nonzero coefficients. We first computed, for each such linear function and each balanced F and G, the value of

$$\phi_M = \sum_{s,t,u \in \mathrm{GF}(q)} F(s)G(t)F(u)G(M(s,t,u)).$$

For a given i, we do not know which such M arise, but they must all be distinct. Since there are q^2+q values of j for which $\alpha^{j-i} \in \mathrm{orbit}(\alpha^\tau)$, we get an upper bound on $\mu(i,F,G)$ by summing the q^2+q largest positive values of ϕ_M, doing the same for the negative values, and taking the maximum of the absolute values of these two sums. Unfortunately, this computation is doubly exponential in e, where $q=2^e$. Exploiting symmetry in the set of balanced functions, for $e=4$ this computation took a few hours on a DEC 3000 Alpha-based workstation. When $e=5$, we estimate the computation would take several years.

For $e=4$, $\mu(i,F,G)$ is bounded by 52 352. This contrasts with the cruder estimate used in the previous section of 1 114 112. Thus we improve our estimate by a factor of about 21.3. Any choice of n gives us a family of 12 870 sequences of period $2^{4n}-1$ such that the variance of the partial period crosscorrelations of any two sequences with window size ν is at most $13.8 \cdot \nu$.

For $e=3$, $\mu(i,F,G)$ is bounded by 1280. This contrasts with the cruder estimate used in the previous section of 36 864. Thus we improve our estimate by a factor of about 28.8. Any choice of n gives us a family of 70 sequences of period $2^{3n}-1$ such that the variance of the partial period crosscorrelations of any two sequences with window size ν is at most $3.5 \cdot \nu$.

These are still worst case scenarios, and it is likely that the actual value of the variance is considerably smaller.

REFERENCES

[1] A. H. Chan and R. Games, "On the linear span of binary sequences from finite geometries, q odd," in *Proc. Crypto 1986.* (Santa Barbara, CA), pp. 405–417.

[2] A. H. Chan, M. Goresky, and A. Klapper, "Cross correlations of linearly and quadratically related geometric sequences and GMW sequences," *Discr. Appl. Math.*, vol. 46, pp. 1–20, 1993.

[3] S. Golomb, *Shift Register Sequences.* Laguna Hills, CA: Aegean Park Press, 1982.

[4] B. Gordon, W. H. Mills and L. R. Welch, "Some new difference sets," *Canad. J. Math.*, vol. 14, pp. 614–625, 1962.

[5] T. Høholdt, H. E. Jensen, and J. Justesen, "Aperiodic correlations and the merit factor of a class of binary sequences," *IEEE Trans. Inform. Theory*, vol. IT-31, pp. 549–552, 1985.

[6] A. Klapper, A. H. Chan, and M. Goresky, "Cascaded GMW sequences," *IEEE Trans. Inform. Theory.*, vol. 39, pp. 177–183, Jan. 1993.

[7] A. Klapper and M. Goresky, "Partial period autocorrelations of geometric sequences," *IEEE Trans. Inform. Theory*, vol. 40, pp. 494–502, Mar. 1994.

[8] P. V. Kumar, "The partial-period correlation moments of arbitrary binary sequences," in *Conf. Rec. GLOBECOM '85, IEEE Global Telecommunications Conf.* New York, 1985, IEEE Publications.

[9] R. Lidl and H. Niederreiter, *Finite Fields, Encyclopedia of Mathematics*, vol. 20. Cambridge, UK: Cambridge Univ. Press, 1983.

[10] R. J. McEliece, *Finite Fields for Computer Scientists and Engineers.* Boston, MA: Kluwer, 1987.

[11] O. Rothaus, "On bent functions," *J. Combinatorial Theory, Ser. A*, vol. 20, pp. 300–305, 1976.

[12] R. A. Rueppel, *Analysis and Design of Stream Ciphers.* New York: Springer-Verlag, 1986.

[13] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 548–553, 1984.

[14] M. K. Simon, J. Omura, R. A. Scholtz, and B. Levitt, *Spread-Spectrum Communications*, vol. 1. Computer Science Press, 1985.

Generalization of GMW Sequences and No Sequences

Jong-Seon No, *Member, IEEE*

***Abstract*— In this correspondence, GMW sequences and families of No sequences are generalized. Generalized GMW sequences have ideal autocorrelation and balance properties and generalized No sequences also have optimal correlation properties in terms of Welch's lower bound. The linear spans of the generalized GMW and No sequences appear to be large although we do not at present have a closed-form expression for the linear span. A count of the numbers of cyclically distinct generalized GMW sequences and generalized No sequences that can be constructed is provided. Generalized GMW sequences have also been found in the literature by Klapper *et al.* under the name "cascaded GMW sequences."**

***Index Terms*—Generalized GMW sequences, generalized No sequences, linear span, autocorrelation values, correlation functions.**

I. INTRODUCTION

Pseudonoise (PN) sequences have been successfully employed as spreading sequences for low probability of intercept and as signature sequences for code-division multiple access in a spread-spectrum communication system [2]. Several characteristics which are desirable in a family of PN sequences for the above applications are long period, low out-of-phase autocorrelation values, low crosscorrelation values, low nontrivial partial-period correlation values, large linear span, a balance of symbols, the availability of a large number of distinct sequences, and ease of implementation.

Several families of pseudorandom sequences having good correlation properties such as m-sequences, GMW sequences, Kasami sequences, Gold sequences, bent sequences, No sequences, and d-form sequences [1], [4]–[6], [8]–[11], [13]–[15] have been discovered. But the linear spans of m-sequences, Kasami sequences, and Gold sequences are very short. PN sequences with large linear span, which are needed for low probability of intercept system, have been found such as GMW sequences, bent sequences, and No sequences.

In this correspondence, the generalization of GMW sequences is introduced, which has ideal autocorrelation and balance properties. Families of No sequences are generalized, which also have optimal correlation properties in terms of Welch's lower bound [12]. The linear spans of the generalized GMW sequences and generalized No sequences appear to be very large although we do not at present have closed-form expressions for the linear spans. In Section II, GMW sequences are generalized, those ideal full-period autocorrelation properties are derived, and a count of the number of cyclically distinct generalized GMW sequences that can be constructed is provided. It is also shown how the families of No sequences can be generalized in an identical fashion and optimal correlation properties are derived in Section III. Here, the number of distinct families of generalized No sequences of given period is derived, too. Proofs of all theorems, which are just straightforward extensions of the proofs for GMW and No sequences [5], [6], [8] are omitted.

Manuscript received October 13, 1994; revised May 29, 1995. The work of some parts of this correspondence were carried out independently in the author's Ph.D. dissertation [5], in the paper by Klapper *et al.* [13], and in the paper by Klapper [14].

The author is with the Department of Electronic Engineering, Kon-kuk University, 93-1 MoJin-Dong, KwangJin-Gu, Seoul, 133-701, Korea.

Publisher Item Identifier S 0018-9448(96)00020-X.

II. Generalization of GMW Sequences

The GMW sequences analyzed in [8] are the characteristic functions of certain Gordon, Mills, and Welch difference sets. We consider the characteristic functions of a larger class of GMW difference sets. These sequences, of course, share the ideal autocorrelation and balance properties of an m-sequence and may be regarded as a straightforward generalization of the GMW sequences considered in [8]. We begin by defining generalized GMW sequences.

Definition 1: Let n and m_i, $i = 1, 2, \cdots, d$, be integers satisfying

$$m_d \mid n \text{ and } m_i \mid m_{i+1}, \quad \text{for } 1 \le i \le d-1. \tag{1}$$

A *generalized GMW sequence* is then defined as the multiple trace function sequence of period N given by

$$s_g(t) = \mathrm{tr}_1^{m_1}\{[\mathrm{tr}_{m_1}^{m_2}\{[\mathrm{tr}_{m_2}^{m_3}\{\cdots\{[\mathrm{tr}_{m_d}^{n}(\alpha^t)]^{r_d}\}\cdots\}]^{r_2}\}]^{r_1}\} \tag{2}$$

where α is an element of order $N = 2^n - 1$ and for $1 \le i \le d$

$$\gcd(r_i, 2^{m_i} - 1) = 1, \quad 1 \le r_i < 2^{m_i} - 1. \tag{3}$$

We use the base-T expression of t to obtain a two-variable representation.

$$t = t_1 \cdot T + t_2, \quad 0 \le t_1 \le 2^{m_d} - 2, \quad 0 \le t_2 \le T - 1 \tag{4}$$

where $T = \frac{2^n-1}{2^{m_d}-1}$. Using a two-variable representation of t, the GMW sequences can be expressed in the two-dimensional representation (matrix form). That is, we can write the GMW sequence, $s_g(t)$ in the first row from $t = 0$ to $T - 1$, in the second row from $t = T$ to $2T - 1$, in the third row from $t = 2T$ to $3T - 1$, etc. This yields the expression

$$s_g(t) = \mathrm{tr}_1^{m_1}\{[\mathrm{tr}_{m_1}^{m_2}\{[\mathrm{tr}_{m_2}^{m_3}\{\cdots\{\beta^{r_d \cdot t_1} \cdot [\mathrm{tr}_{m_d}^{n}(\alpha^{t_2})]^{r_d}\}\cdots\}]^{r_2}\}]^{r_1}\} \tag{5}$$

where $\beta = \alpha^T$ and the subsequence of period $2^{m_d} - 1$ obtained by fixing t_2 is given by

$$s_{\mathrm{sub}}(t_1) = \mathrm{tr}_1^{m_1}\{[\mathrm{tr}_{m_1}^{m_2}\{[\mathrm{tr}_{m_2}^{m_3}\{\cdots\{[\mathrm{tr}_{m_{d-1}}^{m_d}(\delta^{t_1})]^{r_{d-1}}\}\cdots\}]^{r_2}\}]^{r_1}\} \tag{6}$$

where $\delta = \beta^{r_d}$ is a primitive element of GF(2^{m_d}) and the associated phase function $f(\alpha, \cdot)$ is defined by

$$\beta^{f(\alpha,t_2)} = \mathrm{tr}_{m_d}^{n}(\alpha^{t_2}) \tag{7}$$

where $\beta^{-\infty} = 0$.

For the particular case when $d = 2$, the above sequence has the expression

$$s_g(t) = \mathrm{tr}_1^{m_1}\{[\mathrm{tr}_{m_1}^{m_2}\{[\mathrm{tr}_{m_2}^{n}(\alpha^t)]^{r_2}\}]^{r_1}\} \tag{8}$$

while the subsequence of period $2^{m_2} - 1$ is given by

$$s_{\mathrm{sub}}(t_1) = \mathrm{tr}_1^{m_1}\{[\mathrm{tr}_{m_1}^{m_2}(\delta^{t_1})]^{r_1}\} \tag{9}$$

where $\delta = \alpha^{T \cdot r_2}$. Thus in this case, the subsequence is a GMW sequence. The locations of the all-zero columns in the two-dimensional representation of the above generalized GMW sequence and the GMW sequence remain unchanged. The only difference is that the columns of m-sequences in the GMW sequence are now replaced by GMW sequences. As GMW sequences have the balance property, the above generalized GMW sequences in (8) also possess the balance property. Using the same proof as in the case of GMW sequences [8], we can prove that this generalized GMW sequence has the ideal full-period autocorrelation property. By mathematical induction, it is easy to prove that all generalized GMW sequences with d arbitrary have the balance property and ideal full-period autocorrelation values.

The generalized GMW sequence defined in (2) has the ideal full-period autocorrelation values [13], i.e.

$$R_a(\tau) = \begin{cases} N, & \tau = 0 \bmod N \\ -1, & \text{otherwise.} \end{cases} \tag{10}$$

By extending the proof used in counting the number of cyclically distinct GMW sequences available (of period N), we can determine the number of cyclically distinct generalized GMW sequences of given period that can be generated.

Theorem 1: The number of cyclically different generalized GMW sequences of given period N is given by

$$N_{g\mathrm{GMW}} = \frac{\phi(2^n - 1)}{n} \cdot \prod_{i=1}^{d} \frac{\phi(2^{m_i} - 1)}{m_i} \tag{11}$$

where $\phi(\cdot)$ is Euler's *phi* function.

It is very difficult to find an exact closed-form expression for the linear span for a generalized GMW sequence. The author's conjecture is that the linear span of a generalized GMW sequence is larger than that of the associated GMW sequence. Implementation, of course, is more complicated than in the case of GMW sequences.

III. Generalization of No Sequences

The generalization of No sequences may be carried out exactly as in the case of GMW sequences. By replacing the subsequences, which are m-sequences, by generalized GMW sequences in the two-variable representation of No sequences, we obtain generalized families of No sequences [6]. Proofs for optimality of the correlation values of the generalized No sequence family can be easily given using the proof given in [6] for the No sequence family and the correlation property of subsequences, the *columns* of the generalized No sequences which in this case are generalized GMW sequences. The balance property of families of generalized No sequences is identical to that of the No sequence families because a generalized GMW sequence also has the balance property. The definition of a generalized No sequence family is given as follows.

Definition 2: Let n and m_i, $i = 1, 2, \cdots, d$, be integers satisfying

$$n = 2 \cdot m_d \text{ and } m_i \mid m_{i+1}, \quad \text{for } 1 \le i \le d-1. \tag{12}$$

A family of *generalized No sequences*

$$S_g = \{s_i(t) \mid 0 \le t \le N-1, \quad 1 \le i \le 2^m\} \tag{13}$$

is a set of multiple trace function sequences defined as

$$s_i(t) = \mathrm{tr}_1^{m_1}\{[\mathrm{tr}_{m_1}^{m_2}\{[\mathrm{tr}_{m_2}^{m_3}\{\cdots\{[\mathrm{tr}_{m_d}^{n}(\alpha^{2t}) + \gamma_i \cdot \alpha^{T \cdot t}]^{r_d}\}\cdots\}]^{r_2}\}]^{r_1}\} \tag{14}$$

where $N = 2^n - 1$, γ_i is in GF(2^{m_d}), $T = 2^{m_d} + 1$, and for $1 \le i \le d$,

$$\gcd(r_i, 2^{m_i} - 1) = 1, \quad 1 \le r_i < 2^{m_i} - 1. \tag{15}$$

The subsequences of period $2^{m_d} - 1$ of the generalized No sequences in (14) are shown to be generalized GMW sequences using the two-variable representation of the generalized No sequences. Using the expansion

$$t = t_1 \cdot T + t_2, \quad 0 \le t_1 \le 2^{m_d} - 2, \quad 0 \le t_2 \le T - 1, \tag{16}$$

we obtain the two-variable representation

$$s_g(t) = \mathrm{tr}_1^{m_1}\{[\mathrm{tr}_{m_1}^{m_2}\{\cdots\{\beta^{2r_d \cdot t_1} \cdot [\mathrm{tr}_{m_d}^{n}(\alpha^{2t_2}) + \gamma_i \cdot \alpha^{T \cdot t_2}]^{r_d}\}\cdots\}]^{r_1}\} \tag{17}$$

TABLE I
EXAMPLES OF NONTRIVIAL GENERALIZED NO SEQUENCES

n	Period, N	Generalized No Sequences
12	4,095	$tr_1^3\{[tr_3^6\{[tr_6^{12}(\alpha^{2t})+\gamma_i\cdot\alpha^{65t}]^r\}]^3\}$
		$gcd(r,63)=1,\ 1\le r<63$
16	65,535	$tr_1^4\{[tr_4^8\{[tr_8^{16}(\alpha^{2t})+\gamma_i\cdot\alpha^{257t}]^r\}]^7\}$
		$gcd(r,255)=1,\ 1\le r<255$
18	262,143	$tr_1^3\{[tr_3^9\{[tr_9^{18}(\alpha^{2t})+\gamma_i\cdot\alpha^{513t}]^r\}]^3\}$
		$gcd(r,511)=1,\ 1\le r<511$
20	1,048,575	$tr_1^5\{[tr_5^{10}\{[tr_{10}^{20}(\alpha^{2t})+\gamma_i\cdot\alpha^{1025t}]^{r_2}\}]^{r_1}\}$
		$gcd(r_1,31)=1,\ 1\le r_1<31,\ gcd(r_2,1023)=1,\ 1\le r_2<1023$
24	16,777,215	$tr_1^3\{[tr_3^{12}\{[tr_{12}^{24}(\alpha^{2t})+\gamma_i\cdot\alpha^{4097t}]^r\}]^3\}$
		$gcd(r,4095)=1,\ 1\le r<4095$
		$tr_1^4\{[tr_4^{12}\{[tr_{12}^{24}(\alpha^{2t})+\gamma_i\cdot\alpha^{4097t}]^r\}]^7\}$
		$gcd(r,4095)=1,\ 1\le r<4095$
		$tr_1^6\{[tr_6^{12}\{[tr_{12}^{24}(\alpha^{2t})+\gamma_i\cdot\alpha^{4097t}]^{r_2}\}]^{r_1}\}$
		$gcd(r_1,63)=1,\ 1\le r_1<63,\ gcd(r_2,4095)=1,\ 1\le r_2<4095$
		$tr_1^3\{[tr_3^6\{[tr_6^{12}\{[tr_{12}^{24}(\alpha^{2t})+\gamma_i\cdot\alpha^{4097t}]^{r_2}\}]^{r_1}\}]^3\}$
		$gcd(r_1,63)=1,\ 1\le r_1<63,\ gcd(r_2,4095)=1,\ 1\le r_2<4095$
28	268,435,455	$tr_1^7\{[tr_7^{14}\{[tr_{14}^{28}(\alpha^{2t})+\gamma_i\cdot\alpha^{16385t}]^{r_2}\}]^{r_1}\}$
		$gcd(r_1,127)=1,\ 1\le r_1<127,$
		$gcd(r_2,16383)=1,\ 1\le r_2<16383$

where $\beta=\alpha^T$ is a primitive element of GF(2^{m_d}) and the subsequence of period $2^{m_d}-1$ is given by

$$s_{\rm sub}(t_1)=\mathrm{tr}_1^{m_1}\{[\mathrm{tr}_{m_1}^{m_2}\{[\mathrm{tr}_{m_2}^{m_3}\times\{\cdots\{[\ \mathrm{tr}_{m_{d-1}}^{m_d}(\delta^{2t_1})]^{r_{d-1}}\}\cdots\}]^{r_2}\}]^{r_1}\} \quad (18)$$

where $\delta=\beta^{r_d}$ is a primitive element of GF(2^{m_d}) and the phase function $f_i(\alpha,\cdot)$ is defined via

$$\beta^{f_i(\alpha,t_2)}=\mathrm{tr}_{m_d}^{n}(\alpha^{2t_2})+\gamma_i\cdot\alpha^{T\cdot t_2}. \quad (19)$$

The phase function $f_i(\alpha,t_2)$ of generalized No sequences is the same as that of No sequences and the subsequences have ideal autocorrelation values because generalized GMW sequences have the ideal full-period autocorrelation property. Therefore, the family of generalized No sequences has the optimal correlation property in terms of Welch's lower bound [6], [12] and the proof for the correlation properties of No sequences [6], [8] works for the case of generalized No sequences as well. Further, the distribution of correlation values in a family of generalized No sequences is exactly the same as those in a family of No sequences and a family of Kasami sequences.

Theorem 2: The full-period correlation function $R(\tau)$ of the family of generalized No sequences defined in (14) takes on values in the set

$$\{-2^{m_d}-1,-1,2^{m_d}-1\} \quad (20)$$

which means that the generalized No sequences have optimal correlation properties.

We already know that the counting problem for GMW sequences is the same as that of No sequences [6], [8]. Therefore, counts for the number of cyclically distinct generalized GMW sequences and generalized No sequence families are the same.

Theorem 3: The number of distinct families of generalized No sequences for a given period N is given as

$$N_{g\rm No}=\frac{\phi(2^n-1)}{n}\cdot\prod_{i=1}^{d}\frac{\phi(2^{m_i}-1)}{m_i} \quad (21)$$

where $\phi(s)$ is Euler's *phi* function.

The author's conjecture is that the linear span of a generalized No sequence is larger than that of the associated No sequences and that it is possible to derive the lower and upper bounds on the linear span of the generalized No sequences. Linear spans for some cases of generalized No sequences are found by Klapper [14]. Implementation in the case of a generalized No sequence family needs to be investigated. All of nontrivial generalized No sequences are listed in Table I for period $N\le 2^{28}-1$.

REFERENCES

[1] S. W. Golomb, *Shift Register Sequences*. San Francisco, CA: Holden-Day, 1967; revised edition, Laguna Hills, CA: Aegean Park Press, 1982.

[2] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications. Volume I.* Rockville, MD: Comput. Sci. Press, 1985.

[3] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[4] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, pp. 593–620, May 1980.

[5] J. S. No, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," Ph.D. dissertation, Univ. So. Calif., Los Angeles, May 1988.

[6] J. S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans. Inform. Theory*, vol. IT-35, no. 2, pp. 371–379, Mar. 1989.

[7] ——, "Exact linear span expressions for a family of recently discovered binary pseudorandom sequences," in *Proc. 1988 IEEE Int. Symp. on Information Theory* (Kobe, Japan, June 19–24, 1988), p. 10.

[8] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. 30, pp. 548–553, May 1984.

[9] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 858–864, Nov. 1982.

[10] P. V. Kumar, R. A. Scholtz, and L. R. Welch, "Generalized bent functions and their properties," *J. Combinatorial Theory, Ser. A*, vol. 40, pp. 90–107, Sept. 1985.

[11] R. Gold, "Optimal binary sequences for spread spectrum multiplexing," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 619–621, Oct. 1967.

[12] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inform. Theory*, vol. IT-20, pp. 397–399, May 1974.

[13] A. Klapper, A. H. Chan, and M. Goresky, "Cascaded GMW sequences," *IEEE Trans. Inform. Theory*, vol. 39, pp. 177–183, Jan. 1993.

[14] A. Klapper, "d-form sequences: Families of sequences with low correlation values and large linear spans," *IEEE Trans. Inform. Theory*, vol. 41, pp. 423–431, Mar. 1995.

[15] M. Antweiler and L. Bömer, "Complex sequences over GF(p^M) with a two-level autocorrelation function and a large linear span," *IEEE Trans. Inform. Theory*, vol. 38, pp. 120–130, Jan. 1992.