Estimates of the Distance Distribution of Codes and Designs

Alexei Ashikhmin, *Member, IEEE,* Alexander Barg, *Senior Member, IEEE,* and Simon Litsyn, *Senior Member, IEEE*

***Abstract*—We consider the problem of bounding the distance distribution for unrestricted block codes with known distance and/or dual distance. Applying the polynomial method, we provide a general framework for previously known results. We derive several upper and lower bounds both for finite length and for sequences of codes of growing length. Asymptotic results in the paper improve previously known estimates. In particular, we prove the best known bounds on the binomiality range of the distance spectrum of codes with a known dual distance.**

***Index Terms*—Binomial spectrum, constant weight codes, distance distribution, Krawtchouk polynomials, polynomial method.**

I. Introduction

INTUITIVELY, it is clear that if the distance of a code is known, its distance distribution cannot be arbitrary. This paper is an attempt to quantify this statement. The distance distribution of a code with given parameters is important, in particular, for bounding the probability of decoding error under different decoding procedures from maximum likelihood decoding to error detection. Apart from this, it can be helpful in revealing structural properties of codes and establish nonexistence of some codes.

Our main tool is the polynomial (linear programming) method. This approach was pioneered by Sidel'nikov [25] and applied to Bose–Chaudhuri–Hocquenghem (BCH) codes correcting a small number of errors. Essentially the only feature of BCH codes used in [25] was the width of the dual-weight spectrum, known due to the Carlitz–Uchiyama bound. This study was taken up in [8], [13], [14], [15], [11]. These papers focused on establishing the range of weights in which the distance distribution of a code C is close to the average distribution of a code chosen in the Hamming space H_2^n with uniform probability (i.e., the binomial spectrum $A_w = \binom{n}{w}|C|/2^n$). However, implicitly some of these works contained bounds on the distance distribution of any code with known distance d or dual distance d'.

Another approach to bounding distance spectrum of (linear) codes with a known distance and/or dual distance was proposed in [9], see also [10]. In the frame of the polynomial method these results can be viewed as equivalents of the Singleton bound (see more on this in [1], [3]). Generally the method in [9], [10] seems to be somewhat weaker than the polynomial method employed here.

In Section II of this paper, we formulate a general bound on the distance distribution of a code in a Q-polynomial association scheme. The most detailed analysis is performed for H_2^n. By modifying some polynomials known in Delsarte's theory we derive bounds on the distance distribution of a code with given d and d'. We also specify the results for the cases when only d is known (i.e., d' can be any number between 0 and n), and vice versa, only d' is known. The results can be summarized as follows. For a given code with known d or d' the gap between the lower and upper bounds derived below depends on the "quality" of the code: the better the code, the smaller the gap. For some optimal codes the bounds turn out to be tight. Asymptotic versions of the bounds improve previously known results; in particular, we prove that the distance distribution of a design of a given strength in H_2^n is bounded above by the binomial distribution for a wider range of distances than previously known. From a purely coding-theoretic point of view the most important problem studied in the paper is bounding the distance distribution of a code with a known distance d. A nontrivial estimate of it for large values of the distance is given in Theorem 3. This estimate in a large range of parameters is better than bounds on the size of a code of constant weight and distance d.

Our results imply the following facts, made more precise in Section III.

- If a family of codes meets the upper bound from [23], then every small segment of distance values contains a binomial component in the distance distribution. [1]
- If the distance distribution of any family of codes is bounded above by the binomial spectrum, then every small segment of distance values, except maybe distances close to the minimum distance of the code, contains a binomial component.

Sections III and V deal with different ranges of code parameters. In each of these sections, we first derive a general bound on the distance distribution for some fixed d and d' and then look at particular cases when only one of these two parameters is known. Accordingly, the corresponding subsections have titles *Codes* and *Designs*. In Section IV, we use the general method of Section II to derive an asymptotic bound on the distance distribution of constant weight codes. In Appendix A, we provide an

Manuscript received April 5, 2000; revised July 8, 2000. This work was supported in part by Binational Science Foundation (BSF) under Grant 1999099.

A. Ashikhmin and A. Barg are with Bell Laboratories, Lucent Technologies, Murray Hill, NJ 07974 USA (e-mail: aea@research.bell-labs.com; abarg@research.bell-labs.com).

S. Litsyn is with the Department of Electrical Engineering-Systems, Tel-Aviv University, Ramat-Aviv 69978, Israel (e-mail: litsyn@eng.tau.ac.il).

Communicated by P. Solé, Associate Editor for Coding Theory.

Publisher Item Identifier S 0018-9448(01)01332-3.

[1]It is not known presently whether such codes exist. We concur with a conjecture in [23] that they do not.

alternative proof of Theorem 3. It is based on new inequalities for orthogonal polynomials found recently in [12], which may be useful also in other coding problems.

Asymptotic results claimed in the paper are related to sequences of codes of growing length n. For instance, when we say that a code meets a certain asymptotic upper (lower) bound relating R and δ, we actually mean that there exists a sequence of codes whose rate tends to R as n grows and the distance d/n is in the limit not greater (less) than δ. Asymptotic bounds on other parameters are treated in a similar fashion.

Let $H(x) = -x\log x - (1-x)\log(1-x)$ be the binary entropy function. (The base of logarithms is 2 throughout.) In the paper A_i is always the element of the distance distribution of a code of length n and a_ξ is its exponent: $a_\xi = \frac{1}{n}\log A_{\xi n}$.

II. Preliminaries

Let X be a finite metric space with distance function $\partial(\cdot,\cdot)$ and let $C \subset X$ be a code. Let D be the diameter of X. The distance distribution of the code is a $(D+1)$-vector $(A_0, A_1, \ldots, A_D)$, where

$$A_i = (1/|C|)|\{(\boldsymbol{c}, \boldsymbol{c}') \in C^2 : \partial(\boldsymbol{c}, \boldsymbol{c}') = i\}|.$$

Suppose X affords the structure of a Q-polynomial association scheme and let $q_t(x)$, $t = 0, 1, \ldots, D$, denote the corresponding set of Q-polynomials. The Q-transform of the distance distribution of C is defined as a vector $(A'_0, A'_1, \ldots, A'_D)$, where

$$A'_j = \frac{1}{|C|}\sum_{i=0}^{D} A_i q_j(i)$$

$$\sum_{j=0}^{D} A'_j = |X|/|C| \tag{1}$$

and by the Delsarte inequalities [6] all the numbers A'_i are nonnegative. We have $A_0 = A'_0 = 1$; if $d = d(C)$ is the minimum distance of C, then $A_1 = \cdots = A_{d-1} = 0$. Furthermore, if $d' - 1$ is the strength of C as a design in X, then $A'_1, \ldots, A'_{d'-1} = 0$. Below, we call d' the dual distance. We write $A_i(C)$ when we need to specify the code.

Let $g_w(x)$ be a real function defined on $\{0, 1, \ldots, D\}$, where w, $0 \le w \le D$, is an integer parameter. Define a moment function of the distance distribution of C

$$F_w(C) := \sum_{i=d}^{D} g_w(i) A_i(C).$$

We propose to derive bounds on $F_w(C)$. The reason for introducing the parameter w is to make expressions for the moment function algebraically independent for different w; see more on this in the end of this section.

Below we derive bounds on F_w for any code with a given d and/or d'. In this case we write $F_w(d, d')$. The same meaning is ascribed to the distance coefficients $A_i(d, d')$ and their exponents $a_\xi(\delta, \delta')$ (we put $i = \xi n$, $d = \delta n$, $d' = \delta' n$).

The following theorem enables us to construct upper and lower bounds on $F_w(d, d')$.

Theorem 1: Let $Z_w(x) = \sum_{i=0}^{D} z_i q_i(x)$ be a polynomial such that

$$z_i \le 0, \qquad \text{for } d' \le i \le D$$

and

$$Z_w(i) \ge g_w(i), \qquad \text{for } d \le i \le D. \tag{2}$$

Then

$$F_w(d, d') \le |C| z_0 - Z_w(0). \tag{3}$$

Let $Y_w(x) = \sum_{i=0}^{D} y_i q_i(x)$ be a polynomial such that

$$y_i \ge 0, \qquad \text{for } d' \le i \le D$$

and

$$Y_w(i) \le g_w(i), \qquad \text{for } d \le i \le D. \tag{4}$$

Then

$$F_w(d, d') \ge |C| y_0 - Y_w(0). \tag{5}$$

Proof: Using (1), we obtain

$$\sum_{i=0}^{D} Z_w(i) A_i = \sum_{i=0}^{D} A_i \sum_{j=0}^{D} z_j q_j(i) = \sum_{j=0}^{D} z_j |C| A'_j \le z_0 |C|.$$

Hence

$$F_w(d, d') = \sum_{i=d}^{D} g_w(i) A_i \le \sum_{i=d}^{D} Z_w(i) A_i \le z_0|C| - Z_w(0).$$

The proof of inequality (5) is similar. □

Remark: Bounds on $F_w(d, d')$ also imply bounds on $A_j(d, d')$ for any fixed j. Indeed, let $g_w(i) \ge 0$, $i = d, \ldots, n$, and $g_w(j) > 0$. Then

$$A_j(d, d') \le \frac{F_w(d, d')}{g_w(j)}. \tag{6}$$

Regarding lower bounds, it is convenient to choose $g_w(i) > 0$ for $i = d, d+1, \ldots, a$ and $g_w(i) \le 0$ for $i = a+1, \ldots, D$, where a is some number that usually depends on w. Then, if we are able to establish that $F_w(d, d') > 0$, this implies the existence of $j \in [d, a]$ such that

$$A_j(d, d') \ge \frac{F_w(d, d')}{g_w(j)}. \tag{7}$$

While such estimates can be asymptotically tight, they are too crude for codes of finite length. We discuss two ways of sharpening them. Denote by $\underline{F}_w(d, d')$ and $\overline{F}_w(d, d')$ lower and upper bounds on $F_w(d, d')$ and by $\underline{A}_j$ and by $\overline{A}_j$ lower and upper bounds on $A_j(d, d')$, respectively.

In [11], the following procedure was suggested to estimate the distance distribution of BCH codes. (The procedure actually works for any code with known d and d'.) First estimate A_d as follows:

$$\frac{\underline{F}_w(d, d')}{g_w(d)} \le A_d(d, d') \le \frac{\overline{F}_w(d, d')}{g_w(d)}.$$

Next, estimate other spectrum components through the recursion

$$\frac{1}{g_w(j)}\left(\underline{F}_w(d,\,d') - \sum_{i=d}^{j-1} g_w(i)\overline{A}_i\right) \le A_j(d,\,d') \le \frac{1}{g_w(j)}\left(\overline{F}_w(d,\,d') - \sum_{i=d}^{j-1} g_w(i)\underline{A}_i\right). \tag{8}$$

In the present paper, we use a different approach, which proved to be better in our examples. Namely, we choose the function g so that the matrix

$$G = [g_{wi}] = g_w(i), \qquad d \le w,\ i \le n \tag{9}$$

is nonsingular. Then, we compute

$$U = G^{-1} = [u_{ji}], \qquad d \le j,\ i \le n$$

and find lower and upper bounds on $A_j(d,\,d')$ as follows:

$$\sum_{i=d}^{n} u_{ji} b_i \le A_j(d,\,d') \le \sum_{i=d}^{n} u_{ji} c_i \tag{10}$$

where

$$b_i = \begin{cases} \overline{F}_i(d,\,d'), & \text{if } u_{ji} \le 0 \\ \underline{F}_i(d,\,d'), & \text{if } u_{ji} > 0 \end{cases}$$

and

$$c_i = \begin{cases} \overline{F}_i(d,\,d'), & \text{if } u_{ji} \ge 0 \\ \underline{F}_i(d,\,d'), & \text{if } u_{ji} < 0. \end{cases}$$

Our main examples are $X = H_2^n$, the Hamming scheme, and $X = J^{w,n}$, the binary Johnson scheme. If $X = H_2^n$, then $q_t(x) = K_t(x)$, where

$$K_t(x) = \sum_{i=0}^{n} (-1)^i \binom{x}{i}\binom{n-x}{t-i}(q-1)^{t-i} \tag{11}$$

is a Krawtchouk polynomial. Note that if C is a linear code in H_2^n, then d' is the distance of the orthogonal code C'.

A polynomial that satisfies (2) or (4) will be called feasible. In what follows, we construct several feasible polynomials and use them to derive bounds on the distance distribution, relying on (6) and (7) for growing code length and on (10) for codes of finite length.

III. An Asymptotic Bound

In this section, we will construct polynomials $Z_w(x)$ and $Y_w(x)$ with the help of the Christoffel–Darboux kernel (43).

Denote by $x_1^{(t)}$ the smallest root of $K_t(x)$. Let $t = \frac{n}{2} - \sqrt{d(n-d)}$, $\tau = \frac{t}{n}$, and $\delta = \frac{d}{n}$. Let us choose $g_w(i)$ and $Z_w(i)$ as follows:

$$g_w(i) = (K_w(i))^2$$

and

$$Z_w(i) = (K_w(i))^2 - \frac{c}{a-i}\,(K_{t+1}(i) + K_t(i))^2 \tag{12}$$

where a is such that

$$x_1^{(t+1)} \le a \le x_1^{(t)} \quad \text{and} \quad \frac{K_t(a)}{K_{t+1}(a)} = -1.$$

We assume through the rest of this section that d' is even.

Proposition 2: Let C be a code with distance d and dual distance d'. Let

$$c = \begin{cases} \dfrac{t+1}{2}\,\dfrac{\binom{n-d'}{w-d'/2}}{\binom{n-d'}{t-d'/2}}, & \text{if } d'/2 \le w \le t \\ 0, & \text{if } 0 \le w \le d'/2. \end{cases} \tag{13}$$

Then, for sufficiently large n

$$F_w(d,\,d') \le |C|\left[\binom{n}{w} - c\binom{n}{t}\right] - \binom{n}{w}^2 + \frac{c}{a}\left[\binom{n}{t+1} + \binom{n}{t}\right]^2, \qquad 0 \le w < t \le \frac{n}{2}. \tag{14}$$

Proof: By (46), $\frac{1}{n}x_1^{(t)} = \frac{1}{2} - \sqrt{\tau(1-\tau)} + o(1) = \delta + o(1)$. Therefore, for sufficiently large n

$$Z_w(i) \ge g_w(i), \qquad d \le i \le n.$$

The coefficients of the Krawtchouk expansion of the polynomial $\frac{1}{a-i}\,(K_{t+1}(i) + K_t(i))^2$, say β_j, can be estimated from below as follows [4]:

$$\beta_j \ge \frac{2}{t+1}\binom{n-j}{t-\frac{j}{2}}\binom{j}{\frac{j}{2}}. \tag{15}$$

By (44) in Appendix B, the Krawtchouk coefficients of $(K_w(i))^2$ are

$$\alpha_j = \binom{n-j}{w-\frac{j}{2}}\binom{j}{\frac{j}{2}}. \tag{16}$$

The definition of the constant c implies that $z_{d'} = \alpha_{d'} - c \cdot \beta_{d'} \le 0$. Note that $z_{d'}$ tends to zero for growing n. It is not difficult to check that β_j is decreasing on j slower than α_j when $0 \le j \le 2w$ (to verify this, compare the quantities α_{j+1}/α_j and β_{j+1}/β_j). Hence

$$z_j \le \alpha_j - c \cdot \beta_j \le 0 \qquad (j = d',\,\ldots,\,n).$$

Thus, $Z_w(i)$ is feasible.

Now, computing $Z_w(0)$ with the help of (45), we complete the proof. □

Let us consider the cases when only d or only d' is known.

A. Codes

We start with the case of known d, assuming that $d' = 0$ (note that if a polynomial is feasible for a given d and $d' = 0$ it is also feasible for any d'). Let

$$\omega^* = (1/2) - \sqrt{\xi(1-\xi)}. \tag{17}$$

Theorem 3: Let C be a code of distance δn. Its distance distribution is bounded above as follows:

$$a_\xi(\delta, 0) \le H\left(\tfrac{1}{2} - \sqrt{\delta(1-\delta)}\right) + H(\xi) - 1 + o(1) \qquad (\delta \le \xi \le 1/2). \quad (18)$$

Proof: Let $\omega = w/n$. Substituting $d' = 0$ into (13), we get from (14)

$$a_\xi(\delta, 0) \le H(\omega) + H(\tau) - \frac{1}{n}\log g_{\lfloor \omega n \rfloor}(\lfloor \xi n \rfloor) + o(1).$$

To estimate $A_{\lfloor \xi n \rfloor}$, we have to choose ω. A good choice is $\omega = \omega^*$ (in fact, this choice is optimal, though we leave this fact without proof). From (48), it follows that

$$\frac{1}{n}\log g_{\lfloor \omega^* n \rfloor}(\lfloor \xi n \rfloor) = 1 + H(\omega^*) - H(\xi).$$

Now, a simple substitution completes the proof. □

Another proof of this theorem is given in Appendix A. It is based on some new bounds on orthogonal polynomials derived recently in [12].

Theorem 3 gives a universal bound on the growth of the distance coefficients in a code with a given distance. Let us examine the question when this bound is nontrivial. It can be trivial for one of the two reasons: the right-hand side of (18) is greater than the total size of the code, or it is greater than any known upper bound on the size of a code of constant weight ξn and distance δn.

Let us examine the last option. Let $R(\xi, \delta)$ be the maximal size of a code of constant weight ξn and Hamming distance δn. One of the bounds on this quantity is [23]

$$R(\xi, \delta) \le R_1(\xi, \delta) := H\left(\tfrac{1}{2}\left(1 - \sqrt{1 - (\sqrt{4\xi(1-\xi) - \delta(2-\delta)} - \delta)^2}\right)\right) \qquad (0 \le \delta \le \xi(1-\xi)); \quad (19)$$

for large distances this bound is the best known. A better bound for small δ was obtained in [24] based on a result in [18] (in this form it is given in [2]).

Proposition 4 [24]: Let

$$\xi_0 = \operatorname*{arg\,min}_{(1-\sqrt{1-2\delta})/2 \le \alpha \le 1/2} 1 - H(\alpha) + R_1(\alpha, \delta).$$

Then

$$R(\xi, \delta) \le H(\xi) - H(\xi_0) + R_1(\xi_0, \delta) \qquad (\xi_0 \le \xi \le 1/2). \quad (20)$$

Comparison of these results shows that we can estimate distance distributions better than the general bounds (19) and (20) for large code distances. More specifically, it is clear that whenever (20) is valid, is better than (18) (indeed, the right-hand side of (20) equals $H(\xi) - 1$ plus the *second* bound of [23], as opposed to the first one in (18)). However, it is known that for $0.273 \le \delta \le 1/2$ the value $\xi_0 = 1/2$. For these δ bound (20) is void. Moreover, calculations show that in this range of distances, $R_1(\xi, \delta)$ in (19) as a bound on the distance distribution is also inferior to (18). For distances $0.24 \le \delta \le 0.273$ there is a segment of weights beginning with δ where (18) is better than both (20) and (19). The whole picture is shown in Fig. 1.

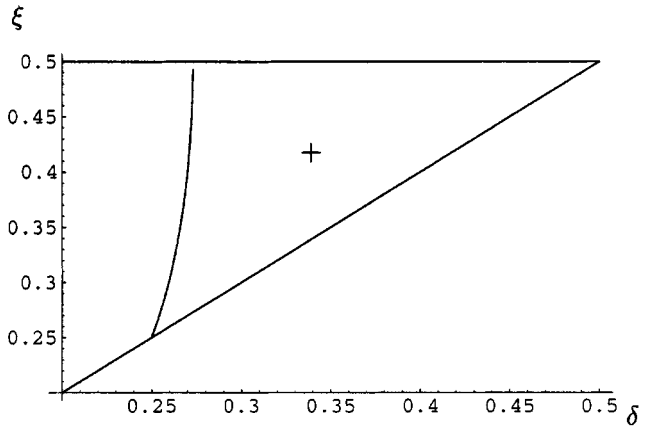

Fig. 1. Region in the (δ, ξ)-plane, marked with a $+$, where (18) is the best estimate of the distance distribution.

It is more difficult to compare (18) with the total size of the code since this bound does not involve explicitly the code rate R. As shown below, for putative sequences of codes meeting the 1st bound of [23], the bound (18) is tight, so it is certainly nontrivial for all $\delta \in (0, 1/2)$. For codes meeting the Gilbert–Varshamov (GV) bound $R = 1 - H(\delta)$ the right-hand side of (18) is less than R whenever

$$(1 - H(\delta)) - (H((1/2) - \sqrt{\delta(1-\delta)}) + H(\xi) - 1) > 0. \quad (21)$$

For small δ this holds true for all ξ outside a small segment around 1/2 (for $\delta \to 0$ this segment shrinks to the point 1/2).

Another approach to bounding the distance distribution of codes was taken in [20]. In particular, in [20] it is proved that in any *linear* code the number of vectors of any weight $i = \xi n$ does not exceed $O(|C|/\sqrt{n})$. When Theorem 3 is nontrivial (for instance, for all ξ such that (21) holds true), it shows that the number of vectors of weight i has a much slower exponential growth than $|C|$. However, there is a range of code parameters when the bound in [20] is better than both. In [26], the authors study the threshold probability of a code C with a given distance d, i.e., the crossover probability $\theta(C)$ of a binary symmetric channel such that the error probability of maximum likelihood decoding of C in this channel equals $1/2$. They give a lower bound on $\theta(C)$ via an upper bound on the distance distribution of C, and then rely on upper bounds on constant weight codes. Our estimate (18) sometimes yields a better bound on $\theta(C)$.

Theorem 3, together with earlier results, implies interesting results on the distance distribution of certain sequences of codes. The following theorem is a combination of results in [22] and [15].

Theorem 5: For sufficiently large n and any $0 \le \omega \le H^{-1}(R)$ there exists $\xi \in [\delta, \frac{1}{2} - \sqrt{\omega(1-\omega)}]$ such that

$$a_\xi(\delta, 0) \ge R + H(\omega) - (2/n)\log K_{\lfloor \omega n \rfloor}(\lfloor \xi n \rfloor) + o(1). \quad (22)$$

Moreover, every subinterval of the interval $(\delta, 1/2)$ of length $n^{-\frac{1}{2}+\epsilon}$, $\epsilon > 0$, contains a point ξ such that this inequality holds true.

Now let us assume that a code G of rate R meets the first form of the linear programming bound from [23], i.e.,

$$\delta(G) = \delta_{lp}(R) := 1/2 - \sqrt{H^{-1}(R)(1 - H^{-1}(R))}.$$

Then Theorems 3 and 5 imply the following necessary condition on the existence of G.

Corollary 1: The distance distribution of G is asymptotically binomial in the following sense: the equality

$$a_\xi(G) = R + H(\xi) - 1 + o(1)$$

holds for some ξ within every subinterval of length $n^{-\frac{1}{2}+\epsilon}$, $\epsilon > 0$, of the interval $(\delta_{lp}(R), 1/2)$.

Proof: It follows from the observation that the right-hand sides of (18) and (22) under the assumptions of the corollary can be made the same. Indeed, let us put $\xi = \frac{1}{2} - \sqrt{\omega(1-\omega)}$ in Theorem 5. Then, together with (48) we obtain $R + H(\xi) - 1 + o(1)$ on the right-hand side of (22). On the other hand, a substitution of $H(\frac{1}{2} - \sqrt{\delta(1-\delta)}) = R$ into (18) gives

$$a_\xi(G) \le R + H(\xi) - 1 + o(1), \qquad \delta_{lp} < \xi < \tfrac{1}{2}$$

and the claim follows. □

This corollary complements a result in [2] in the following way. In that paper, we proved that the distance distribution of codes meeting the second bound of [23] is asymptotically binomial for code rates $0.421 < R \le 1$. Here, we prove the same for all $R \in (0, 1)$ with respect to codes that meet the first bound of [23]. The first and second bounds coincide for $0 \le R \le 0.305$. Hence, as conclusion, binary codes of rate R that meet the McEliece *et al.* bounds (if such exist) are proved to have asymptotically binomial distance distribution for $R \in (0, 0.3) \cup (0.421, 1)$.

As another example, consider a sequence of codes with rate and distance related by $R = 1 - H(\delta)$ and with distance distribution $A_w \le n\binom{n}{w}|C|2^{-n}$ (these codes can be chosen among linear codes meeting the GV bound). For them, Theorem 5 implies the existence of an exactly binomial component in any subinterval of weights of length $n^{\frac{1}{2}+\epsilon}$ located between $n\delta_{lp}(R)$ and $n/2$. The proof is basically the same as that of Corollary 1; details are omitted.

B. Designs

The following bounds on the distance distribution of a code as a function of its dual distance were implicitly obtained in [14].

Theorem 6 [14]:

$$a_\xi(0, \delta') \le \begin{cases} R + H(\xi) - 1 + o(1), & 0 \le \frac{1}{2} - \sqrt{\xi(1-\xi)} \le \delta'/2 \\ R + H(\delta'/2) - \dfrac{2}{n}\log K_{d'/2}(\lfloor \xi n \rfloor) + o(1), & \\ \qquad\qquad \delta'/2 < \frac{1}{2} - \sqrt{\xi(1-\xi)} \le 1/2. & \end{cases}$$

Actually the authors of [14] were interested in estimating the range of weights $\mathcal{I} \subset [0, 1/2]$ where the distance distribution of a code (design) is at most binomial: $a_\xi \le R + H(\xi) - 1 + o(1)$ for any $\xi \in \mathcal{I}$. Theorem 6 implies that

$$[1/2(1 - \sqrt{\delta'(2-\delta')}), 1/2] \subseteq \mathcal{I}.$$

We will now show that this inclusion generally is strict, thereby extending the binomiality interval, and also improve the second estimate in Theorem 6 for some code parameters.

Let us use the polynomial (12). To guarantee its feasibility for any d we put $d = 0$. If $\omega^* \le \delta'/2$ we choose $\omega = \omega^*$ (17). By (13), $c = 0$. Now, with the help of (48) after simple computations, we get the first case of Theorem 6. The more interesting case is the one with $\omega^* = \frac{1}{2} - \sqrt{\xi(1-\xi)} \ge \frac{\delta'}{2}$, i.e., $\xi \le (1/2)(1 - \sqrt{\delta'(2-\delta')})$. In this situation, the choice of ω is *a priori* unclear, and, hence, c can be greater than zero. Thus

$$\begin{aligned} F_w(0, d') &\le |C|\left[\binom{n}{w} - c\binom{n}{t}\right] - \binom{n}{w}^2 + \frac{c}{a}\left[\binom{n}{t+1} + \binom{n}{t}\right]^2 \\ &\le |C|\binom{n}{w} + \frac{c}{a}\left[\binom{n}{t+1} + \binom{n}{t}\right]^2, \\ &\qquad \frac{d'}{2} \le w \le n\left[\frac{1}{2} - \sqrt{\xi(1-\xi)}\right]. \end{aligned} \quad (23)$$

Let us compute the exponents of each term in (23)

$$\begin{aligned} &\frac{1}{n}\log|C|\binom{n}{w} \\ &\quad = R + H(\omega) + o(1) \\ &\frac{1}{n}\log\frac{c}{a}\left[\binom{n}{t+1} + \binom{n}{t}\right]^2 \\ &\quad = (1-\delta')H\left(\frac{\omega - \delta'/2}{1-\delta'}\right) + 2 - (1-\delta') + o(1) \\ &\quad = (1-\delta')H\left(\frac{\omega - \delta'/2}{1-\delta'}\right) + 1 + \delta' + o(1). \end{aligned}$$

Eventually, we obtain the theorem.

Theorem 7: For any $\omega \in [0, \frac{1}{2} - \sqrt{\xi(1-\xi)}]$

$$\begin{aligned} a_\xi(0, \delta') \lesssim &-\frac{2}{n}\log K_{\lfloor \omega n \rfloor}(\lfloor \xi n \rfloor) \\ &+ \max\left\{R + H(\omega), (1-\delta')H\left(\frac{\omega - \delta'/2}{1-\delta'}\right) + 1 + \delta'\right\}. \end{aligned}$$

It follows from this theorem that, for codes of sufficiently large size, the interval of binomiality can be expanded compared to Theorem 6. Namely, let

$$\xi_1 := (1/2)(1 - \sqrt{\delta'(2-\delta')})$$

and ξ_2 be the root of the equation

$$R = (1-\delta')H\left(\frac{\omega^* - \delta'/2}{1-\delta'}\right) + 1 + \delta' - H(\omega^*).$$

If the root of this equation is negative, we put $\xi_2 = 0$.

Corollary 2: Let C be a code of rate R with dual distance d'. For any $\xi \in [\min\{\xi_1, \xi_2\}, 1/2]$, the code C has asymptotically binomial distance distribution

$$a_\xi(0, \delta') \le R + H(\xi) - 1 + o(1).$$

This result can extend substantially the binomiality range in codes' spectra compared to Theorem 6; see the example in the end of Section V.

IV. Constant Weight Codes

In this section, we apply Theorem 1 to codes in the Johnson space $J^{w,n}$. The corresponding metric $\partial(c, c')$ equals half the Hamming distance between c and c'. As above, let C be a code and $A = (A_0, A_1, \ldots, A_w)$ be its distance distribution. In this case, the family of q-polynomials is formed by some Hahn polynomials $Q_t(x)$, orthogonal on $(0, 1, \ldots, w)$ with weight $\mu(i) = \frac{\binom{w}{i}\binom{n-w}{i}}{\binom{n}{w}}$. Hahn polynomials share many properties of Krawtchouk polynomials. The collection of basic facts was derived in [6], the asymptotics of the extremal zero was found in [23] (with a refinement in [19]), and the exponential asymptotics outside the oscillatory segment was computed in [1] and [22].

The following theorem is proved similarly to Theorem 6 by taking in Theorem 1 $Z(x) = Q_t^2(x)$ with a suitable t dependent on ξ.

Theorem 8: Let C be a code of rate R in $J^{w,n}$ with dual distance $d' = \delta' n$. Let $n \to \infty$ and $w = \omega n$. Then

$$a_\xi(0, \delta') \lesssim \begin{cases} R + \omega H\left(\dfrac{\xi}{\omega}\right) + (1-\omega) \cdot H\left(\dfrac{\xi}{1-\omega}\right) - H(\omega), \\ \quad \text{if } x_1^{(d'/2)} \Big/ n < \xi \le 2\omega(1-\omega) \\ R + H(\delta'/2) - (2/n) \log Q_{\frac{\delta'}{2}}(\xi n), \\ \quad \text{if } \xi \le x_1^{(d'/2)} \Big/ n \end{cases}$$

where

$$x_1^{(\tau n)} = n \frac{\omega(1-\omega) - \tau(1-\tau)}{1 + 2\sqrt{\tau(1-\tau)}}.$$

Note that the first of the two estimates, again, states that in a certain range depending on $d^\perp$, the distance distribution of a code is bounded above by the mathematical expectation of the distance distribution of a code chosen in $J^{w,n}$ with uniform probability. To justify this, notice that the sphere in $J^{w,n}$ of radius i has size $\binom{w}{i}\binom{n-w}{i}$, so the normalized uniform measure of the spheres in $J^{w,n}$ is given by $\mu(i)$. This theorem admits improvements along the lines of Theorem 7.

V. Bounds for High-Rate Codes

In this section, we will construct several polynomials that give tight bounds on the distance distributions of good codes of rate close to one.

We start with deriving bounds for codes of finite length, confining ourselves to the case of odd minimum distance $d = 2e + 1$. The case of even d can be analyzed similarly. Upon deriving upper and lower bounds on the distance distribution of a code with known d, d', we consider a few examples in which the bounds are virtually tight. In one example we also compute bounds on the probability of undetected error and of decoding error, illustrating the use of the distance distribution coefficients. Then we turn to asymptotics, again looking separately at codes and designs. The bounds derived in this part supplement the results of the previous section, covering the range of code rates $R \to 1$.

Let n be fixed. For any w, $d \le w \le n$, let

$$g_w(x) = \sum_j g_j K_j(x)$$

be the polynomial of degree $\le n$ with the Krawtchouk coefficients

$$g_j = K_{w-e}(j) L_e(j) \qquad (d \le w \le n)$$

where

$$L_e(x) = K_0(j) + K_1(j) + \cdots + K_e(j)$$

is the Lloyd polynomial.

In what follows, we construct feasible polynomials $Z_w(i)$ and $Y_w(i)$, which enable us to compute numerically lower and upper bounds on the distance distribution of a code. Since these bounds cannot be formulated as closed-form expressions, we do not present the results in the form of theorems.

Let $Z_w(i)$ be the polynomial with the Krawtchouk coefficients

$$z_j = K_{w-e}(j) L_e(j) - c L_e^2(j) \tag{24}$$

where c is chosen below. Let us compute $g_w(i)$ and $Z_w(i)$. Using (41), (44), and (42) in Appendix B, we have

$$\sum_{j=0}^{n} K_{w-e}(j) K_t(j) K_j(i) = \sum_{j=0}^{n} K_j(i) \sum_{s=0}^{n} p^s_{w-e,\,t} K_s(j) = 2^n p^i_{w-e,\,t}.$$

From this, we obtain

$$g_w(i) = 2^n \sum_{t=0}^{e} p^i_{w-e,\,t}. \tag{25}$$

In a similar way, one can compute $Z_w(i)$. In particular, for $i \ge d$

$$\sum_j (L_e(j))^2 K_j(i) = \frac{2^n}{\binom{n}{i}} \langle L_e^2, K_i \rangle = \frac{2^n}{\binom{n}{i}} \sum_{s,t} \langle K_s K_t, K_i \rangle = \frac{2^n}{\binom{n}{i}} \sum_{s,t} \sum_{u=0}^{s+t} p^u_{st} \langle K_u, K_i \rangle = 0.$$

So, we see that

$$Z_w(i) = g_w(i), \qquad d \le i \le n \tag{26}$$

$$Z_w(0) = -c \cdot 2^n \sum_{t=0}^{e} \binom{n}{t}. \tag{27}$$

TABLE I

j	3	4	5	6	7	8	14	18	22	24
$\log \overline{A}_j$	8.483	11.973	14.971	17.815	20.345	22.714	32.874	36.722	38.616	38.904
$\log \underline{A}_j$	7.938	11.675	14.312	17.468	19.643	22.333	32.306	35.881	37.146	36.650

This prompts the following choice of c:

$$c = \max_{d' \le j \le n} \frac{K_{w-e}(j)}{L_e(j)}. \tag{28}$$

It is clear that with this choice $z_j \le 0$, $d' \le j \le n$; thus, $Z_w(i)$ is feasible. By (45) in Appendix B

$$z_0 = \binom{n}{w-e} \sum_{t=0}^{e} \binom{n}{t} - c \left(\sum_{t=0}^{e} \binom{n}{t} \right)^2. \tag{29}$$

Now, one can compute numerically an upper estimate of $F_w(d, d')$ from Theorem 1 and (25)–(29).

To estimate $F_w(d, d')$ from below, choose $Y_w(i)$ with the coefficients

$$y_j = K_{w-e}(j) L_e(j) - c(L_e(j))^2 \tag{30}$$

where

$$c = \max_{d' \le j \le n} - \frac{K_{w-e}(j)}{L_e(j)}.$$

This polynomial is feasible for the same reasons as the previous one.

Example 1: For the sake of argument, let us apply the results of this section to perfect codes. Let C be a code with minimum distance $d = 2e + 1$ that meets the Hamming bound, that is

$$|C| \sum_{t=0}^{e} \binom{n}{t} = 2^n. \tag{31}$$

Let us find an estimate for $A_d(C)$. Putting $w = d$ and simplifying, we obtain $g_d(d) = 2^n \binom{2e+1}{e+1}$. Now, using (26), (27), (29), and taking into account (31), we compute $\frac{1}{g_d(d)} (z_0|C| - z_{e+1}(0))$. So, finally

$$A_d(C) \le \binom{n}{e+1} \Big/ \binom{2e+1}{e+1}.$$

Using the same arguments for the polynomial $Y_d(x)$, we get

$$A_d(C) \ge \binom{n}{e+1} \Big/ \binom{2e+1}{e+1}.$$

Thus, we have derived the well-known expression for the minimum distance component of the distance distribution of a perfect code. Moreover, if C meets the Hamming bound, then from the definitions of the polynomials $g_w(i)$, $Z_w(i)$, and $Y_w(i)$ and (31) we have

$$z_0|C| - Z_w(0) = y_0|C| - Y_w(0), \qquad d \le w \le n.$$

In other words, $F_w(C)$ is found exactly for all w. Now (8) or (10) enable us to reconstruct the entire distance distribution of C.

Example 2: Let us estimate the distance distribution of a code C of length 47, size $9 \cdot 2^{38}$, and minimum distance 3, which is the best known for these parameters [21]. Computing the matrix (9), one can check that it is invertible. Now, using in (10) the polynomials defined by (24) and (30), we find upper and lower bounds on the spectrum of the code. The results of computations for some values of j are presented in Table I (the bounds are computed for all $d \le j \le n$).

One can see that the upper and lower bounds are close to one another. Using these bounds, let us find upper and lower bounds on the probability of undetected error $P_{ue}(C)$ and of decoding error $P_{de}(C)$ for C under complete decoding. We assume that codewords of C are sent over the binary symmetric channel with crossover probability p. Then

$$\sum_{i=d}^{n} \underline{A}_i p^i (1-p)^{n-i} \le P_{ue}(C) \le \sum_{i=d}^{n} \overline{A}_i p^i (1-p)^{n-i}.$$

For P_{de}, let us assume that $c \in C$ is the vector transmitted over the channel and e is the error vector. We use the following crude estimates:

$$\sum_{c' \ne c} \Pr(\partial(c', e) \le 1) \le P_{de}(C) \le 1 - \Pr(\|e\| \le 1).$$

The results are shown in Fig. 2. In both cases, the difference between the upper and lower bounds is within the 50% range.

If some additional information about the code or its dual code is available, we can tighten the bounds even further. Consider the following example.

Example 3: Let C be an extended BCH code correcting $e = 3$ errors. C has length 2^m, dimension $2^m - 3m - 1$, and minimum distance 8. Since the code C' contains the all-one word, we can rewrite the estimates on $F_w(C)$ as follows:

$$|C|(y_0 + y_n) - Y_w(0) \le F_w(C) \le |C|(z_0 + z_n) - Z_w(0)$$

where

$$z_j \le 0 \quad \text{and} \quad y_j \ge 0, \qquad \text{for } d' \le j \le n - d'.$$

It is well known that $d' \ge n/2 - 2\sqrt{n}$. Moreover, C' is a subcode of the Reed–Muller code of the second order, and, therefore, A'_j can be nonzero only if j is a multiple of $2^{\lceil m/2 \rceil - 1}$. Hence, we have to guarantee nonpositivity of z_j and nonnegativity of y_j only for such j's. Define polynomials $g_w(i)$, $Z_w(i)$, and $Y_w(i)$ for even w, $d \le w \le n - d$, by their coefficients as follows:

$$\begin{aligned} g_j &= K_{w-e}(j) K_e(j) \\ z_j &= K_{w-e}(j) K_e(j) - c_u \cdot (K_e(j))^2 \\ y_j &= K_{w-e}(j) K_e(j) + c_l \cdot (K_{e-1}(j))^2. \end{aligned}$$

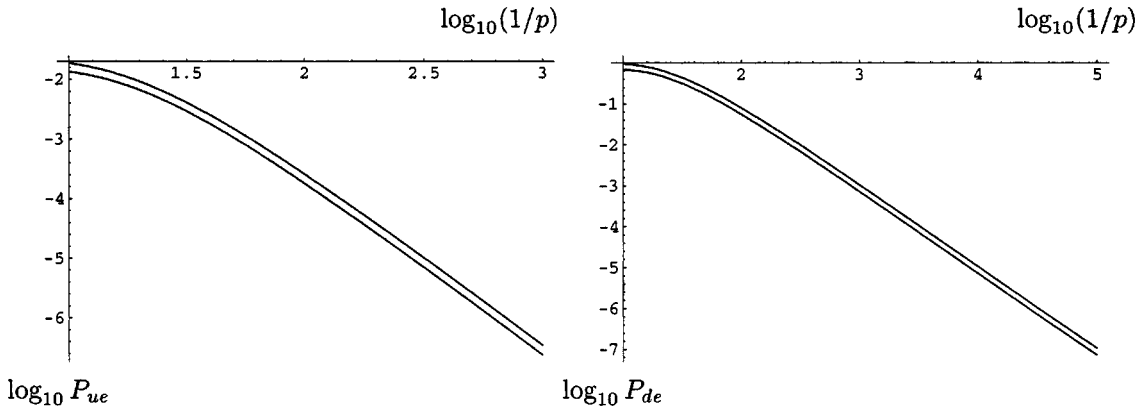

Fig. 2. Estimates of P_{ue} and P_{de} for the $[47,\ 9\cdot 2^{38},\ 3]$ code of Example 3.

Here, c_u and c_l are the minimum possible nonnegative numbers such that z_j and y_j satisfy the aforementioned conditions. Since the second terms of $Z_w(i)$ and $Y_w(i)$ are positive, such c_l and c_u always exist.

This is all we need to compute bounds on $A_j(C)$ with the help of Theorem 1 and expression (10). For instance, let $m=8$. The bounds for the first five distance distribution components are presented in Table II.

Note that these estimates are slightly better than the results in [11] and [8]. Estimates for the distance distribution of BCH codes with other values of c can be found similarly.

Now, let us move to the asymptotic case. Let $V_w(i)$ be the polynomial with the coefficients

$$v_j=\frac{w+1}{2(a-j)}\left(K_{w+1}(j)+K_w(j)\right)^2$$

where a is a real number such that $x_1^{(w+1)}\le a\le x_1^{(w)}$ and $K_w(a)=-K_{w+1}(a)$. Let us define polynomials $g_w(i)$ and $Z_w(i)$ as follows:

$$\begin{aligned} g_w(i)&=2^n\binom{n-i}{w-\frac{i}{2}}\binom{i}{\frac{i}{2}}\\ Z_w(i)&=V_w(i)-c\cdot 2^n\binom{n-i}{\frac{d-1}{2}-\frac{i}{2}}\binom{i}{\frac{i}{2}},\qquad w\ge\frac{d}{2}. \end{aligned}\tag{32}$$

We put $w=\omega n$ for the rest of this section.

Proposition 9: Let C be a code with distance d and dual distance d'. Let

$$c=\begin{cases}\dfrac{w+1}{2(a-d')}\dfrac{\left(K_{w+1}(d')+K_w(d')\right)^2}{\left(K_{\frac{d-1}{2}}(d')\right)^2},\\ \qquad \text{if } 0\le d'\le n\left(\dfrac{1}{2}-\sqrt{\omega(1-\omega)}\right)\\ 0,\quad \text{if } n\left(\dfrac{1}{2}-\sqrt{\omega(1-\omega)}\right)\le d'\le\dfrac{n}{2}.\end{cases}\tag{33}$$

TABLE II

j	8	10	12	14	16
$\log \overline{A}_j$	24.860	33.969	42.790	51.135	59.060
$\log \underline{A}_j$	24.437	33.919	42.785	51.134	59.059

Then, for sufficiently large n,

$$\begin{aligned} F_w(d,d')&\le |C|\left[\frac{w+1}{2a}\left(\binom{n}{w+1}+\binom{n}{w}\right)^2-c\binom{n}{\frac{d-1}{2}}^2\right]\\ &\quad -2^n\binom{n}{w}+c2^n\binom{n}{\frac{d-1}{2}}. \end{aligned}$$

Proof: To derive the bound, we use the polynomial $Z_w(x)$ (32) in Theorem 1. First, let us prove that it is feasible. Using the Christoffel–Darboux formula (43) and (42), we obtain

$$\begin{aligned} v_j&=\binom{n}{w}\left(K_{w+1}(j)+K_w(j)\right)\frac{1}{K_w(a)}\sum_{i=0}^{w}\frac{K_i(j)K_i(a)}{\binom{n}{i}}\\ &=\frac{1}{K_w(a)}\binom{n}{w}\sum_{i=0}^{w}\frac{K_i(a)}{\binom{n}{i}}\sum_{s=0}^{n}\left[p^s_{w+1,\,i}K_s(j)+p^s_{wi}K_s(j)\right]\\ &=\sum_{s=0}^{n}\frac{K_s(j)}{K_w(a)}\binom{n}{w}\sum_{i=0}^{w}\frac{K_i(a)}{\binom{n}{i}}\left(p^s_{w+1,\,i}+p^s_{wi}\right). \end{aligned}$$

Again relying on (42), we calculate for integer x

$$\begin{aligned} V_w(x)&=\sum_{j=0}^{n}v_jK_j(x)\\ &=\frac{1}{K_w(a)}\binom{n}{w}\sum_{s=0}^{n}\sum_{i=0}^{w}\frac{K_i(a)}{\binom{n}{i}}\left(p^s_{w+1,\,i}+p^s_{w,\,i}\right)\\ &\quad\cdot\sum_{j=0}^{n}K_j(x)K_s(j)\\ &=2^n\frac{1}{K_w(a)}\binom{n}{w}\sum_{i=0}^{w}\frac{K_i(a)}{\binom{n}{i}}\left(p^x_{w+1,\,i}+p^x_{w,\,i}\right). \end{aligned}$$

Assume that w and x are even. In other cases, the arguments are similar. Estimating the sum in the last expression by the term $i = w$, we have

$$V_w(x) \geq 2^n \binom{n-x}{w-\frac{x}{2}} \binom{x}{\frac{x}{2}}. \tag{34}$$

From this estimate and from the definition of $Z_w(i)$, it follows that

$$Z_w(i) \geq g_w(i), \qquad d \leq i \leq n.$$

It remains to prove that $z_i \leq 0$ for $d' \leq i \leq n$. First, observe that $z_{d'} = 0$. Indeed, by (44)

$$\sum_{j=0}^{n} (K_{\frac{d-1}{2}}(j))^2 K_j(i) = \sum_j \sum_s p^s_{\frac{d-1}{2},\frac{d-1}{2}} K_s(j) K_j(i) = 2^n p^i_{\frac{d-1}{2},\frac{d-1}{2}}.$$

So, the Krawtchouk coefficients in the expansion

$$2^n \binom{n-i}{\frac{d-1}{2}-\frac{i}{2}} \binom{i}{\frac{i}{2}} = \sum_{j=0}^{n} \beta_j K_j(i)$$

are $\beta_j = (K_{\frac{d-1}{2}}(j))^2$. Together with the definition of c (33) this implies that $z_{d'} = 0$. Let us show that $z_j = v_j - c\beta_j \leq 0$, $d' \leq j \leq n$, for large n. First if $x_1^{(w)} < d'$ then $c = 0$ and $v_j < 0$, so let us assume that $d' \leq x_1^{(w)}$. Note that we only need to consider the values of j in the interval $d' \leq j \leq x_1^{(w)}$ because for greater j by the above we have $v_j < 0$. Since $v_{d'} = c\beta_{d'}$, it suffices to show that for large n the quantity $c\beta_j$ decreases on j slower than v_j.

Observe that

$$\log v_j \sim 2 \log K_w(j)$$

and

$$\log \beta_j \sim 2 \log K_{d/2}(j).$$

For $w > d/2$ we have $x_1^{(w)} \leq x_1^{(d/2)}$, so both polynomials are positive and decline rapidly as j grows. We will prove that for large n the decline rate of $K_{d/2}(j)$ is slower that of $K_w(j)$. Let $j = \xi n$ and write the derivative of the exponent of $K_w(j)$ in the form $(d/d\xi) \log K_{\omega n}(\xi n) = n\phi(\omega, \xi) + o(n)$. Then from (47) we get

$$\phi(\omega, \xi) = \log \frac{1 - 2\omega + \sqrt{1 - 4\omega + 4\omega^2 - 4\xi + 4\xi^2}}{2 - 2\xi}$$

valid for $0 < \xi < (1/2) - \sqrt{\omega(1-\omega)}$. It is easy to check that for a fixed ξ in this interval, $\phi(\omega, \xi)$ is a decreasing function of ω. Therefore, the exponent of v_j is falling faster than that of β_j for $d' \leq j \leq x_1^{(w)}$. This finishes the proof of feasibility of the polynomial (32).

It remains to compute the bound (3). Using (40) and (45), we find $Z_w(0)$ and z_0. Thereby, the proof is completed. □

Let us again consider the cases when only d or only d' is known.

A. Codes

In this case, substitution of $d' = 0$ yields a known result. It was obtained in [17], based on a result in [5].

Proposition 10: Let C be a code with distance $d = \delta n$. Then

$$a_\xi(\delta, 0) \leq H(\xi) - H\left(\frac{\delta}{2}\right) + o(1), \qquad \delta \leq \xi \leq \frac{1}{2}. \tag{35}$$

The proof amounts to a straightforward calculation, which we omit. This bound is inferior to (20) and other bounds of this form [17] on the size of a constant weight code.

The following theorem presents a lower bound on $A_{\lfloor \xi n \rfloor}$.

Theorem 11: For sufficiently large n and any $\omega \geq H^{-1}(1 - R)$ there exists $\xi \in [0, 2\omega]$ such that

$$a_\xi(\delta, 0) \geq 2H(\omega) + R - 1 - (1-\xi) H\left(\frac{\omega - \xi/2}{1-\xi}\right) - \xi + o(1). \tag{36}$$

Proof: Let us choose $Y_w(i) = g_w(i)$. Then by (44) $y_j = (K_w(j))^2$, and $Y_w(i)$ is obviously feasible. Compute

$$\log y_0 = 2nH(\omega), \qquad \log Y_w(0) = n(1 + H(\omega))$$

and note that $\frac{1}{n} \log y_0 + R \geq \frac{1}{n} \log Y_w(0)$ for $w = n\omega \geq nH^{-1}(1-R)$. So for such values of w the term $|C| y_0$ grows exponentially faster than $Y_w(0)$. As suggested in the remark after Theorem 1, we have $g_w(i) = 0$ for $i > 2w$, hence there exists an index $i \in [0, 2w]$ such that

$$A_i(d, 0) \geq \frac{|C| y_0}{g_w(i)} (1 - o(1)).$$

We conclude by computing logarithms. □

Remark: As a continuation of Example 1, let us observe that the above results imply that the distance distribution of a perfect code is asymptotically binomial

$$a_\xi = R + H(\xi) - 1 + o(1), \qquad \delta \leq \xi \leq \tfrac{1}{2}.$$

This follows by combining the estimates of the two preceding statements. Since nontrivial perfect codes of growing length do not exist, we do not include the details. However, there is some theoretical interest in the fact that the distance distribution of codes that meet in the asymptotics a linear-programming bound, converges to the binomial distribution [this holds true for both instances considered in this paper, and is also true in the Johnson space with respect to the bound (19)].

B. Designs

The following bounds on A_j as a function of d' were implicitly obtained in [14].

Theorem 12 [14]: Let C be a code with dual distance $d' = \delta' n$. Then, the bound is in the equation at the bottom of the page.

$$a_\xi(0, \delta') \leq \begin{cases} R - 1 + H(\xi) + o(1), & \text{if } \dfrac{(1-2\delta')^2}{2} \leq \xi \leq \dfrac{1}{2} \\ R + 2H\left(\dfrac{1}{2} - \sqrt{\delta'(1-\delta')}\right) - 1 - \xi - (1-\xi) H\left(\dfrac{1}{2} - \dfrac{\sqrt{\delta'(1-\delta')}}{1-\xi}\right) + o(1), & \text{if } 0 \leq \xi < \dfrac{(1-2\delta')^2}{2}. \end{cases}$$

We will rederive the first part of this theorem, improve the second part, and as a corollary, extend the interval of binomiality for codes of sufficiently large size. Let

$$\omega^{**} = (1/2)(1 - \sqrt{1 - 2\xi})$$

and let $q(n)$ be some function of polynomial growth.

First, suppose that $\frac{1}{2} - \sqrt{\omega(1-\omega)} \le \delta'$. Then, by (33), $c = 0$ and $Z_w(x) = V_w(x)$. From this, we have

$$\begin{aligned} F_w(0, \delta') &\le |C| v_0 - V_w(0) \\ &= q(n)|C|\binom{n}{w}^2 - 2^n\binom{n}{w} < q(n)|C|\binom{n}{w}^2 \end{aligned}$$

and

$$a_\xi(0, \delta') \le R + 2H(\omega) - 1 - (1-\xi)H\left(\frac{\omega - \xi/2}{1-\xi}\right) - \xi + o(1).$$

The optimal choice of ω is $\omega = \omega^{**}$. Hence, whenever $0 \le \frac{1}{2} - \sqrt{\omega^{**}(1-\omega^{**})} \le \delta'$, or, equivalently, $\frac{(1-2\delta')^2}{2} \le \xi \le \frac{1}{2}$, the following inequality is true:

$$a_\xi(0, \delta') \le R + 1 - H(\xi) + o(1).$$

This is the first part of Theorem 12.

Now, let $\frac{1}{2} - \sqrt{\omega(1-\omega)} \ge \delta'$. Then, $c > 0$ and

$$\begin{aligned} F_w(0, d') &\le |C|\left(q(n)\binom{n}{w}^2 - 2^n c\right) - 2^n\binom{n}{w} + c2^n \\ &\le q(n)|C|\binom{n}{w}^2 + c2^n. \end{aligned}$$

We obtain the following theorem..

Theorem 13: Let $0 \le \xi \le \frac{(1-2\delta')^2}{2}$. Then, for any

$$\omega \in \left[\frac{1}{2} - \sqrt{\delta'(1-\delta')}, \frac{1}{2}\right]$$

$$a_\xi(0, \delta') \lesssim \min[R + 2H(\omega), (2/n)\log K_w(d') + 1] - (1-\xi)H\left(\frac{\omega - \xi/2}{1-\xi}\right) - 1 - \xi.$$

As mentioned earlier, the interval of binomiality can be extended for sufficiently large codes. Let $\xi_1 = (1-2\delta')^2/2$ and let ξ_2 be the root of the following equation:

$$R = (2/n)\log K_{\lfloor n\omega^{**}\rfloor}(\lfloor \delta' n \rfloor) + 1 - 2H(\omega^{**}).$$

If the root of this equation is negative, we put $\xi_2 = 0$.

Corollary 3: Let C be a code of rate R and dual distance d'. Then, for any $\xi \in [\min\{\xi_1, \xi_2\}, 1/2]$ the code C has the binomial distance distribution

$$a_\xi(0, \delta') \le R - 1 + H(\xi) + o(1).$$

Example 4: As mentioned in the end of Section III, the improvement in the estimate of the binomial range over the known results can be substantial. For instance, consider codes with $\delta' = 0.2$. Then, Theorem 6 guarantees that the distance distribution is binomial for $0.2 \le \xi \le 1/2$ and Theorem 12 does the same for $0.18 \le \xi \le 1/2$. Corollaries 2 and 3 are much better results for high code rates, see Fig. 3. In this example, the binomiality range is extended for code rates $R \in [0.795, 1]$. Corollary 2 gives the best results for $0.795 \le R \le 0.93$, for $R > 0.93$, Corollary 3 gives a slightly wider range of distances.

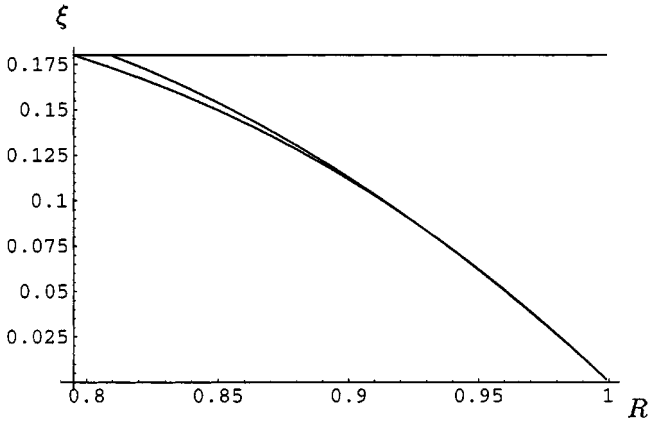

Fig. 3. Binomiality range for the distance distribution of codes with $\delta' = 0.2$. The distance distribution is asymptotically binomial in the interval $[\xi(R), 1/2]$. The plot shows the curve $\xi(R)$ from Theorem 12 (straight line) and Corollaries 2 and 3.

APPENDIX A
ANOTHER PROOF OF THEOREM 3

Let d be the code distance and $t = \lfloor n/2 - \sqrt{d(n-d)}\rfloor$. We note that d is approximately equal to the first zero $x_1^{(t)}$ of the Krawtchouk polynomial $K_t(x)$. Let m, $x_1^{(t+1)} < m < x_1^{(t)}$, be the number such that $nK_{t+1}(m) = -K_t(m)$. Such a choice is possible for any n because of the interlacing property of the zeros of K_t and K_{t+1}: $x_1^{(t+1)} < x_1^{(t)} < x_2^{(t+1)}$. Let us define the polynomial $Z(x)$ as follows:

$$Z(x) = \frac{(K_t(x) + nK_{t+1}(x))^2}{x - m}. \tag{37}$$

The Krawtchouk coefficients of $Z(x)$ are nonpositive. Indeed, we have

$$Z(x) = \frac{1}{(K_{t+1}(m))^2}\,\frac{(K_{t+1}(m)K_t(x) - K_t(m)K_{t+1}(x))^2}{x - m}$$

so this follows by (43). Further, $Z(x) < 0$ for $0 \le x < m$ and $Z(x) \ge 0$ for $m \le x \le n$. Therefore, if we take in Theorem 1 $g(i) \equiv Z(i)$, the polynomial $Z(x)$ is feasible with respect to the conditions of the theorem.

Recall that by [23] for any code, $|C| \le -Z(0)/z_0$. So, assuming that the rate R of the code is

$$0 < R < H(1/2 - \sqrt{\delta(1-\delta)})$$

we see that the dominating term in the difference $z_0|C| - Z(0)$ is the second one. Hence, we can write the estimate on A_w in the form

$$A_w \le \frac{-Z(0)(1 - o(1))}{Z(w)}. \tag{38}$$

To compute the bound (3), we find

$$Z(0) = -\frac{1}{m}\binom{n}{t}^2\left(\frac{n(n-t)}{t+1} + 1\right)^2.$$

To complete the proof, we have to estimate $Z(w)$. Note that this problem is essentially different from the standard situation since w is greater than the first zero $x_1^{(t)}$. Therefore, the point w is in the *oscillatory segment* for both K_t and K_{t+1}.

Lemma 14: Let $x \in [d, n/2]$ be an integer and $\alpha(x) = \binom{n}{x}2^{-n}$. Then

$$(K_t(x) + K_{t+1}(x))^2 \geq O(1)\binom{n}{t}/\alpha(x). \tag{39}$$

Using this estimate in (38) and taking logarithms, we obtain the exponential bound claimed in the theorem. The rest of this appendix is devoted to the proof of (39).

We begin with the following result from [16].

Lemma 15 [16]: Let $s = 2\sqrt{k(n-k)}$. Then, for $k \leq n/2$ and integer $t \in (\frac{n-s}{2}, \frac{n}{2})$,

$$(K_k(t))^2 - K_k(t-1)K_k(t+1) \geq \frac{s-n+2x}{s}\,\frac{(t-1)!(n-t-1)!}{((n/2-1)!)^2}\,U_k(n/2)$$

where for k even

$$U_k(n/2) = \frac{4k(n-k)}{n^2}\binom{n/2}{k/2}^2$$

and for k odd

$$U_k(n/2) = 4\binom{n/2-1}{(k-1)/2}^2.$$

First, note that, as verified easily using the Stirling formula

$$\frac{s-n+2x}{s}\,\frac{(x-1)!(n-x-1)!}{((n/2-1)!)^2}\,U_k(n/2) = p(n)\frac{\binom{n}{k}}{\alpha(t)}$$

where $p(n)$ is a function of at most polynomial growth in n. So for $k \leq n/2$ and

$$n/2 - \sqrt{k(n-k)} \leq t \leq n/2 + \sqrt{k(n-k)}$$

we have

$$(K_k(t))^2 - K_k(t-1)K_k(t+1) \geq p(n)\frac{\binom{n}{k}}{\alpha(t)}.$$

Now, since

$$\binom{n}{k}K_t(k) = \binom{n}{t}K_k(t)$$

we obtain for integer $x \leq n/2$ and

$$t \in [n/2 - \sqrt{x(n-x)},\, n/2 + \sqrt{x(n-x)}]$$

$$(K_t(x))^2 - \frac{(t+1)(n-t+1)}{t(n-t)}\,K_{t-1}(x)K_{t+1}(x) \geq p(n)\frac{\binom{n}{t}}{\alpha(x)}.$$

Thus, in the interval considered, either

$$(K_t(x))^2 \geq \frac{p(n)}{2}\,\frac{\binom{n}{t}}{\alpha(x)}$$

or

$$|K_{t-1}(x)K_{t+1}(x)| \geq \frac{p(n)t(n-t)}{2(t+1)(n-t+1)}\,\frac{\binom{n}{t}}{\alpha(x)}.$$

In the last case, since by (40)

$$\alpha(x)(K_{t-1}(x))^2 \leq \|K_{t-1}\|^2 = \binom{n}{t-1}$$

we conclude that

$$\frac{(n-t)}{(t+1)}\,\frac{\binom{n}{t}}{\alpha(x)} \geq |K_{t+1}(x)|^2 \geq \frac{p^2(n)t(n-t)^2}{4(t+1)^2(n-t+1)}\,\frac{\binom{n}{t}}{\alpha(x)}.$$

Recall that t is linear in n, so these inequalities imply that $p(n) = O(1)$. Since $(K_t(x))^2 \leq \binom{n}{t}/\alpha(x)$, the same conclusion also follows for the first case. Thus, at any integer point

$$n/2 - \sqrt{t(n-t)} \leq x \leq n/2$$

at least one of the following asymptotic equalities holds true:

$$|K_t(x)| = O(1)\|K_t\|\Big/\sqrt{\alpha(x)}$$
$$|K_{t+1}(x)| = O(1)\|K_t\|\Big/\sqrt{\alpha(x)}\,.$$

This finishes the proof of (39).

Appendix B
Useful Identities

Let $\{K_k(x)\}$ be the family of Krawtchouk polynomials (11). They are orthogonal on $(0, 1, \ldots, n)$ with weight $\alpha(i) = \binom{n}{i}/2^n$

$$\langle K_i, K_j\rangle := \int K_iK_j\,d\alpha = \delta_{ij}\binom{n}{i}. \tag{40}$$

For any polynomial $Z(x) = \sum_{i=0}^n z_iK_i(x)$

$$z_j = \frac{\langle Z, K_j\rangle}{\langle K_j, K_j\rangle} = 2^{-n}\sum_{i=0}^n Z(i)K_i(j). \tag{41}$$

The following properties are standard:

$$\sum_{i=0}^n K_k(i)K_i(j) = 2^n\delta_{jk} \tag{42}$$

$$K_{t+1}(x)K_t(a) - K_t(x)K_{t+1}(a) = \frac{2(a-x)}{t+1}\binom{n}{t}\sum_{i=0}^t\frac{K_i(x)K_i(a)}{\binom{n}{i}}. \tag{43}$$

$$K_t(x)K_s(x) = \sum_{j=0}^n p_{ts}^jK_j(x) \tag{44}$$

where

$$p_{ts}^j = \binom{n-j}{(t+s-j)/2}\binom{j}{(t-s+j)/2}$$

if $t-s+j$ is even and zero if it is odd [the equality in (44) is asserted only at $0, 1, \ldots, n$, regardless of the degree of the polynomial on the left]. From (11), we see that

$$K_k(0) = \binom{n}{k}. \tag{45}$$

Polynomial $K_t(x)$ has degree t and its t simple zeros are located between 0 and n. Let $x_1^{(t)}$ be the smallest zero of $K_t(x)$; let $n \to \infty$, $t \to \infty$, $k/n < 1/2$. Then, [23], [19],

$$x_1^{(t)} = \frac{n}{2} - \sqrt{t(1-t)} + O\left(t^{1/6}\sqrt{n}\right). \tag{46}$$

Let $t = \tau n$, $0 \le x = \xi n \le x_1^{(t)}$. By [7], we have

$$\frac{1}{n}\log K_t(x) = H(\tau) + \int_0^{\xi} \log \frac{1-2\tau+\sqrt{(1-2\tau)^2-4y(1-y)}}{2-2y}\, dy + o(1). \tag{47}$$

For $\tau = (1/2) - \sqrt{\xi(1-\xi)}$, this gives

$$\frac{1}{n}\log K_t(x) = \frac{1 + H(\tau) - H(\xi)}{2}. \tag{48}$$

REFERENCES

[1] A. Ashikhmin and A. Barg, "Binomial moments of the distance distribution: Bounds and applications," *IEEE Trans. Inform. Theory*, vol. 45, pp. 438–452, Mar. 1999.

[2] A. Ashikhmin, A. Barg, and S. Litsyn, "New bounds on generalized weights," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1258–1263, July 1999.

[3] ——, "Estimates of the distance distribution of nonbinary codes, with applications," in *Codes and Association Schemes*, A. Barg and S. Litsyn, Eds. Providence, RI: AMS, 2001, to be published.

[4] A. Ashikhmin and S. Litsyn, "Upper bounds on the size of quantum codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 1206–1215, July 1999.

[5] E. R. Berger, "Some additional upper bounds for fixed-weight codes of specified minimum distance," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 307–308, Mar. 1967.

[6] P. Delsarte, "An algebraic approach to the association schemes of coding theory," *Philips Res. Repts. Suppl.*, vol. 10, pp. 1–97, 1973.

[7] G. Kalai and N. Linial, "On the distance distribution of codes," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1467–1472, Aug. 1995.

[8] T. Kasami, T. Fujiwara, and S. Lin, "An approximation to the weight distribution of binary linear codes," *IEEE Trans. Inform. Theory*, vol. 31, pp. 769–780, Nov. 1985.

[9] G. L. Katsman and M. A. Tsfasman, "Spectra of algebraic-geometric codes," *Problemy Peredachi Informatsii*, vol. 23, no. 4, pp. 19–34, 1987.

[10] G. L. Katsman, M. A. Tsfasman, and S. G. Vladuţ, "Spectra of linear codes and error probability of decoding," in *Coding Theory and Algebraic Geometry*. Berlin, Germany: Springer, 1992, pp. 82–98.

[11] O. Keren and S. Litsyn, "More on the distance distribution of BCH codes," *IEEE Trans. Inform. Theory*, vol. 45, pp. 251–255, Jan. 1999.

[12] I. Krasikov, "Nonnegative quadratic forms and bounds on orthogonal polynomials," priprint, 1999.

[13] I. Krasikov and S. Litsyn, "On the accuracy of the binomial approximation to the distance distribution of codes," *IEEE Trans. Inform. Theory* , vol. 41, pp. 1472–1474, Aug. 1995.

[14] ——, "Estimates for the range of binomiality in codes' spectra," *IEEE Trans. Inform. Theory*, vol. 43, pp. 987–991, May 1997.

[15] ——, "Bounds on spectra of codes with known dual distance," *Des. Codes Cryptogr.*, vol. 13, no. 3, pp. 285–297, 1998.

[16] ——, "On the distance distribution of BCH codes and their duals," *Des. Codes Cryptogr.*, to be published.

[17] V. I. Levenshtein, "Upper-bound estimates for fixed-weight codes," *Probl. Pered. Inform.*, vol. 7, no. 4, pp. 3–12, 1971.

[18] ——, "On the minimal redundancy of binary error-correcting codes," *Inform. Contr.*, vol. 28, no. 4, pp. 268–291, 1975. Translated from Russian by A. M. Odlyzko (*Probl. Pered. Inform.*, vol. 10, no. 2, pp. 26–42, 1974).

[19] ——, "Bounds for packings of metric spaces and some of their applications" (in Russian), *Prob. Kibern.*, no. 40, pp. 43–110, 1983.

[20] N. Linial and A. Samorodnitsky, "Linear codes and character sums," preprint, 1999.

[21] S. Litsyn, "An updated table of the best binary codes known," in *Handbook of Coding Theory*, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, vol. 1, pp. 463–498.

[22] ——, "New upper bounds on error exponents," *IEEE Trans. Inform. Theory* , vol. 45, pp. 385–398, Mar. 1999.

[23] R. J. McEliece, E. R. Rodemich, H. Rumsey, and L. R. Welch, "New upper bound on the rate of a code via the Delsarte-Mac Williams inequalities," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 157–166, Mar. 1977.

[24] A. Samorodnitsky, "On the optimum of Delsarte's linear program," preprint, 1998.

[25] V. M. Sidelnikov, "The spectrum of weights of binary Bose–Chaudhuri–Hocquenghem codes," *Probl. Pered. Inform.*, vol. 7, no. 1, pp. 14–22, 1971.

[26] J.-P. Tillich and G. Zémor, "Discrete isoperimetric inequalities and the probability of decoding error," *Combin., Probab., Comput.*, to be published.