Improved p-ary Codes and Sequence Families from Galois Rings

San Ling[1] and Ferruh Özbudak[2]

[1] Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Republic of Singapore
matlings@nus.edu.sg*

[2] Department of Mathematics and Institute of Applied Mathematics, Middle East Technical University, İnönü Bulvarı, 06531, Ankara, Turkey
ozbudak@math.metu.edu.tr†

Abstract. In this paper, a recent bound on some Weil-type exponential sums over Galois rings is used in the construction of codes and sequences. The bound on these type of exponential sums provides a lower bound for the minimum distance of a family of codes over $\mathbb{F}_p$, mostly nonlinear, of length p^{m+1} and size $p^2 \cdot p^{m\left(D - \lfloor \frac{D}{p^2} \rfloor\right)}$, where $1 \leq D \leq p^{m/2}$. Several families of pairwise cyclically distinct p-ary sequences of period $p(p^m - 1)$ of low correlation are also constructed. They compare favorably with certain known p-ary sequences of period $p^m - 1$. Even in the case $p = 2$, one of these families is slightly larger than the family $Q(D)$ of [H-K, Section 8.8], while they share the same period and the same bound for the maximum non-trivial correlation.

1 Introduction

Bounds on exponential sums over finite fields, such as the Weil-Carlitz-Uchiyama bound, have been found to be useful in applications such as coding theory and sequence designs. The analog of the Weil-Carlitz-Uchiyama bound for Galois rings was presented by [K-H-C]. An improved bound for a related Weil-type exponential sum over Galois rings of characteristic 4, which is also sometimes called the trace of exponential sums, was obtained in [H-K-M-S] and was used in [S-K-H] to construct a family of binary codes with the same length and size as the Delsarte-Goethals codes, but whose minimum distance is significantly bigger. The shortening of these codes also leads to efficient binary sequences.

* The research of this author is partially supported by NUS-ARF research grant R-146-000-029-112 and DSTA research grant POD0411403.

† The research of this author is partially supported by the Turkish Academy of Sciences in the framework of Young Scientists Award Programme (F.Ö./TÜBA-GEBIP/2003-13).

T. Helleseth et al. (Eds.): SETA 2004, LNCS 3486, pp. 236–242, 2005.

Recently, an analog of the bound of [H-K-M-S] was obtained for Galois rings of characteristic p^2, for all primes p [L-O]. In this paper, we explore some applications of this bound to the construction of codes and sequences.

We fix the following conventions throughout the paper: p is a prime number; $m \geq 2$ is an integer; $\mathbb{F}_p$ and $\mathbb{F}_{p^m}$ are finite fields of cardinality p and p^m; $\mathrm{GR}(p^2, m)$ is a Galois ring of characteristic p^2 with cardinality p^{2m}; $\mathbb{Z}_{p^2}$ is the ring of integers modulo p^2; $\mathrm{Tr}_m : \mathrm{GR}(p^2, m) \rightarrow \mathbb{Z}_{p^2}$ is the trace map from $\mathrm{GR}(p^2, m)$ onto $\mathbb{Z}_{p^2}$; Γ_m is the Teichmüller set in $\mathrm{GR}(p^2, m)$; β is a primitive $(p^m - 1)$-th root of unity in $\mathrm{GR}(p^2, m)$; $\rho : \mathrm{GR}(p^2, m) \rightarrow \mathrm{GR}(p^2, m)/p\mathrm{GR}(p^2, m) \cong \mathbb{F}_{p^m}$ is reduction modulo p map in $\mathrm{GR}(p^2, m)$. We extend ρ to the polynomial ring mapping $\rho : \mathrm{GR}(p^2, m)[x] \rightarrow \mathbb{F}_{p^m}[x]$ by its action on the coefficients. Let Frob be the Frobenius operator on $\mathrm{GR}(p^2, m)$ (cf. [K-H-C], [L-O]). Frob is extended to $\mathrm{GR}(p^2, m)[x]$ naturally. A polynomial $f(x) \in \mathrm{GR}(p^2, m)[x]$ is called *non-degenerate* if it cannot be written in the form $f(x) = \mathrm{Frob}(g(x)) - g(x) + u \bmod p^2$, where $g(x) \in \mathrm{GR}(p^2, m)[x]$ and $u \in \mathrm{GR}(p^2, m)$.

2 $\mathbb{Z}_{p^2}$-Linear Codes

Definition 1. *For a finite $\mathbb{Z}_{p^2}$-module $S \subseteq \mathrm{GR}(p^2, m)[x]$, let*

$$S_0 = \{a(x) \in \Gamma_m[x] : \textit{there exists } b(x) \in \Gamma_m[x] \textit{ such that } a(x) + pb(x) \in S\},$$

and

$$S_1 = \{b(x) \in \Gamma_m[x] : \textit{there exists } a(x) \in \Gamma_m[x] \textit{ such that } a(x) + pb(x) \in S\}.$$

For a prime number p, the weight function w_p on $\mathbb{N}$ is defined as the sum of digits of the representation of $u \in \mathbb{N}$ in base p. For every $f(x) = a(x) + pb(x) \in \mathrm{GR}(p^2, m)[x]$, where $a(x),\ b(x) \in \Gamma_m[x]$ are uniquely determined, we recall that the *weighted degree* D_f of $f(x)$ is

$$D_f = \max\{p \deg(a(x)), \deg(b(x))\}.$$

For a positive integer D, let $I(D)$ be the set of positive integers

$$I(D) = \{i : i \not\equiv 0 \mod p \text{ and } 0 \leq i \leq D\}$$

and let $S(D) \subseteq \mathrm{GR}(p^2, m)[x]$ be the finite $\mathbb{Z}_{p^2}$-module

$$S(D) = \{f(x) \in \mathrm{GR}(p^2, m)[x] : f(x) = \sum_{i \in I(D)} f_i x^i \text{ and } D_f \leq D\}.$$

Let $f(x) = a(x) + pb(x)$ be a non-degenerate polynomial with $a(x), b(x) \in \Gamma_m[x]$. We recall some definitions which depend on $f(x)$. Let $I_f, J_f \subseteq \mathbb{N}$ be subsets defined as

$$a(x) = \sum_{i \in I_f} a_i x^i \text{ and } b(x) = \sum_{j \in J_f} b_j x^j, \text{ where } a_i, b_j \in \Gamma_m \setminus \{0\}.$$

We define nonnegative integers W_f, $l_{f,m}$ and $h_{f,m}$ as

$$W_f = \max\Big\{\ p\ \max\{w_p(i) \mid i \in I_f\},\quad \max\{w_p(j) \mid j \in J_f\}\ \Big\},$$

$$l_{f,m} = \left\lceil \frac{m}{W_f} \right\rceil - 1 \ \text{ and } \ h_{f,m} = \left\lfloor \frac{m}{W_f} \right\rfloor .$$

The following result is proved in [L-O].

Theorem 1. *For a non-degenerate polynomial $f(x) \in \mathrm{GR}(p^2, m)[x]$, we have*

$$\Big| \sum_{a \in \mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2}} \sum_{x \in \Gamma_m} e^{2\pi i \frac{\mathrm{Tr}_m(af(x))}{p^2}} \Big| \le p^{l_{f,m}+1} \left\lfloor \frac{p^{h_{f,m}} \frac{p^2-p}{2} (D_f - 1) \left\lfloor 2p^{\frac{m}{2} - h_{f,m}} \right\rfloor}{p^{l_{f,m}+1}} \right\rfloor .$$

Definition 2. *For $1 \le D \le p^{m/2}$, let*

$$W_D = \max\big\{W_f : f(x) \in S(D) \setminus \{0\}\big\},\ \ l_{D,m} = \left\lceil \frac{m}{W_D} \right\rceil - 1$$

and

$$h_{D,m} = \left\lfloor \frac{m}{W_D} \right\rfloor .$$

For $n \ge 1$, the Gray map (cf. [C], [G-S], [L-B], [L-S]) Φ over $\mathbb{Z}_{p^2}^n$ is defined as follows: For $u \in \mathbb{Z}_{p^2}$ let $u = r_0(u) + pr_1(u)$ with $r_0(u),\ r_1(u) \in \{0, 1, \ldots, p-1\}$. We denote the addition modulo p as $\oplus$. For $(u_0, u_1, \ldots, u_{n-1}) \in \mathbb{Z}_{p^2}^n$, we have $\Phi(u_0, u_1, \ldots, u_{n-1}) = (a_0, a_1, \ldots, a_{pn-1}) \in \mathbb{F}_p^{pn}$ such that for $0 \le j \le p-1$ and $0 \le t \le n-1$, $a_{jn+t} = r_1(u_t) \oplus jr_0(u_t)$.

Definition 3. *For $1 \le D \le p^{m/2}$, let $C(D)$ be the $\mathbb{Z}_{p^2}$-linear code of length p^m defined as $C(D) = \Big\{ \big(\mathrm{Tr}_m(f(0)) + u, \mathrm{Tr}_m(f(\beta)) + u, \ldots, \mathrm{Tr}_m(f(\beta^{p^m-1})) + u\big) : f(x) \in S(D)$ and $u \in \mathbb{Z}_{p^2} \Big\}$.*

Theorem 2. *For $1 \le D \le p^{m/2}$, $\Phi(C(D))$ is a p-ary code of length p^{m+1} of minimum distance*

$$d_{\min} \ge p^{m+1} - p^m - p^{l_{D,m}} \left\lfloor \frac{p^{h_{D,m}} \frac{p^2-p}{2} (D-1) \left\lfloor 2p^{\frac{m}{2} - h_{D,m}} \right\rfloor}{p^{l_{D,m}+1}} \right\rfloor \qquad (1)$$

and of size $\big|\Phi(C(D))\big| = p^2 \cdot p^{m\left(D - \lfloor \frac{D}{p^2} \rfloor\right)}$.

Next we consider the nonlinearity of $\Phi(C(D))$. Let T denote the set of ordered pairs $(a,b) \in \mathbb{F}_p^2$ such that $a+b \geq p$ (we identify $\mathbb{F}_p$ with $\{0,1,\ldots,p-1\}$). Let χ denote the characteristic function of T, i.e.,

$$\chi(a,b) = \begin{cases} 1 \text{ if } (a,b) \in T, \\ 0 \text{ otherwise.} \end{cases}$$

For $\mathbf{a} = (a_1,\ldots,a_n) \in \mathbb{F}_p^n$ and $\mathbf{b} = (b_1,\ldots,b_n) \in \mathbb{F}_p^n$, we define

$$\chi(\mathbf{a},\mathbf{b}) = (\chi(a_1,b_1),\ldots,\chi(a_n,b_n)) \in \mathbb{F}_p^n.$$

Recall that for $\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_n) \in \mathbb{Z}_{p^2}^n$, we denote $r_0(\boldsymbol{\alpha}) = (\rho(\alpha_1),\ldots,\rho(\alpha_n)) \in \mathbb{F}_p^n$. The following lemma is found in [L-B, Theorem 4.6].

Lemma 1. *If C is a $\mathbb{Z}_{p^2}$-linear code of length n, then $\Phi(C)$ is a linear code over $\mathbb{F}_p$ if and only if, for all $\boldsymbol{\alpha},\boldsymbol{\beta} \in C$, we have $p\chi(r_0(\boldsymbol{\alpha}), r_0(\boldsymbol{\beta})) \in C$.*

Using Lemma 1, we determine whether $\Phi(C(D))$ is linear or nonlinear in some cases.

Theorem 3. *For $1 \leq D \leq p-1$, the code $\Phi(C(D))$ is linear. If $p \geq 3$ and $p \leq D \leq p^{m/2}/2$, then $\Phi(C(D))$ is nonlinear.*

Proof. First we prove that $\Phi(C(D))$ is linear for $D \leq p-1$. For $\boldsymbol{\alpha},\boldsymbol{\beta} \in C(D)$, there exist $f_1(x), f_2(x) \in S(D)$ and $u_1, u_2 \in \mathbb{Z}_{p^2}$ such that

$$\begin{aligned} \boldsymbol{\alpha} &= \left(\mathrm{Tr}_m(f_1(0)) + u_1, \mathrm{Tr}_m(f_1(\beta)) + u_1, \ldots, \mathrm{Tr}_m(f_1(\beta^{p^m-1})) + u_1\right), \text{ and} \\ \boldsymbol{\beta} &= \left(\mathrm{Tr}_m(f_2(0)) + u_2, \mathrm{Tr}_m(f_2(\beta)) + u_2, \ldots, \mathrm{Tr}_m(f_2(\beta^{p^m-1})) + u_2\right). \end{aligned}$$

As $D \leq p-1$, we have $f_1(x), f_2(x) \in pS(D)_1$. Hence

$$r_0(\boldsymbol{\alpha}) = (\rho(u_1),\ldots,\rho(u_1)), \;\; r_0(\boldsymbol{\beta}) = (\rho(u_2),\ldots,\rho(u_2)) \text{ and}$$

$$p\chi(r_0(\boldsymbol{\alpha}), r_0(\boldsymbol{\beta})) = \begin{cases} (p,\ldots,p) \text{ if } \rho(u_1)+\rho(u_2) \geq p, \\ (0,\ldots,0) \text{ if } \rho(u_1)+\rho(u_2) < p. \end{cases}$$

Since $(p,\ldots,p), (0,\ldots,0) \in \mathbb{Z}_{p^2}^{p^m}$ are elements of $C(D)$, the proof for the case $D \leq p-1$ is completed.

Next we consider the case $p \geq 3$ and $p \leq D \leq p^{m/2}/2+1$. The polynomial $f(x) = x$ belongs to $S(D)$ and hence

$$\boldsymbol{\alpha} = (\mathrm{Tr}_m(0), \mathrm{Tr}_m(\beta), \ldots, \mathrm{Tr}_m(\beta^{p^m-1})) \in C(D).$$

Clearly,

$$r_0(\boldsymbol{\alpha}) = (\mathrm{tr}_m(0), \mathrm{tr}_m(\omega), \ldots, \mathrm{tr}_m(\omega^{p^m-1})).$$

For each $a \in \mathbb{F}_p$, $\chi(a,a) = 1$ if and only if $a \geq \frac{p+1}{2}$. By the properties of the trace map tr_m, it follows that every element $a \in \mathbb{F}_p$ appears in exactly p^{m-1}

coordinates of $r_0(\boldsymbol{\alpha})$. Hence $\chi(r_0(\boldsymbol{\alpha}), r_0(\boldsymbol{\alpha}))$ has 1 at exactly $p^{m-1}(p-1)/2$ coordinates, and the remaining positions are 0. By (1), the minimum distance $d_{\min}$ of $\Phi(C(D))$ satisfies

$$d_{\min} \geq p^{m+1} - p^m - (p-1)(D-1)p^{m/2}.$$

The distance between $\Phi(p\chi(r_0(\boldsymbol{\alpha}), r_0(\boldsymbol{\alpha})))$ and the zero codeword is $p^m(p-1)/2$. For $D < p^{m/2}/2 + 1$, it is easy to see that

$$p^{m+1} - p^m - (D-1)p^{m/2} > p^m(p-1)/2.$$

Therefore $p\chi(r_0(\boldsymbol{\alpha}), r_0(\boldsymbol{\alpha})) \notin C(D)$, which completes the proof.

3 *p*-ary Sequences with Low Correlation

For a p-ary sequence $\{s(i)\}_{i=0}^{\infty}$ and $\tau \geq 0$, the *cyclic shift of* $\{s(i)\}_{i=0}^{\infty}$ *by* τ is the p-ary sequence $\{s(i+\tau)\}_{i=0}^{\infty}$. Two p-ary sequences $\{s_1(i)\}_{i=0}^{\infty}$ and $\{s_2(i)\}_{i=0}^{\infty}$ are *cyclically distinct* if for each $\tau \geq 1$ neither is $\{s_1(i)\}_{i=0}^{\infty}$ the cyclic shift of $\{s_2(i)\}_{i=0}^{\infty}$ by τ nor is $\{s_2(i)\}_{i=0}^{\infty}$ the cyclic shift of $\{s_1(i)\}_{i=0}^{\infty}$ by τ.

For $n = p^m - 1$, the generalized Nechaev-Gray map (cf. [N], [L-B], [L-S]) Ψ over $\mathbb{Z}_{p^2}^n$ is defined as follows: For $u \in \mathbb{Z}_{p^2}$ let $u = r_0(u) + pr_1(u)$ with $r_0(u),\ r_1(u) \in \{0, 1, \dots, p-1\}$. Recall that $\oplus$ denotes the addition modulo p. For $(u_0, u_1, \dots, u_{n-1}) \in \mathbb{Z}_{p^2}^n$, we have $\Psi(u_0, u_1, \dots, u_{n-1}) = (a_0, a_1, \dots, a_{pn-1}) \in \mathbb{F}_p^{pn}$ such that for $0 \leq j \leq p-1$ and $0 \leq t \leq n-1$, $a_{jn+t} = r_1((1-p)^t u_t) \oplus jr_0((1-p)^t u_t)$. It is shown in [L-B, Corollary 3.6] that, if C is a cyclic code over $\mathbb{Z}_{p^2}$, then $\Psi(C)$ is a cyclic p-ary code.

Let $\mathcal{P}_{m,D}^1$ be the subset of $S(D) \times \mathbb{Z}_{p^2}$ defined as

$$\mathcal{P}_{m,D}^1 = \Big\{(f(x), u) \in S(D) \times \mathbb{Z}_{p^2} : \rho(f(x)) \neq 0, \\ \text{and } \{\mathrm{Tr}_m(f(\beta^i))\}_{i=0}^{\infty} \text{ has period } p^m - 1\Big\}.$$

We introduce an equivalence relation on $\mathcal{P}_{m,D}^1$: We say that $(f(x), u),\ (g(x), v) \in \mathcal{P}_{m,D}^1$ are related if there exist $0 \leq j,\ k \leq p-1$ and $0 \leq t \leq (p^m - 1) - 1$ such that

$$g(x) = (1+p)^j (1-p)^t f(\beta^t x) \ \text{ and } \ v = (1+p)^j (1-p)^t u + kp.$$

Let $\widehat{\mathcal{P}}_{m,D}^1$ be a full set of representatives of the equivalence relation. We also assume, without loss of generality, that the elements of $\widehat{\mathcal{P}}_{m,D}^1$ are of the form $(f(x), u)$ with $u \in \{0, 1, \dots, p-1\} \subseteq \mathbb{Z}_{p^2}$. Let $\mathcal{F}_{m,D}^1$ be the family of p-ary sequences given as

$$\mathcal{F}_{m,D}^1 = \big\{\{\Psi(\mathrm{Tr}_m(f(\beta^i)) + u)\}_{i=0}^{\infty} : (f(x), u) \in \widehat{\mathcal{P}}_{m,D}^1\big\}.$$

Let $\mathcal{P}_{m,D}^2$ be the subset of $pS(D)_1 \times (\mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2})$ defined as

$$\mathcal{P}_{m,D}^2 = \Big\{(pf(x), u) \in pS(D)_1 \times (\mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2}) : \{\mathrm{Tr}_m(pf(\beta^i))\}_{i=0}^{\infty} \text{ has period } p^m - 1\Big\}.$$

We say $(pf(x), u),\ (pg(x), v) \in \mathcal{P}^2_{m,D}$ are *cyclically related* if there exist $0 \le j \le p-1$ and $0 \le t \le (p^m-1)-1$ such that $pg(x) = (1+p)^j(1-p)^t pf(\beta^t x)$ and $v = (1+p)^j(1-p)^t u$. Cyclically related elements of $\mathcal{P}^2_{m,D}$ form an equivalence relation. Let $\overline{\mathcal{P}}^2_{m,D}$ denote the set of equivalence classes in $\mathcal{P}^2_{m,D}$. In fact, we can choose a full set of representatives $\widetilde{\mathcal{P}}^2_{m,D}$ of the equivalence classes in $\overline{\mathcal{P}}^2_{m,D}$ such that

$$\widetilde{\mathcal{P}}^2_{m,D} = \Big\{(pf(x), u) \in \mathcal{P}^2_{m,D} : u \in \{1, \ldots, p-1\} \subseteq (\mathbb{Z}_{p^2} \setminus p\mathbb{Z}_{p^2})\Big\}.$$

Let $\mathcal{F}^2_{m,D}$ be the family of p-ary sequences given as

$$\mathcal{F}^2_{m,D} = \Big\{\{\Psi(\mathrm{Tr}_m(pf(\beta^i)) + u)\}_{i=0}^{\infty} : (pf(x), u) \in \widetilde{\mathcal{P}}^2_{m,D}\Big\}.$$

Let $\mathcal{F}_{m,D}$ be the family of p-ary sequences defined as

$$\mathcal{F}_{m,D} = \mathcal{F}^1_{m,D} \cup \mathcal{F}^2_{m,D}.$$

Theorem 4. *The families $\mathcal{F}^1_{m,D}$, $\mathcal{F}^2_{m,D}$ and $\mathcal{F}_{m,D}$ have the following properties:*

i) The period of each sequence in $\mathcal{F}_{m,D}$ (resp. $\mathcal{F}^1_{m,D}$ and $\mathcal{F}^2_{m,D}$) is $p(p^m-1)$.
ii) The sequences in $\mathcal{F}_{m,D}$ (resp. $\mathcal{F}^1_{m,D}$ and $\mathcal{F}^2_{m,D}$) are pairwise cyclically distinct.
iii) $|\mathcal{F}^1_{m,D}| = \frac{1}{p^m-1}\sum_{l|(p^m-1)} \mu(l)\left\{p^{m(\lfloor \frac{D}{l}\rfloor - \lfloor \frac{D}{p^2 l}\rfloor)} - p^{m(\lfloor \frac{D}{l}\rfloor - \lfloor \frac{D}{pl}\rfloor)}\right\}$,
$|\mathcal{F}^2_{m,D}| = \frac{p-1}{p^m-1}\sum_{l|(p^m-1)} \mu(l) p^{m(\lfloor \frac{D}{l}\rfloor - \lfloor \frac{D}{pl}\rfloor)}$, *and*
$|\mathcal{F}_{m,D}| = |\mathcal{F}^1_{m,D}| + |\mathcal{F}^2_{m,D}|$, *where $\mu(\cdot)$ is the Möbius function.*
iv) For the maximal non-trivial correlation $\theta_{\max}$ of $\mathcal{F}_{m,D}$ (resp. $\mathcal{F}^1_{m,D}$ and $\mathcal{F}^2_{m,D}$), we have

$$\theta_{\max} \le \frac{1}{p-1} p^{l_{D,m}+1} \left\lfloor \frac{p^{h_{D,m}} \frac{p^2-p}{2}(D-1)\left\lfloor 2p^{\frac{m}{2}-h_{D,m}}\right\rfloor}{p^{l_{D,m}+1}} \right\rfloor + p.$$

Remark 1. For $p=2$, from $\mathcal{F}^1_{m,D}$ we retrieve the family of binary sequences $Q(D)$ of [H-K, Section 8.8]. Let $\mathcal{F}^{1,0}_{m,D}$ be the subfamily of $\mathcal{F}^1_{m,D}$ defined as

$$\mathcal{F}^{1,0}_{m,D} = \big\{\{\Psi(\mathrm{Tr}_m(f(\beta^i)))\}_{i=0}^{\infty} : (f(x), 0) \in \widehat{\mathcal{P}}^1_{m,D}\big\}.$$

Note that $\mathcal{F}^1_{m,D}$ is larger than $\mathcal{F}^{1,0}_{m,D}$ with the same upper bound on the maximal non-trivial correlation. For $p=2$, from $\mathcal{F}^{1,0}_{m,D}$ we obtain the family of binary sequences of [S-K-H].

Remark 2. $\mathcal{F}_{m,D}$ is larger than $\mathcal{F}^1_{m,D}$ while the sequences in them have the same period and the same upper bound for their maximal non-trivial correlation in Theorem 4.

For more details of the results above we refer the reader to [L-O2].

References

[C] C. Carlet, "$\mathbb{Z}_{2^k}$-linear codes", *IEEE Trans. Inform. Theory*, vol. 44, no. 4, pp. 1543-1547, July 1998.

[C-H] I. Constantinescu and T. Heise, "A metric for codes over residue class rings of integers", *Prob. Inform. Transmission*, vol. 33, pp. 208-213.

[G-S] M. Greferath and S.E. Schmidt, "Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code", *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2522-2524, November 1999.

[H-K] T. Helleseth and P.V. Kumar, "Sequences with low correlation", in *Handbook of Coding theory Vol. I, II.* Edited by V.S. Pless and W.C. Huffman, pp. 1765-1853, North-Holland, Amsterdam, 1998.

[K-H-C] P.V. Kumar, T. Helleseth and A.R. Calderbank, "An upper bound for Weil exponential sums over Galois rings with applications", *IEEE Trans. Inform. Theory*, vol. 41, no. 2, pp. 456-468. March 1995.

[H-K-M-S] T. Helleseth, P.V. Kumar, O. Moreno and A.G. Shanbhag, "Improved estimates via exponential sums for the minimum distance of $\mathbb{Z}_4$-linear trace codes", *IEEE Trans. Inform. Theory*, vol. 42, no. 4, pp. 1212-1216, July 1996.

[L-B] S. Ling and J.T. Blackford, "$\mathbb{Z}_{p^{k+1}}$-linear codes", *IEEE Trans. Inform. Theory*, vol. 48, no. 9, 2592-2605, September 2002.

[L-O] S. Ling and F. Özbudak, "An Improvement on the bounds of Weil exponential sums over Galois rings with some application", *IEEE Trans. Inform. Theory*, vol. 50, no. 10, pp. 2529-2539, October 2004.

[L-O2] S. Ling and F. Özbudak, "Improved p-ary codes and sequence families from Galois rings of characteristic p^2", submitted, 2004.

[L-S] S. Ling and P. Solé, "Nonlinear p-ary sequences", *Appl. Alg. Eng. Comm. Comp.*, vol. 14, pp. 117-125, 2003.

[N] A. A. Nechaev, "The Kerdock code in a cyclic form", *Discr. Math. Appl.*, vol. 1, pp. 365-384, 1991.

[S-K-H] A.G. Shanbhag, P.V. Kumar and T. Helleseth, "Improved binary codes and sequence families from $\mathbb{Z}_4$-linear codes", *IEEE Trans. Inform. Theory*, vol. 42, no. 5, pp. 1582-1587, September 1996.