[2] M. Berggren, "An algorithm for characterizing error event sequences in partial response channels," Diploma Project, Swiss Fed. Inst. Tech., Zurich, Switzerland, Aug. 1996.
[3] R. Karabed and P. H. Siegel, "Coding for higher-order partial-response channels," in *Coding and Signal Processing for Information Storage*, M. R. Raghuveer, S. A. Dianat, S. W. McLaughlin, and M. Hassner, Eds., *Proc. SPIE 2605*, Oct. 1995, pp. 115–126.
[4] R. Karabed, P. H. Siegel, and E. Soljanin, "Constrained coding for binary channels with high intersymbol interference," submitted for publication to *IEEE Trans. Inform. Theory*.
[5] D. Lind and B. H. Marcus, *An Introduction to Symbolic Dynamics and Coding*. Cambridge, U.K.: Cambridge Univ. Press, 1995.
[6] B. H. Marcus, P. H. Siegel, and J. K. Wolf, "Finite-state modulation codes for data storage," *IEEE J. Select. Areas Commun*., vol. 10, pp. 5–37, Jan. 1992.
[7] B. E. Moision, P. H. Siegel, and E. Soljanin, "Distance-enhancing codes for digital recording," *IEEE Trans. Magn*., vol. 34, no. 1, pt. 1, pp. 69–74, Jan. 1998.
[8] J. Moon and B. Brickner, "Maximum transition run codes for data storage systems," *IEEE Trans. Magn*., vol. 32, pp. 3992–3994, Sept. 1996.
[9] W.-H. Sheen and G. L. Stuber, "Error probability for reduced-state sequence estimation," *IEEE J. Select. Areas Commun*., vol. 10, pp. 571–578, Apr. 1992.
[10] P. H. Siegel "Coded modulation for binary partial response channels: state-of-the-art," in *Proc. 1996 Information Theory Workshop* (Haifa, Israel, June 9–13, 1996).
[11] E. Soljanin, "On coding for binary partial-response channels that don't achieve the matched-filter-bound," in *Proc. 1996 Information Theory Workshop* (Haifa, Israel, June 9–13, 1996).
[12] A. J. Viterbi and J. K. Omura, *Principles of Digital Communication and Coding*. New York: McGraw-Hill, 1979.
[13] A. D. Weathers, S. A. Altekar, and J. K. Wolf, "Distance spectra for PRML channels," *IEEE Trans. Magn*., vol. 33, no. 5, pt. 1, pp. 2809–2811, Sept. 1997.

On the Distance Distribution of Duals of BCH Codes

Ilia Krasikov and Simon Litsyn, *Member, IEEE*

***Abstract*—We derive upper bounds on the components of the distance distribution of duals of BCH codes.**

***Index Terms*—BCH codes, distance distribution.**

I. Introduction

Let C be the code dual to the extended t-error correcting Bose-Chaudhuri–Hocquenghem (BCH) code of length $q = 2^m$, and let $B = (B_0, \cdots, B_q)$ stand for the distance distribution of C. Our aim is to derive *upper bounds* on B_i's. The following theorems summarize our present knowledge.

The first one shows that outside a certain interval B_i's vanish. This is a refinement of the celebrated result by Weil [18] and Carlitz–Uchiyama [3] due to Serre [14] (it has been adapted for duals of BCH codes in [6] and [12]).

Manuscript received November 24, 1997; revised July 16, 1998.
I. Krasikov is with the School of Mathematical Sciences, Tel-Aviv University, Ramat-Aviv 69978, Tel-Aviv, Israel. He is also with the Beit-Berl College, Kfar-Sava, Israel.
S. Litsyn is with the Center for Discrete Mathematics, Rutgers University, Piscataway, NJ 08854 USA, on leave from the Department of Electrical Engineering–Systems, Tel-Aviv University, Ramat-Aviv 69978, Tel-Aviv, Israel (e-mail: litsyn@eng.tau.ac.il).
Communicated by A. Barg, Associate Editor for Coding Theory.
Publisher Item Identifier S 0018-9448(99)00083-8.

Theorem 1: If $|q/2 - i| > 2(t-1)[2 \cdot 2^{m/2}]$, $i \neq 0, q$, then $B_i = 0$. □

The next result deals with divisibility properties and is based on the Ax theorem [2], see [7], [11], [13], and [16].

Theorem 2: Let a be the smallest positive integer $\geq m/[\log_2 2t]$. If i is not a multiple of 2^a then $B_{q/2-i} = 0$. □

Apart from some particular cases, namely $t = 1, 2, 3,$ when all the values of the distribution were computed explicitly, to the extent of our knowledge, no general estimates of B_i's were published.

In this correspondence we derive upper bounds on B_i's. Roughly speaking, these bounds show that the distance distribution can be upper-bounded by the corresponding normal distribution. To derive the bounds we use the linear programming approach along with some estimates on the magnitude of Krawtchouk polynomials of fixed degree in a vicinity of $q/2$.

II. Preliminaries

Let $F = \boldsymbol{F}_q$ be the finite field of $q = 2^m$ elements and Tr denote the trace function from F to $\boldsymbol{F}_2$. Let $\mathcal{G}_t$ be an additive subgroup of $F[x]$

$$\mathcal{G}_t = \left\{ G(x) = \sum_{i=1}^{t} a_i x^{2i-1}: \quad a_i \in F \right\}.$$

Let α be a primitive element in F. For every $G(x) \in \mathcal{G}_t$ and $\epsilon \in \boldsymbol{F}_2$ we define a vector in $\boldsymbol{F}_2^q$

$$\boldsymbol{c}(G, \epsilon) = (\mathrm{Tr}\,(G(0)) + \epsilon,\ \mathrm{Tr}\,(G(1)) + \epsilon,\ \mathrm{Tr}\,(G(\alpha)) + \epsilon, \cdots, \mathrm{Tr}\,(G(\alpha^{q-2})) + \epsilon).$$

When $G(x)$ runs over $\mathcal{G}_t$, the set of vectors $\boldsymbol{c}(G, \varepsilon)$ constitute the code dual to the extended BCH codes of length q and with minimum distance $2t+2$, see, e.g., [1], [10], and [15]. Let $w(\boldsymbol{c}(G, \epsilon))$ stand for the number of nonzero coordinates in $\boldsymbol{c}(G, \epsilon)$. For $i \in [0, q]$

$$B_i = |\{G(x) \in \mathcal{G}_t,\ \epsilon \in \boldsymbol{F}_2\colon\ w(\boldsymbol{c}(G, \epsilon)) = i\}|.$$

It is easy to check that $B_0 = 1$ and $\sum_{i=0}^{q} B_i = 2|\mathcal{G}_t| = 2q^t$. By the MacWilliams identity

$$\sum_{j=0}^{q} B_j P_i(j) = \begin{cases} 2q^t, & i = 0 \\ 0, & 1 \leq i < 2t+2. \end{cases} \tag{1}$$

Here $P_i(j)$ are Krawtchouk polynomials (orthogonal on the interval $[0, q]$ with weight $\binom{q}{j}$) defined by the following recurrence (for their properties see, e.g., [5], and [8]–[10]):

$$(k+1)P_{k+1}(x) = (q-2x)P_k(x) - (q-k+1)P_{k-1}(x) \tag{2}$$
$$P_0(x) = 1 \qquad P_1(x) = q - 2x.$$

We need the following facts about Krawtchouk polynomials:

Orthogonality Relation:

$$\sum_{i=0}^{q} \binom{q}{i} P_\ell(i) P_k(i) = \delta_{\ell,k} 2^q \binom{q}{\ell}.$$

Expansion in the Basis of Krawtchouk Polynomials: For a polynomial $\alpha(x) = \sum_{i=0}^{r} \alpha_i P_i(x)$

$$\alpha_i = 2^{-q} \sum_{j=0}^{q} P_j(i)\alpha(j). \tag{3}$$

The Christoffel–Darboux Formula:

$$\binom{q}{t} \sum_{i=0}^{t} \frac{P_i(x)P_i(y)}{\binom{n}{i}} = \frac{t+1}{2(y-x)} \left(P_{t+1}(x)P_t(y) - P_t(x)P_{t+1}(y)\right).$$

Letting $y \to x$ and taking the limit, we get

$$\binom{q}{t} \sum_{i=0}^{t} \frac{(P_i(x))^2}{\binom{n}{i}} = \frac{t+1}{2} \left(P_{t+1}(x)P_t'(x) - P_t(x)P_{t+1}'(x)\right).$$

The following lemma is crucial in our considerations, and is a version of a result implicitly appearing in the thesis by Delsarte [4].

Lemma 1: Let

$$\alpha(x) = \sum_{i=0}^{r} \alpha_i P_i(x), \qquad 0 \le r < 2t+2$$

then

$$2q^t \alpha_0 = \sum_{j=0}^{q} \alpha(j) B_j. \tag{4}$$

Proof: Calculating $2q^t \sum_{i=0}^{r} \alpha_i B_i'$, and taking into account that $\alpha_i = 0$ for $i > r$, we get the claim from (1). □

To obtain a bound on B_k, choose in the previous lemma as $\alpha(x)$ a nonnegative polynomial of degree less than $2t+2$. It yields

$$B_k \le 2q^t \, \frac{\alpha_0}{\alpha(k)}. \tag{5}$$

The following lemma gives a polynomial minimizing the right-hand side of this inequality under an extra condition $\alpha(x) = \beta(x)^2$ for some polynomial $\beta(x)$.

Lemma 2: For k given, an optimal polynomial is

$$\begin{aligned}\alpha(x) &= \left(\sum_{i=0}^{t} \frac{P_i(x)P_i(k)}{\binom{q}{i}}\right)^2 \\ &= \frac{(t+1)^2}{4\binom{q}{t}^2 (k-x)^2} \left(P_{t+1}(k)P_t(x) - P_t(k)P_{t+1}(x)\right)^2 \end{aligned} \tag{6}$$

yielding

$$B_k \le \frac{4\binom{q}{t} q^t}{(t+1)(P_{t+1}(k)P_t'(k) - P_t(k)P_{t+1}'(k))}.$$

Proof: Let $\beta(x) = \sum_{j=0}^{t} \beta_j P_j(x)$ and $\alpha(x) = \beta^2(x)$. Then

$$\begin{aligned}\alpha_0 &= \frac{1}{2^q} \sum_{i=0}^{q} \binom{q}{i} \alpha(i) \\ &= \frac{1}{2^q} \sum_{i=0}^{q} \binom{q}{i} \left(\sum_{j=0}^{t} \beta_j P_j(i)\right)^2 \\ &= \frac{1}{2^q} \sum_{j,\,\ell=0}^{t} \beta_j \beta_\ell \sum_{i=0}^{q} \binom{q}{i} P_j(i) P_\ell(i)\end{aligned}$$

by orthogonality of Krawtchouk polynomials

$$\begin{aligned}&= \frac{1}{2^q} \sum_{j,\,\ell=0}^{t} \beta_j \beta_\ell \delta_{j,\,\ell} \binom{q}{j} 2^q \\ &= \sum_{j=0}^{t} \beta_j^2 \binom{q}{j}.\end{aligned}$$

Thus for k given

$$\begin{aligned}\max_\beta \frac{\alpha(k)}{\alpha_0} &= \max_\beta \frac{\left(\sum_{j=0}^{t} \beta_j P_j(k)\right)^2}{\sum_{j=0}^{t} \beta_j^2 \binom{q}{j}} \\ &= \max_\beta \frac{\left(\sum_{j=0}^{t} \left(\beta_j \sqrt{\binom{q}{j}}\right)\left(P_j(k) \Big/ \sqrt{\binom{q}{j}}\right)\right)^2}{\sum_{j=0}^{t} \beta_j^2 \binom{q}{j}}\end{aligned}$$

by Cauchy–Schwartz inequality

$$\le \sum_{j=0}^{t} \frac{P_j^2(k)}{\binom{q}{j}}$$

by the Christoffel–Darboux formula

$$= \frac{t+1}{2\binom{q}{t}} \left(P_{t+1}(k)P_t'(k) - P_t(k)P_{t+1}'(k)\right).$$

This bound is clearly achieved for $\beta_j = (P_j(k))/\binom{q}{j}$, that is, the optimal choice for a given k is

$$\begin{aligned}\alpha(x) &= \left(\sum_{j=0}^{t} \frac{P_j(k)P_j(x)}{\binom{q}{j}}\right)^2 \\ &= \frac{(t+1)^2}{4\binom{q}{t}^2 (k-x)^2} \left(P_{t+1}(k)P_t(x) - P_t(k)P_{t+1}(x)\right)^2.\end{aligned}$$

Then the second claim follows from (5). □

III. Estimates of B_k

To use the bound of Lemma 2 one needs a lower estimate for the Christoffel–Darboux kernel $P_{t+1}(k)P_t(x) - P_t(k)P_{t+1}(x)$. Assume that q is sufficiently large and t is fixed. In this situation, a classical connection (see, e.g., [17, eq. (2.82.7)]) between Krawtchouk and Hermite polynomials can be employed. However, we need somehow more involved estimates for the accuracy of approximation of Krawtchouk polynomials by Hermite polynomials.

The Hermite polynomials $H_k(x)$ are defined by the recurrence relation

$$\begin{aligned}H_{k+1}(x) &= 2xH_k(x) - 2kH_{k-1}(x) \\ H_0(x) &= 1 \qquad H_1(x) = 2x.\end{aligned} \tag{7}$$

Let ε_t stand for the largest root of $H_t(x)$.

Lemma 3:

$$\begin{aligned}P_k\left(\frac{q-\sqrt{2q}y}{2}\right) &= \frac{1}{k!2^{k/2}} \left(q^{k/2} H_k(y) + 4q^{(k-2)/2}\right) \binom{k}{3} H_{k-2}(y) \\ &\quad + 2\binom{k}{4} H_{k-4}(y) + q^{(k-4)/2} R_k(y)\end{aligned} \tag{8}$$

where $R_0(y) = R_1(y) = 0$, and

$$\begin{aligned}R_{k+1}(y) &= 2yR_k(y) - \frac{2k(q-k+1)}{q} R_{k-1}(y) \\ &\quad + 8(k-1)\binom{k}{4}(3H_{k-3}(y) + 2yH_{k-4}(y)).\end{aligned} \tag{9}$$

In particular, for fixed k and y

$$P_k\left(\frac{q-\sqrt{2q}y}{2}\right) = \frac{q^{k/2}}{k!2^{k/2}} H_k(y) + O\left(\frac{1}{q}\right). \tag{10}$$

Proof: Relations (8) and (9) are verified just by substitution into (2) and using (7). □

In what follows we use the prime sign to denote the derivative in y.

Corollary 1: For k and y fixed and $x = (q - \sqrt{2q}y)/2$

$$\frac{d}{dx} P_k(x) = -\frac{q^{(k-1)/2}}{2^{(k-1)/2}k!} H_k'(y) + O\left(\frac{1}{q}\right). \quad \square$$

Using these approximations we get the following.

Lemma 4: For fixed y and $x = (q - \sqrt{2q}y)/2$

$$P_{t+1}(x) \frac{d}{dx} P_t(x) - P_t(x) \frac{d}{dx} P_{t+1}(x) = \frac{q^t}{2^{t+1}((t+1)!)^2} \left((H_{t+1}'(y))^2 - H_{t+1}(y)H_{t+1}''(y)\right) + O(q^{t-1}). \tag{11}$$

Proof: With accuracy up to $O(1/q)$ we have from Lemma 3

$$P_{t+1}(x) \frac{d}{dx} P_t(x) - P_t(x) \frac{d}{dx} P_{t+1}(x) = \frac{q^t}{2^t t!(t+1)!} \left(H_t(y)H_{t+1}'(y) - H_{t+1}(y)H_t'(y)\right)$$

and using $H_{t+1}'(x) = 2(t+1)H_t(x)$ (see, e.g., [17, p. 106]) we get the claim. □

Now we are in a position to translate the derived estimates to bounds for B_k.

Theorem 3: For fixed y and $k = (q - \sqrt{2q}y)/2$

$$B_k \leq \frac{q^t(t+1)!2^{t+3}}{(H_{t+1}'(y))^2 - H_{t+1}(y)H_{t+1}''(y)} \left(1 + O\left(\frac{1}{q}\right)\right). \tag{12}$$

□

To use this expression we need estimates for Hermite polynomials when $y < \sqrt{2t}$.

The denominator of (12) can be easily computed if x does not belong to the interval where the roots of $P_t(x)$ are located (or, which is asymptotically the same, $|y| > \varepsilon_t$). Indeed, by (2), $P_t(x)$ is a polynomial of degree t in q, and

$$\sum_{i=0}^{t} \frac{(P_i(x))^2}{\binom{q}{i}} = \frac{(P_t(x))^2}{\binom{q}{t}} \left(1 + O\left(\frac{1}{q}\right)\right).$$

In this case, we have

$$\frac{P_t^2(x)}{\binom{q}{t}} \approx \frac{q^t H_t^2(y)}{2^t(t!)^2\binom{q}{t}} \approx \frac{(H_t(y))^2}{2^t t!}.$$

Theorem 4: Let $y = \frac{q-2k}{\sqrt{2q}}$. For $|\frac{q}{2} - k| > \frac{(t-1)\sqrt{q}}{\sqrt{t+2}}$

$$B_k \leq \frac{q^t t! 2^{t+1}}{(H_t(y))^2} \left(1 + O\left(\frac{1}{q}\right)\right).$$

Proof: Follows from the estimate on the largest root of $H_t(y)$ due to Laguerre, see [17, p. 120]

$$\varepsilon_t \leq \frac{\sqrt{2}(t-1)}{\sqrt{t+2}} \tag{13}$$

and $y = O(t)$ by Theorem 1. □

To apply this estimate one needs asymptotics for Hermite polynomials. For the interval under consideration it is well known and can be found, e.g., in [17, p. 200]. When y belongs to the interval where the roots of $H_t(y)$ exist, another approach should be employed.

Lemma 5: Let

$$W_t(y) = (H_t'(y))^2 - H_t(y)H_t''(y).$$

Then

$$W_t(0) = \begin{cases} 2t\binom{t}{t/2} t!, & \text{for } t \text{ even} \\ 4t\binom{t-1}{(t-1)/2} t!, & \text{otherwise} \end{cases}$$

and

$$W_t(y) \geq e^{y^2} \frac{\sqrt{2t} - |y|}{\sqrt{2t}} W_t(0), \qquad |y| \leq \sqrt{2t}$$

$$W_t(y) \leq e^{y^2} \frac{\sqrt{2t} + |y|}{\sqrt{2t}} W_t(0).$$

Proof: We start with calculating $W_t(0)$. It is known that

$$H_t(0) = \begin{cases} (-1)^{t/2} \frac{t!}{(t/2)!}, & \text{for } t \text{ even} \\ 0, & \text{otherwise.} \end{cases}$$

From the differential equation for Hermite polynomials

$$H_t''(y) = 2yH_t'(y) - 2tH_t(y)$$

and

$$H_t'(y) = 2tH_{t-1}(y) \tag{14}$$

we get for t even

$$W_t(0) = 2t(H_t(0))^2 = 2t\binom{t}{t/2} t!.$$

For t odd

$$W_t(0) = 4t^2(H_{t-1}(0))^2 = 4t\binom{t-1}{(t-1)/2} t!.$$

Notice that $W_t(y)$ is strictly positive. Indeed, let y_i stand for the ith root of $H_t(y)$. Then

$$H_t(y) = 2^t \prod_{i=1}^{t} (y - y_i)$$

and differentiating it we get

$$H_t'(y) = H_t(y) \sum_{i=1}^{t} \frac{1}{y - y_i},$$

$$H_t''(y) = H_t'(y) \sum_{i=1}^{t} \frac{1}{y - y_i} - H_t(y) \sum_{i=1}^{t} \frac{1}{(y - y_i)^2}$$

$$= H_t(y) \left(\sum_{i=1}^{t} \frac{1}{y - y_i}\right)^2 - \sum_{i=1}^{t} \frac{1}{(y - y_i)^2}.$$

Thus

$$W_t(y) = (H_t(y))^2 \sum_{i=1}^{t} \frac{1}{(y - y_i)^2} > 0.$$

Without loss of generality we assume y is nonnegative. Using (14) we obtain

$$W_t(y) = 2t(H_t(y))^2 - 2yH_t(y)H_t'(y) + (H_t'(y))^2$$

$$W_t'(y) = 4ty(H_t(y))^2 - 2(1 + 2y^2)H_t(y)H_t'(y) + 2y(H_t'(y))^2.$$

Denoting $t = \mu^2/2$, we get

$$W_t'(y) + \frac{1 - 2\mu y + 2y^2}{\mu - y} W_t(y) = \frac{(\mu H_t(y) - H_t'(y))^2}{\mu - y}$$

$$W_t'(y) - \frac{1 + 2\mu y + 2y^2}{\mu + y} W_t(y) = -\frac{(\mu H_t(y) + H_t'(y))^2}{\mu + y}.$$

From the first equality, for $0 \le y < \mu$, and taking into account that $W_t(y) > 0$, we conclude

$$\frac{W_t'(y)}{W_t(y)} \ge -\frac{1-2\mu y+2y^2}{\mu-y}. \tag{15}$$

On the other hand, from the second equality

$$\frac{W_t'(y)}{W_t(y)} \le \frac{1+2\mu y+2y^2}{\mu+y}. \tag{16}$$

Integrating (15), we obtain

$$\int_0^y \frac{W_t'(z)}{W_t(z)}\,dz = \ln\,\frac{W_t(y)}{W_t(0)} \ge y^2 + \ln\,\frac{\mu-y}{\mu}$$

thus proving the lower bound on $W_t(y)$. Similarly, integrating (16), we get the claimed upper bound. □

Notice, that the estimates of the lemma are quite accurate for $y < \sqrt{2t}$. Indeed, the maximum of the function

$$e^{y^2}\,\frac{\sqrt{2t}-|y|}{\sqrt{2t}}$$

is achieved at

$$|y| = \frac{\sqrt{t}+\sqrt{t-1}}{\sqrt{2}} \approx \sqrt{2t} - \frac{1}{\sqrt{8t}} > \varepsilon_t$$

i.e., almost at the end of the interval $|y| < \sqrt{2t}$. Even at this point the ratio between the upper and lower bound is less than $8t$, and all the roots of $H_t(y)$ are within this interval.

Numerical evidence suggests that (11) still gives an accurate approximation in a much wider interval of t and y. It is tempting to conjecture that actually the Christoffel–Darboux kernel can be well approximated by Hermite polynomials for all $t = o(\sqrt{q})$.

Now we can give an upper bound on B_k for the interval containing zeroes of $H_t(y)$.

Theorem 5: Let $\left|\frac{q}{2-k}\right| < \sqrt{(t+1)q}$, then

$$B_k \le \frac{\sqrt{q}\,q^t 2^{t+4}}{\sqrt{t+1}|2\sqrt{q(t+1)}-q+2k|\binom{t+1}{(t+1)/2}} \cdot e^{-((q-2k)^2/8q)}\left(1+O\left(\frac{1}{q}\right)\right), \qquad \text{for } t \text{ odd}$$

$$B_k \le \frac{\sqrt{q}\,q^t 2^{t+3}}{\sqrt{t+1}|2\sqrt{q(t+1)}-q+2k|\binom{t}{t/2}} \cdot e^{-((q-2k)^2/8q)}\left(1+O\left(\frac{1}{q}\right)\right), \qquad \text{for } t \text{ even}$$

$$B_k \le \frac{4\sqrt{2\pi q}q^t}{\left|2\sqrt{q(t+1)}-q+2k\right|} \cdot e^{-((q-2k)^2/q)}\left(1+O\left(\frac{1}{t}\right)\right), \qquad \text{for sufficiently large } t.$$

□

ACKNOWLEDGMENT

The authors are grateful to A. Barg and R. J. McEliece for many useful comments.

REFERENCES

[1] D. R. Anderson, "A new class of cyclic codes," *SIAM J. Appl. Math.*, vol. 16, pp. 181–197, 1968.
[2] J. Ax, "Zeroes of polynomials over finite fields," *Amer. J. Math.*, vol. 86, pp. 255–261, 1964.
[3] L. Carlitz and S. Uchiyama, "Bounds for exponential sums," *Duke Math. J.*, vol. 24, pp. 37–41, 1957.
[4] Ph. Delsarte, "An algebraic approach to the association schemes of coding theory," *Philips Res. Rept. Suppl.*, no. 10, 1973.
[5] I. Krasikov and S. Litsyn, "On integral zeroes of Krawtchouk polynomials," *J. Comb. Theory*, Ser. A 150, pp. 441–447, 1996.
[6] G. Lachaud, "Artin–Schreier curves, exponential sums and the Carlitz–Uchiyama bound for geometric codes," *J. Number Theory*, vol. 39, no. 1, pp. 485–494, 1991.
[7] S. Litsyn, C. J. Moreno, and O. Moreno, "Divisibility properties and new bounds for cyclic codes and exponential sums in one and several variables," *AAECC*, vol. 5, no. 2, pp. 105–116, 1994.
[8] V. Levenshtein, "Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1303–1321, Sept. 1995.
[9] J. H. van Lint, *Introduction to Coding Theory.* New York: Springer-Verlag, 1992.
[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam, The Netherlands: North Holland, 1983.
[11] R. J. McEliece, "Weight congruences for p-ary cyclic codes," *Discr. Math.*, vol. 3, pp. 177–192, 1972.
[12] C. J. Moreno and O. Moreno, "An improved Bombieri–Weil bound and applications to coding theory," *J. Number Theory*, vol. 42, pp. 32–46, 1992.
[13] O. Moreno and C. J. Moreno, "The MacWilliams–Sloane conjecture on the tightness of the Carlitz–Uchiyama bound and the weights of duals of BCH codes," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1894–1907, Nov. 1994.
[14] J. P. Serre, "Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini," *C. R. Acad. Sci. Paris*, vol. 296 Série I, pp. 397–402, 1983.
[15] V. M. Sidel'nikov, "On mutual correlation of sequences," *Sov. Math.–Dokl.*, vol. 12, no. 1, pp. 197–201, 1971.
[16] G. Solomon and R. J. McEliece, "Weights of cyclic codes," *J. Comb. Theory*, vol. 1, pp. 459–475, 1966.
[17] G. Szegö, "Orthogonal polynomials," *Amer. Math. Soc. Colloq. Publ.* (Providence, RI), vol. 23, 1975.
[18] A. Weil, "On some exponential sums," *Proc. Nat. Acad. Sci. USA.*, 1948, pp. 204–207, vol. 34.