New Upper Bounds on the Rate of a Code via the Delsarte–MacWilliams Inequalities

ROBERT J. McELIECE, MEMBER, IEEE, EUGENE R. RODEMICH, HOWARD RUMSEY, JR., AND LLOYD R. WELCH

Abstract—**With the Delsarte–MacWilliams inequalities as a starting point, an upper bound is obtained on the rate of a binary code as a function of its minimum distance. This upper bound is asymptotically less than Levenshtein's bound, and so also Elias's.**

I. Introduction

LET V_n DENOTE the set of all 2^n binary n-tuples, and, for $\mathbf{x},\mathbf{y} \in V_n$, denote by $\|\mathbf{x} - \mathbf{y}\|$ the Hamming distance[1] between $\mathbf{x}$ and $\mathbf{y}$, i.e., the number of components in which $\mathbf{x}$ and $\mathbf{y}$ differ. A subset $C = \{\mathbf{x}_1, \cdots, \mathbf{x}_M\} \subseteq V_n$ is called a *code of length* n; the $\mathbf{x}_i$ are called *codewords*; the *minimum distance* of C is $d_{\min}(C) = \min\{\|\mathbf{x}_i - \mathbf{x}_j\| : i \neq j\}$; and the code's rate is $R(C) = n^{-1} \log_2 M$. We are interested in the relationship between a code's rate and its minimum distance, and in this paper we shall obtain asymptotic upper bounds on $R(C)$ in terms of $d_{\min}(C)$.

To describe our results compactly, we need more notation. First, we define $M(n,d)$ to be the largest possible number of codewords in a code of length n and minimum distance at least d. Next, define $R(n,d) = n^{-1} \log_2 M(n,d)$ as the rate of the best code of length n and minimum distance at least d. Finally, for each real number $0 \leq \delta \leq 1$, define

$$R(\delta) = \sup \overline{\lim_{n\to\infty}} R(n,d_n), \tag{1.1}$$

where the supremum in (1.1) is taken over all sequences (d_n) for which $d_n/n \to \delta$.

It is known (see, e.g., [2, ch. 13]) that $R(0) = 1$, and $R(\delta) = 0$ for $\frac{1}{2} \leq \delta \leq 1$, but $R(\delta)$ is unknown for $0 < \delta < \frac{1}{2}$. Until fairly recently, the best upper and lower bounds for $R(\delta)$ in this range were

$$1 - g(4\delta(1-\delta)) \leq R(\delta) \leq 1 - g(2\delta), \tag{1.2}$$

where in (1.2) the function $g(x)$, plotted in Fig. 1, is defined for $0 \leq x \leq 1$ by

$$g(x) = H_2((1 - \sqrt{1-x})/2),$$

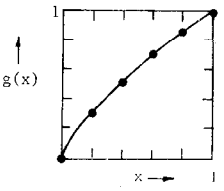

Fig. 1. The function $g(x)$.

$$H_2(x) = -x \log_2 x - (1-x) \log_2 (1-x). \tag{1.3}$$

The function $g(x)$ is monotonically increasing and concave on [0,1]. The lower bound in (1.2), which is usually expressed as $1 - H_2(\delta)$, is due to Gilbert; the upper bound, to Elias. The Gilbert and Elias bounds are plotted in Fig. 2, the unknown function $R(\delta)$ lying somewhere between them. Gilbert's lower bound is still the best one, but recently Sidelnikov [6] and Levenshtein [5] obtained new upper bounds on $R(\delta)$ which are strictly less than Elias', for all $0 < \delta < \frac{1}{2}$. However, the numerical improvement over the Elias bound is not large. (See Table I.)

In this paper, we will obtain a new upper bound to $R(\delta)$, for $0 < \delta < \frac{1}{2}$, which, so far as we know, is strictly less than any other bound. It is

$$R(\delta) \leq \min_{0 \leq u \leq 1-2\delta} 1 + g(u^2) - g(u^2 + 2\delta u + 2\delta). \tag{1.4}$$

Note that, if we evaluate the expression $1 + g(u^2) - g(u^2 + 2\delta u + 2\delta)$ at $u = 1 - 2\delta$, we obtain $g((1-2\delta)^2)$, and so (1.4) implies the bound

$$R(\delta) \leq g((1-2\delta)^2). \tag{1.5}$$

Surprisingly, the bound (1.4) is actually equal to (1.5) for $0.273 \leq \delta \leq \frac{1}{2}$ and so the minimization over u improves (1.5) only for relatively small values of δ. Also note that for $u = 0$, (1.4) yields the Elias bound; it is easy to check that the derivative of $g(u^2) - g(u^2 + 2\delta u + 2\delta)$ at $u = 0$ is negative, so the bound (1.4) is always strictly less than the Elias bound. (However, the bound (1.5) is larger than the Elias bound for $\delta < 0.150$, and even larger than the obsolete Hamming bound $1 - H_2(\delta/2)$ for $\delta < 0.114$.) The bounds (1.4), (1.5), and Levenshtein's bound are plotted in Fig. 3, and tabulated in Table I.[2]

Manuscript received April 19, 1976. This paper presents the results of one phase of research carried out at the Jet Propulsion Laboratory, California Institute of Technology, under Contract No. NAS 7-100, sponsored by the National Aeronautics and Space Administration.

R. J. McEliece, E. R. Rodemich, and H. Rumsey are with the Jet Propulsion Laboratory, Pasadena, CA 91103.

L. R. Welch is with the University of Southern California, Los Angeles, CA 90007.

[1] For a single vector $\mathbf{x}$, $\|\mathbf{x}\| = \|\mathbf{x} - \mathbf{0}\|$ is the Hamming weight of $\mathbf{x}$.

[2] One of the referees has invited us to make a conjecture about the relationship between our bound $N(\delta)$, Gilbert's bound $G(\delta)$, and the actual value $R(\delta)$, so here goes. *Conjecture:* $G(\delta) < R(\delta) < N(\delta)$, for all $0 < \delta < 1/2$. (See also footnotes 4 and 7.)

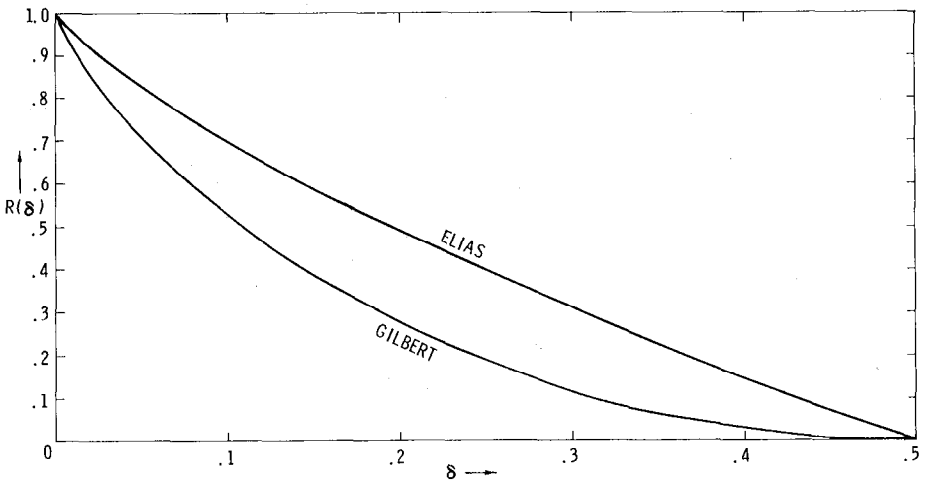

Fig. 2. Elias and Gilbert bounds.

TABLE I
BOUNDS ON $R(\delta)$
L = LEVENSHTEIN, E = ELIAS, G = GILBERT

	Upper Bounds				Lower Bounds
δ	1.5	1.4	L	E	G
.00	1.000	1.000	1.000	1.000	1.000
.02	.943	.918	.919	.919	.859
.04	.886	.854	.856	.856	.758
.06	.831	.797	.801	.801	.673
.08	.776	.744	.749	.750	.598
.10	.722	.693	.701	.702	.531
.12	.669	.644	.655	.656	.471
.14	.617	.597	.612	.613	.416
.16	.567	.551	.570	.571	.366
.18	.517	.505	.529	.531	.320
.20	.469	.461	.490	.492	.278
.22	.422	.418	.451	.454	.240
.24	.377	.375	.414	.417	.205
.26	.333	.333	.377	.381	.173
.28	.291	.291	.342	.346	.145
.30	.250	.250	.307	.312	.119
.32	.212	.212	.272	.278	.096
.34	.175	.175	.238	.245	.075
.36	.141	.141	.205	.213	.057
.38	.110	.110	.172	.181	.042
.40	.081	.081	.140	.150	.029
.42	.056	.056	.107	.119	.019
.44	.035	.035	.076	.088	.010
.46	.017	.017	.045	.059	.005
.48	.005	.005	.018	.029	.001
.50	.000	.000	.000	.000	.000

Here is the plan of the rest of the paper. In Section II, we outline our proofs of (1.4) and (1.5). In Section III, we will prove (1.5); and in Section IV, we will prove (1.4). As we have pointed out, (1.4) contains (1.5) as a special case, and so Section III is not strictly necessary to our exposition. However, we have included a separate proof of (1.5) in order to introduce the reader to the rather intricate ideas necessary for the full proof of (1.4). In any case, the general bound (1.4) is not much better than the minimum of the Elias bound and (1.5), so we regard (1.5) as the most significant contribution of this paper.

II. THE DELSARTE–MACWILLIAMS INEQUALITIES AND LINEAR PROGRAMMING BOUNDS

Let $C = \{\mathbf{x}_1, \cdots, \mathbf{x}_M\}$ be a code of length n with $\|\mathbf{x}_\mu - \mathbf{x}_\nu\| \geq d$ if $\mu \neq \nu$. For each $i = 0,1, \cdots, n$, define a_i to be the average number of codewords at distance i from a given

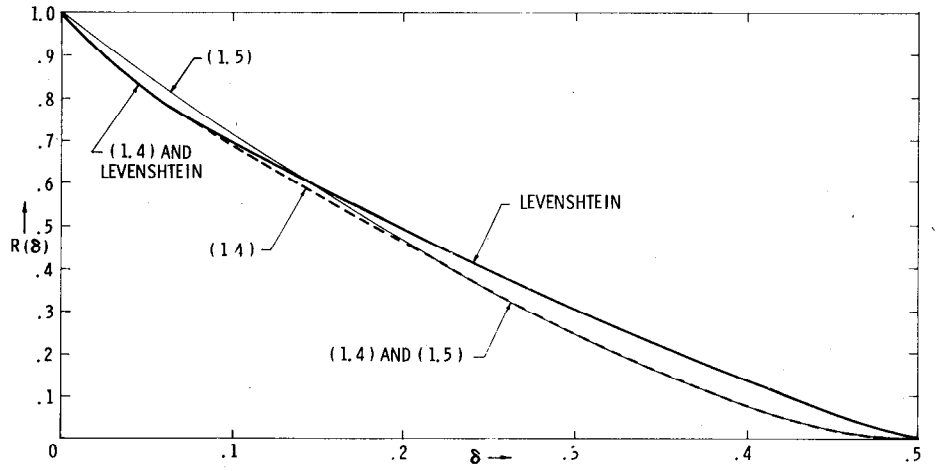

Fig. 3. Bounds (1.4) and (1.5) versus Levenshtein's bound.

codeword[3], i.e.,

$$a_i = \frac{1}{M} \cdot |\{(\mu,\nu): \| \mathbf{x}_\mu - \mathbf{x}_\nu \| = i\}|. \tag{2.1}$$

The vector $\mathbf{a} = (a_0, a_1, \cdots, a_n)$ is called the *distance distribution* of the code; it is immediate that

$$\begin{aligned} a_0 &= 1 \\ a_1 = a_2 &= \cdots = a_{d-1} = 0 \\ a_0 + a_1 + \cdots + a_n &= M. \end{aligned} \tag{2.2}$$

Now let $K_j(i)$ be the coefficient of y^j in the polynomial $(1-y)^i(1+y)^{n-i}$. The Delsarte–MacWilliams inequalities are

$$\sum_{i=0}^{n} a_i K_j(i) \geq 0, \qquad j = 0,1,\cdots,n. \tag{2.3}$$

(A simple proof of these inequalities is given in [8]. The numbers $K_j(i)$ are discussed at length in Appendix A.)

Now let us denote by $M_{\mathrm{LP}}(n,d)$ the value of the following linear program

maximize: $a_0 + a_1 + \cdots + a_n$,

subject to:
$$a_0 = 1, \tag{2.4a}$$
$$a_1 = \cdots = a_{d-1} = 0 \tag{2.4b}$$
$$a_i \geq 0, \qquad i = d, d+1, \cdots, n, \tag{2.4c}$$
$$\sum_{i=0}^{n} a_i K_j(i) \geq 0, \qquad j = 0,1,\cdots,n. \tag{2.4d}$$

Then, because of (2.2) and (2.3), it follows that $M(n,d) \leq M_{\mathrm{LP}}(n,d)$; this is the *linear programming bound.* Also, define, for $0 \leq \delta \leq 1$,

$$R_{\mathrm{LP}}(\delta) = \sup \varlimsup_{n\to\infty} \frac{1}{n} \log_2 M_{\mathrm{LP}}(n, d_n), \tag{2.5}$$

where the supremum is the same as in (1.1). Clearly $R(\delta) \leq R_{\mathrm{LP}}(\delta)$. In Section III, we will show that,[4] for $0 \leq \delta \leq \frac{1}{2}$,

$$R_{\mathrm{LP}}(\delta) \leq g((1-2\delta)^2), \tag{2.6}$$

and this will establish (1.5).

We now describe how the tighter bound (1.4) arises. If B is a subset of V_n, denote by $M_B(n,d)$ the maximum number of codewords $\mathbf{x}_1, \cdots, \mathbf{x}_M$ which can be chosen from B such that $\| \mathbf{x}_\mu - \mathbf{x}_\nu \| \geq d$, for all $\mu \neq \nu$. Then it is well-known that

$$M(n,d) \leq \frac{2^n}{|B|} M_B(n,d). \tag{2.7}$$

(A proof of (2.7) may be found in [5, corollary 1 to lemma 3] or [3, theorem 3.7]. The result is variously attributed to Elias or Bassalygo.)

If in (2.7) we take for B the set of all $\binom{n}{w}$ vectors of weight w for some fixed $w \in \{0,1,\cdots,\lfloor n/2 \rfloor\}$, and denote the corresponding $M_B(n,d)$ by $M(n,d,w)$, (2.7) becomes

$$M(n,d) \leq \frac{2^n}{\binom{n}{w}} M(n,d,w). \tag{2.8}$$

Now if we define $R(\delta,\alpha)$ by

$$R(\delta,\alpha) = \sup \varlimsup_{n\to\infty} \frac{1}{n} \log_2 M(n, d_n, w_n), \tag{2.9}$$

[3] In (2.1), and elsewhere, we use the notation $|X|$ to denote the number of elements in the finite set X.

[4] We do not believe this bound to be tight for any $0 < \delta < 1/2$.

[5] To obtain (2.10), we have used the fact that $1/n \log_2 \binom{n}{\alpha n} = H_2(\alpha) + o(n)$, for $\alpha \leq \frac{1}{2}$, a result which can be deduced from Stirling's approximation to the factorial.

TABLE II
BOUNDS ON $R(\delta,\alpha)$ FOR $\delta = 0.48 (\delta^* = 0.40)$

	upper bounds		
α	Levenshtein	(2.16)	Gilbert (lower bound)
.40	0.00000	0.00000	0.00000
.41	0.00117	0.00027	0.00004
.42	0.00361	0.00085	0.00016
.43	0.00657	0.00158	0.00031
.44	0.00965	0.00236	0.00049
.45	0.01240	0.00311	0.00066
.46	0.01457	0.00378	0.00082
.47	0.01612	0.00433	0.00096
.48	0.01721	0.00475	0.00107
.49	0.01764	0.00501	0.00113
.50	0.01764	0.00509	0.00115

where the supremum in (2.9) is taken over all sequences (d_n) and (w_n) for which $d_n/n \to \delta$ and $w_n/n \to \alpha$, it follows from (1.1) and (2.8) that[5]

$$R(\delta) \le 1 - H_2(\alpha) + R(\delta,\alpha), \tag{2.10}$$

for all $0 \le \alpha \le \frac{1}{2}$.

In Section IV, we will restrict ourselves entirely to the problem of obtaining a bound for $M(n,d,w)$. The asymptotic form of this bound, when combined with (2.10), will yield our main result (1.4). We conclude this section with a brief description of our technique for bounding $M(n,d,w)$.

Let $\{\mathbf{x}_1, \cdots, \mathbf{x}_M\}$ be a set of M binary codewords of length n and weight w such that $\|\mathbf{x}_\mu - \mathbf{x}_\nu\| \ge d$, if $\mu \ne \nu$. For each $i = 0,1,\cdots,w$, let a_i be the average number of codewords at distance $2i$ from a given codeword[6], i.e.,

$$a_i = \frac{1}{M} \cdot |\{(\mu,\nu): \|\mathbf{x}_\mu - \mathbf{x}_\nu\| = 2i\}|. \tag{2.11}$$

As before (cf. (2.2)), it is immediate that

$$a_0 = 1$$
$$a_i = 0, \qquad \text{for } 1 \le i < d/2$$
$$a_0 + \cdots + a_w = M. \tag{2.12}$$

Delsarte [3, theorem 3.3] has discovered numbers $Q_j(i)$ which serve the same function in this setting as the $K_j(i)$ did earlier; viz.,

$$\sum_{i=0}^{w} a_i Q_j(i) \ge 0, \qquad j = 0,1,\cdots,w. \tag{2.13}$$

(Actually, Delsarte has established a beautiful general theory of "association schemes" in which the pivotal inequalities (2.3) and (2.13) appear as extremely special cases. The numbers $Q_j(i)$ are defined and many of their properties are given in Appendix B.) As before, if we denote by $M_{\mathrm{LP}}(n,d,w)$ the value of the following linear program

maximize: $a_0 + a_1 + \cdots + a_w$

subject to:
$$a_0 = 1 \tag{2.14a}$$
$$a_i = 0, \qquad \text{for } 1 \le i < d/2, \tag{2.14b}$$
$$a_i \ge 0, \qquad \text{all } i, \tag{2.14c}$$
$$\sum_{i=0}^{w} a_i Q_j(i) \ge 0, \qquad j = 0,1,\cdots,w, \tag{2.14d}$$

then $M(n,d,w) \le M_{\mathrm{LP}}(n,d,w)$. Now define $R_{\mathrm{LP}}(\delta,\alpha)$ by

$$R_{\mathrm{LP}}(\delta,\alpha) = \sup \overline{\lim_{n\to\infty}} \frac{1}{n} \log_2 M_{\mathrm{LP}}(n,d_n,w_n), \tag{2.15}$$

where the supremum is the same as in (2.9). In Section IV, we will prove that[7] for fixed δ, $0 < \delta < \frac{1}{2}$,

$$R_{\mathrm{LP}}(\delta,\alpha) \le \begin{cases} 0, & 0 \le \alpha \le \delta^* \\ g(u^2), & \delta^* \le \alpha \le \frac{1}{2}, \end{cases} \tag{2.16}$$

where $\delta^* = (1 - \sqrt{1-2\delta})/2$ and $u = -\delta + (\delta^2 - 2\delta + 4\alpha(1-\alpha))^{1/2}$. As α varies from δ^* to $\frac{1}{2}$, u increases monotonically from 0 to $1 - 2\delta$; and since $H_2(\alpha) = g(u^2 + 2\delta u + 2\delta)$, together (2.10) and (2.16) yield the bound (1.4). In [5], Levenshtein has also given an upper bound on $R(\delta,\alpha)$. The complexity of Levenshtein's bound has prevented us from making an analytic comparison of the two, but apparently the bound (2.16) is superior to Levenshtein's, at least for relatively large δ. For example, in Table II we have tabulated Levenshtein's bound, our bound (2.16), and the Gilbert lower bound $H_2(\alpha) - \alpha H_2(\delta/2\alpha) - (1-\alpha) H_2(\delta/2(1-\alpha))$, for $\delta = 0.48$ and $0.40 \le \alpha \le 0.50$.

[6] Note that since the $\mathbf{x}_i$ all have the same weight, the distances among them are necessarily even.

[7] We do not believe the interesting part of this bound to be tight, i.e., we conjecture that $R_{LP}(\delta,\alpha) < g(u^2)$, for $0 < \delta < 1/2$, $\delta^* < \alpha \le 1/2$.

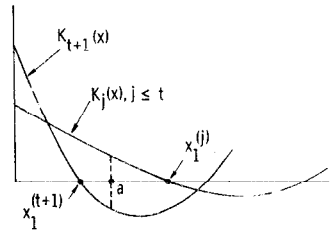

Fig. 4. Relationship between $K_{t+1}(x)$ and $K_j(x), j \le t$.

III. Proof of (2.6)

Our first result is really only a formulation of the dual of the linear program (2.4).

Theorem 1: Let $(\lambda_0,\lambda_1,\cdots,\lambda_n)$ be real numbers satisfying

$$\lambda_0 > 0, \lambda_j \ge 0, \qquad j = 1,\cdots,n \tag{3.1}$$

$$\sum_{j=0}^{n} \lambda_j K_j(i) \le 0, \qquad i = d,d+1,\cdots,n. \tag{3.2}$$

Then,

$$M_{\mathrm{LP}}(n,d) \le \frac{1}{\lambda_0} \sum_{j=0}^{n} \lambda_j K_j(0). \tag{3.3}$$

Proof: Let $(a_0,a_1,\cdots,a_n)$ be real numbers satisfying the constraints (2.4) for which $a_0 + \cdots + a_n = M_{\mathrm{LP}}(n,d)$, and let $b_j = \Sigma_{i=0}^{n} a_i K_j(i)$. Then, (by (3.1) and (2.4d))

$$\lambda_0 b_0 \le \sum_{j=0}^{n} \lambda_j b_j = \sum_{i=0}^{n} a_i \sum_{j=0}^{n} \lambda_j K_j(i) \le \sum_{j=0}^{n} \lambda_j K_j(0) \tag{3.4}$$

(by (3.2) and (2.4a,b,c)). Now by definition $K_0(i)$ = coefficient of 1 in $(1-y)^i(1+y)^{n-i} = 1$, and so $b_0 = \Sigma_{i=0}^{n} a_i = M_{\mathrm{LP}}(n,d)$. This fact, combined with (3.4), yields Theorem 1.

It is known that $K_j(i)$ is a polynomial of degree j in i. This polynomial, which we denote by $K_j(x)$, is called a *Krawtchouk* polynomial. In the following argument, we shall frequently refer to results about Krawtchouk polynomials and refer the reader to Appendix A for details. At first, n and d will be fixed integers; later, after we have derived the bound (3.13) on $M(n,d)$, we will proceed to asymptotic analysis.

Let t be an integer, $1 \le t \le n/2$, and let a be a real number in the interval $[0,n]$. (They will be specified more precisely later.) Define

$$P^*(x) = K_{t+1}(x)K_t(a) - K_t(x)K_{t+1}(a).$$

According to property (A.16),

$$P^*(x) = \frac{2(a-x)}{t+1}\binom{n}{t} \sum_{k=0}^{t} \frac{K_k(x)K_k(a)}{\binom{n}{k}}. \tag{3.5}$$

Now define

$$P(x) = \frac{P^*(x)^2}{a-x} \tag{3.6}$$

$$= \frac{2}{t+1}\binom{n}{t}\left[K_{t+1}(x)K_t(a) - K_t(x)K_{t+1}(a)\right] \cdot \sum_{k=0}^{t} \frac{K_k(x)K_k(a)}{\binom{n}{k}}. \tag{3.7}$$

Now (see Appendix A) for each $j, K_j(x)$ has j distinct real zeros in the interval $(0,n)$. Denote by $x_1^{(j)}$ the smallest such zero. Then by (A.17), $x_1^{(t+1)} < x_1^{(t)}$. Let us now choose a so that

$$x_1^{(t+1)} < a < x_1^{(t)}. \tag{3.8}$$

Then since $K_j(0) = \binom{n}{j} > 0$ (A.8), it follows that $K_j(a) > 0$, for $j \le t$, and $K_{t+1}(a) < 0$. (See Fig. 4.) Hence in (3.7) $P(x)$ is expressed as a sum, with nonnegative coefficients, of products of Krawtchouk polynomials. By (A.19), any product $K_i(x)K_j(x)$ can be expressed as a sum $\Sigma\alpha_k K_k(x)$ with each $\alpha_k \ge 0$. We conclude that $P(x)$ itself has an expansion in Krawtchouk polynomials with nonnegative coefficients.

Next, observe from (3.6) that $P(x) \le 0$, if $x \ge a$. Hence if we assume $a \le d$, it follows that $P(x) \le 0$ if $x \ge d$. Hence if $P(x) = \Sigma_0^n \lambda_j K_j(x)$, the λ_j satisfy the hypotheses of Theorem 1, and so $M_{\mathrm{LP}}(n,d) \le P(0)/\lambda_0$. From (3.6), we have

$$P(0) = \frac{1}{a}\left[\binom{n}{t+1}K_t(a) - \binom{n}{t}K_{t+1}(a)\right]^2 = \frac{1}{a}\binom{n}{t}^2 K_t(a)^2\left[\frac{n-t}{t+1} - Q\right]^2, \qquad \left(Q = \frac{K_{t+1}(a)}{K_t(a)}\right). \tag{3.9}$$

To compute λ_0 we use the formula (A.12) $\lambda_0 = \int P(x)\,d\beta$ and the orthogonality properties (A.11) and conclude

$$\lambda_0 = -\frac{2}{t+1} \cdot K_{t+1}(a)K_t(a) \int K_t^2(x)\,d\beta = -\frac{2}{t+1}\binom{n}{t}K_t(a)^2 Q. \tag{3.10}$$

Combining (3.9) and (3.10), we get the following bound:

$$M_{\mathrm{LP}}(n,d) \le \binom{n}{t} \frac{(n-t-(t+1)Q)^2}{-2a(t+1)Q},$$

$$\text{where } \begin{cases} Q = K_{t+1}(a)/K_t(a) \\ x_1^{(t+1)} < a < x_1^{(t)} \\ a < d. \end{cases} \quad (3.11)$$

To simplify this, choose t so that $x_1^{(t)} \le d$ and a so that $Q = K_{t+1}(a)/K_t(a) = -1$ (see Fig. 4.) Then (3.11) becomes

$$M_{\mathrm{LP}}(n,d) \le \binom{n}{t} \frac{(n+1)^2}{2a(t+1)} \quad (3.12)$$

(provided $x_1^{(t)} \le d$, $t \le n/2$). Now, since $a \ge x_1^{(t+1)}$ and by (A.18) $x_1^{(t+1)} \ge 1$, we get

$$M_{\mathrm{LP}}(n,d) \le \binom{n}{t} \frac{(n+1)^2}{2(t+1)} \le \binom{n}{t} (n+1)^2 \quad (3.13)$$

(provided $x_1^{(t)} \le d$, $t \le n/2$).

We now proceed to an asymptotic analysis of (3.13). Choose τ so that $1/2 - \sqrt{\delta(1-\delta)} < \tau < \frac{1}{2}$, and let (d_n) and (t_n) be sequences of integers such that $d_n/n \to \delta$ and $t_n/n \to \tau$. Now, according to (A.20), $\overline{\lim}\, x_1^{(t_n)}/n \le 1/2 - \sqrt{\tau(1-\tau)} < \delta$, and so, for sufficiently large n, the hypotheses of (3.13) will be satisfied. Thus

$$\begin{aligned} &\overline{\lim_{n\to\infty}} \frac{1}{n} \log_2 M_{\mathrm{LP}}(n,d_n) \\ &\le \overline{\lim_{n\to\infty}} \left[\frac{1}{n} \log_2 \binom{n}{t_n} + \frac{1}{n} \log_2 (n+1)^2 \right] \\ &= \overline{\lim_{n\to\infty}} \frac{1}{n} \log_2 \binom{n}{t_n} \\ &= H_2(\tau), \end{aligned} \quad (3.14)$$

since $n^{-1} \log_2 \binom{n}{t_n} \to H_2(t_n)$. Combining (3.14) with (2.5), we see that $R_{\mathrm{LP}}(\delta) \le H_2(\tau)$ whenever $1/2 - \sqrt{\delta(1-\delta)} < \tau < \frac{1}{2}$. Since $H_2(\tau)$ is a continuous function of τ, this implies $R_{\mathrm{LP}}(\delta) \le H_2(1/2 - \sqrt{\delta(1-\delta)}) = g((1-2\delta)^2)$, which is the promised bound (2.6).

IV. Proof of (2.16)

(The techniques involved in this section are virtually identical to those of Section III, and so we have omitted some of the computational details.)

Our first result is analogous to Theorem 1; its proof is virtually the same, so we omit it.

Theorem 2: If $\lambda_0, \lambda_1, \cdots, \lambda_w$ are real numbers satisfying

$$\lambda_j > 0, \qquad \lambda_j \ge 0, \qquad j = 1, \cdots, n \quad (4.1)$$

$$\sum_{j=0}^{w} \lambda_j Q_j(i) \le 0, \qquad \text{for } i \ge d/2, \quad (4.2)$$

then

$$M_{\mathrm{LP}}(n,d,w) \le \frac{1}{\lambda_0} \sum_{j=0}^{w} \lambda_j Q_j(0). \quad (4.3)$$

For fixed (n,d,w), choose an integer t, $1 \le t \le w$, a real number a in the interval $(0,w)$, and define

$$P^*(x) = Q_{t+1}(x)Q_t(a) - Q_t(x)Q_{t+1}(a). \quad (4.4)$$

By (B14),[8]

$$P^*(x) = (a-x) \cdot \frac{(n-2t)(n-2t-1)}{(t+1)(w-t)(w'-t)} \cdot \mu_t \sum_{k=0}^{t} \frac{Q_k(x)Q_k(a)}{\mu_k}, \quad (4.5)$$

where $w' = n - w$, and the constants μ_k are given by (B.1). Now define[9]

$$P(x) = P^*(x)^2/(a-x) \quad (4.6)$$

$$= \frac{(n-2t)(n-2t-1)}{(t+1)(w-t)(w'-t)} \mu_t \left[Q_{t+1}(x)Q_t(a) - Q_t(x)Q_{t+1}(a) \right] \cdot \sum_{k=0}^{t} \frac{Q_t(x)Q_k(a)}{\mu_k} \quad (4.7)$$

Now (see Appendix B) for each j, $Q_j(x)$ has j distinct real zeros in the open interval $(0,w)$, and if $x_1^{(j)}$ denotes the least zero of $Q_j(x)$, $x_1^{(j+1)} < x_1^{(j)}$ (see (B.16)). If we choose a so that

$$x_1^{(t+1)} < a < x_1^{(t)}, \quad (4.8)$$

then since $Q_j(0) = \mu_j > 0$ (B.10), it follows that $Q_j(a) > 0$ for $j \le t$ and $Q_{t+1}(a) < 0$. (The situation is the same as in Fig. 4.) Hence in (4.7) $P(x)$ is expressed as a sum, with nonnegative coefficients, of products of Q_j-polynomials. By (B.17), (B.18) this implies that $P(x) = \sum_{j=0}^{w} \lambda_j Q_j(x)$ with each $\lambda_j \ge 0$. Next, observe from (4.6) that $P(x) \le 0$, if $x > a$, and so, if we assume $a \le d/2$, it follows that $P(x) \le 0$, if $x \ge d/2$, and so we can apply Theorem 2 and conclude that $M_{\mathrm{LP}}(n,d,w) \le P(0)/\lambda_0$. If we further assume that $x_1^{(t)} \le d/2$ and that a is chosen in the interval $(x_1^{(t+1)}, x_1^{(t)})$ so that $Q_{t+1}(a)/Q_t(a) = -1$, then using (4.6) and (4.4) we calculate

$$P(0) = \frac{1}{a} Q_t(a)^2 \binom{n}{t}^2 \left[\frac{n^2 - (2t-1)n - 2t}{(n-t+1)(t+1)} \right]^2. \quad (4.9)$$

To compute λ_0, we apply the formula (B.14) $\lambda_0 = \int P(x)\, d\beta(x)$ to (4.6) and use the orthogonality relations (B.13). The result is

$$\lambda_0 = \mu_t \frac{(n-2t)(n-2t-1)}{(t+1)(w-t)(w'-t)} Q_t(a)^2. \quad (4.10)$$

Combining these results and recalling that $x_1^{(t+1)} < a$, we

[8] Throughout this section, we will invoke facts about the numbers $Q_j(i)$ which are discussed in detail in Appendix B.

[9] The polynomial defined by (4.5) may have degree $> w$. We should really define $P(x)$ to be the unique polynomial of degree at most w which agrees with the right side of (4.5) for $x = 0,1,\cdots,w$.

obtain the following bound on $M_{\mathrm{LP}}(n,d,w)$:

$$M_{\mathrm{LP}}(n,d,w) \le \binom{n}{t} \frac{(n^2-(2t-1)n-2t)^2(w-t)(w'-t)}{x_1^{(t+1)}(t+1)(n-t+1)(n-2t-1)(n-2t)(n-2t+1)}, \tag{4.11}$$

provided $x_1^{(t)} \le d/2$.

We now proceed to an asymptotic analysis of the bound (4.11). Let (d_n), (w_n), and (t_n) be sequences of integers with

$$\begin{aligned} d_n/n &\to \delta \\ w_n/n &\to \alpha \\ t_n/n &\to \beta, \qquad 0 \le \beta < \alpha < \tfrac{1}{2}. \end{aligned} \tag{4.12}$$

Now by (B.10), the polynomial $Q_{t_n}{}^{(n,w_n)}(x)$ is positive at $x = 0$ and, by (B.11), it is also positive at $x = 1$ for sufficiently large n. Hence, if it has any zeroes in the interval (0,1), it must have at least two. This is, however, not possible since by the remarks following (B.16) there must be an integer between any two zeroes, and so we conclude that

$$x_1^{(t_n)} \ge 1, \qquad n \text{ sufficiently large.} \tag{4.13}$$

This means that the fraction on the right of (4.11) is growing no faster than $0(n^6)$, and so the bound is dominated by the binomial coefficient $\binom{n}{t_n}$. But $n^{-1}\log_2\binom{n}{t_n} \to H_2(\beta)$, and so, combining (4.11) with (2.15), we obtain the bound $R_{\mathrm{LP}}(\delta,\alpha) \le H_2(\beta)$, provided β is chosen so that $x_1^{(t_n)} \le d_n/2$, for large n. But according to (B.21) this will be the case if $(\alpha(1-\alpha) - \beta(1-\beta)) \cdot (1 - 2\sqrt{\beta(1-\beta)})/(1-2\beta)^2 \le \delta/2$. Summarizing,

$$R_{\mathrm{LP}}(\delta,\alpha) \le H_2(\beta), \tag{4.14a}$$

if

$$\frac{\alpha(1-\alpha)-\beta(1-\beta)}{(1-2\beta)^2}\,(1-2\sqrt{\beta(1-\beta)}) \le \delta/2. \tag{4.14b}$$

If $\alpha(1-\alpha) \le \delta/2$ already, then (4.14b) will be satisfied with $\beta = 0$ and so

$$R_{\mathrm{LP}}(\delta,\alpha) = 0, \qquad \text{if } \alpha(1-\alpha) \le \delta/2. \tag{4.15}$$

Otherwise define v and u by $v^2/4 = \alpha(1-\alpha)$, $u^2/4 = \beta(1-\beta)$. Then the condition (4.14b) becomes simply $(v^2-u^2)/(1+u) \le 2\delta$. Clearly, the smallest u for which this is satisfied is the unique positive solution to $(v^2-u^2)/(1+u) = 2\delta$, i.e., $u^2 + 2\delta u + 2\delta = v^2$. But, since $H_2(\beta) = g(u^2)$, this means that

$$R_{\mathrm{LP}}(\delta,\alpha) \le g(u^2), \qquad \text{if } \alpha(1-\alpha) \ge \delta/2. \tag{4.16}$$

This, combined with (4.15), gives the promised bound (2.16).

ACKNOWLEDGMENT

The authors wish to thank Philippe Delsarte, Andrew Odlyzko, and Neil Sloane for their helpful comments on this paper.

APPENDIX A

Some Properties of Krawtchouk Polynomials

In this appendix we collect for reference purposes several important properties of the Krawtchouk polynomials $K_j(x)$ defined in Section II.[10] First recall the definition

$$K_j(x) = \operatorname*{coef}_{y^j}(1-y)^x(1+y)^{n-x}. \tag{A.1}$$

From (A.1), it follows that

$$K_j(x) = \sum_{k=0}^{j} (-1)^k \binom{x}{k}\binom{n-x}{j-x}. \tag{A.2}$$

If in (A.1) we write $(1-y)^x = (1+y-2y)^x$ and expand, we get the alternative formula

$$K_j(x) = \sum_{k=0}^{j} (-2)^k \binom{x}{k}\binom{n-k}{j-k}. \tag{A.3}$$

From (A.2) or (A.3), it follows that $K_j(x)$ is a polynomial of degree j in x, and it is easily verified that

$$K_0(x) = 1, \tag{A.4}$$

$$K_1(x) = -2x + n, \tag{A.5}$$

$$K_2(x) = 2x^2 - 2xn + (n^2-n)/2, \tag{A.6}$$

$$K_j(x) = \frac{(-2)^j}{j!}x^j + \text{lower degree terms}, \tag{A.7}$$

$$K_j(0) = \binom{n}{j}, \tag{A.8}$$

$$K_j(1) = \frac{n-2j}{j}\binom{n-1}{j-1}, \qquad \text{if } j \ne 0. \tag{A.9}$$

From (A.1), it is easy to verify that $\binom{n}{i}K_j(i) = \text{coef of } y^jz^i \text{ in } (1+y+z-yz)^n$; since this is symmetric in y and z, it follows that

$$\binom{n}{i}K_j(i) = \binom{n}{j}K_i(j). \tag{A.10}$$

We come now to the crucial *orthogonality properties*. Let $\beta(x)$ be a step function with jumps of $2^{-n}\binom{n}{k}$ at $x = k$, $k = 0,1,\cdots,n$. Regard $\beta(x)$ as a Stieltjes integrator, i.e., for any polynomial $P(x)$, define $\int P(x)\,d\beta = 2^{-n}\sum_k P(k)\binom{n}{k}$. The polynomials $K_j(x)$ are *orthogonal* with respect to β, i.e.,

$$\int K_i(x)K_j(x)\,d\beta = \binom{n}{i}\delta_{i,j}, \tag{A.11}$$

(see Szego [7, §2.82]). Hence for any $P(x)$ of degree at most n,

$$\begin{aligned} P(i) &= \sum_{k=0}^{n}\alpha_k K_k(i), \qquad i = 0,1,\cdots,n, \\ \alpha_k &= \binom{n}{k}^{-1}\int P(x)\,d\beta. \end{aligned} \tag{A.12}$$

Many important facts follow from this orthogonality. (Formulas (A.13)–(A.18) are all derived from facts in Szego [7, §3.2–3.4].)

For example, there is a recurrence formula

$$(j+1)K_{j+1}(x) - (n-2x)K_j(x) + (n-j+1)K_{j-1}(x) = 0. \tag{A.13}$$

[10] The dependence of $K_j(x)$ on n will usually be suppressed, but, if necessary (e.g. in the proof of (A.20)), we will use the notation $K_j^{(n)}(x)$.

By using the reciprocity formula (A.10), it is easy to transform (A.13) into a *difference equation*

$$(n - i)K_j(i + 1) - (n - 2j)K_j(i) + iK_j(i - 1) = 0. \quad \text{(A.14)}$$

Also, we have the *Christoffel-Darboux* formula, which says that if $P_0,P_1,\cdots$, are polynomials orthogonal with respect to the Stieltjes integrator $\alpha(x)$, i.e., $\int P_i(x)P_j(x)\,d\alpha(x) = \delta_{ij}\mu_j$, then

$$\sum_{k=0}^{j} \frac{P_k(x)P_k(y)}{\mu_k} = \frac{1}{\mu_j}\frac{L_j}{L_{j+1}}\left[\frac{P_{j+1}(x)P_j(y) - P_j(x)P_{j+1}(y)}{x - y}\right], \quad \text{(A.15)}$$

where L_j is the leading coefficient of $P_j(x)$. For the Krawtchouk polynomials, $\mu_k = \binom{n}{k}$ by (A.11), and $L_j/L_{j+1} = -(j + 1)/2$ by (A.7), and (A.15) becomes

$$K_{j+1}(x)K_j(y) - K_j(x)K_{j+1}(y) = \frac{2(y - x)}{j + 1}\binom{n}{j}\sum_{k=0}^{j}\frac{K_k(x)K_k(y)}{\binom{n}{k}}. \quad \text{(A.16)}$$

Furthermore, $K_j(x)$ has j distinct real zeroes $x_1^{(j)} < x_2^{(j)} < \cdots < x_j^{(j)}$ in the open interval $(0,n)$, and the zeroes of K_j and K_{j+1} are interlaced:

$$x_{i-1}^{(j)} < x_i^{(j+1)} < x_i^{(j)}, \qquad i = 1,2,\cdots,j + 1, \quad \text{(A.17)}$$

where in (A.17) we have defined $x_0^{(j)} = 0$, $x_{j+1}^{(j)} = n$. In addition, each interval $(x_i^{(j)},x_{i+1}^{(j)})$ must contain a point of increase of $\beta(x)$, i.e., an integer. Since by (A.8), $K_j(0) > 0$ and by (A.9), $K_j(1) > 0$ if $j < n/2$, it follows that

$$x_1^{(j)} \geq 1, \qquad \text{if } j < n/2. \quad \text{(A.18)}$$

The next two results about Krawtchouk polynomials we shall derive in detail. Our first result is that any product $K_i(x)K_j(x)$ can be expressed as a linear combination of the K_k with nonnegative coefficients,[11] i.e.,

$$K_i(x)K_j(x) = \sum_{k=0}^{n}\alpha_k K_k(x), \qquad \alpha_k \geq 0. \quad \text{(A.19)}$$

To prove (A.19), observe that $K_i(x)K_j(x)$ is the coefficient of y^iz^j in $(1 - y)^x(1 + y)^{n-x}(1 - z)^x(1 + z)^{n-x} = (1 + yz)^n(1 - (y + z)/(1 + yz))^x(1 + (y + z)/(1 + yz))^{n-x} = (1 + yz)^n\,\Sigma_{k=0}^{n}K_k(x)((y + z)/(1 + yz))^k = \Sigma_{k=0}^{n}K_k(x)(y + z)^k(1 + yz)^{n-k}$. The coefficients of this last polynomial in y and z are obviously nonnegative and in fact this shows that in (A.19),

$$\alpha_k = \binom{n - k}{(i + j - k)/2}\binom{k}{(i - j + k)/2},$$

where a binomial coefficient with fractional or negative lower index is to be interpreted as zero.[12]

Finally, we come to an important result about the asymptotic behavior of the smallest zero $x_1^{(j)}$ of $K_j^{(n)}(x)$. Let (j_n) be a sequence of integers for which $j_n/n \to \tau$, $0 \leq \tau \leq 1$, and let $x_1^{(j_n)}$ denote the smallest zero of $K_{j_n}^{(n)}(x)$. Then

$$\limsup_{n\to\infty}\frac{x_1^{(j_n)}}{n} \leq 1/2 - \sqrt{\tau(1 - \tau)}. \quad \text{(A.20)}$$

(Actually it is possible to prove that for $\tau \leq 1/2$, the limit in (A.20) exists and equals $1/2 - \sqrt{\tau(1 - \tau)}$ (for $\tau \geq 1/2$, the limit is 0), but the present estimate is sufficient for our purposes and is much easier to prove.)

[11] Formula (A.19) must be taken to mean that the polynomials on the left and right are equal for $x = 0,1,\cdots,n$, since, viewed as a polynomial, $K_i(x)K_j(x)$ has degree $i + j$, which may exceed n.

[12] Note that α_k is the number of vectors of weight i in V_n at distance j from a fixed vector of weight k.

To prove (A.20), observe that if it is false, then for all sufficiently small[13] ϵ, there exists an infinite sequence of n such that $x_1^{(j_n)} \geq n(r + 2\epsilon)$, where $r = r(\tau) = 1/2 - \sqrt{\tau(1 - \tau)}$. Define for each n in this sequence integers i and j by

$$i = i_n = \lfloor n(r + \epsilon)\rfloor \quad \text{(i)}$$

$$j = j_n. \quad \text{(ii)}$$

Let $K_j(x) = (-2)^j/j!\,(x - x_1)(x - x_2)\cdots(x - x_j)$. Then,

$$\log\frac{K_j(i + 1)}{K_j(i)} = \sum_{k=1}^{j}\log\left(1 + \frac{1}{i - x_k}\right).$$

But from (i) $|i - x_k| \geq \epsilon n$, and so $\log(1 + (i - x_k)^{-1}) = (i - x_k)^{-1} + 0(n^{-2})$. Therefore,

$$\log\frac{K_j(i + 1)}{K_j(i)} = \sum_{k=1}^{j}\frac{1}{i - x_k} + 0(n^{-1}).$$

Similarly,

$$\log\frac{K_j(i - 1)}{K_j(i)} = -\sum_{k=1}^{j}\frac{1}{i - x_k} + 0(n^{-1}).$$

Hence

$$\log\frac{K_j(i + 1)}{K_j(i)} - \log\frac{K_j(i)}{K_j(i - 1)} = 0(n^{-1}),$$

and so

$$\frac{K_j(i + 1)}{K_j(i)} = \frac{K_j(i)}{K_j(i - 1)}(1 + 0(n^{-1})). \quad \text{(iii)}$$

Now the difference equation (A.14) can be written as

$$(n - i)\frac{K_j(i + 1)}{K_j(i)}\cdot\frac{K_j(i)}{K_j(i - 1)} - (n - 2j)\frac{K_j(i)}{K_j(i - 1)} + i = 0.$$

If we denote the ratio $K_j(i)/K_j(i - 1)$ by ρ, this becomes

$$(n - i)\rho^2(1 + 0(n^{-1})) - (n - 2j)\rho + i = 0. \quad \text{(iv)}$$

Since ρ is real, the discriminant of (iv) must be nonnegative, i.e.,

$$(n - 2j)^2 - 4i(n - i) + 0(n) \geq 0.$$

However, by (i) and (ii), this is equivalent to

$$(1 - 2\tau)^2 - 4(r + \epsilon)(1 - r - \epsilon) + 0(n^{-1}) \geq 0,$$

but $(1 - 2\tau)^2 = 4r(1 - r)$ and so

$$-\epsilon(1 - 2r) + \epsilon^2 + 0(n^{-1}) \geq 0. \quad \text{(v)}$$

But, if ϵ is selected so that $-\epsilon(1 - 2r) + \epsilon^2 < 0$, i.e., $\epsilon < 1 - 2r$, (v) is clearly violated for sufficiently large n. This completes the proof of (A.20).

APPENDIX B

Some Properties of the Q-Polynomials

In this appendix we collect for reference purposes several important properties of the numbers $Q_j(i)$ cited in Section II (2.13). Most of these properties were originally discovered by Delsarte [3], and we have given references to his work where appropriate.

The numbers $Q_j(i)$ actually depend on j, i, n, and w, and if it is necessary to emphasize this dependence, we will use the notation $Q_j^{(n,w)}(i)$. To define these numbers, we first introduce

[13] In the following argument, ϵ should be thought of as fixed. Its value will be specified more precisely later. (See the remarks following (v), below.)

the auxiliary constants

$$\mu_j = \binom{n}{j} - \binom{n}{j-1} = \binom{n}{j}\frac{n-2j+1}{n-j+1} \tag{B.1}$$

$$\upsilon_i = \binom{w}{i}\binom{w'}{i}, \qquad w' = n - w. \tag{B.2}$$

Then the definition is

$$Q_j(i) = \frac{\mu_j}{\upsilon_i} \cdot \operatorname*{coef}_{y^i z^i} (1-yz)^j (1+y)^{w-j}(1+z)^{w'-j}. \tag{B.3}$$

If in (B.3) we expand $(1+y)^{w-j} = ((1-yz) + y(1+z))^{w-j} = \Sigma_{k=0}^{w-j}\binom{w-j}{k}(1-yz)^{w-j-k}y^k\,(1+z)^k$, we get the formula (cf. [3, eq. (4.33)])

$$Q_j(i) = \frac{\mu_j}{\upsilon_i} \cdot \sum_{k=0}^{w-j} (-1)^{i-k}\binom{w-k}{i-k}\binom{w-j}{k}\binom{w'-j+k}{k}. \tag{B.4}$$

Similarly, expanding $(1-yz)^j = \Sigma_{k=0}^{j}\binom{j}{k}(-yz)^k$, we get (cf. [3, the equation between (4.33) and (4.34)])

$$Q_j(i) = \frac{\mu_j}{\upsilon_i}\sum_{k=0}^{i}(-1)^{i-k}\binom{j}{i-k}\binom{w-j}{k}\binom{w'-j}{k}. \tag{B.5}$$

Also, expanding $(1-yz)^j$, $1))1+y)(1-z) + (1-y)(1+z))/2]^j = 2^{-j}\,\Sigma_{k=0}^{j}\binom{j}{k}(1+y)^k(1-z)^k(1-y)^{j-k}\,(1+z)^{j-k}$, we get, using the formulas (A.1) and (A.10),

$$Q_j(i) = \frac{\mu_j}{2^j}\sum_{k=0}^{j}\frac{\binom{j}{k}}{\binom{w}{j-k}\binom{w'}{k}}K_{j-k}^{(w)}(i)K_k^{(w')}(i). \tag{B.6}$$

Finally, we remark that $Q_j(x)$ belongs to the family of *Hahn polynomials* and that it can be expressed as [1], [4]

$$Q_j(x) = \mu_j {}_3F_2(-j,-x,j-n-1;-w,-w';1)$$

$$= \mu_j\sum_{k=0}^{j}(-1)^k\frac{\binom{j}{k}\binom{n+1-j}{k}}{\binom{w}{k}\binom{w'}{k}}\binom{x}{k}. \tag{B.7}$$

Formulas (B.6) and (B.7) show that $Q_j(i)$ is a polynomial of degree j in i. We shall denote this polynomial by $Q_j(x)$ or $Q_j^{(n,w)}(x)$. From (B.3)–(B.6), the following elementary properties are easily verified:

$$Q_0(x) = 1, \tag{B.8}$$

$$Q_1(x) = (n-1)\left(1 - \frac{nx}{ww'}\right), \tag{B.9}$$

$$Q_j(0) = \mu_j, \tag{B.10}$$

$$Q_j(1) = \mu_j\left(1 - \frac{j(n+1-j)}{ww'}\right), \tag{B.11}$$

$$Q_j(x) = \frac{(-1)^j}{j!}\frac{\binom{n}{w}}{\binom{n-2j}{w-j}}x^j + \text{lower degree terms}. \tag{B.12}$$

Delsarte has shown ([3, sections 2, 4]) that the polynomials $Q_j(x)$ are orthogonal with respect to the Stieltjes integrator $\beta(x)$ with jumps of $\binom{w}{i}\binom{w'}{i}\binom{n}{w}^{-1}$, at $i = 0,1,\cdots,w$, i.e., that

$$\int Q_j(x)Q_k(x)\,d\beta(x) = \mu_j\delta_{j,k}. \tag{B.13}$$

Hence for any polynomial $P(x)$ of degree at most w,

$$P(i) = \sum_{j=0}^{w}\alpha_j Q_j(i), \qquad i = 0,1,\cdots,w,$$

where

$$\alpha_j = \mu_j^{-1}\int P(x)Q_j(x)\,d\beta(x)$$

$$= \mu_j^{-1}\sum_{i=0}^{w}P(i)\binom{w}{i}\binom{w'}{i}\binom{n}{w}^{-1}. \tag{B.14}$$

Now we invoke the general theory of orthogonal polynomials (see Szegö [7, chapter 2] and Appendix A), and obtain the Christoffel–Darboux formula for the $Q_j(x)$, viz.,

$$Q_{j+1}(x)Q_j(y) - Q_j(x)Q_{j+1}(y)$$

$$= (y-x)\cdot\frac{(n-2j)(n-2j-1)}{(j+1)(w-j)(w'-j)}\mu_j\sum_{k=0}^{j}\frac{Q_k(x)Q_k(y)}{\mu_k}. \tag{B.15}$$

Each $Q_j(x)$ has j distinct real zeroes $x_1^{(j)} < x_2^{(j)} < \cdots < x_j^{(j)}$ in the open interval $(0,w)$, and the zeroes of $Q_j(x)$ and $Q_{j+1}(x)$ are interlaced:

$$x_{i-1}^{(j)} < x_i^{(j+1)} < x_i^{(j)}, \qquad i = 1,2,\cdots j+1, \tag{B.16}$$

where in (B.17) we have defined $x_0^{(j)} = 0$, $x_{j+1}^{(j)} = w$. Each open interval $(x_i^{(j)},x_i^{(j+1)})$ must contain a point of increase of $\beta(x)$, i.e., an integer.

If we expand the product $Q_j(x)Q_l(x)$ as

$$Q_j(i)Q_l(i) = \sum_{k=0}^{w}q_{j,l}^{(k)}Q_k(i), \tag{B.17}$$

where, according to (B.14), the constants $q_{j,l}^{(k)}$ are given by

$$q_{j,l}^{(k)} = \mu_k^{-1}\int Q_j(x)Q_l(x)Q_k(x)\,d\beta(x), \tag{B.18}$$

then Delsarte ([3, lemma 2.4]) has shown that

$$q_{j,l}^{(k)} \geq 0, \qquad \text{all } j,k,l, \in \{0,1,\cdots,w\}. \tag{B.19}$$

The last result we take from Delsarte is the following difference equation [3, p. 49]:

$$(w-i)(w'-i)Q_j(i+1) - (ww' - j(n-2i)$$
$$- j(n+1-i))Q_j(i) + i^2Q_j(i-1) = 0. \tag{B.20}$$

Our final result here concerns the asymptotic behavior of the smallest zero $x_1^{(j)}$ of $Q_j^{(n,w)}(x)$ as j, w, and n all approach infinity at the same rate. Thus let (w_n) and (j_n) be sequences of integers with $w_n/n \to \alpha$, $j_n/n \to \beta$ with $\beta \leq \alpha \leq \frac{1}{2}$, and let $x_1(j,w,n)$ denote the smallest zero of $Q_j^{(n,w)}(x)$. Then,

$$\limsup_{n\to\infty}\frac{x_1(j_n,w_n,n)}{n} \leq \frac{\alpha(1-\alpha)-\beta(1-\beta)}{(1-2\beta)^2}$$
$$\cdot(1-2\sqrt{\beta(1-\beta)}). \tag{B.21}$$

(Actually it is possible to prove that the limit in (B.21) exists and equals the right side of (B.21) for all $\beta \leq \alpha \geq \frac{1}{2}$, but, since the proof is very long and we do not require it in the derivation of the bound (2.15), we omit it.)

To prove (B.21), observe that if it is false, then for all sufficiently small[14] ϵ, there exists an infinite sequence of n such that $x_1(j_n,w_n,n) \geq n(F+2\epsilon)$, where F denotes the constant on the right side of (B.21). For a fixed n in this sequence, define $i = i_n = \lfloor (F+\epsilon)\rfloor$, $j = j_n$, $w = w_n$, $w' = n - w_n$, and let $Q_j^{(n,w)}(x) = L_j(x - x_1^{(j)})\cdots(x - x_j^{(j)})$. Then

$$\log\frac{Q_j(i\pm1)}{Q_j(i)} = \sum_{k=1}^{j}\log\left(1 \pm \frac{1}{i - x_k^{(j)}}\right). \tag{i}$$

[14] In the following argument ϵ should be regarded as fixed. Its value will be specified more precisely later (see the remarks following (xi), below).

But $i \le n(F+\epsilon)$ and $x_1^{(j)} \ge n(F+2\epsilon)$, and so $|i - x_k^{(j)}| \ge \epsilon n$, for $k = 1,2,\cdots,j$. Thus

$$\log\left(1 \pm \frac{1}{i - x_k^{(j)}}\right) = \frac{\pm 1}{i - x_k^{(j)}} + 0(n^{-2}). \tag{ii}$$

Combining (i) and (ii), we have

$$\log \frac{Q_j(i \pm 1)}{Q_j(i)} = \pm \sum_{k=1}^{j} \frac{1}{i - x_k^{(j)}} + 0(n^{-1}). \tag{iii}$$

Subtracting the "+" equation from the "−" equation in (iii), we obtain

$$\log \frac{Q_j(i+1)}{Q_j(i)} - \log \frac{Q_j(i)}{Q_j(i-1)} = 0(n^{-1}), \tag{iv}$$

and so

$$\frac{Q_j(i+1)}{Q_j(i)} = \frac{Q_j(i)}{Q_j(i-1)} \cdot \{1 + 0(n^{-1})\}. \tag{v}$$

The difference equation (B.20) can be written as

$$(w-i)(w'-i)\frac{Q_j(i+1)}{Q_j(i)} \cdot \frac{Q_j(i)}{Q_j(i-1)} - (ww' - j(n-2i) - j(n+1-i))\frac{Q_j(i)}{Q_j(i-1)} + i^2 = 0. \tag{vi}$$

If we denote the ratio $Q_j(i)/Q_j(i-1)$ by ρ, then (vi) becomes

$$(w-i)(w'-i)\rho^2(1 + 0(n^{-1})) - (ww' - i(n-2i) - j(n+1-j))\rho + i^2 = 0. \tag{vii}$$

Since ρ is perforce real, the discriminant of the quadratic equation (vii) must be at least 0, i.e.,

$$(ww' - j(n-2i) - j(n+1-i))^2 - 4(w-i)(w'-i)i^2 + 0(n^3) \ge 0. \tag{viii}$$

Despite appearances, this is actually only quadratic in (i), and a little rearrangement of (viii) yields

$$(n-2j)^2 i^2 - 2n(w-j)(w'-j)i + (w-j)^2(w'-j)^2 + 0(n^3) \ge 0. \tag{ix}$$

The two zeroes of the quadratic polynomial $(n-2j)^2 i^2 - 2n(w-j)(w'-j)i + (w-j)^2 (w'-j)^2$ are given by

$$i_1, i_2 = \frac{(w-j)(w'-j)}{(n-2j)^2}(n \pm 2\sqrt{j(n-j)}). \tag{x}$$

Recalling that $w_n/n \to \alpha$, $j_n/n \to \beta$, etc., then for large n,

$$\frac{i_1}{n}, \frac{i_2}{n} \to \frac{\alpha(1-\alpha) - \beta(1-\beta)}{(1-2\beta)^2}(1 \pm 2\sqrt{\beta(1-\beta)}). \tag{xi}$$

Hence, if ϵ is selected so that $i = i_n = \lfloor n(F+\epsilon) \rfloor$ lies between i_1 and i_2, the discriminant in (ix) will for large n behave like a *negative* constant times n^4, a contradiction. This completes the proof of (B.21).

References

[1] R. Askey, *Orthogonal Polynomials and Special Functions.* (vol. 21 in SIAM's Regional Conference Lectures in Applied Math.) Philadelphia: SIAM, 1975.

[2] E. R. Berlekamp, *Algebraic Coding Theory.* New York: McGraw-Hill, 1968.

[3] P. Delsarte, *An Algebraic Approach to the Association Schemes of Coding Theory.* Eindhoven: Philips Research Reports Supplements no. 10, 1973.

[4] S. Karlin and J. L. McGregor, "The Hahn polynomials, formulas, and an application," *Scripta Mathematica,* vol. 26, pp. 33–46, 1961.

[5] V. I. Levenshtein, "On the minimal redundancy of binary error-correcting codes" (in Russian), Problemy Peredachi Informatsii, vol. 10, pp. 26–42, 1974. (English translation in *Information and Control,* vol. 28, pp. 268–291, 1975.)

[6] V. M. Sidelnikov,, "Upper bounds on the cardinality of a binary code with a given minimum distance" (in Russian), *Problemy Peredachi Informatsii,* vol. 10, pp. 43–51, 1974. (English translation in *Information and Control,* vol. 28, pp. 292–303, 1975.)

[7] G. Szego, *Orthogonal Polynomials.* Providence: American Mathematical Society, 1939.

[8] L. R. Welch, R. J. McEliece, and H. Rumsey, Jr., "A low-rate improvement on the Elias bound," *IEEE Trans. Inform. Theory,* vol. IT-20, pp. 676–678, Sept. 1974.