[15] T. Kløve and V. I. Korzhik, *Error Detecting Codes*, Kluwer (1995).

[16] T. Kløve, "Bounds on the weight distribution of cosets," *IEEE Trans. Inform. Theory*, **42** (6) (1996), 2257–2260.

[17] V. I. Korzhik, "Bounds on the probability of undetected error and optimum group codes in a channel with feedback," *Radiotechnika*, **20** (1) (1965), 27–33. English translation in *Telecommun. Radio Eng.*, **20** (1, pt.2) (1965), 87–92.

[18] V. K. Leontiev, "Error-detecting encoding," *Problemy Peredachi Informatsii*, **8** (3) (1972), 6–14

[19] V. I. Levenshtein, "Bounds on the probability of undetected error," *Problemy Peredachi Informatsii*, **13** (1) (1977), 3–18.

[20] ———, "Bounds for packings of metric spaces and some applications," *Problemy kibernetiki*, **40** (1983), 43–110 (in Russian).

[21] ———, "Straight-line bound for the undetected error exponent," *Problemy Peredachi Informatsii*, **25** (1) (1989), 33–37.

[22] ———, "Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces," *IEEE Trans. Inform. Theory*, **41** (3) (1995), 1303–1321.

[23] ———, "Equivalence of Delsarte's bounds for codes and designs in symmetric association schemes and some applications," preprint (1997).

[24] S. Litsyn, "New upper bounds on error exponents," *IEEE Trans. Inform. Theory*, to appear.

[25] R. J. McEliece and J. Omura, "An improved upper bound on the block coding error exponent for binary-input discrete memoryless channels," *IEEE Trans. Inform. Theory*, **23** (5) (1977), 611–613.

[26] R. J. McEliece, E. R. Rodemich, H. Rumsey, and L. R. Welch, "New upper bound on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Trans. Inform. Theory*, **23** (2) (1977), 157–166.

[27] F. J. MacWilliams, "A theorem on the distribution of weights in a systematic codes," *Bell Syst. Techn. Journal*, **42** (1963), 79–94.

[28] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland (1981).

[29] C. E. Shannon, R. G. Gallager, and E. R. Berlekamp, "Lower bounds to error probability for codes on discrete memoryless channels, II", *Information and Control*, **10** (1967), 522–552.

[30] A. Schrijver, *Theory of Linear and Integer Programming*, John Wiley & Sons (1986).

[31] J. Simonis, "The effective length of subcodes," *Applicable Algebra in Engineering, Communication and Computing*, **5** (1994), 371–377.

[32] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic Geometry Codes*, Kluwer (1990).

[33] A. Viterbi and J. Omura, *Principles of Digital Communication and Coding*, McGraw Hill (1979).

[34] J. K. Wolf, A. M. Michelson, and A. H. Levesque, " On the probability of undetected error for linear block codes," *IEEE Trans. Commun*, **30** (1982), 317–324.

Theorem 24 (Rodemich, 1979, see [8].) *Let $f(x)$ be any real polynomial and let $f(x) = \sum_{t=0}^{w} f_t Q_t(x)$ be its expansion in the basis of Hahn polynomials (40) in the Johnson scheme J_v^n, where*

$$f_0 > 0,\ f_t \geq 0, \quad 1 \leq t \leq n.$$

Let $F(x)$ be the polynomial of degree at most n given by its values at integer points as follows:

$$F(i) = \begin{cases} \frac{\binom{v}{i/2}\binom{n-v}{i/2}}{\binom{n}{i}} f(i/2), & i = 0, 2, \ldots, 2v, \\ 0 & \text{otherwise,} \end{cases}$$

and let $F(x) = \sum_{k=0}^{n} F_k P_k(x)$ be its Krawtchouk expansion. Then $F_k \geq 0$, $1 \leq k \leq n$, and

$$F_0 = \frac{\binom{n}{v}}{2^n} f_0.$$

References

[1] K. A. S. Abdel-Ghaffar, "A lower bound on the undetected error probability and strictly optimal codes," *IEEE Trans. Inform. Theory*, **43** (5) (1997), 1489–1502.

[2] A. Barg, "The matroid of supports of a linear code," *Applicable Algebra in Engineering, Communication and Computing*, **8** (1997), 165–172.

[3] A. Barg and A. Ashikhmin, "Binomial moments of the distance distribution and the probability of undetected error," Bell Labs TM BL0112110-971204-15, *Designs, Codes and Cryptography*, to appear.

[4] L. A. Bassalygo, "New upper bounds for codes correcting errors," *Problemy Peredachi Informatsii*, **1** (4) (1965), 41–44.

[5] A. R. Calderbank, E. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction via codes over GF(4)," *IEEE Trans. Inform. Theory*, **44** (4) (1998), 1369-1387.

[6] P. Delsarte, "Bounds for unrestricted codes, by linear programming," *Philips Res. Repts*, **27** (1972), 272–289.

[7] ———, "Bilinear forms over a finite field, with applications to coding theory," *J. Combinatorial Theory Ser. A*, **25** (1978), 226–241.

[8] ———, "Application and generalization of the MacWilliams transform in coding theory," in *Proc. 15th Sympos. Inform. Theory in the Benelux* (1994), 9–44.

[9] R. G. Gallager, *Information Theory and Reliable Communication*, John Wiley & Sons (1968).
IEEE Trans. Inform. Theory, **11** (1) (1965), 3–18.

[10] C. Greene, "Weight enumeration and the geometry of linear codes," *Stud. Appl. Math.*, **55** (1976), 119–128.

[11] T. Helleseth, T. Kløve, and V. I. Levenshtein, "On the information function of an error-correcting code," *IEEE Trans. Inform. Theory*, **43** (2) (1997), 549–557.

[12] G. Kalai and N. Linial, "On the distance distribution of codes," *IEEE Trans. Inform. Theory*, **41** (5) (1995), 1467–1472.

[13] G. L. Katsman and M. A. Tsfasman, "Spectra of algebraic geometric codes," *Problemy Peredachi Informatsii*, **23** (4) (1988), 19–34.

[14] G. L. Katsman, M. A. Tsfasman, and S. G. Vladuts, "Spectra of linear codes and error probability of decoding," in H. Stichtenoth and M. A. Tsfasman, Eds., *Coding Theory and Algebraic Geometry*, Lect. Notes Math., vol. **1518**, Berlin: Springer (1992), pp. 82–98.

Let $t = \tau n$, $0 \le x = \xi n < x_{k,v}$. Similarly to (76), up to $o(1)$ terms, we have (see [24])

$$\frac{1}{n}\log Q_t(x) = H(\tau) + \int_o^\xi \log\Big[\frac{\nu(1-\nu) - y(1-2y) - \tau(1-\tau)}{2(\nu-y)(1-\nu-y)} + \frac{\sqrt{[\nu(1-\nu) - y(1-2y) - \tau(1-\tau)]^2 - 4(\nu-y)(1-\nu-y)y^2}}{2(\nu-y)(1-\nu-y)}\Big]dy \quad (80)$$

On the other hand, as above, taking in (78) $k = j$, we get

$$\frac{1}{n}\log Q_t(x) = \frac{1}{2}\Big[H(\tau) + H(\nu) - \nu H\Big(\frac{\xi}{\nu}\Big) - (1-\nu)H\Big(\frac{\xi}{1-\nu}\Big)\Big]. \quad (81)$$

It can be checked that for

$$\tau = \tau_\nu(\xi) := \frac{1}{2}\Big(1 - \sqrt{1 - 4\big(\sqrt{\nu(1-\nu) - \xi(1-\xi)} - \xi\big)^2}\Big), \quad (82)$$

i.e.,

$$\xi = \frac{\nu(1-\nu) - \tau(1-\tau)}{1 + 2\sqrt{\tau(1-\tau)}},$$

these estimates are equal, i.e., (82) is exponentially tight.

Appendix B. Proof of (39).

Recall that $\tau = \frac{1}{2} - \sqrt{\omega^*(1-\omega^*)}$. This function is monotone decreasing in ω^* for $\omega^* \in [0, 1/2]$. The function $\phi'_\xi(\tau, \xi)$ is monotone decreasing in τ; hence, it is also decreasing in ω^*. Therefore, if we prove (39) for $\omega^* = \omega/2$, this will also imply the proof in the case $\omega^* = \delta_{LP1} \ge \omega/2$.

Put $\omega^* = \omega/2$, $0 < \omega \le 1$. Consider the function

$$g(\tau, \xi) = \frac{((1-2\tau) + \sqrt{(1-2\tau)^2 - 4\xi(1-\xi)})^2}{(2-2\xi)^2} - \frac{\omega - \xi}{1-\xi}, \quad 0 < \xi \le \omega/2.$$

Substituting the value of τ, we get

$$g(\omega, \xi) = \frac{\big(\sqrt{\omega(2-\omega)} + \sqrt{\omega(2-\omega) - 4\xi(1-\xi)}\,\big)^2 - 4(\omega-\xi)(1-\xi)}{(2-2\xi)^2}.$$

Note that $g(\omega, \omega/2) = 0$. Further, the denominator of $g(\omega, \xi)$ is positive; the derivative of the numerator

$$4\omega - 4\frac{(1-2\xi)\sqrt{\omega(2-\omega)}}{\sqrt{(2-\omega)\omega - 4\xi(1-\xi)}}$$

has no real zeros. Its value for $\xi = 0$ is $-4(1-\omega) < 0$. Hence, $g(\omega, \xi)$ is positive for $0 < \xi < \omega^*$. This implies (39).

Appendix C.

$$\sum_{i=0}^{n} i^2 P_i(k) \quad = \quad 2^{n-2}[n(n+1)\delta_{k,0} - 2n\delta_{k,1} + 2\delta_{k,2}]. \tag{71}$$

From (10) we see that

$$P_k(0) = \binom{n}{k}. \tag{72}$$

Let $Z(x) = \sum_{i=0}^{n} z_i P_i(x)$ be any polynomial of degree $\leq n$ written to the basis of Krawtchouk polynomials. Then

$$z_j = 2^{-n} \sum_{i=0}^{n} Z(i) P_i(j) \tag{73}$$

Polynomial $P_k(x)$ has degree k and its k simple zeros are located between 0 and n. Let x_k be the smallest zero of $P_k(x)$; let $n \to \infty, k \to \infty, k/n < 1/2$. Then [26], [20], [22]

$$x_k = \frac{n}{2} - \sqrt{k(1-k)} + O\left(k^{1/6}\sqrt{n}\right). \tag{74}$$

Let $k = \tau n$, $0 \leq x = \xi n \leq x_k$. By [12] we have, up to $o(1)$ terms,

$$\frac{1}{n} \log P_k(x) = H(\tau) + \int_0^{\xi} \log \frac{1 - 2\tau + \sqrt{(1-2\tau)^2 - 4y(1-y)}}{2 - 2y} dy. \tag{75}$$

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

$$\frac{1}{n} \log P_k(x) = \frac{1 + H(\tau) - H(\xi)}{2} \tag{76}$$

(another way of proving this estimate [12] is by putting $k = j$ in (66)).

Let $Q_t(x)$ be the dual Hahn polynomial (40), i.e., the Q-polynomial in the Johnson scheme J_v^n. The Hahn polynomials satisfy the following orthogonality relations:

$$\sum_{i=0}^{v} Q_k(i) Q_j(i) \binom{v}{i} \binom{n-v}{i} \Big/ \binom{n}{v} = \left[\binom{n}{j} - \binom{n}{j-1}\right] \delta_{j,k}. \tag{77}$$

Polynomial $Q_t(x)$ has degree t and its t simple zeros are located between 0 and n. We have

$$Q_t(0) = \binom{n}{t} - \binom{n}{t-1} \tag{78}$$

Let $x_{t,v}$ be the smallest zero of $Q_t(x)$; let $n \to \infty$, $v \to \infty$, $t \to \infty$, $0 \leq \frac{t}{n} < \frac{v}{n} \leq (1/2)$. Then [26], [20, Lemma 6.6]

$$x_{t,v} = \frac{v(n-v) - t(n-t)}{n + 2\sqrt{t(n-t)}} + O(\sqrt{v} + v^{2/3}(t/n)^{1/6}). \tag{79}$$

linear polynomial in the Johnson scheme gives the Bassalygo-Elias bound [4] in the Hamming scheme. Another example of using this theorem is given in [23].

Our approach carries over to nonbinary codes, and in fact, the Singleton bound was already reported in [1],[3]. Other channel models for which its application does not present significant difficulties, include general binary discrete memoryless channels and the Gaussian channel. Estimating the probability of undetected error via binomial moments is particularly well-suited for quantum stabilizer codes on the completely depolarized channel [5].

We also used our estimates to obtain asymptotic upper bounds on the exponent on the probability of undetected error of binary codes on the BSC. Another way of obtaining these bounds was recently suggested in by Litsyn [24].The bounds on the error exponents in [24] are obtained by first deriving linear programming existence-type bounds on the components of the distance distribution of the code. Our approach seems to be better suited for computing the probability of undetected error for codes of finite length. The reason for this is that we estimate the probability of undetected error using the entire distance spectrum of the code, whereas in [24] it is estimated by the probability of transition only to codewords at a given distance i from the transmitted codeword. To compute bounds, one has to take minimum over this i. Moreover, the bounds in [24] involve a factor of order $1/n$ which does not appear in our bounds since we use a different form of the distance enumerator (7). Asymptotic results of our papers are the same; any improvement within the frame of the linear programming method would be likely to imply new asymptotic upper bounds on the size of the code with a given distance. The asymptotic derivation of the undetected error exponent seems more straightforward since we only need to estimate the exponent of Krawtchouk and Hahn polynomials in a small neighborhood of the first zero, whereas in the method of [24] one has to bound this exponent for all values of the argument from 0 to the first zero. On the other hand, Litsyn's method provides a more natural framework for estimating the probability of decoding error.

Appendix A: Useful identities.

Let $P_k(x)$ be the Krawtchouk polynomial (10). The proof of the following identities is found in [6], [20], [22].

$$\sum_{i=0}^{n} \binom{n}{i} P_k(i) P_j(i) = \delta_{j,k} \binom{n}{j} 2^n \tag{66}$$

$$P_i^2(x) = \sum_{j=0}^{n} \binom{n-j}{i-j/2} \binom{j}{j/2} P_j(x) \tag{67}$$

$$\sum_{i=0}^{n} \binom{n-i}{n-w} P_i(j) = 2^w \binom{n-j}{w} \tag{68}$$

$$\sum_{i=0}^{n} P_i(k) = 2^n \delta_{k,0} \tag{69}$$

$$\sum_{i=0}^{n} i P_i(k) = 2^{n-1} [n\delta_{k,0} - \delta_{k,1}] \tag{70}$$

We can use this theorem on any upper bound on $E(R,p)$ that is equal to $1-R$ for $R^* \le R \le 1$ as in Theorems 17, 20, 21, The resulting bound connects the point $(R^*, 1-R^*)$ in the $(R, E(R,p))$-plane with the point $(0, -\log\sqrt{p(1-p)})$. However, the resulting bounds are inferior to Theorems 20, 21, and we omit this.

Other applications of the bounds of the previous section include lower estimates on the individual components of the distance distribution of codes. Results of this type are central to the work of Litsyn [24]. He derived linear programming existence-type bounds on coefficients A_i of the distance distribution of codes. We can apply results of the previous section to derive similar estimates. Indeed, if C is a code of rate R with a known value of B_w, then at least one coefficient $A_i, 1 \le i \le w$ is greater than $B_w / w\binom{n-i}{n-w}$. For instance, Theorem 15 implies the following.

Theorem 23 *Let C be a code of rate R. Let $w, 1 \le w \le n$, be any number such that $w \to \infty$ and let $w = \omega n$. Then there exists a number $i = \xi n, 1 \le \xi \le \omega$, such that*

$$A_{\lfloor \xi n \rfloor} \gtrsim R - 1 + H(\omega^*) + (1-\omega^*) H\Big(\frac{1-2\omega}{1-\omega^*}\Big) - (1-\xi) H\Big(\frac{1-2\omega}{1-\xi}\Big), \tag{65}$$

where

$$\omega^* = \begin{cases} \omega, & \delta_{LP}(R) \le \omega \le 1, \\ \delta_{LP}(R), & \delta_{LP}(R)/2 \le \omega \le \delta_{LP}(R). \end{cases}$$

Though Litsyn's estimates are different from this theorem, they enable one to prove the same asymptotic bounds on the undetected error exponent $E_{ue}(R,p)$ (see [24]). Litsyn also suggested a way of using his estimates for bounding from below the probability of decoding error of binary codes on the binary symmetric channel under the maximum likelihood decoding rule. This allowed him to improve the upper bounds on the exponent of the probability of decoding error of Shannon et al. [29], McEliece and Omura [25]. Exponential lower bounds of the form (65) can also be used to obtain bounds on the decoding error exponent better than those of [29], [25].

6 Discussion

In this paper we developed a linear programming approach to deriving lower bounds on binomial moments of the distance distribution of binary codes. Since the conditions on the feasible polynomial differ from the standard Delsarte's problem, finding solutions presents several analytic and combinatorial difficulties. We obtained several optimal or nearly optimal lower bounds for codes of finite length. As in [20], [22], optimality of the bounds depends on the relations between the distance and the size of the code. In this paper we restricted our attention to optimal linear and quadratic polynomials. As in [20], [22], involving polynomials of larger degree gives bounds for codes of larger size (smaller distance).

Derivation of the second form of the LP bound is simplified considerably by using Rodemich's theorem which provides a powerful analytic alternative to the indirect method used for translating LP bounds in the Johnson scheme to the Hamming scheme. For instance, the optimal

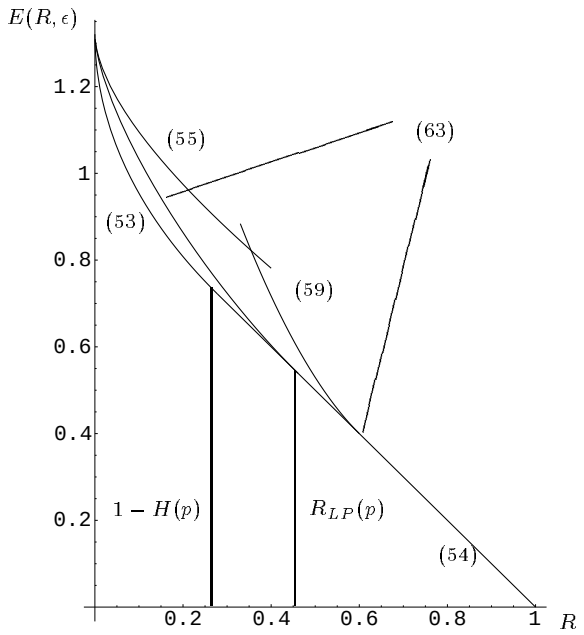


Figure 3: Bounds on $E(R,p)$, $p=0.2$.

PROOF. Let us use estimate (45) in (50). This gives

$$E(R,p)_{ue} \le 1-R-H(\omega^*)-(1-\omega^*)H\left(\frac{1-\omega}{1-\omega^*}\right)-(1-2w)\log(1-2p)-2w\log p, \tag{64}$$

where $\delta_{LP}(R) \le \omega \le 1$ and ω^* is $\delta_{LP}(R)$ or ω according as $\delta_{LP}(R) \ge \omega$ or not. Let $1/2 > p \ge \delta_{LP}(R)$. Put in (64) $\omega = p$. As in (62), in this case we get

$$E(R,p) \le 1-R.$$

Otherwise, put

$$2\omega = \frac{2p\delta_{LP}(R)-p-\delta_{LP}(R)}{p-1}.$$

After several simplification steps we arrive at the first part of our claim. ∎

According to the remark made after (32), estimate (63) is better than (60) for $0 < p \le 0.273...$ Bounds (54),(53),(59),(63) are shown in Fig. 3.

The following analytic result is due to Levenshtein.

Theorem 22 [19] *Let C be a code of length n, $0 \le u \le 1$. Then*

$$P_{ue}(C,p) \ge (|C|-1)^{1-\frac{1}{u}}(p^u+(1-p)^u)^{\frac{n}{u}}P_{ue}\left(C,\frac{p^u}{p^u+(1-p)^u}\right)^{\frac{1}{u}}.$$

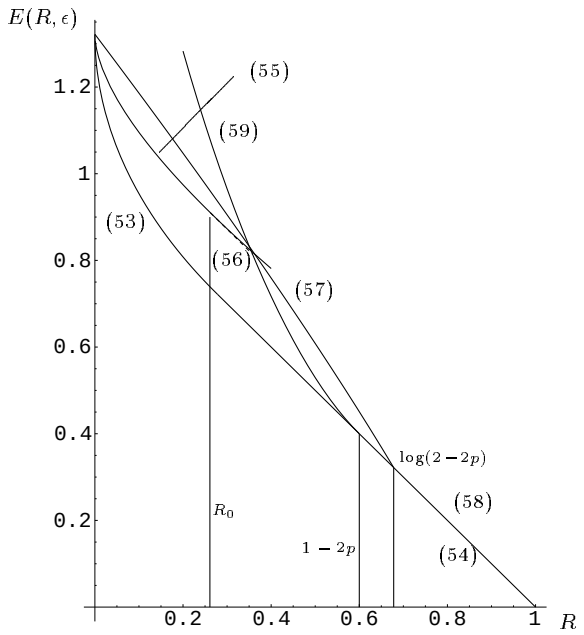


Figure 2: Bounds (53)-(59) on $E(R,p)$, $p = 0.2$.

PROOF. Use estimate (35) in (50). This gives

$$E_{ue}(R,p) \le 1 - R - H(\omega^*) - (1-\omega^*)H\left(\frac{1-\omega}{1-\omega^*}\right) - (1-\omega)\log(1-2p) - \omega\log p, \tag{61}$$

where $\delta_{LP1}(R) \le \omega \le 1$ and ω^* is $\delta_{LP1}(R)$ or $\omega/2$ according as $2\delta_{LP1}(R) \ge \omega$ or not.

Let $1/2 > p \ge \delta_{LP1}(R)$. Put in (61) $\omega = 2p$.

$$\begin{aligned} E_{ue}(R,p) &\le 1 - R - H(p) - (1-p)H\left(\frac{1-2p}{1-p}\right) - (1-2p)\log(1-2p) - 2p\log p \\ &= 1 - R \end{aligned} \tag{62}$$

Otherwise, if $0 < p < \delta_{LP1}(R)$, put in (61)

$$w = \frac{2p\delta_{LP1}(R) - p - \delta_{LP1}(R)}{p-1}.$$

After several simplification steps we arrive at the first part of our claim. ∎

The following theorem uses Theorem 15 to improve this result for low transition probabilities.

Theorem 21

$$E_{ue}(R,p) \le \begin{cases} 1 - R - H(\delta_{LP}(R)) + T(\delta_{LP}(R),p), & 0 \le R \le R_{LP}(p) \\ 1 - R, & R_{LP}(p) \le R \le 1, \end{cases} \tag{63}$$

where $R_{LP}(\cdot)$ is given by (32).

Let us consider asymptotic bounds. Toward this end, let

$$E_{ue}(n,R,p) = -\frac{1}{n}\log P_{ue}(\lceil 2^{Rn}\rceil, n, p).$$

We are interested in upper bounds on

$$\overline{E}_{ue}(R,p) = \limsup_{n\to\infty} \frac{1}{n} E_{ue}(n,R,p)$$

and lower bounds on

$$\underline{E}_{ue}(R,p) = \liminf_{n\to\infty} \frac{1}{n} E_{ue}(n,R,p)$$

Let $E_{ue}(R,p)$ be the common limit of these functions, provided that it exists. Let

$$T(u,v) = -u\log v - (1-u)\log(1-v).$$

The known lower bounds on $E_{ue}(R,p)$ include

$$E_{ue}(R,p) \geq \begin{cases} T(H^{-1}(1-R),p), & 0 \leq R \leq 1-H(p) \quad [19] \quad (53) \\ 1-R, & 1-H(p) \leq R \leq 1 \quad [17] \quad (54) \end{cases}$$

Let $\rho(R)$ be any upper bound on the distance of codes of rate R such that $\rho''(R) \geq 0$ and let $R_0 = R_0(p)$ be defined by $\rho'(R_0) = (\log(p/(1-p)))^{-1}$. Let $\sigma(R) = -R/\log(2^{1-R}-1)$. Then

$$E_{ue}(R,p) \leq \begin{cases} T(\rho(R),p), & 0 \leq R \leq R_0, \quad [19] \quad (55) \\ T(\rho(R_0),p) + R_0 - R, & R_0 \leq R \leq 1, \quad [21] \quad (56) \\ T(\sigma(R),p) - R, & 0 \leq R \leq \log(2-2p), \quad [19] \quad (57) \\ 1-R, & \log(2-2p) \leq R \leq 1. \quad [18],[19] \quad (58) \end{cases}$$

Last year we observed [3] that the Abdel-Ghaffar–Singleton bound [1] yields an essential asymptotic improvement of the upper bounds (56)-(57).

Theorem 19 [3]

$$E_{ue}(R,p) \leq \begin{cases} -H(R) - (1-R)\log p - R\log(1-2p), & 0 \leq R \leq 1-2p, \\ 1-R, & 1-2p \leq R \leq 1. \end{cases} \quad (59)$$

This result extended the region in which the lower bound $1-R$ is tight from $[\log(2-2p),1]$ [18],[19] to $[1-2p,1]$. Bounds (53)-(59) are shown in Fig. 2.

Clearly, Theorems 14 and 15 of the previous section should yield even better bounds.

Theorem 20

$$E_{ue}(R,p) \leq \begin{cases} 1-R-H(\delta_{LP1}(R)) + T(\delta_{LP1}(R),p) & 0 \leq R \leq R_{LP1}(p), \\ 1-R, & R_{LP1}(p) \leq R \leq 1, \end{cases} \quad (60)$$

where $R_{LP1}(\cdot)$ is given by (33).

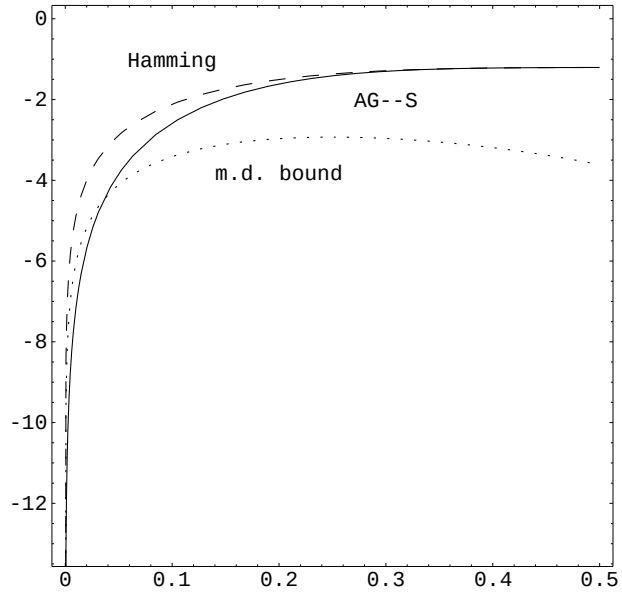


Figure 1: Hamming, Abdel-Ghaffar–Singleton, and minimum distance bounds on $P_{ue}(12, 256, p)$.

PROOF. Follows by (22) and (50). ∎

The Plotkin-type bound (51) is the best for codes of small size. The comparison carried out in [1] shows that for codes of size M such that $\log_2 M \approx n/2$ or greater the bound (52) is usually better than (51).

It is clear that a code that meets any of the bounds derived in the previous section is optimal for error detection. This yields the following proposition.

Proposition 18 *The Hamming codes, the Nordstrom-Robinson code, binary and ternary Golay codes, Hadamard codes, MDS codes are optimal for error detection.*

Optimality of the simplex code for error detection was proved in [18]. Since the dual of an optimal linear code is also optimal (e.g., [15]) optimality of the Hamming code for error detection was also a known fact.

Suppose the length n and code size M are fixed. The advantage of our approach lies in the possibility of optimizing lower bounds on B_w for individual w, something that is out of reach when working with distance spectrum coefficients A_i. This together with Lemma 5 gives an extremely powerful tool of deriving lower bounds on $P_{ue}(M, n, p)$. We shall give only one example; the reader should bear in mind that they are numerous.

Example 7. In [1] it is shown that (52) is better than the other bounds known for codes with $n = 12, M = 256$ for all but very small transition probabilities p. Let us use the estimates of the binomial moments computed in Example 6 to improve the bound.

The results are shown in Fig. 1. The minimum distance bound $P(M, n, p) \geq p^d(1-p)^{n-d}$, where d is the largest possible distance of a $(12, 256)$ code, is better than the Singleton bound for very small transition probabilities. The Hamming bound is the best for all $p \in (0, 1)$. Since the values of B_w given by the Hamming bound in this example coincide with the optimal solutions, no further improvements are possible.

5 Applications

Suppose a code C is used for transmission over a binary symmetric channel with crossover probability p. Suppose the decoding rule is the following: if the sequence received from the channel is a codeword, this is the output of the decoder, otherwise it detects an error. This decoding is used in transmission systems with feedback and automated repeat request. Thus, the decoding error is only possible if the error vector itself is a codeword. The problem is to estimate the probability P_{ue} of this, called the *probability of undetected error*. This problem has a long history in coding theory, see [15]. Formally, let $\{A_0, A_1, \ldots, A_n\}$ be the distance distribution of C, and let

$$P_{ue}(C,p) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i}. \tag{49}$$

Further, let

$$P_{ue}(M,n,p) = \min_{|C|=M} P_{ue}(C,p).$$

The known lower bounds on $P_{ue}(M,n,p)$ include the bounds by Korzhik [17], Leontiev [18], Levenshtein [19],[21], Wolf et al.[34], Kløve [16], Abdel-Ghaffar [1]. We show that some of these bounds correspond to our bounds on binomial moments of the previous section and give some improvements. Toward this end, use (7) to rewrite (49) as

$$P_{ue}(C,p) = \sum_{i=1}^{n} B_i p^i (1-2p)^{n-i}. \tag{50}$$

Let us prove the bound [17].

Theorem 16 (The Korzhik-Plotkin bound) *Let* $s_0 = nM/2(M-1)$. *Then*

$$P_{ue}(M,n,p) \geq (M-1)p^{s_0}(1-p)^{n-s_0}. \tag{51}$$

PROOF. By (20) we have

$$\begin{aligned} P_{ue}(M,n,p) &\geq (M-1)\sum_{w=s_0}^{n} \binom{n-s_0}{w-s_0} p^w (1-2p)^{n-w} \\ &= (M-1)p^{s_0}\sum_{w=0}^{n-s_0} \binom{n-s_0}{w} p^w (1-2p)^{n-s_0-w} \\ &= (M-1)p^{s_0}(1-p)^{n-s_0}. \end{aligned}$$

∎

The Singleton bound yields the bound of Abdel-Ghaffar [1].

Theorem 17 (The Abdel-Ghaffar–Singleton bound)

$$P_{ue}(M,n,p) \geq \sum_{w=n-k+1}^{n} \binom{n}{w} (M2^{w-n}-1)p^w(1-2p)^{n-w}. \tag{52}$$

PROOF. By (79), for the polynomial (42) we have

$$Z(0) = \frac{1}{aQ_t^2(w^*/2)} \frac{\binom{n-w^*}{n-2w}\binom{n}{w^*}}{\binom{v}{w^*/2}\binom{n-v}{w^*/2}} \binom{n}{t}^2 \Big[\frac{n^2-(2t-1)n-2t}{(n-t+1)(t+1)}\Big]^2. \tag{46}$$

Let $Z(x) = \sum_{i=0}^n z_i P_i(x)$ be the expansion of $Z(x)$ in the Krawtchouk basis. Again use Rodemich's theorem to deduce the expression for z_0:

$$z_0 = 2^{-n}\binom{n}{v} \frac{\binom{n-w^*}{n-2w}\binom{n}{w^*}}{\binom{v}{w^*/2}\binom{n-v}{w^*/2}} \frac{1}{Q_t^2(w^*/2)} \Big[\binom{n}{t} - \binom{n}{t-1}\Big] \frac{(n-2t)(n-2t-1)}{(t+1)(v-t)(n-v-t)}. \tag{47}$$

From this and (46) we see that as long as

$$\frac{1}{n}\log(|C|z_0) > \frac{1}{n}\log Z(0)$$

or

$$\frac{1}{n}\log(\binom{n}{v}2^{-n}|C|) > \frac{1}{n}\log\binom{n}{t}$$

or

$$H(\nu) - H(\tau) > 1 - R(C), \tag{48}$$

we have $Z(0) = o\big(|C|z_0\big)$, and by (16) we obtain

$$B_{2w} \gtrsim z_0|C|.$$

Hence for this asymptotic estimate to be valid, $H(\nu)$ can be taken arbitrarily close to $1-R(C)-H(\tau)$. Recall that $\tau = \tau_\nu(\omega^*)$. Then we can use (82) in (47) to compute the bound. Observe that up to $o(1)$ terms,

$$(1/n)\log\Big(\binom{n}{v}\binom{n}{t}\Big/\binom{v}{w^*/2}\binom{n-v}{w^*/2}\Big) = (1/n)\log Q_t^2(\omega^*/2).$$

Thus,

$$B_{2w} \gtrsim |C|2^{-n}\binom{n-w^*}{n-2w}\binom{n}{w^*}$$

Finally, let us choose ω^*. As in (36), the optimal choice is $\omega^* = \omega$. If $\omega > \delta_{LP}(R(C))$, by (41) we have

$$H(\nu) - H(\tau) = 1 - R_{LP}(\omega^*) \geq 1 - R(C).$$

If $\delta_{LP}(R(C))/2 \leq \omega \leq \delta_{LP}(R(C))$, to satisfy (48) we must take $\omega^* = \delta_{LP}(R(C))$. ∎

Let $Z(x)$ be a unique real polynomial of degree at most n drawn through points $Z(i)$, $i = 0, 1, \ldots, n$, where

$$Z(i) = \begin{cases} \dfrac{\binom{v}{i/2}\binom{n-v}{i/2}}{\binom{n}{i}} f(i/2), & i = 0, 2, \ldots, 2v, \\ 0 & \text{otherwise.} \end{cases} \tag{42}$$

In the remaining part of this section we prove the asymptotic feasibility of $Z(x)$ and compute the bound (16). Analytically the derivation is similar to the previous section, so we omit some details.

By [26], the coefficients of the Hahn expansion of $f(x)$ are nonnegative. Then Rodemich's theorem implies that the Krawtchouk coefficients of $Z(x)$ are nonnegative. Thus, to prove that $Z(x)$ is admissible we only need to show that

$$\frac{1}{n}\log(Z(\xi n)) \lesssim (1-\xi)H\Big(\frac{1-2\omega}{1-\xi}\Big), \quad 0 < \xi \le 1. \tag{43}$$

We have, up to $o(1)$ terms,

$$\begin{aligned} \frac{1}{n}\log Z(\xi n) = {} & \nu H\Big(\frac{\xi}{2\nu}\Big) + (1-\nu)H\Big(\frac{\xi}{2(1-\nu)}\Big) - H(\xi) + (1-\omega^*)H\Big(\frac{1-2\omega}{1-\omega^*}\Big) \\ & + H(\omega^*) - \nu H\Big(\frac{\omega^*}{2\nu}\Big) - (1-\nu)H\Big(\frac{\omega^*}{2(1-\nu)}\Big) + \frac{2}{n}\big[\log Q_t(n\xi/2) - \log Q_t(n\omega^*/2)\big]. \end{aligned} \tag{44}$$

Again the proof can be broken into two cases, namely, $\xi \in (0, \omega^*]$ and $\xi \in (\omega^*, 1)$. The last case is easy since by our choice of τ and (80), $w^* = a - o(1)$. Therefore, in the interval considered $Z(x)$ is never positive and the right-hand side of (14) is never negative.

To prove (43) for $\xi \in (0, \omega^*]$, note that

$$\frac{1}{n}\log Z(\omega^* n) = (1-\omega^*)H\Big(\frac{1-2\omega}{1-\omega^*}\Big).$$

Since $\xi < x_{\lfloor \tau n \rfloor, \lfloor \nu n \rfloor}$, we can substitute (81) into (44) and compute the derivative

$$\frac{\partial}{\partial \xi}\Big(\log Z(\xi n) - (1-\xi)H\Big(\frac{1-2\omega}{1-\xi}\Big)\Big).$$

Computations with Mathematica show that this function is positive in the interval considered, which confirms the required inequality.

Let us use program (42) to derive a lower bound on B_{2w}.

Theorem 15 *Let C be a code of rate $R(C)$. Then*

$$\frac{1}{n}\log B_{\lfloor 2\omega n \rfloor} \gtrsim R(C) - 1 + H(\omega^*) + (1-\omega^*)H\Big(\frac{1-2\omega}{1-\omega^*}\Big), \tag{45}$$

where

$$\omega^* = \begin{cases} \omega, & \delta_{LP}(R(C)) \le \omega \le 1, \\ \delta_{LP}(R(C)), & \delta_{LP}(R(C))/2 \le \omega \le \delta_{LP}(R(C)). \end{cases}$$

To prove the second case, i.e., that (37) holds for $\xi \in (\omega^*, 1]$, that is, $w^* < x \le n$, we recall that a is the smallest zero of $P_t(x) + P_{t+1}(x)$, therefore $x_{t+1} < a < x_t$; then by (75), $a \searrow x_{t+1}$ as $n \to \infty$. Then we have, for large n and all integer x, $w^* < x \le n$,

$$Z(x) \le 0 \le \binom{n-x}{n-w}.$$

Finally, since $Z(x)$ differs from the corresponding polynomial in [26] only by a constant factor, we rely on [26] for the proof that the coefficients z_j of its Krawtchouk expansion are nonnegative. Thus, for large n, $Z(x)$ satisfies both (14) and (15).

We conclude that the program given by (34) is feasible. The theorem is proved. ∎

4.2 The second form of the LP bound

As in [26], the estimate of Theorem 14 can be improved by deriving a bound of the form similar to (35) in the Johnson scheme and extending it to the Hamming scheme. We shall use a direct analytic method of Rodemich (see [8, p.27]), which gives the same asymptotic result as the argument in [26]. We quote Rodemich's theorem in the form convenient for us in Appendix C.

Let w be an integer between 1 and $n/2$. Let us estimate the binomial moment B_{2w} of a code C of length n. Let v, w^* be integer parameters, $1 \le w^* \le 2w \le 2v \le n$. In order to define a program that yields the desired bound, let us introduce some notation. Let

$$Q_t(x) = \left[\binom{n}{t} - \binom{n}{t-1}\right] \sum_{k=0}^{t} (-1)^k \binom{t}{k}\binom{n+1-t}{k}\binom{x}{k} \Big/ \binom{v}{k}\binom{n-v}{k} \tag{40}$$

be the (dual) Hahn polynomial. Some properties of Hahn polynomials are summarized in Appendix A. Let a be the smallest zero of $Q_t(x) + Q_{t+1}(x)$, i.e., $x_{t+1,v} < a < x_{t,v}$, where $x_{t,v}$ denotes the smallest zero of $Q_t(x)$.

We again begin with an appropriate modification of the polynomial in [26]. Let

$$f(x) = \frac{1}{(a-x)Q_t^2(\omega^*/2)}\big(Q_t(x) + Q_{t+1}(x)\big)^2 \frac{\binom{n-w^*}{n-2w}\binom{n}{w^*}}{\binom{v}{w^*/2}\binom{n-v}{w^*/2}}$$

Let $v = \nu n, w = \omega n, w^* = \omega^* n, t = \tau n$. Choose $\tau = \tau_\nu(\omega^*/2)$, where $\tau_\nu(\cdot)$ is given by (83). Then by (80),

$$\omega^* = 2\frac{\nu(1-\nu) - \tau(1-\tau)}{1 + 2\sqrt{\tau(1-\tau)}} = x_{\lfloor \tau n \rfloor, \lfloor \nu n \rfloor} - o(1)$$

Choose ν to be the root of the equation

$$H(\nu) - H(\tau) = 1 - R_{LP}(\omega^*). \tag{41}$$

where $\omega^* \in [\delta_{LP1}, \omega]$. Differentiate the right-hand side of this inequality on ω^*. The derivative

$$\log \frac{\omega - \omega^*}{\omega^*}$$

is zero for $\omega^* = \omega/2$ and negative for $\omega^* \in (\omega/2, \omega)$. Thus, we put $\omega^* = \omega/2$ if this value is not less than $\delta_{LP1}(R)$ and put $\omega^* = \delta_{LP1}(R)$ otherwise. This proves (35).

Let us prove that polynomial (34) is admissible with respect to (14)–(15). We are only going to prove the asymptotic feasibility, i.e., the fact that for n sufficiently large we have

$$\frac{1}{n}\log Z(\xi n) \lesssim \frac{1}{n}\log \binom{n-\xi n}{n-w} = (1-\xi)H\Big(\frac{1-\omega}{1-\xi}\Big)(1+o(1)), \quad 0<\xi<1. \tag{37}$$

The proof will be broken into two cases, $\xi \in (0, \omega^*]$ and $\xi \in (\omega^*, 1)$. For the first case we have, up to $o(1)$ terms,

$$\frac{1}{n}\log Z(\xi n) = \frac{2}{n}\big[\log P_t(\xi n) - \log P_t(\omega^* n)\big] + (1-\omega^*)H\Big(\frac{1-\omega}{1-\omega^*}\Big). \tag{38}$$

Our choice of τ implies $\omega^* = \frac{1}{2} - \sqrt{\tau(1-\tau)}$, i.e., by (75),

$$x_{\lfloor \tau n \rfloor} = \omega^* n + o(1).$$

Thus, we can use (76) in (38) to obtain

$$\frac{1}{n}\log Z(\xi n) = 2\Big[\int_0^{\xi} \log \frac{1-2\tau+\sqrt{(1-2\tau)^2-4y(1-y)}}{2-2y}dy - \int_0^{\omega^*} \log \frac{1-2\tau+\sqrt{(1-2\tau)^2-4y(1-y)}}{2-2y}dy\Big] + (1-\omega^*)H\Big(\frac{1-\omega}{1-\omega^*}\Big).$$

Let

$$\phi(\tau,\xi) = 2\int_0^{\xi} \log \frac{1-2\tau+\sqrt{(1-2\tau)^2-4y(1-y)}}{2-2y}dy - (1-\xi)H\Big(\frac{1-\omega}{1-\xi}\Big).$$

We have

$$\frac{1}{n}\log Z(\xi n) - (1-\xi)H\Big(\frac{1-\omega}{1-\xi}\Big) = \phi(\tau,\xi) - \phi(\tau,\omega^*).$$

We need to prove that this is negative for $\xi \in (0,1)$. The function $\phi(\tau,\xi)$ is continuous for $\xi \in (0,\omega^*]$; hence in this interval

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

It is not difficult to see that for $\xi \in (0,\omega^*)$

$$\phi'_\xi(\tau,\xi) > 0 \tag{39}$$

(see Appendix B); thus, the difference $\phi(\tau,\xi) - \phi(\tau,\omega^*)$ is negative for all ξ in the interval $\xi \in (0,\omega^*]$ and approaches 0 as ξ approaches its right end.

Thus, for n sufficiently large and $x \in [1, w^*]$, $Z(x)$ satisfies (37).

4.1 The first form of the LP bound

To derive a bound better than (28), we take an appropriate modification of the polynomial in [26]. Let

$$Z(x) = \frac{1}{(a-x)P_t^2(w^*)}(P_t(x)+P_{t+1}(x))^2\binom{n-w^*}{n-w}, \tag{34}$$

where $w^* = \omega n$ is an integer parameter, $1 \le w^* \le w$, $t = \tau n$, $\tau = \frac{1}{2} - \sqrt{\omega^*(1-\omega^*)}$, and a is the smallest zero of $P_t(x)+P_{t+1}(x)$, i.e., $P_t(a) = -P_{t+1}(a)$. The reason for this choice of $Z(x)$ is the following: the polynomial has to be equal to the right-hand side of (14) for at least one x. This point is left a free parameter, chosen later. This polynomial yields the following estimate on B_w.

Theorem 14 *Let C be a code of rate R. Then*

$$\frac{1}{n}\log B_{\lfloor \omega n \rfloor} \gtrsim R - 1 + H(\omega^*) + (1-\omega^*)H\Big(\frac{1-\omega}{1-\omega^*}\Big). \tag{35}$$

$$\omega^* = \begin{cases} \omega/2, & \text{if } 2\delta_{LP1}(R) \le \omega \le 1 \\ \delta_{LP1}(R), & \delta_{LP1}(R) \le \omega \le 2\delta_{LP1}(R). \end{cases}$$

Proof. We first prove the bound (35) and then prove feasibility of the program (34). From (73) we get, up to $o(1)$ terms,

$$Z(0) = \frac{1}{a}\Big(\frac{n-t}{t+1}\Big)^2\binom{n}{t}^2\binom{n-w^*}{n-w}\Big/P_t^2(\omega^*)$$

Further, by [26],

$$z_0 = \frac{2}{t+1}\binom{n}{t}\binom{n-w^*}{n-w}\Big/P_t^2(\omega^*).$$

Let us find the range of parameters where the estimate (16) is dominated by the first summand. Whenever

$$\frac{1}{n}\log\binom{n}{t}|C| = H(\tau) + R > 2H(\tau),$$

i.e.,

$$R > H(\tau),$$

we have $Z(0) = o(z_0|C|)$. The restriction $R > H(\tau)$ by our choice of τ is equivalent to $R > R_{LP1}(\omega^*)$ which is always the case whenever $\omega^* > \delta_{LP1}(R)$. Therefore, for n sufficiently large we have

$$\frac{1}{n}\log B_{\lfloor \omega n \rfloor} \gtrsim H(\tau) - \frac{2}{n}\log P_{\tau n}(\omega^* n) + R + (1-\omega^*)H\Big(\frac{1-\omega}{1-\omega^*}\Big),$$

Now use (77) to rewrite this as

$$\frac{1}{n}\log B_{\lfloor \omega n \rfloor} \gtrsim R - 1 + H(\omega^*) + (1-\omega^*)H\Big(\frac{1-\omega}{1-\omega^*}\Big), \tag{36}$$

Proposition 12 *Let C be a code of length n, let $1 \le w \le n$, and $u = \lfloor (w-1)/2 \rfloor$. Then*

$$B_w \ge \binom{n}{u} \Big[\binom{n}{u} 2^{-n} |C| - 1 \Big] \Big/ \binom{2u}{u}.$$

Note that this bound is nontrivial when, roughly speaking, $\log |C| - n + \log \binom{n}{w/2} \ge 0$. This gives a considerable improvement over the Singleton bound, which is only nontrivial when $\log |C| - n + w \ge 0$. For instance, for $n = 31$ the improvement holds for $11 \le w \le 16$.

4 Asymptotic bounds

In this section we derive a few asymptotic lower bounds on binomial moments B_w of a code C of length $n \to \infty$ and rate $R = (1/n) \log |C|$. Let $w = \omega n$, $0 < \omega < 1$. Let $H(x) = -x \log x - (1-x) \log (1-x)$ be the binary entropy. We write $f(n) \gtrsim g(n)$ if $f(n) \ge g(n)(1+o(1))$, where $o(1)$ is a positive infinitesimal.

The asymptotic Singleton bound, immediate from (23), has the following form.

Theorem 13 *Let C be a code of rate R. Then*

$$\frac{1}{n} \log B_{\lfloor \omega n \rfloor} \gtrsim R - 1 + \omega + H(\omega), \quad \omega > 1 - R. \tag{28}$$

Below we derive two forms of the linear programming (LP) bound that are analogous to the two forms of the bound in [26]. We shall use a functional dependence between two real variables $R \in [0,1]$ and $\delta \in [0, 1/2]$ given by the two following parametric equations:

$$R = 1 - H(\alpha) + H(\tau) \tag{29}$$

$$\delta = \min_{0 \le \alpha \le 1/2} 2 \frac{\alpha(1-\alpha) - \tau(1-\tau)}{1 + 2\sqrt{\tau(1-\tau)}}, \tag{30}$$

introduced in [26], Eqns (2.10) and (4.14b). For a given R, $\delta = \delta_{LP}(R)$ is the maximal possible relative distance of a code of rate R. It can be checked that for $0 \le R \le 0.3052\ldots$ the minimum in (30) is attained for $\alpha = 1/2$. Then the function $\delta(R)$ takes on the following simple form:

$$\delta_{LP1}(R) = \frac{1}{2} - \sqrt{H^{-1}(R)(1 - H^{-1}(R))}. \tag{31}$$

The inverse functions

$$R_{LP}(\delta) = \min_{\frac{1}{2}\left(1-\sqrt{1-2\delta}\right) \le \alpha \le \frac{1}{2}} \big(1 - H(\alpha) + H(\tau_\alpha(\delta/2))\big), \tag{32}$$

$$R_{LP1}(\delta) = H\Big(\frac{1}{2} - \sqrt{\delta(1-\delta)}\Big) \tag{33}$$

where $\tau_\alpha(\cdot)$ is defined in (83), give the maximal possible rate of codes with relative distance δ [26]. Again it can be checked that $R_{LP}(\delta) \le R_{LP1}(\delta)$ with equality for $0.273\ldots \le \delta \le 1/2$.

Theorem 11 *Let C be a code and let $w \in [1,n]$. Then*

$$B_w \geq \binom{n}{w}(2^{w-n}|C|-1) + n\binom{m}{w-1}\Big(\frac{2^{w-1}}{w} - 2^{w-n}|C|\Big),\ n = 2m+1 \tag{25}$$

$$B_w \geq \binom{n}{w}(2^{w-n}|C|-1) + \frac{1}{n-2}\binom{m}{w}\Big(2^w(n+w-3) - 2^{w-n+1}(wn-2)|C|\Big),\ n = 2m. \tag{26}$$

PROOF. Straightforward calculation. ∎

Example 5. Let C be the Hamming code. We have $A_1, A_2 = 0$ and $A_i \neq 0$ for $3 \leq i \leq n-2, n$. On the other hand, $Z(j) = \binom{n-j}{n-w}$ for $3 \leq j \leq n$. Further, $A_i' \neq 0$ only if $i = (n+1)/2, n$. One can check that $z_j = 0$ if and only if $j = (1/2)(n \pm 1), n$. Thus both conditions in part (b) of Theorem 3 are satisfied. We conclude that the Hamming code is extremal with respect to the bound (25). Binomial moments of its weight distribution are given by the right-hand side of (25). Therefore, its weight spectrum can be calculated using Corollary 4.

Example 6. Let C be a code with $n = 12, |C| = 256$. We get the following estimates for B_w.

w :	3	4	5	6	7	8	9	10	11	12
optimal solution of the LP problem:	14	174	922	2812	5544	7425	6820	4158	1524	255
Hamming bound (26):	14	174	922	2812	5544	7425	6820	4158	1524	255
Singleton bound:	0	0	792	2772	5544	7425	6820	4158	1524	255

We see that bounds of Theorem 11 can be very good for codes of large size. In Section 5 we use this example in comparing bounds on the probability of undetected error.

More generally, let

$$z_j = P_u^2(j)\Big(2^n\binom{2u}{u}\Big)^{-1},$$

where $u = \lfloor (w-1)/2 \rfloor$. Using in succession (74),(67), and (66), we get, for integer x,

$$\begin{aligned} Z(x) &= \Big(2^n\binom{2u}{u}\Big)^{-1}\sum_{j=0}^{n}\binom{n-j}{u-j/2}\binom{j}{j/2}\sum_{t=0}^{n}P_j(t)P_t(x) \\ &= \binom{2u}{u}^{-1}\binom{n-x}{u-x/2}\binom{x}{x/2}, \end{aligned} \tag{27}$$

where the final expression is 0 if x is odd. To prove feasibility of this program, we need only to prove (14), or the inequality

$$\binom{n-j}{u-j/2}\binom{j}{j/2} \leq \binom{n-j}{w-j}\binom{2u}{u}, \quad 2 \leq j \leq w \leq n.$$

This is obvious for $1 \leq w \leq n/2$ and requires cumbersome calculations for greater w. This program gives the following

Proposition 10 *MDS codes are extremal (have the smallest possible binomial moments B_w for $w, 1 \le w \le n$).*

Example 4 Let $n = 30$ and $|C| = 16$. We found by computer the optimal solutions of the linear programming problem for all $1 \le w \le n$. We give a table listing these solutions and estimates given by the Singleton and the Plotkin bounds.

w :	15	16	17	18	19	20	21
optimal solution of the LP problem:	0	15	210	1365	5460	15015	30030
Plotkin bound:	0	15	210	1365	5460	15015	30030
Singleton bound:	0	0	0	0	0	0	0

22	23	24	25	26	27	28	29	30
45045	51480	45045	30030	15015	5460	1365	210	15
45045	51480	45045	30030	15015	5460	1365	210	15
0	0	0	0	0	5060	1305	210	15

One can see that for these parameters the Plotkin bound gives an optimal solution of the LP problem (11)-(12) and provides a considerable improvement over the Singleton bound.

3.3 Hamming-type bounds

Let $C \subset F$ be a code and let $w \in [1, n]$. Let $n = 2m + 1$. Consider the program

$$z_j = 2^{w-n}\Big[\binom{n-j}{w} - \frac{n-j}{w}\binom{m}{w-1}\frac{w(n-2j-1)+2j}{n-1}\Big], \quad 0 \le j \le n. \tag{24}$$

To compute $Z(x)$ we use (68) and (69)-(72). The result is of the form

$$Z(x) = \binom{n-x}{n-w} - \frac{2^{w-1}}{w}\binom{m}{w-1}\Big[\frac{2(w-1)}{(n-1)}\binom{n-x}{n-2} - (w-2)\binom{n-x}{n-1}\Big].$$

Let us check feasibility. Restriction (14) is obviously satisfied for $j \ge 3$, and the cases $j = 1$ and $j = 2$ follow by direct substitution. To prove (15), rewrite the expression for z_j in the form

$$z_j = 2^{w-n}\frac{n-j}{w}\Big[\binom{n-j-1}{w-1} - \binom{m}{w}\frac{w(n-1)-2j(w-1)}{n-1}\Big].$$

The first term in the brackets is a $\cup$-convex function of j and the second term is a linear decreasing function of j. One can check that they are equal for $j = m, m+1$; thus, for all other j the first term is greater.

For n even, $n = 2m$, the polynomial should be taken in the form

$$Z(x) = \binom{n-x}{n-w} - \frac{2^w}{n}\binom{m}{w}\Big[\frac{2(w-1)}{(n-2)}\binom{n-x}{n-2} - (w-2)\binom{n-x}{n-1}\Big].$$

(4) $A(x,y) = A_m x^m y^m + y^n$. Then the first condition in part (b) of Theorem 3 yields 2 linear equations on (z_0, z_1, z_2). The third equation was obtained by assuming $Z(m+1) = 0$.

Example 3 (Hadamard codes). Let C be a code of length $n = 2m$ and size $M = 4m$. Suppose $|C|$ is extremal with respect to the above bound, i.e.,

$$B_w = 2(n-1)\binom{n/2}{n-w}, \quad 1 \le w \le n-1.$$

Then the smallest w with $B_w > 0$ is $m = n/2$, which is also the distance of C. Then by (3) we get $A_m = B_m = 2(n-2) = |C| - 2$. For every $m+1 \le w \le n-1$ we then get $B_w = \binom{n-m}{n-w} A_m = 2(n-1)\binom{m}{n-w}$, i.e., $A_{m+1} = \cdots = A_{n-1} = 0$. Thus, $A_n = 1$. This yields the distance distribution of the Hadamard codes [28]. Thus, the Hadamard codes are extremal with respect to Definition A.

3.2 The Singleton bound

Let

$$Z(x) = \binom{n-x}{n-w}. \tag{22}$$

To prove the feasibility of this choice, we only have to check (15). By (74) and (68) we have

$$z_j = 2^{-n} \sum_{u=0}^{n} \binom{n-u}{n-w} P_u(j) = \begin{cases} 2^{w-n}\binom{n-j}{w}, & 0 \le j \le n-w, \\ 0, & n-w \le j \le n. \end{cases}$$

Thus we get the following.

Theorem 9 *Let C be a code of length n. Then*

$$B_w \ge \max\{0, (2^{w-n}|C| - 1)\binom{n}{w}\}, \quad 1 \le w \le n. \tag{23}$$

Other combinatorial and linear-algebraic proofs of this are given in [1], [3]. They show that the same result holds for any q-ary code C, $q \ge 2$, namely,

$$B_w \ge \max\{0, (q^{w-n}|C| - 1)\binom{n}{w}\}, \quad 1 \le w \le n.$$

Suppose C is extremal with respect to this bound. Let $k = \log_q |C|$. Then by Corollary 4,

$$\begin{aligned} A_i &= \sum_{j=n-k+1}^{i} (-1)^{j-i} \binom{n-j}{n-i} \binom{n}{j} (q^{j-n+k} - 1) \\ &= \binom{n}{i} \sum_{j=n-k+1}^{i} (-1)^{j-i} \binom{i}{j} (q^{j-n+k} - 1). \end{aligned}$$

We see that the distance of C equals $n-k+1$ (alternatively, $z_j \ne 0$ for $1 \le j \le k$, i.e., by Theorem 3(b) the dual distance is $k+1$), that is, C is an MDS code. Therefore, the above expression gives the distance spectrum of MDS codes, linear or nonlinear (cf. [6, Thm. 15]). This also proves the following proposition.

3.1.2 Quadratic polynomials

Theorem 8 *Let C be a code of length n. Then for n even,*

$$B_w \geq \frac{1}{n-2}\binom{n/2}{n-w}\Big[|C|(2n-w-3)-2(n^2-nw-2)\Big], \quad n/2 \leq w \leq n-1.$$

For n odd,

$$B_w \geq \frac{n}{2w-n+1}\binom{(n-1)/2}{n-w}[|C|-2(n-w)], \quad (n+1)/2 \leq w \leq n-1.$$

PROOF. We begin with n even. Let $n=2m$. Take $Z(x)=z_0P_0(x)+z_1P_1(x)+z_2P_2(x)$, where

$$z_0=\frac{2n-w-3}{n-2}\binom{m}{n-w}, \quad z_1=\frac{n^2-wn-2}{n(n-2)}\binom{m}{n-w}, \quad z_2=2\frac{n-w-1}{n(n-2)}\binom{m}{n-w}.$$

To prove feasibility of this program, we need to prove (14). The polynomial $Z(x)$ is of the form

$$Z(x)=\frac{2}{n(n-2)}\binom{m}{n-w}[(3nx-2x^2-n^2)w+(n^3-2n-2n^2x+2nx+2x+2nx^2+2x^2)]. \tag{21}$$

Observe that $Z(x)=\binom{n-x}{n-w}$ for $x=m,m+1$. Suppose that $x\leq m-1$. The term in brackets in (21) is a linear decreasing function of w for x fixed. On the other hand, the quantity

$$2\binom{n-x}{n-w}\Big/\binom{m}{n-w}n(n-2)$$

(the right-hand side of (14) divided by the factor in (21) is a $\cup$-convex function of w). It can be seen that $Z(x)=\binom{n-x}{n-w}$ for $w=n-2$, $w=n-1$. Thus, for all $w\leq n-3$ for any fixed $x\leq m-2$ $Z(x)$ is strictly less than $\binom{n-x}{n-w}$.

The case $x\geq m+2$ is treated similarly.

Further,

$$Z(0)=\frac{2(n^2-wn-2)}{n-2}\binom{m}{n-w},$$

Substitution of $Z(0)$ and z_0 in (16) proves our claim for n even.

For n odd, take

$$z_0=\frac{n}{2w-n+1}\binom{m}{n-w},\ z_1=\frac{n-w}{2w-n+1}\binom{m}{n-w},\ z_2=2\frac{n-w-1}{(n-1)(2w-n+1)}\binom{m}{n-w},$$

where $n=2m+1$. The remaining part of the proof is similar to the first case and will be omitted. ∎

A few words about how polynomials in this theorem were found may be in order. The optimal quadratic polynomial in Delsarte's problem gives the bound $|C|\leq\frac{4d}{2d-(n-1)}$ on the size of a code C of distance d [20],[22]. Codes that meet this bound have the distance enumerator

we get $z_0 = \binom{n-s}{n-w} - z_1(n-2s)$ and substitute this in $Z(x)$. For the function $\beta(z_1, s) := z_0|C| - Z(0)$ we then get

$$\beta(z_1, s) = (|C|-1)\Big[\binom{n-s}{n-w} - 2sz_1\Big] - |C|z_1 n.$$

We want this to be as large as possible, hence z_1 has to be small. By (14) the smallest possible value of z_1 is determined from the condition

$$Z(s+1) = \binom{n-s-1}{n-w}. \tag{18}$$

It is not difficult to see that if equalities (17) and (18) hold, then (14) holds for every $i \in [1, n]$, i.e., the program $\{z_0, z_1, 0, \ldots, 0\}$ is feasible. Since

$$Z(s+1) = \binom{n-s}{n-w} - z_1(n-2s) - z_1(n-2s-2) = \binom{n-s}{n-w} - 2z_1,$$

from (18) we get

$$z_1 = \frac{1}{2}\binom{n-s-1}{n-w-1}. \tag{19}$$

Upon substitution of this value in $\beta(z_1, s)$ this function depends only on s. Let us choose s that maximizes it. Observe that

$$\beta(z_1, s+1)/\beta(z_1, s) \geq 1$$

for all s, $1 \leq s \leq n|C|/2(|C|-1)$. Hence the maximum of $\beta(z_1, s)$ is attained for $s = \min\{w, n|C|/2(|C|-1)\}$. Let

$$s_0 = n\frac{|C|}{2(|C|-1)} = \frac{n}{2} + \frac{1}{2}\frac{n}{|C|-1}$$

and suppose that this is at most w. Then the proof is completed by substituting s_0 in the expressions for z_0 and z_1. ∎

Corollary 7 *Let $s_0 \leq w$. Then*

$$B_w \geq (|C|-1)\binom{n-s_0}{n-w}, \quad 1 \leq w \leq n. \tag{20}$$

PROOF. For $w = n$ the claim is obvious from (3). Otherwise, from (17), (19), and the previous theorem we have

$$\begin{aligned}
B_w &\geq \frac{1}{2}\binom{n-s_0-1}{n-w-1}\left(\left[2\frac{n-s_0}{n-w} - n + 2s_0\right](|C|-1) - n\right) \\
&= \binom{n-s_0-1}{n-w-1}\left(\frac{n-s_0}{n-w}\right)(|C|-1) = \binom{n-s_0-1}{n-w-1}\frac{n}{n-w}\left(\frac{|C|}{2}-1\right) \\
&= \binom{n-s_0}{n-w}\frac{n}{n-s_0}\left(\frac{|C|}{2}-1\right) \\
&= (|C|-1)\binom{n-s_0}{n-w}.
\end{aligned}$$

∎

Example 2. The $[16, 8, 6]$ Nordstrom-Robinson code is extremal. This again can be checked by using its distance distribution [28] and solving the corresponding linear programming problem. The next code in the sequence of Kerdock codes, with the parameters $[64, 28, 12]$, is not extremal.

Some further general examples will be given below.

3 Lower bounds

This section is devoted to lower bounds on B_w. First we find optimal polynomials of low degrees for Problem (14)-(16) and give examples of extremal codes meeting these bounds. Then we pass to polynomials of higher degree and derive further lower bounds that correspond to some other extremal codes.

Before deriving specific lower bounds on B_w, let us give a generic lower bound which proves useful in applications (see[3]).

Lemma 5 [3] *Let $1 \le s < w \le n$. Then*

$$B_w \ge B_s \binom{n-s}{n-w} \Big/ \binom{w-1}{s-1}.$$

In particular, for given length n and code size M we can use known upper bounds on the distance of any (n, M) code together with (3) to derive lower bounds on the binomial moments.

3.1 Low-degree polynomials

In this section we derive a few lower bounds on B_w useful in the analysis of specific codes and in applications.

3.1.1 The Plotkin bound

Let us choose an optimal linear polynomial

$$Z(x) = z_0 P_0(x) + z_1 P_1(x) = z_0 + z_1(n - 2x),$$

given n and the size of the code $|C|$.

Theorem 6 *Let $s_0 := \frac{n|C|}{2(|C|-1)}$ and suppose that $s_0 \le w$. The optimal linear polynomial for the problem (13) has the form*

$$Z(x) = \binom{n-s_0}{n-w} - (x + s_0)\binom{n-s_0-1}{n-w-1}.$$

PROOF. Let $s \in [1, w+1]$. We shall choose the line $Z(x)$ in such a way that it be equal to the function $\binom{n-x}{n-w}$ in two points, s and $s+1$. From the equation

$$z_0 + z_1(n - 2s) = \binom{n-s}{n-w} \tag{17}$$

PROOF. Part (a) is the duality theorem of linear programming. Part (b) follows by the complementary slackness theorem [30]. ∎

This corollary is helpful in finding optimal polynomials and deriving bounds in Section 3 since it suggests values of i at which $Z(i)$ should be equal to the right-hand side of (14) and values of j at which z_j should be (non)zero.

Definition A. We call a code *extremal* if the binomial moments of its distance distribution form an optimal program for the problem (11)-(12) for all $w, 1 \le w \le n$.

If C is an extremal code, there is an optimal assignment of the dual variables. Since this assignment depends on w, we denote it by $\{z_0^{(w)}, z_1^{(w)}, \ldots, z_n^{(w)}\}$. The corresponding polynomial is denoted by $Z_w(x)$.

Corollary 4 *The distance spectrum $\{A_0, A_1, \ldots, A_n\}$ of an extremal code C with distance d satisfies*

$$\begin{aligned} A_0 &= 1, A_1 = \cdots = A_{d-1} = 0 \\ A_i &= \sum_{w=d}^{i} (-1)^{w-i} \binom{n-w}{n-i} [z_0^{(w)} |C| - Z_w(0)], \quad i \ge d. \end{aligned}$$

PROOF. Follows from Theorem 3(a) and (6). ∎

This corollary is analogous to a result of Delsarte; see [6] or Theorem 17.22 in [28]. Note that Delsarte's theorem applied on codes that meet the classical linear programming bound yields only the locations of zeros in the distance spectrum. This information is often sufficient to solve the MacWilliams equations and compute the distance enumerator of the code as is done in Theorem 6.2 of [28]. Further, Levenshtein [20] derived optimal polynomials of any fixed degree for the Delsarte problem. He observed [22] that for codes that meet the bound from [20], the MacWilliams equations can be solved, and thus, their weight spectrum in principle is known. On the contrary, Corollary 4 gives an explicit expression for the weight spectrum of extremal codes via the coefficients of the linear program.

Let us give some examples of extremal codes.

Example 1. The Golay code $[23, 12, 7]$ is extremal according to Definition A. This is checked by computing the binomial moments of its weight spectrum [28, Sect. 20.2] and explicitly solving (by computer) the corresponding linear programming problem. Both the optimal objective function and the binomial moments have the form

w	7	8	9	10	11	12	...	22	23
B_w	253	4554	37950	194810	691978	1812538	...	47081	4095.

Its extension, the $[24, 12, 8]$ code, is also extremal. Though throughout this paper we deal mostly with binary codes, our approach works verbatim for any alphabet. In particular, we checked that the $[11, 6, 5]$ ternary Golay code is also extremal as is its extension, the $[12, 6, 6]$ ternary code.

or

$$z_0|C| - \sum_{i=0}^{n} z_i \binom{n}{i} \to \max \tag{13}$$
$$z_j \geq 0, \quad 1 \leq j \leq n$$
$$z_0 \lessgtr 0$$
$$\sum_{k=0}^{n} z_k P_k(j) \leq \binom{n-j}{n-w}, \quad 1 \leq j \leq n.$$

Any feasible solution of the dual problem gives a lower estimate of the optimum in the primal problem. Thus we arrive at the following theorem, which is central to our approach.

Theorem 2 *Let $Z(x) = \sum_{k=0}^{n} z_k P_k(x)$ be a polynomial such that*

$$Z(j) \leq \binom{n-j}{n-w}, \quad 1 \leq j \leq n \tag{14}$$
$$z_j \geq 0, \quad 1 \leq j \leq n. \tag{15}$$

Then

$$B_w \geq z_0|C| - Z(0). \tag{16}$$

PROOF. Follows from the previous discussion and (73). ∎

Note the difference between this theorem and the conditions on the choice of the polynomial in the standard (Delsarte's) linear programming bound [6]: there one requires that $Z(j) \leq 0$ for every integer $j = w, \ldots, n$, where w is a given integer. Inequalities (14) are much more restrictive since one has to guarantee not only this, but also to ensure that the values $Z(j)$ are less than given positive numbers for $j \in [1, w]$.

Below we shall use the following properties of the optimal solutions of the primal and dual problems, see e.g., Sect. 7.4 and 7.9 in [30].

Theorem 3 *Let $\{A\} = \{A_1, \ldots, A_n\}$ and $\{z\} = \{z_0, \ldots, z_n\}$ be solutions to (11)-(12) and (13), respectively. Let $\{A'_0, A'_1, \ldots, A'_n\}$ be the MacWilliams transform of A given by $A'_j = (1/|C|) \sum_{i=0}^{n} P_j(i) A_i, 0 \leq j \leq n$.*
(a) *Solutions $\{A\}$ and $\{z\}$ are optimal if and only if*

$$\sum_{i=1}^{w} A_i \binom{n-i}{n-w} = z_0|C| - \sum_{i=0}^{n} \binom{n}{i} z_i, \quad 1 \leq w \leq n$$

(b) *Solutions $\{A\}$ and $\{z\}$ are optimal if and only if the following two conditions hold:*

$$(A_i \neq 0) \Rightarrow \sum_{k=0}^{n} z_k P_k(i) = \binom{n-i}{n-w}.$$

and

$$(A'_i \neq 0) \Rightarrow (z_i = 0).$$

[17] and the Singleton bound yields a recent bound of Abdel-Ghaffar [1]. As observed in [3], the asymptotic bound corresponding to Abdel-Ghaffar's bound improved the best then known upper bounds by Leontiev [18] and Levenshtein [19], [21]. It also extends the range of code rates R in which the exponent of undetected error is tight from the previously known $[\log_2(2-2p), 1]$ to $[1-2p, 1]$. We show that the bounds of Section 4 further extend this region to $[R_{LP}(p), 1]$ and improve the known upper bounds for all code rates $R \in (0, R_{LP}(p)]$. Here $R_{LP}(p)$ is the maximal possible rate of a code with distance pn, see (32).

We developed the linear programming approach to bounding the binomial moments in November 1997. In January 1998 we received a preprint by Litsyn [24], which uses the linear programming method to derive asymptotic existence-type bounds on individual components of the distance spectrum of codes. The approach of Litsyn differs from ours, both analytically and combinatorially. He used his bounds to derive asymptotic bounds on error exponents of codes on the binary symmetric channel and, in particular, proved Theorems 20 and 21. Further discussion of our results and the results of [24] is carried out in Section 6.

2 The linear program

In this section we develop a polynomial approach to bounding from below the binomial moments B_w of the distance distribution. We apply our general theorem to derive a number of lower estimates on B_w for a code C with given length n and size $|C|$.

Let $w \in [1, \ldots, n]$ be a fixed parameter. We need to minimize B_w, i.e. the sum

$$\sum_{j=1}^{w} \binom{n-j}{n-w} A_j \tag{11}$$

subject to the restrictions

$$\begin{aligned} A_j &\geq 0, \quad 1 \leq j \leq n \\ \sum_{j=1}^{n} A_j &= |C| - 1v \\ \sum_{j=1}^{n} A_j P_k(j) &\geq -\binom{n}{k}, \quad 1 \leq k \leq n \end{aligned} \tag{12}$$

see (9), (73). The dual program has $n+1$ variables $(z_0, z_1, \ldots, z_n)$ of which z_0 can take on any value and all the other variables are nonnegative. The dual problem has the form (see, e.g., [30])

$$\begin{aligned} & z_0(|C|-1) - \sum_{i=1}^{n} z_i \binom{n}{i} \to \max \\ & z_j \geq 0, \quad 1 \leq j \leq n \\ & z_0 \gtreqless 0 \\ & z_0 + \sum_{k=1}^{n} z_k P_k(j) \leq \binom{n-j}{n-w}, \quad 1 \leq j \leq n. \end{aligned}$$

where in the last equality we have put $i = n - j$. ∎

Specifying (1) for linear codes, we get $B_w = \sum_{|E|=w}(2^{\dim \mathcal{C}_0(E)} - 1)$, familiar from [34],[13]. Thus, binomial moments of the weight spectrum of C describe the cumulative cardinality of subcodes of C with support of size at most w, see [27],[13],[2],[3]. In this form they were implicitly used by MacWilliams [27] in the proof of the celebrated MacWilliams identities. Namely, using (5), one has

$$B_u = 2^{u-k} B^{\perp}_{n-u} + \binom{n}{u}(2^{n-k} - 1), \tag{8}$$

see [27],[28, Exercise 5.6]. Binomial moments also arise naturally in the study of weight distributions of algebraic-geometric codes [13],[14] and in relating weight distributions and support weight distributions of linear codes to the classical polynomials on linear matroids [10],[2]. A closely related circle of problems was studied in [31],[11]. q-analogs of the binomial moments were studied by Delsarte in his work on association schemes of bilinear forms [7]. Finally, binomial moments arise in the study of the probability of undetected error, see [34],[1],[3].

The potential of the binomial moments that stems from Lemma 1, though made clear by [13], [32], remained largely unclaimed (however, see [14]).

The distance spectrum coefficients (2) satisfy the Delsarte inequalities [6]

$$\sum_{i=0}^{n} P_k(i) A_i \geq 0, \quad 0 \leq k \leq n, \tag{9}$$

where the numbers $P_k(i)$ are the values of Krawtchouk polynomials

$$P_k(x) = \sum_{\alpha=0}^{n} (-1)^{\alpha} \binom{x}{\alpha} \binom{n-x}{k-\alpha}. \tag{10}$$

These linear conditions were used in [6] to prove an upper bound (the "linear programming bound") on the size of a code $|C| = \sum_{i=0}^{n} A_i$ with given length and distance. In this paper we introduce a linear programing problem for bounding *from below* the numbers B_w is an arbitrary code C (Section 2). Section 3 is devoted to lower bounds derived with the use of this problem. We begin with the study of bounds that follow by setting all but very few of the inequalities (9) to equality. This accounts for Plotkin-type and some other bounds. Then we prove the Singleton and Hamming-type bounds. These bounds show that some known codes have minimal possible binomial moments of the distance distribution for given length and size. This includes MDS codes, 1-error-correcting perfect codes, both Golay codes, the Nordstrom-Robinson code, Hadamard codes. Thus, the distance distribution of each of these codes corresponds to a vertex vin the optimal polyhedron of our linear programming problem.

In Section 4 we study the asymptotic versions of these bounds, and introduce linear programs which correspond to the McEliece-Rodemich-Rumsey-Welch bounds [26].

Section 5 is devoted to the application of these bounds to deriving lower bounds on the probability P_{ud} of undetected error of unrestricted codes used over a binary symmetric channel with crossover probability p. We show that our Plotkin bound yields the Korzhik bound on P_{ud}

Lemma 1 *Let*

$$A(x,y) = \sum_{i=1}^{n} A_i x^{n-i} y^i \tag{4}$$

be the distance enumerator of C. *Then*

$$B_w = \sum_{j=1}^{w} \binom{n-j}{n-w} A_j, \quad 1 \le w \le n. \tag{5}$$

$$A_i = \sum_{w=1}^{i} (-1)^{w-i} \binom{n-w}{n-i} B_w, \quad 1 \le i \le n, \tag{6}$$

$$A(x,y) = \sum_{i=1}^{n} B_i (x-y)^{n-i} y^i. \tag{7}$$

Remark. Technically it is more convenient to us to sum in (4) from $i = 1$ rather than from 0 in the standard definition.

PROOF. Relation (5) follows by observing that (1) and (5) are two ways of counting the (normalized) size of one and the same set,

$$\Big\{ (E,(c,c')) \,|\, E \subset \{1,2,\ldots,n\}, |E| = w;\, (c,c') \in \mathcal{C}(E)^2, c \ne c' \Big\}.$$

Indeed the size of this set is given by the sum

$$\sum_{j=1}^{w} \sum_{c \in C} \sum_{|E|=w} \sum_{\substack{c' \in C \\ \mathsf{supp}\,(c,c') \subset E \\ \mathsf{dist}\,(c,c')=j}} 1.$$

This sum is equal to $|C|$ times the right-hand side of (5). Interchanging the first and the third sums, we observe that it is also equal to $|C|$ times the right-hand side of (1).

Let us prove (6). Multiply (5) by $(-1)^{s-w}\binom{n-w}{n-s}$ and sum both parts on w:

$$\begin{aligned} \sum_{w=1}^{s} (-1)^{s-w} \binom{n-w}{n-s} B_w &= \sum_{w=1}^{s} (-1)^{s-w} \binom{n-w}{n-s} \sum_{i=1}^{w} \binom{n-i}{n-w} A_i \\ &= \sum_{i=1}^{s} A_i \sum_{w=i}^{s} (-1)^{s-w} \binom{n-w}{n-s} \binom{n-i}{n-w} = A_s, \end{aligned}$$

where the last equality follows by a well-known convolution formula for binomial numbers.

Finally, let us prove (7).

$$\begin{aligned} \sum_{w=1}^{n} B_w (x-y)^{n-w} y^w &= \sum_{w=1}^{n} B_w y^w \sum_{j=0}^{n-w} (-1)^{n-w-j} \binom{n-w}{j} x^j y^{n-w-j} \\ = \sum_{j=0}^{n} y^{n-j} x^j \sum_{w=1}^{n-j} (-1)^{n-w-j} \binom{n-w}{j} B_w &= \sum_{i=0}^{n} x^{n-i} y^i \sum_{w=1}^{i} (-1)^{i-w} \binom{n-w}{n-i} B_w, \end{aligned}$$

1 Introduction

Let $F = GF(2)^n$ be the n-dimensional Hamming space. Let $\mathcal{A} \subset F$ be a set of vectors. Define the *support* of $\mathcal{A}$ as follows:

$$\mathsf{supp}\,\mathcal{A} = \{e \in \{1, 2, \ldots, n\} : \exists_{c,c' \in \mathcal{A}}(c_e \neq c'_e)\}.$$

Note that the support of a set $\mathcal{A} \subset F$ is translationally invariant, that is $\mathsf{supp}\,\mathcal{A} = \mathsf{supp}\,(x + \mathcal{A})$.

Let $C \subset F$ be an arbitrary subset, which we call a *code*. Let $E \subset \{1, 2, \ldots, n\}$. Let $\sim_E$ be the equivalence relation given by

$$(c \sim_E c') \Leftrightarrow \mathsf{supp}\,(c, c') \subseteq E.$$

Let $\mathcal{D}_E(C)$ be a partition of C into equivalence classes (subcodes) according to $\sim_E$.

Definition 1 A subcode $\mathcal{C}(E) \in \mathcal{D}_E(C)$ is called a *restriction* of C with respect to E.

Thus, the $\mathcal{C}(E)$ are maximal subcodes of C with support in E. If $|E| = w$, $1 \leq w \leq n$, then we refer to these subcodes as to *w-restrictions* of C. In the linear case, for any given E the structure of w-restrictions of C is simple. Namely, there is the linear subcode $\mathcal{C}_0(E)$ with $\mathsf{supp}\,(\mathcal{C}_0(E)) \subseteq E$ and its $2^{\dim C - \dim \mathcal{C}_0(E)} - 1$ proper cosets in $C/\mathcal{C}_0(E)$.

We are ready to define our main object of study.

Definition 2 Let $E \subset \{1, 2, \ldots, n\}$, $|E| = w$, $1 \leq w \leq n$. Let B_w be the (normalized) number of ordered pairs (c, c') of codewords of C in all w-restrictions of C, i.e.,

$$B_w = \frac{1}{|C|} \sum_E \sum_{\mathcal{C}(E) \in \mathcal{D}_E(C)} |\mathcal{C}(E)|(|\mathcal{C}(E)| - 1), \tag{1}$$

where the first sum is extended to all subsets $E \in \{1, 2, \ldots, n\}$ of size w. By definition, let $B_0 = 0$.

Let

$$A_i = \frac{1}{|C|} \sum_{c \in C} |\{c' \in C \ : \ \mathsf{dist}\,(c, c') = i\}|. \tag{2}$$

The set $\{A_0, A_1, \ldots, A_n\}$ is called the distance distribution (spectrum) of C. If C is linear, then this set is called the weight spectrum of the code. Note that if d is the distance of C, then

$$\begin{aligned} B_1 &= \ldots = B_{d-1} = 0, \\ B_d &= A_d, \\ B_n &= |C| - 1. \end{aligned} \tag{3}$$

The main goal of our paper is to study lower bounds on B_w.

We call the numbers B_w *binomial moments* of the distance distribution of C. The following result accounts for the importance of the binomial moments (and explains their name). The linear case is implicit in [27] and explicit in [13]. The general case appears in part in [1] and in the complete form in [3].

Binomial Moments of the Distance Distribution: Bounds and Applications

A.Ashikhmin * A. Barg †

Abstract

We study a combinatorial invariant of codes vwhich counts the number of ordered pairs of codewords in all subcodes of restricted support in a code. This invariant can be expressed as a linear form of the components of the distance distribution of the code with binomial numbers as coefficients. For this reason we call it a binomial moment of the distance distribution. Binomial moments appear in the proof of the MacWilliams identities and in many other problems of combinatorial coding theory. We introduce a linear programming problem for bounding these linear forms from below. It turns out that some known codes (1-error-correcting perfect codes, Golay codes, Nordstrom-Robinson code, etc) yield optimal solutions of this problem, i.e., have minimal possible binomial moments of the distance distribution. We derive several general feasible solutions of this problem, which give lower bounds on the binomial moments of codes with given parameters, and derive the corresponding asymptotic bounds.

Applications of these bounds include new lower bounds on the probability of undetected error for binary codes used over the binary symmetric channel with crossover probability p and optimality of many codes for error detection. Asymptotic analysis of the bounds enables us to extend the range of code rates in which the upper bound on the undetected error exponent is tight.

Keywords: Distance distribution, binomial moments, linear programming, extremal codes, undetected error, Rodemich's theorem.

*Los Alamos National Laboratory, Group CIC-3, Mail Stop P990, Los Alamos, NM 87545. E-mail alexei@c3serve.c3.lanl.gov

†Bell Laboratories, Lucent Technologies, 600 Mountain Avenue 2C-375, Murray Hill, NJ 07974. E-mail abarg@research.bell-labs.com.