2} + \frac{q^{n-1}-1}{4q^{n-3}r^2(q-1)} + \\ + \frac{q^n-1}{(q-1)\,q^{n-1}} \sum_{k=1}^{t-1} \zeta_k^{-1}, \tag{12}$$

then substituting from (10) in the light of (7), we can directly connect the loss in SLSF with the order q of the basic field and the type of mapping of GF(q) into σ.

For long sequences (n ≫ 1), (12) simplifies to

$$\gamma_\infty = \begin{cases} \dfrac{q}{q-1}\left\{1 + \sum_{k=1}^{q-2} \zeta_k^{-1}\right\} & \text{for } q = 2^w,\ t = q-1,\ r = q/2, \\ \dfrac{q}{q-1}\left\{\dfrac{q}{4r^2} + \sum_{k=1}^{t-1} \zeta_k^{-1}\right\} & \text{otherwise} \end{cases} \tag{13}$$

Using (12) and (13), we can find the binary sequences of the class in question with low values of γ. The relevant computational procedure can be computerized in the form of a search for extrema of γ with fixed q when variables t and r are varied (i.e., the period of $\{u_s\}$, which must always divide into q - 1, and the number of "-1" symbols in the period of $\{u_s\}$), and for different mappings of $u_s = f(\mu^s)$ with given t and r (which appear in (12) and (13) via the DFT components ζ_K).

If we confine ourselves for a rough guide to long sequences, i.e., use (13), we can greatly restrict the range of variation of t and r. In fact, we note that

$$t^{-1} \sum_{k=0}^{t-1} \zeta_k = t^{-1}\left((t-2r)^2 + \sum_{k=1}^{t-1} \zeta_k\right) = \rho(0) = t,$$

whence

$$\sum_{k=1}^{t-1} \zeta_k = 4r(t-r). \tag{14}$$

It is easily shown that, under condition (14), the set of values $\zeta_k = 4r(t-r)/(t-1)$, $k = \overline{1, t-1}$ minimizes the form $\sum_{k=1}^{t-1} \zeta_k^{-1}$, the minimum being $(t-1)^2/4r(t-r)$. Hence, instead of (13), we can write

$$\gamma_\infty \geqslant \begin{cases} 2 - & \text{for } q = 2^w,\ t = q-1,\ r = q/2, \\ \dfrac{q}{q-1}\left(\dfrac{q}{4r^2} + \dfrac{(t-1)^2}{4r(t-r)}\right) - & \text{otherwise} \end{cases} \tag{15}$$

Clearly, sequences with parameters corresponding to the top line of (15) (in particular, binary M-sequences [2]), are of no interest, since they lose half their energy with sidelobe suppression. Moreover, as may be seen from the bottom line of (15), necessary conditions for γ_∞ to be close to 1 are $q/4r^2 \leqslant 1$ and $(t-1)^2/4r(t-r) \leqslant 1$. The second of these inequalities imposes restrictions on r ($t-\sqrt{2t-1})/2 \leqslant r \leqslant (t+\sqrt{2t-1})/2$), whereas the first, since $t \geq r$, fixes the limits $t\sqrt{q/2} \leqslant t \leqslant q-1$.

The present method allows interesting families of binary sequences to be found without having recourse to computer synthesis. The relevant coding rules here correspond to the trivial mappings f: GF(q) → σ. First take an example leading to a familiar family. Let t = r = 1, i.e., the entire multiplicative group of GF(q) maps into the element "-1" of set σ. In other words $\{a_i\}$ only contains "+1" symbols at the positions where zero elements of GF(q) appear in the M-sequence $\{c_i\}$. It is easily seen that such a mapping f generates the so-called Singer codes [2], which exist for any periods $N=(q^n-1)/(q-1)$. The second term in braces in (13) vanishes here, and $\gamma_\infty=q^2/4(q-1)$. The minimum of this quantity corresponds to Singer codes over GF(3) and is equal to γ_∞ = 1.125, which corresponds to an 0.51-dB loss in threshold signal due to SLSF mismatch.

Now let r = t - 1, i.e., in each subset of elements $\{\mu^{st}, \mu^{st+1}, \ldots, \mu^{st+t-1}\}$, $s=\overline{1, (q-1)/t}$, only one element maps into "+1," and the rest into "-1." Then, in accordance with (5),

$$\rho(l)=\begin{cases} t, & l \equiv 0 \pmod t, \\ t-4, & l \not\equiv 0 \pmod t, \end{cases}$$

which, after substitution in (11), gives $\zeta_k=4$, $k \not\equiv 0 \pmod t$, after which we obtain from (13):

$$\gamma_\infty = \frac{q}{4(q-1)}\left\{\frac{q}{(t-1)^2}+(t-1)\right\}. \qquad (16)$$

The minimum of (16), regarded as a function of t, is $\gamma_{\infty\min} = 3q\sqrt[3]{q}/4\sqrt[3]{4}(q-1)$, and is reached for $t_{opt} = \sqrt[3]{2q}+1$. Hence, as the period of $\{u_s\}$, we need to choose a divisor of q - 1 closest to t_{opt}. Moreover, $\gamma_{\infty\ \min}$ increases with q, with the result that low loss can be achieved in the SLSF for a given coding rule, only with relatively small q.

Table 1

	q, t, r	n	2	3	4	5	6	γ_∞
1	3, 1, 1	N	4	13	40	121	364	1,125
		γ	1,000	1,040	1,088	1,112	1,120	
2	5, 4, 3	N	24	124	624	3124	15624	1,111
		γ	1,067	1,098	1,108	1,111	1,111	
3	7, 3, 2	N	24	171	1200	8403	58824	1,094
		γ	1,071	1,083	1,092	1,094	1,094	
4	13, 4, 2	N	56	732	9520	123764	1608936	1,204
		γ	1,171	1,201	1,204	1,204	1,204	

We now turn to some concrete data. In Table 1, we show loss γ for the coding rules of the present section, with several values of parameters q, t, r, evaluated both for finite lengths $N=(q^n-1)t/(q-1)$, in accordance with (12), and also for n → ∞ (γ_∞). In particular, the table demonstrates the existence of extremely interesting families of sequences with sidelobe suppression loss less than for the familiar Singer codes (row 1). For instance, for the sequences of lines 2 and 3, the loss 10 lg γ_∞ in threshold signal is not more than 0.46 and 0.39 dB, respectively.

Let us give an example to demonstrate the algorithm for generating the described sequences. Let q = 5, t = 4, r = 3 (row 2 of Table 1), while n = 2. A primitive polynomial of degree 2 over GF(5) is, in particular, $\{c_i\}=\ldots, 0, 1, 1, 4, 2, 4, 0, 2, 2, 3, 4, 3, 0, 4, 4, 1, 3, 1, 0, 3, 3, 2, 1, 3, 0, 1, 1, \ldots$. We now replace all the zeros, and e.g., all the ones by "+1," the

other symbols of $\{c_i\}$ are replaced by "-1." The resulting binary sequence is $\{a_i\}$=..., 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, ..., which is easily shown to have the PACF

$$R(m) = 20\delta_{m,24l} + 4\delta_{m,6l};\ m, l = \ldots, -1, 0, 1, \ldots.$$

With this PACF, γ_∞ is very easily evaluated; it is 1.067 (0.28 dB).

An example of a more complicated coding rule, obtained by computer minimization of (13) with respect to mappings f: $\mu^s \to u^s$, $s=0, \overline{t-1}$, is provided by the rule, generating binary sequences of length $N=23^n-1$, $n=2, 3, \ldots$, with parameters t = 22, r = 12. The corresponding mapping f replaces by the symbols "+1" ten elements of the multiplicative group of GF(q), having indices s equal to 0, 2, 3, 4, 5, 8, 11, 12, 13, 18. The 12 remaining elements are replaced by "-1." For sequences of this family, γ_∞ is not greater than 1.13.

To sum up, generation of binary sequences on the basis of the mapping of elements of q-ary M-sequences into the set {-1, 1}, offers scope for synthesizing signals with low loss in the SLSF. The particular interest of sequences of this class lies in the simplicity of the generating circuits, consisting of a standard generator of M-sequence $\{c_i\}$ on the basis of a q-ary shift register with linear feedback (generator of field $GF(q^n)$ [6]) and a logic converter, associating with each symbol of $\{c_i\}$ its mapping in accordance with the chosen rule f: $GF(q) \to \sigma$.

REFERENCES

1. V. P. Ipatov, "Full suppression of sidelobes of periodic correlation functions of PSK signals," Radiotekhnika i elektronika, vol. 22, no. 8, p. 1600, 1977.
2. M. B. Sverdlik, Optimal Discrete Signals [in Russian], Sovetskoe radio Press, Moscow, 1975.
3. N. Tsirler, "Linear recursion relations," Kiberneticheskii Sbornik, no. 6, p. 55, 1963; IL Press, Moscow.
4. I. N. Amiantov, Selected Topics in Statistical Communications Theory [in Russian], Sovetskoe radio Press, Moscow, 1971.
5. V. P. Ipatov, "Selection of pair of periodic PSK signal-filter," Izv. VUZ. Radioelektronika [Radio Electronics and Communications Systems], vol. 21, no. 4, p. 60, 1978.
6. A. Gill, Linear Sequential Machines [Russian translation], Nauka Press, Moscow, 1974.

13 October 1978