DIMACS Series in Discrete Mathematics
and Theoretical Computer Science

Estimates of the distance distribution of nonbinary codes, with applications

Alexei Ashikhmin, Alexander Barg, and Simon Litsyn

ABSTRACT. We use the polynomial method to derive upper and lower bounds on the distance distribution of nonbinary codes in the Hamming space. Applications of the bounds include a better asymptotic upper bound on the weight distribution of Goppa codes from maximal curves, a new upper bound on the size of a q-ary code with a given rth generalized weight, improved estimates of the size of secant spaces of algebraic curves over F_q, and remarks on the error exponents for the q-ary symmetric channel.

1. Introduction

Polynomial method is a powerful technique for obtaining bounds on parameters of codes in distance-transitive spaces [**20**], [**6**]. Its applications to bounding distance distribution of codes with various restrictions on their minimum distance d and/or dual distance $d^\perp$ are by now well understood [**16**], [**18**], [**3**], [**21**], [**5**]. They include nontrivial asymptotic (upper and lower) estimates of the average number of neighbors of a code vector in a code with a given d. This was first studied in a particular case in a series of works on BCH codes [**23**], [**11**], [**14**], and on a more general level in [**5**]. If, on the other hand, the value of $d^\perp$ is fixed, then it is possible to prove that the distance distribution of any code is bounded above by a binomial distribution in some segment of weights around $n/2$ and by some other function outside it [**16**], [**18**], [**5**]. Ramifications of this technique include, in particular, an upper bound on the minimum distance of self-dual binary codes [**17**], [**19**], proved via establishing the presence of a binomial component A_w in the weight distribution for sufficiently low w.

For nonbinary linear codes, and in particular, for codes from algebraic curves, estimates of the weight distribution were derived in [**12**], [**13**]. The present paper aims at improving these results by deriving inequalities, which are tighter in many cases and in addition do not rely on linearity of codes. The general method is presented in Section 2. It is applicable to any linear form of the distance coefficients, for instance, probability of undetected error (see [**3**], [**4**] for details) or probability of error for bounded-distance decoding.

1991 *Mathematics Subject Classification.* 94B65.
Research supported in part by Binational Science Foundation (BSF) under grant 1999099.

©0000 (copyright holder)

Known applications of these estimates include an improved lower bound on the reliability function of the q-ary symmetric channel for large q [**13**]. Another application of the bounds derived below is related to bounds on the size of codes with a given d_r (rth higher weight), and follows the lines of [**7**] where only the case $q = 2$ was studied. We improve the results in [**27**] for $r \geq 2$. In [**28**] the bounds of [**27**] were applied to deriving new estimates of the minimal size of secant spaces of algebraic curves. These results are also improved in the present paper.

We usually omit proofs that are generalized straightforwardly from the binary case.

2. Preliminaries

2.1. Notation. Let $X = F_q^n$ be the Hamming space and $C \subset X$ a code. Let $R = (1/n)\log_q |C|$ be the *rate* of C. Its *distance distribution* is the $(n+1)$-vector $(A_0, A_1, \ldots, A_n)$, where

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

The minimal $d \geq 1$ such that $A_i \neq 0$ is called the *distance* of C. Let $a_\xi = \log_q A_{\xi n}$.

The dual distance distribution is defined as a vector $(A_0^\perp, A_1^\perp, \ldots, A_n^\perp)$, where

$$A_j^\perp = \frac{1}{|C|} \sum_{i=0}^{n} A_i K_j(i), \tag{1}$$

$$\sum_j A_j^\perp = |X|/|C|,$$

where $K_j(i)$ is the Krawtchouk number (see Sect. 2.3 below). We have $A_0^\perp = 1, A_i^\perp \geq 0$. The *dual distance* of C is defined as $d^\perp = \min_{1 \leq i \leq n}\{i : A_i^\perp > 0\}$. Let $\delta = d/n, \delta^\perp = d^\perp/n$.

Let

$$\begin{aligned} H_q(x) &:= x\log_q(q-1) - x\log_q x - (1-x)\log_q(1-x), \\ \alpha_0(x) &:= R - 1 + H_q(x), \\ \mu(i) &:= \binom{n}{i}(q-1)^i/q^n. \end{aligned}$$

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

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

Below we derive bounds on F_w for any code with a given d and/or $d^\perp$. In this case we write $F_w(d, d^\perp)$. The same meaning is ascribed to the distance coefficients $A_w(d, d^\perp)$ and their exponents $a_\xi(\delta, \delta^\perp)$, where we put $i = \xi n$, $d = \delta n$, $d^\perp = \delta^\perp n$. The following proposition is a starting point of our estimates.

PROPOSITION 1. [**5**] *Let $Z_w(x) = \sum_{i=0}^n z_i K_i(x)$ be a polynomial such that*

$$z_i \leq 0 \text{ for } d^\perp \leq i \leq n, \text{ and } Z_w(i) \geq g_w(i) \text{ for } d \leq i \leq n. \tag{2}$$

Then

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

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

$$y_i \ge 0 \text{ for } d^\perp \le i \le n, \text{ and } Y_w(i) \le g_w(i) \text{ for } d \le i \le n. \tag{4}$$

Then

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

2.3. Krawtchouk polynomials. This is a family of polynomials $K_k(x) = K_k(q; n, x)$ orthogonal on $\{0, 1, \dots, n\}$ with weight equal $\mu(i)$ at $i = 0, \dots, n$ and 0 otherwise. We have

$$\langle K_i, K_j \rangle = q^n \mu(i) \delta_{ij}.$$

In particular, $K_0 = 1$. For any polynomial $Z(x) = \sum_{i=0} z_i K_i(x)$ we thus have

$$z_i = \frac{\langle Z, K_i \rangle}{\|K_i\|^2}.$$

The following properties are standard:

$$\frac{K_{k+1}(x)K_k(y) - K_k(x)K_{k+1}(y)}{y - x} = \frac{q\mu(k)}{k+1} \sum_{j=0}^{k} \frac{K_j(x)K_j(y)}{\mu(j)} \tag{6}$$

$$\sum_{i=0}^{n} \binom{n-i}{n-w} K_i(j) = q^w \binom{n-j}{w} \tag{7}$$

$$\mu(i) K_j(i) = \mu(j) K_i(j) \tag{8}$$

$$\sum_{i=0}^{n} K_j(i) K_i(k) = q^n \delta_{jk} \tag{9}$$

$$K_i(x) K_j(x) = \sum_{\sigma=0}^{n} p_{ij}^\sigma K_\sigma(x), \tag{10}$$

where $p_{ij}^\sigma \ge 0$ are the intersection numbers of the Hamming scheme:

$$p_{ij}^\sigma = \sum_{\alpha=0}^{\lfloor \frac{i+j-\sigma}{2} \rfloor} \binom{\sigma}{j-\alpha} \binom{j-\alpha}{\sigma+\alpha-i} \binom{n-\sigma}{\alpha} (q-1)^\alpha (q-2)^{i+j-\sigma-2\alpha}$$

Let $t = \tau n$, then for the minimal zero x_t of K_t we have [**2**] $x_t \to n\gamma(\tau)$, where

$$\gamma(\tau) = \big(q - 1 - (q-2)\tau - 2\sqrt{(q-1)\tau(1-\tau)}\,\big)/q.$$

Note that γ maps the segment $[0, (q-1)/q]$ onto itself, is monotone decreasing, and that $\gamma \circ \gamma = \mathrm{id}$.

Asymptotics of $K_k(x)$ for $q = 2$ outside the oscillatory segment was found in [**10**]; for arbitrary q this method yields the following:

$$n^{-1} \log_q K_{\sigma n}(\xi n) = \phi(\sigma, \xi) + o(1), \tag{11}$$

where

$$\phi(\sigma, \xi) = H_q(\sigma) + \int_0^\xi \log_q \frac{(1-y)\beta + y - q\sigma + \sqrt{((1-y)\beta + y - q\sigma)^2 - 4\beta y(1-y)}}{2\beta(1-y)} dy,$$

with $\beta := q-1$. In particular, for $\xi = \gamma(\sigma)$, this gives

$$\phi(\sigma, \gamma(\sigma)) = (1 + H_q(\sigma) - H_q(\xi))/2. \tag{12}$$

3. The Singleton bound

In this section we basically re-derive some known results [**12**], [**13**], with a slight improvement and by a different method (described above). The "Singleton" bound is particularly simple and illustrates well the general principle.

In this section C is a code over an alphabet of size $q \geq 2$. Let $k = \log_q |C|, k^\perp = n - k$. Let us choose $g_w(i)$ as follows:

$$g_w(i) = \binom{n-i}{n-w}, w \geq d.$$

Take

$$Z_w(i) = \binom{n-i}{n-w} - c \cdot \binom{n-i}{n-(d-1)}, \tag{13}$$

where c is a constant, chosen later. Using (7), one obtains

$$z_j = q^{w-n}\binom{n-j}{w} - c \cdot q^{d-1-n}\binom{n-j}{d-1}.$$

Since z_j must be nonpositive when j is greater than or equal to $d^\perp$, it is natural to choose c so that $z_{d^\perp} = 0$, i.e.,

$$c = \begin{cases} q^{w-d+1}\frac{\binom{n-d^\perp}{w}}{\binom{n-d^\perp}{d-1}}, & \text{if } d \leq w < n - d^\perp + 1, \\ 0, & \text{if } n - d^\perp + 1 \leq w \leq n. \end{cases} \tag{14}$$

The ratio

$$\frac{\binom{n-j}{w}}{\binom{n-j}{d-1}} = \frac{(d-1)!}{w!}(n-j-d+1)\dots(n-j-w+1)$$

is decreasing on j. Hence $z_j \leq 0, j = d^\perp, \dots, n$. Further,

$$Z_w(i) = \binom{n-i}{n-w} = g_w(i), i = d, \dots, n.$$

Thus the polynomial $Z_w(i)$ is feasible, and we arrive at the following theorem.

THEOREM 2.

$$F_w(d, d^\perp) \leq \binom{n}{w}(q^{k+w-n} - 1) + c\binom{n}{d-1}(1 - q^{k+d-n-1}), 1 \leq d \leq w,$$

Now let us assume that only the distance (or dual distance) of a code is known. We start with the case of known d. To guarantee feasibility of polynomial (13), we put $d^\perp = 1$ in (14). Now from Theorem 2 we obtain the following corollary.

COROLLARY 1.

$$F_w(d,1) \leq \binom{n}{w}\Big[\frac{(n-w) + q^{d-(n-k+1)}(w-d+1)}{n-d+1}q^{w-d+1} - 1\Big] \tag{15}$$

$$\leq \binom{n}{w}(q^{w-d+1} - 1), \ d \leq w. \tag{16}$$

PROOF. The first inequality follows from Theorem 2 by direct substitution. For the second one note that the coefficient of the term q^{w-d+1} in (15) equals 1 if $d = n - k + 1$ and is less than 1 otherwise. □

The following bound was obtained in [**3**] by an application of the polynomial method.

THEOREM 3. [**3**]

$$F_w(d,1) \geq \min\{0, \binom{n}{w}(q^{w-n+k}-1)\},\ d \leq w \leq n.$$

It is well known that for MDS codes this bound is tight. Let us prove this using the results in this section. Consider the following example.

EXAMPLE 1. *Let C be an MDS code, that is $d = n - k + 1$. Then by Corollary 1 we have*

$$F_w(d,1) \leq \binom{n}{w}(q^{w-n+k}-1), d \leq w \leq n.$$

Comparing this with Theorem 3, we see that this bound on $F_w(C)$ is in fact exact. This gives a triangular system of equations for the distance distribution of MDS codes; solving it, we obtain the distribution itself.

Now let us assume that we know only the dual distance $d^\perp$. For the same reason as in the previous case we assume $d = 1$. To derive a bound on $F_w(0, d^\perp)$ we use the MacWilliams equation. From the proof in [**22**] it follows that

$$F_w(C) = q^{w-k^\perp} F_{n-w}(C^\perp) + \binom{n}{w}(q^{w-k^\perp}-1).$$

Now using the estimate for $F_w(C^\perp)$ from Corollary 1, we obtain the following.

COROLLARY 2.

$$F_w(1,d^\perp) \leq \binom{n}{w}\Big[\frac{w + q^{d^\perp-(k+1)}(n-w-d^\perp+1)}{n-d^\perp+1} q^{k-d^\perp+1} - 1\Big] \tag{17}$$

$$\leq \binom{n}{w}(q^{k-d^\perp+1}-1), \quad d^\perp \leq w \leq n - d^\perp. \tag{18}$$

PROOF. To prove the first part, substitute (15) into the MacWilliams equation. For the second part note that the coefficient of the term $q^{k-d^\perp+1}$ in (17) equals 1 if $d^\perp = k + 1$ and is less than 1 otherwise. □

Remark: Estimates (16) and (18) were obtained in [**12**] by linear-algebraic arguments.

4. Asymptotic upper bounds and applications

4.1. Upper bounds. The mean distance distribution of a code C chosen in X with uniform probability is given by

$$\mathcal{A}_i = \mu(i)|C| = \binom{n}{i}(q-1)^i|C|/q^n \quad (1 \leq i \leq n)$$

and it is straightforward to show that there exist codes with

$$A_i \leq n^2\binom{n}{i}(q-1)^i|C|/q^n = q^{n\alpha_0(i/n)+o(n)} \quad (1 \leq i \leq n). \tag{19}$$

Codes with distance distribution bounded above by the right-hand side of (19) have a number of important properties; therefore, the bounds obtained in coding theory are usually compared to this "binomial" distribution. In particular, the following upper bound was derived in [**13**] relying on Corollaries 1 and 2 above[1,2]:

$$a_\xi \le \begin{cases} H_q(\xi) - \frac{q\delta}{q-1}, & \delta \le \xi \le \xi^*, \\ \alpha_0(\xi) + (1-\delta^\perp)(1 - H_q(\frac{\xi}{1-\delta^\perp})), & \xi^* \le \xi \le \frac{(q-1)(1-\delta^\perp)}{q}, \\ \alpha_0(\xi), & \frac{(q-1)(1-\delta^\perp)}{q} \le \xi \le \frac{q-1}{q}, \end{cases} \tag{21}$$

where $\xi^* = (1-\delta^\perp)H_q^{-1}((R - \delta^\perp + q\delta/(q-1))/(1-\delta^\perp))$. This estimate of the distance distribution of nonbinary codes is the best available in the literature.

We will state a number of results that improve upon these estimates. Their proofs are given in the next subsection.

THEOREM 4.

$$a_\xi(\delta, 0) \le H_q(\gamma(\delta)) + H_q(\xi) - 1, \quad \delta \le \xi \le (q-1)/q. \tag{22}$$

Comparing this result with the first bound in (21), we see that the estimates differ by $1 - q\delta/(q-1) - H_q(\gamma(\delta))$; this is the difference between the asymptotic Plotkin and Aaltonen [**2**] bounds on the code rate as a function of code's distance. So whenever the latter bound is better (generally, for small code rates), Theorem 4 is an improvement over (21).

THEOREM 5.

$$a_\xi(0, \delta^\perp) \le \begin{cases} R + H(\frac{\delta^\perp}{2}) - \phi(\delta^\perp/2, \xi), & \delta \le \xi \le \gamma(\frac{\delta^\perp}{2}), \\ \alpha_0(\xi), & \gamma(\frac{\delta^\perp}{2}) \le \xi \le \frac{q-1}{q}. \end{cases} \tag{23}$$

Comparing (23) with the second and third parts in (21), we note that whenever $\gamma(\delta^\perp/2) < (q-1)(1-\delta^\perp)/q$, the last theorem yields a wider range in which the distance distribution is asymptotically at most the binomial distance distribution $\mathcal{A}_i$. This holds true for all $\delta^\perp$ if q is small and for small $\delta^\perp$ for large q. The first bound in Theorem 5 also improves the second bound in (21).

THEOREM 6.

$$a_\xi(0, \delta^\perp) \le R - 1 + 2H_q(\omega^*) - g(\xi, \omega^*), \quad 0 \le \xi \le (q-1)/q, \tag{24}$$

where

$$g(x,y) := (\log_2 q)\big[xH_2(\frac{y-\alpha}{x}) + (y-\alpha)H_2(\frac{x+\alpha-y}{y-\alpha})\big] + (1-x)H_q(\frac{\alpha}{1-x}) + (2y - x - 2\alpha)\log_q(q-2), \tag{25}$$

$y - \frac{x}{2} \le \alpha \le y - x$, *and*

$$\omega^* = \begin{cases} \omega^{**} & \text{if } \gamma(\delta^\perp) \le \omega^{**} \le (q-1)/q, \\ \gamma(\delta^\perp) & \text{if } 0 \le \omega^{**} \le \gamma(\delta^\perp), \end{cases}$$

[1] In this formula and similar formulas below we disregard the $o(1)$ terms.

[2] In fact, Corollary 1 implies the bound

$$a_\xi \le H_q(\xi) - \delta. \tag{20}$$

The first of the estimates (21), which is slightly better than this, relies on the Plotkin bound.

where

$$\omega^{**} = \arg\min_{\omega}[2H_q(\omega) - g(\xi, \omega)],$$

Note that function $g(x, y)$ has a unique maximum on α in the segment $y - \frac{x}{2} \leq \alpha \leq y - x$ attained for α that satisfies the equation

$$(q-1)(1-x-\alpha)(2y-x-2\alpha) = (q-2)^2\alpha(x+\alpha-y)^2. \tag{26}$$

In the case that $\omega^* = \gamma(\delta^\perp)$, the bound of this theorem actually is $\alpha_0(\xi)$ (we do not prove this). The bound in this theorem improves in many cases the second estimate in (21). For instance, for $q = 4, R = 0.8, \delta^\perp = 0.1$, the value ω^{**} reaches $\gamma(\delta^\perp)$ for $\xi = 0.5531 < (q-1)(1-\delta^\perp)/q = 0.6375$. Thus, (24) gives the "binomial" bound starting from smaller values of ξ; it is also less than the second estimate in (21) for $\xi \leq 0.5531$. The qualitative picture is unchanged if we take $\delta^\perp = 0.0559$, the Varshamov-Gilbert distance for $R^\perp = 1 - R$. Finally, for high rates (24) is also better than (23). Directions for further (minor) improvements of Theorems 5 and 6 are outlined in [**5**].

Remark: As noted in the end of Sect. 3, estimates (16) and (18), which led to (21), were derived [**12**], [**13**] by another method. Namely, it is well known that the sum $F_w(C) = \sum_{i=0}^{w} \binom{n-i}{n-w} A_i(C)$ equals the sum over all the w-subsets E of $\{1, 2, \ldots, n\}$ of the size of the subcodes $\mathcal{C}(E)$ of C with $\mathrm{supp}(\mathcal{C}(E)) \subseteq E$. Since the distance of $\mathcal{C}(E)$ is at least that of C, we can use an upper bound on the size of a code of length w and distance d to bound $F_w(C)$ above. In [**13**] the authors use the Singleton and Plotkin bounds (cf. (20) and the first inequality in (21)). They also remark that it is possible to use better bounds on the size of codes, which makes the result "slightly better but the formulae are much more complicated and the calculations are very cumbersome." We concur with this remark. More importantly, we tried a few examples with Aaltonen's bound [**2**] to compare this option with Theorem 4. In all the examples, for small and large d and q Theorem 4 gives a uniformly better estimate.

For linear codes from algebraic curves estimate (21) can be improved [**13**]. To state this result let us assume that C is a q-ary geometric Goppa code constructed from a smooth absolutely irreducible projective curve of genus g and an F_q-rational divisor of degree $a \geq 2g - 1$. Let δn and $\delta^\perp n$ be the *designed* distance and dual distance of C. Note that by the construction, $2R = 1 - \delta + \delta^\perp + o(1)$. Then

$$a_\xi \leq \alpha_0(\xi) + (1 - R - \frac{\delta}{2} - \xi \log_q(\sqrt{q}+1)), \quad 0 \leq \xi \leq \frac{(1-\delta^\perp)(\sqrt{q}-1)}{\sqrt{q}}. \tag{27}$$

This bound is better than (21) for normalized weights in the segment $\delta(\frac{1}{q-1} + \frac{1}{2})/\log_q(\sqrt{q}+1) \leq \xi \leq \frac{(1-\delta^\perp)(\sqrt{q}-1)}{\sqrt{q}}$. The improvement is due to an application of the Clifford theorem that bounds above the dimension of the space of functions associated with a special divisor.

The bound in Theorem 4 is inferior to (27). However, it can be improved as follows. We begin with an auxiliary result.

LEMMA 7. *Let $C \subset F_q^n$ be a code with distance $d(C) = d$. Then for any fixed i, $1 \leq i \leq n$, and t, $1 \leq t \leq n - i$, there exists a code $C(t) \subset F_q^{n-t}$ with distance*

$d(C(t)) = d$ such that

$$A_i(C) \le \frac{\binom{n}{t}}{\binom{n-i}{t}} A_i(C(t)).$$

Let $a_\xi(\delta, 0) \le f(\xi, \delta)$, where $f(\xi, \delta)$ is any upper bound on the distance distribution of codes. Then Lemma 7 implies the inequality

$$a_\xi \le \min_{0 \le \tau \le 1-\xi} H_q(\tau) - (1-\xi) H_q\Big(\frac{\tau}{1-\xi}\Big) + (1-\tau) f\Big(\frac{\xi}{1-\tau}, \frac{\delta}{1-\tau}\Big). \tag{28}$$

As it turns out, the first bound in (21) and bounds (20) and (27) are fixed points of this transformation. However, bound (22) is not.

PROPOSITION 8. *Let $0 \le \delta \le (q-2)^2/q^2$ and $\delta \le \xi \le q(q-1)\delta/(q-2)^2$. Then*

$$a_\xi(\delta, 0) \le H_q(\xi) - \big(\delta q \log_q(q-1)\big)/(q-2).$$

EXAMPLE 2. *Let $q = 49$ and consider a sequence of codes from maximal curves, i.e., those with $R = 1 - \delta - (\sqrt{q}-1)^{-1}$. For $\delta = 0.6$ we then obtain $R = 0.333$, which is better than the Varshamov-Gilbert bound $1 - H_q(\delta) = 0.324$. For ξ in the neighborhood of δ Proposition 8 improves all the other bounds mentioned in this section.*

4.2. Proofs. A. Theorem 4. The proof is generalized straightforwardly from the binary case [**5**].

B. Theorem 5. Take in Proposition 1

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

where $2t + 2 \le d^\perp - 1$, and $g_w = Z$. Then by (10) $z_j = p_{tt}^j + p_{t+1,t+1}^j$, so

$$z_0 = \mu(t) q^n \frac{n(q-1) - t(q-2) + 1}{t+1} > 0$$

and $z_j = 0$ for $j \ge d^\perp$. So the polynomial $Z(x)$ satisfies the necessary restrictions, and furthermore,

$$A_i \le z_0 |C| / Z(i).$$

We still have to choose $t = \tau n$. If $\gamma(\xi) < \delta^\perp/2$, put $\tau = \gamma(\xi)$. Then taking logarithms and using (12), we obtain the first part of the claim. The condition on ξ in the first part follows by applying γ to both parts of $\gamma(\xi) < \delta^\perp/2$. If $\gamma(\xi) \ge \delta^\perp/2$, take $\tau = \delta^\perp/2$. This gives the second part.

C. Theorem 6. Take in Proposition 1 $g_w(i) = Z_w(i)$ and $Z_w(x) = \sum z_j K_j(x)$, where

$$z_j = \frac{w+1}{q} \frac{(K_w(j) + K_{w+1}(j))^2}{a - j},$$

$w = \omega n$ is chosen later, and a is the smallest root of the numerator. Clearly, $z_j < 0$ for $a < j$, so the restriction on z_j is satisfied as long as $d^\perp > a$, and therefore, also if $d^\perp > x_t$. Note that

$$\begin{aligned} z_0 &= \frac{w+1}{aq} q^{2n} (\mu(w) + \mu(w+1))^2 \\ &= \frac{n(q-1) - w(q-2) + 1}{aq} \binom{n}{w}^2 (q-1)^{2w} \\ &= \exp(2nH_q(\omega) + o(n)). \end{aligned}$$

Let us use (6) and (10) in succession to rewrite z_j as follows:

$$z_j = \frac{\binom{n}{w}}{K_w(a)} \sum_{i=0}^{w} \frac{K_i(a)}{\binom{n}{i}} \sum_{s=0}^{n} (p_{w+1,i}^{s} + p_{wi}^{s}) K_s(j).$$

Now use (9) to find, for integer x,

$$Z_w(x) = q^n \frac{\binom{n}{w}}{K_w(a)} \sum_{i=0}^{w} \frac{K_i(a)}{\binom{n}{i}} (p_{w+1,i}^{x} + p_{wi}^{x}),$$

and, in particular, $Z_w(0) = q^n \binom{n}{w}(q-1)^w$. Further, $K_i(a) \geq 0$ for $0 \leq i \leq w$, so $A_{\xi n} \leq z_0 |C| / Z_w(\xi n)$. We have for $Z_w(x)$ the inequality

$$\begin{aligned} Z_w(x) &\geq q^n \frac{\binom{n}{w}}{K_w(a)} \max_{0 \leq i \leq w} \frac{K_i(a)}{\binom{n}{i}} (p_{w+1,i}^{x} + p_{wi}^{x}) \\ &\geq q^n p_{ww}^{x}. \end{aligned}$$

Now let $x = \xi n$, $w = \omega n$. Then we obtain

$$a_\xi \leq R + 2H_q(\omega) - 1 - n^{-1} \log_q p_{ww}^{\xi n} \quad (\gamma(\omega) < \delta^\perp).$$

Further, taking logarithm of the summation term in the sum for p_{ww}^{x} we obtain $g(\xi, \omega)$. It remains to optimize on the (hitherto free) parameter ω. We take $\omega = \omega^{**}$ as long as the coefficients z_j of $Z_{\omega n}(x)$ are negative for $j = d^\perp, d^\perp + 1, \ldots, n$. This holds true for large n if $\gamma(\omega^{**}) < \delta^\perp$ (which is the same as $\gamma(\delta^\perp) \leq \omega^{**}$). Otherwise we put $\omega = \gamma(\delta^\perp)$.

D. Lemma 7. Let $C(j, \alpha), 1 \leq j \leq n$, be a subcode of C of size $M(j, \alpha)$ defined as follows:

$$C(j, \alpha) = \{\mathbf{v} \in C : v_j = \alpha\}.$$

It is obvious that for any j

$$\sum_{\alpha \in F_q} M(j, \alpha) = |C|.$$

Let $B_i(j, \alpha)$ be the number of ordered pairs of codewords of $C(j, \alpha)$ at a distance i apart, i.e.,

$$B_i(j, \alpha) = |\{\mathbf{v}, \mathbf{u} \in C(j, \alpha) : \operatorname{dist}(\mathbf{v}, \mathbf{u}) = i\}|.$$

Note that the code $C(j, \alpha)$ has distance distribution $A_i(j, \alpha) = B_i(j, \alpha)/M(j, \alpha)$. It is not difficult to see that

$$\sum_{j=1}^{n} \sum_{\alpha \in F_q} B_i(j, \alpha) = (n - i) A_i |C|.$$

Hence there exists an ℓ such that

$$\sum_{\alpha \in F_q} B_i(\ell, \alpha) \geq \frac{n - i}{n} A_i |C|.$$

Now let $\beta \in F_q$ be such that

$$A_i(\ell, \beta) = \frac{B_i(\ell, \beta)}{M(\ell, \beta)} = \max_{\alpha \in F_q} \frac{B_i(\ell, \alpha)}{M(\ell, \alpha)}.$$

Then

$$\begin{aligned}\frac{n-i}{n}A_i|C| &\le \sum_{\alpha} B_i(\ell,\alpha) \le \sum_{\alpha} M(\ell,\alpha)\frac{B_i(\ell,\beta)}{M(\ell,\beta)} \\ &\le \frac{B_i(\ell,\beta)}{M(\ell,\beta)}|C| = A_i(\ell,\beta)|C|.\end{aligned}$$

Let us shorten C with respect to these ℓ and β, i.e., restrict ourselves to the set of vectors $C(\ell,\beta)$ and project them on $(1,\dots,n)\setminus\ell$. Denote the resulting code by $C(1)$; clearly, it satisfies the assertion of the lemma for $t=1$. The full claim now follows by applying the described procedure recursively t times.

E. Proposition 8. Substitute (22) in (28). Upon simplifying we obtain

$$a_\xi \le H_q(\xi) - 1 + \min_{0\le\tau\le 1-\xi}\left(\tau + (1-\tau)H_q\left(\gamma\left(\frac{\delta}{1-\tau}\right)\right)\right).$$

Note that since (22) is valid for $\xi \le (q-1)/q$, for the shortened code this implies a restriction on τ of the form $\xi \le (1-\tau)(q-1)/q$. The minimum on τ is attained for $\tau = 1-q^2\delta/(q-2)^2$ if $0 \le \delta < (q-2)^2/q^2$ and for $\tau = 0$ if $(q-2)^2/q^2 \le \delta \le (q-1)/q$ (cf. [**1**]). In the first case the value of the minimum equals $(\delta q \log_q(q-1))/(q-2)$; substituting, we obtain the claimed bound. This bound is valid whenever

$$\xi \le \frac{(1-\tau)(q-1)}{q} = \frac{q^2\delta(q-1)}{q(q-2)^2}.$$

4.3. Applications. The main motivation for the estimate (27) in [**13**] was improving upper bounds on the error probability P_e of decoding for q-ary codes used on the q-ary symmetric channel (qSC) with error probability p. The error probability for a code C is defined as

$$P_e(C,p) = \frac{1}{|C|}\sum_{\mathbf{c}\in C}\Pr\{X\setminus D(\mathbf{c})\}$$

where $D(\mathbf{c})$ is the Voronoi region of $\mathbf{c}$ and the probability is computed under the binomial distribution "centered" at $\mathbf{c}$. Let

$$E(R,p) = \limsup\frac{1}{n}\log_q \min_{C\in X, |C|=q^{Rn}}\frac{1}{P_e(C,p)}.$$

It is known that $E(R,p) > 0$ for $R \in (0, 1-H_q(p))$, and one of the main problems of asymptotic coding theory is establishing the exact form of this function [**9**]. The best known lower estimate of $E(R,p)$ is obtained by computing $P_e(C,p)$ for a sequence of codes C_n with distance distribution that satisfies (19) where $p(n)$ is a function of polynomial growth (note that these codes asymptotically attain the Varshamov-Gilbert bound $\delta := \delta_0(R) = H_q^{-1}(1-R)$). Without loss of generality we can assume that codes are linear and the transmitted vector is 0. The result (the "random coding exponent") has the form

$$E(R,p) \ge \begin{cases} -\delta_0 \log_q \pi_q(p), & 0 \le p \le p_e, \quad \text{(a)} \\ 1 - R - \log_q(1+(q-1)\pi_q(p)), & p_e \le p \le p_c, \quad \text{(b)} \\ T_q(\delta_0,p) - 1 + R, & p_c \le p \le \delta_0. \quad \text{(c)} \end{cases} \tag{29}$$

Here

$$\begin{aligned} p_e &= \frac{(2q-q\delta_0-2)-2\sqrt{(q-1)(q-1-q\delta_0)}}{q^2(1-\delta_0)} \\ p_c &= \frac{\delta_0^2}{q\delta_0^2+(q-1)(1-2\delta_0)} \\ \pi_q(p) &= p\frac{q-2}{q-1}+2\sqrt{\frac{p(1-p)}{q-1}} \\ T_q(x,p) &= x\log_q(q-1)-x\log_q p-(1-x)\log_q(1-p). \end{aligned}$$

For codes C_n with distance distribution satisfying (19) and error probability in the channel $p \in (0, p_e)$, the error probability of decoding is determined by decoding errors that result in code vectors of weight $\delta_0 n$. Furthermore, for $p \in (p_e, p_c)$, the typical weight of the code vector in the case of error event is $n(q-1)\pi_q(p)/(1+(q-1)\pi_q(p))$. This value equals $n\delta_0$ for $p = p_e$ and shifts away from it for larger p. For codes on maximal curves and large q there is an interval of code rates in which the minimum distance $\delta = 1-R-(\sqrt{q}-1)^{-1} > \delta_0$. Together with the bound (27) this was used in [**13**] to improve the lower estimate (29) for low p. Since the estimate of Proposition 8 is better than (27), this yields further sharpening of the bound (29a).

As proved by Vlăduţ (see [**13**]), there exist families of algebraic-geometry codes with relative distance

$$\delta \geq \max(\delta_0(R), 1-R-(\sqrt{q}-1)^{-1})$$

and weight spectrum that, depending on R, is either at most binomial (19) or bounded above by a function smaller than binomial. This result gives better estimates of $E(R,p)$ than the results discussed in this section. However, Vlăduţ's proof is an existence theorem, while the family of codes on maximal curves discussed here is polynomially constructible.

5. Asymptotic lower bounds and applications

5.1. Lower bounds. The following theorem is generalized directly from [**21**].

THEOREM 9. *Let C be a sequence of codes of asymptotic rate R. Then for every $\beta \in [0, H_q^{-1}(R)]$ there exists a number $\xi \in (0, \gamma(\beta))$ such that*

$$a_\xi(C) \geq R + H_q(\beta) - (2/n)\log_q K_{\beta n}(\xi n).$$

This is proved by taking in (5) $Y(x)$ equal to the Christoffel-Darboux kernel of Krawtchouk polynomials. The exponent of $K_{\beta n}(\xi n)$ is given in (11).

Let us sketch a possible improvement of this bound. As suggested in [**21**] for $q = 2$, one can derive a similar lower bound for the distance distribution of constant weight codes (codes in the Johnson space $J_2^{w,n}$) and then use the Bassalygo-Elias argument to transfer the bound to the Hamming space. The nonbinary case is much harder because $J_q^{w,n}$ is a symmetric space of rank 2; hence the zonal spherical functions are expressed by bivariate polynomials $Q_{rs}(x,y)$. We have [**25**]

$$Q_{rs}(i,j) = \frac{\binom{n}{s}}{\binom{w}{s}} K_s(q-1; w-j, i-j) H_{r-s}(n-s, w-s; j),$$

where the $H_m(n,w;x)$ are the dual Hahn polynomials (the zonal spherical functions for $J_2^{n,w}$). Consequently, applications of the polynomial method in this space are technically more difficult, and the only nontrivial result is that of [**1**].

For two vectors $\mathbf{x}, \mathbf{y} \in J_q^{n,w}$ let

$$n(\mathbf{x},\mathbf{y}) = |\{i : x_i \neq 0, y_i \neq 0\}|, \quad e(\mathbf{x},\mathbf{y}) = |\{i : x_i = y_i \neq 0\}|,$$

and let $m = \min(w, n-w)$,

$$\begin{aligned} N &= \{(i,j) \in Z^2,\ 0 \le j \le m, j \le i \le w\}, \quad N^* = N - (0,0), \\ K &= \{(r,s) \in Z^2, 0 \le s \le r \le w,\ r - s \le m\} \\ P(p) &= \{(i,j) \in N :\ i + j > p\}. \end{aligned}$$

Let $G \subset J_q^{n,w}$ be a code. Define the set of numbers

$$A_{ij} = A_{ij}(G) = \frac{1}{|G|}\{(\mathbf{x},\mathbf{y} \in G :\ e(\mathbf{x},\mathbf{y}) = w - i,\ n(\mathbf{x},\mathbf{y}) = w - j\}, \quad (i,j) \in N.$$

We have

$$\sum_{(i,j)\in N} A_{ij} = |G|.$$

Let $\{A_u^{(w)}(G),\ 0 \le u \le 2w\}$ be the distance distribution of G. We have

$$A_u^{(w)}(G) = \sum_{(i,j)\in N, i+j=u} A_{ij}(G).$$

By Delsarte's theory we have the following set of inequalities [**25**]:

$$A_{rs}^{\perp} := \frac{1}{|G|} \sum_{(i,j)\in N} A_{ij} Q_{rs}(i,j) \ge 0, \quad (r,s) \in K, \tag{30}$$

Let use use these inequalities to establish the following lower bound on the distance distribution of C. The proof parallels [**21**].

THEOREM 10. *Let C be a code, $1 \le w \le n, 1 \le p \le \min(2w, n)$. Let $F(x,y) = \sum_{(r,s)\in K} f_{rs} Q_{rs}(x,y)$ be a polynomial such that*

$$\begin{aligned} &(i) \quad f_{rs} \ge 0 && (r,s) \in K, \\ &(ii)\ F(i,j) \le 0 && (i,j) \in P(p), \\ &(iii)\ F(i,j) \ge 0 && (i,j) \in N^* - P(p), \end{aligned}$$

where $1 \le p \le 2w$. Then there exists a number $u, 1 \le u \le p-1$, and a pair $(m,\ell) \in N^* - P(p)$ such that

$$A_u(C) \ge \frac{q^n \mu(w)}{w^2 h(u) F(m,\ell)} (f_{00}|C|\mu(w) - F(0,0)).$$

PROOF. Let $C(\mathbf{x}, w) := (C - \mathbf{x}) \cap J_q^{n,w}$. We need the following lemma which extends Lemma 2 in [**21**].

LEMMA 11. *Let $\{A_u\}$ be the distance distribution of a code $C \subset X$. Then*

$$|C| A_u(C) h(u) = \sum_{(i,j)\in N, i+j=u} \sum_{\mathbf{x}\in X} |C(\mathbf{x},w)| A_{ij}(C(\mathbf{x},w)), \tag{31}$$

where $h(u) = p_{ww}^u$ is the intersection number. Explicitly,

$$h(u) = \sum_{s=0}^{u} \binom{u}{s} \binom{s}{2s-u} \binom{n-u}{w-s} (q-1)^{w-s} (q-2)^{2s-u}.$$

PROOF. Let $\mathbf{a}, \mathbf{b}$ be two codewords in C with $\operatorname{dist}(\mathbf{a}, \mathbf{b}) = u$. Let us count the number of vectors $\mathbf{x} \in X$ such that $\mathbf{a}' = \mathbf{x} - \mathbf{a}$ and $\mathbf{b}' = \mathbf{x} - \mathbf{b}$ are both in $J_q^{n,w}$ and $e(\mathbf{a}', \mathbf{b}') = w - i$ and $n(\mathbf{a}', \mathbf{b}') = w - j$. For a given $\mathbf{x}$ the number of such pairs is $|C(\mathbf{x}, w)| A_{ij}(C(\mathbf{x}, w))$, where $i + j = u$, so we obtain the total of

$$\sum_{(i,j)\in N, i+j=u} \sum_{\mathbf{x}\in X} |C(\mathbf{x}, w)| A_{ij}(C(\mathbf{x}, w))$$

such shifts. So the proof will be complete if we show that for a pair $\mathbf{a}, \mathbf{b}$ there are $h(u)$ vectors $\mathbf{x}$ that take it to a pair $\mathbf{a}', \mathbf{b}'$ with the needed properties. We have $\operatorname{dist}(\mathbf{a}, \mathbf{b}) = u$, $\operatorname{dist}(\mathbf{a}, \mathbf{x}) = \operatorname{dist}(\mathbf{b}, \mathbf{x}) = w$. Hence we are looking for the number of triangles with the sides u, w, w; this is precisely p_{ww}^u. □

Next observe that $\sum_{\mathbf{x}\in X} |C(\mathbf{x}, w)| = q^n \mu(w) |C|$. Then

$$\sum_{\mathbf{x}\in X} |C(\mathbf{x}, w)|^2 \geq q^n \mu^2(w) |C|^2$$

since to minimize the sum of squares of some numbers whose sum is fixed we have to take them all equal to each other. Now we compute

$$\begin{aligned}
q^n \mu^2(w) |C|^2 f_{00} &\leq f_{00} \sum_{\mathbf{x}\in X} |C(\mathbf{x}, w)|^2 \\
&= f_{00} \sum_{\mathbf{x}\in X} |C(\mathbf{x}, w)|^2 A_{00}^{\perp}(C(\mathbf{x}, w)) && (A_{00}^{\perp}(C(\mathbf{x}, w)) = 1) \\
&\leq \sum_{\mathbf{x}\in X} |C(\mathbf{x}, w)|^2 \sum_{(r,s)\in K} f_{rs} A_{rs}^{\perp}(C(\mathbf{x}, w)) && \text{(by (i) and (30))} \\
&= \sum_{\mathbf{x}\in X} |C(\mathbf{x}, w)| \sum_{(r,s)\in K} f_{rs} \sum_{(i,j)\in N} A_{ij}(C(\mathbf{x}, w)) Q_{rs}(i, j) && \text{(by (30))} \\
&= \sum_{\mathbf{x}\in X} |C(\mathbf{x}, w)| \sum_{(i,j)\in N} A_{ij}(C(\mathbf{x}, w)) F(i, j) \\
&= F(0, 0) q^n \mu(w) |C| + \sum_{(i,j)\in N^*} \sum_{\mathbf{x}\in X} |C(\mathbf{x}, w)| A_{ij}(C(\mathbf{x}, w)) F(i, j) \\
&\leq F(0, 0) \mu(w) |C| + \sum_{(i,j)\in N^* - P(p)} \sum_{\mathbf{x}\in X} |C(\mathbf{x}, w)| A_{ij}(C(\mathbf{x}, w)) F(i, j),
\end{aligned}$$

the last inequality by assumption (ii). Now by (iii) we conclude that there exists a pair $(m, \ell) \in N^* - P$ such that

$$\sum_{\mathbf{x}\in X} |C(\mathbf{x}, w)| A_{m\ell}(C(\mathbf{x}, w)) \geq \frac{q^n \mu(w) |C| (f_{00} \mu(w) |C| - F(0, 0))}{w^2 F(m, \ell)}.$$

The proof is completed by using this inequality to bound the right-hand side of (31). □

In particular, it is possible to use the polynomial suggested in [**1**] to improve the estimate of Theorem 9.

5.2. Applications. We describe two related applications of Theorem 9 along the lines of [**7**] and [**28**]. Let $C \subset X$ be a linear code. For a code vector $\mathbf{c}$ let $\operatorname{supp}(\mathbf{c}) = \{e : c_e \neq 0\}$. For a subset $A \subset C$ define its support as

$\operatorname{supp}(A) = \cup_{\mathbf{a}\in A}\operatorname{supp}(\mathbf{a})$. The rth generalized weight of C [**29**] is defined as the minimal support of the r-dimensional linear subcode of C. Let

$$\delta_r(R) = \limsup_{n\to\infty} \frac{d_r(C_n)}{n},$$

where the limit is calculated over all sequences of codes of growing length and rate at least R. It is known that $\delta_r(R) : [0,1] \to [0, 1-q^{-r}]$. The following upper bound on $\delta_r(R)$ (the Bassalygo–Elias bound) was obtained in [**8**]:

$$\delta_r(R) \le \delta_r^{\mathrm{el}}(R) := 1 - (\lambda(R))^{r+1}(q-1)^{-r} - (1-\lambda(R))^{r+1}$$

where $\lambda(x) := H_q^{-1}(1-x)$. The following recursive estimate of $\delta_r(R)$ was obtained in [**27**]:

$$\delta_r(R) \le \min_{1\le s\le r-1} \Big(\delta_s^{\mathrm{up}}(R) + (1-\delta_s^{\mathrm{up}}(R))\delta_{r-s}^{\mathrm{up}}\big(\frac{R}{1-\delta_s^{\mathrm{up}}(R)}\big)\Big), \tag{32}$$

where $\delta_i^{\mathrm{up}}(R)$ is any asymptotic upper bound on $\delta_i(R)$. This bound is valid whenever the r.h.s. is defined. Together the last two inequalities give the best upper bound on δ_r currently known for $q \ge 3$. Theorem 9 can be used to improve this result for $r = 2$ (see [**7**] for the binary case).

PROPOSITION 12. *Let $\delta^{\mathrm{up}}(R,\xi)$ be any upper bound on the relative distance of codes of rate R and constant weight ξn. Then*

$$\delta_2(R) \le \min_{0\le\beta\le H_q^{-1}(R)} \max_{0\le\xi\le\gamma(\beta)} \big(\frac{2}{q}\xi + \frac{q-1}{q}\delta^{\mathrm{up}}(R',\xi)\big),$$

where $R' = R + H_q(\beta) - (2/n)\log_q K_{\beta n}(\xi n)$.

PROOF. Let C be a linear code of rate R. By Theorem 9 for every $\beta \in (0, H_q^{-1}(R))$ there exists a constant weight code of size $q^{R'n}$ and weight ξn, $0 < \xi < \gamma(\beta)$. Let $\mathbf{x}, \mathbf{y}$ be two noncollinear vectors from C and $\langle \mathbf{x}, \mathbf{y}\rangle$ their linear span. Let $T = \operatorname{supp}(\mathbf{x}) \cap \operatorname{supp}(\mathbf{y})$, $t = |T|$, and $s = |\{i \in T : x_i = y_i\}|$. Since C is linear, we can assume that $0 \le s \le t/(q-1)$. Now we compute

$$\begin{aligned}\operatorname{dist}(\mathbf{x},\mathbf{y}) &= 2\xi n - t - s \ge 2\xi n - t - \frac{t}{q-1}\\ &= \frac{q}{q-1}(2\xi n - t) - \frac{2}{q-1}\xi n,\end{aligned}$$

which implies the claimed inequality for $|\operatorname{supp}(\langle \mathbf{x}, \mathbf{y}\rangle)| = 2\xi n - t$. □

The result of this proposition can be used in (32) to improve upper bounds for $r \ge 3$, though the complete optimization in (32) soon becomes unmanageable [**7**].

EXAMPLE 3. *Let $q = 3, r = 2, R = 0.19$. Let us compare the bounds on $\delta_2(R)$ in (32) and Proposition 12, taking in (32) $s = 1$. Take $\beta = H_q^{-1}(R) = 0.0434$. We still have to choose an upper bound on $\delta_1(R)$ to use in (32) and an upper bound $\delta^{\mathrm{up}}(R,\xi)$. For instance, bounding $\delta_1(R)$ by $\delta_1^{\mathrm{el}}(R)$, we obtain in (32) $\delta_2(R) \le 0.6899$. The best known upper bounds on $\delta_1(R)$ and $\delta(R,\xi))$ were obtained in* [**1**]. *We have $\delta_1(R) \le 0.4600$; using this in* (32), *we obtain $\delta_2(R) \le 0.6878$. Prop. 12 gives a much better estimate $\delta_2(R) \le 0.6173$. The lower VG bound for this rate is* 0.5231.

The second application is related to a more geometric view of higher weights. Let C be a k-dimensional linear code with the generator matrix $A = [\mathbf{a}_1, \dots, \mathbf{a}_n]$, where $\mathbf{a}_i$ denotes the ith column. C is a linear mapping takes $\mathbf{m} \in F_q^k$ to $\mathbf{m}A \in F_q^n$.

If moreover we assume that A contains no all-zero columns, then the $\mathbf{a}_i$'s can be viewed as a (multi)set of points in PF_q^{k-1}, so that $\mathbf{m} \in (PF_q^{k-1})^*$. This view of linear codes was suggested in [**24**]. Hence we have

$$d(C) = n - \max\left(\#(\mathbf{a}_1, \ldots, \mathbf{a}_n) \cap H : \ H \text{ a hyperplane in } PF_q^{k-1}\right).$$

This definition is extended naturally to cover higher weights [**26**]:

$$d_r(C) = n - \max\left(\#(\mathbf{a}_1, \ldots, \mathbf{a}_n) \cap H : \ H \text{ a space of codim } r \text{ in } PF_q^{k-1}\right)$$

Now let X be a curve over F_q (projective smooth absolutely irreducible) with $\geq n$ F_q-rational points and let H be a projective subspace of PF_q^{k-1} of dimension $\ell = k-1-r$. If $\#H \cap X = m$, then H is called an m-secant ℓ-plane of X. Size of secant spaces is important for the study of geometry of curves over finite fields [**28**]. As observed in that paper, an upper bound on d_r of the form $d_r \leq f_r(n,k)$ implies the existence of an $(n - f_r(n,k))$-secant ℓ-plane for X. Hence Proposition 12 improves the lower asymptotic bound on the size of F_q-rational secant planes.

Finally, lower bounds on the distance distribution were used in [**21**] to improve upper bounds on $E(R,p)$ for the binary symmetric channel. Similar results are possible for the qSC; we will not elaborate on this.

6. Further applications

Let us outline some further results that are possible along the lines of this paper and related works. In Theorems 4–9 we were only interested in the asymptotic bounds on the distance distribution. It is possible to formulate these bounds for specific codes of any given length, taking into account further properties of the codes. As shown in [**5**], this enables one sometimes to improve general results for specific codes. Apart from this, one can use Proposition 1 to derive bounds on other linear forms of the distance coefficients of the code. Among the most well-known examples is the probability of undetected error for a code with the distance distribution $\{A_i, 0 \leq i \leq n\}$ used over a q-ary symmetric channel with crossover probability p, which equals

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

Putting $F_w(C) = P_{ue}(C,p)$ in Proposition 1 we can derive lower bounds on this probability (related results were obtained in [**4**], pt.II). Similar estimates are also possible for the error probability of bounded distance decoding as long as the decoding spheres are disjoint.

References

[1] M. Aaltonen, *A new upper bound on nonbinary block codes*, Discrete Mathematics **83** (1990), no. 2-3, 139–160.

[2] M. J. Aaltonen, *Linear programming bounds for tree codes*, IEEE Trans. Inform. Theory **25** (1977), 85–90.

[3] A. Ashikhmin and A. Barg, *Binomial moments of the distance distribution: Bounds and applications*, IEEE Trans. Inform. Theory **45** (1999), no. 2, 438–452.

[4] A. Ashikhmin, A. Barg, E. Knill, and S. Litsyn, *Quantum error detection, I-II*, IEEE Trans. Inform. Theory **46** (2000), no. 3, 778–800.

[5] A. Ashikhmin, A. Barg, and S. Litsyn, *Estimates of the distance distribution of codes and designs*, IEEE Trans. Inform. Theory, to appear.

[6] ———, *Polynomial method in coding and information theory*, Lanl e-print math.CO/9910175, 1999.
[7] ———, *New bounds on generalized weights*, IEEE Trans. Inform. Theory **45** (1999), no. 4, 1258–1263.
[8] G. Cohen, S. Litsyn, and G Zémor, *Upper bounds on generalized distances*, IEEE Trans. Inform. Theory **40** (1994), 2090–2092.
[9] R. G. Gallager, *Information theory and reliable communication*, John Wiley & Sons, New York e.a., 1968.
[10] G. Kalai and N. Linial, *On the distance distribution of codes*, IEEE Trans. Inform. Theory **41** (1995), no. 5, 1467–1472.
[11] T. Kasami, T. Fujiwara, and S. Lin, *An approximation to the weight distribution of binary linear codes*, IEEE Trans. Inform. Theory **31** (1985), 769–780.
[12] G. L. Katsman and M. A. Tsfasman, *Spectra of algebraic-geometric codes*, Problemy Peredachi Informatsii **23** (1987), no. 4, 19–34, (In Russian).
[13] G. L. Katsman, M. A. Tsfasman, and S. G. Vladuţ, *Spectra of linear codes and error probability of decoding*, Coding theory and algebraic geometry (Luminy, 1991), Springer, Berlin, 1992, pp. 82–98.
[14] O. Keren and S. Litsyn, *More on the distance distribution of BCH codes*, IEEE Trans. Inform. Theory **45** (1999), no. 1, 251–255.
[15] I. Krasikov, *Nonnegative quadratic forms and bounds on orthogonal polynomials*, (1999), preprint.
[16] I. Krasikov and S. Litsyn, *Estimates for the range of binomiality in codes' spectra*, IEEE Trans. Inform. Theory **43** (1997), no. 3, 987–991.
[17] ———, *Linear programming bounds for doubly-even self-dual codes*, IEEE Trans. Inform. Theory **43** (1997), no. 4, 1238–1244.
[18] ———, *Bounds on spectra of codes with known dual distance*, Des. Codes Cryptogr. **13** (1998), no. 3, 285–297.
[19] ———, *An improved bound on the minimum distance of doubly-even codes*, IEEE Trans. Inform. Theory **46** (2000), no. 1, 274–278.
[20] V. I. Levenshtein, *Universal bounds for codes and designs*, Handbook of Coding Theory (V. Pless and W. C. Huffman, eds.), vol. 1, Elsevier Science, Amsterdam, 1998, pp. 499–648.
[21] S. Litsyn, *New upper bounds on error exponents*, IEEE Trans. Inform. Theory **45** (1999), no. 2, 385–398.
[22] F. J. MacWilliams, *A theorem in the distribution of weights in a systematic code*, Bell Syst. Techn. Journ. **42** (1963), 79–94.
[23] V. M. Sidelnikov, *The spectrum of weights of binary Bose-Chaudhuri-Hocquenghem codes*, Problemy Peredači Informacii **7** (1971), no. 1, 14–22.
[24] D. Slepian, *A class of binary signalling alphabets*, Bell Syst. Techn. Journ. **35** (1956), no. 1, 203–234.
[25] H. Tarnanen, M. J. Aaltonen, and J.-M. Goethals, *On the nonbinary Johnson scheme*, **6** (1985), 279–285.
[26] M. A. Tsfasman and S. G. Vlăduţ, *Geometric approach to higher weights*, IEEE Trans. Inform. Theory **41** (1995), 1564–1588.
[27] S. G. Vlăduţ, *An upper bound for generalized Hamming weights*, Arithmetic, Geometry and Coding Theory (R. Pellikaan and S. G. Vlăduţ, eds.), W. de Gruyter, Berlin, 1996, pp. 263–267.
[28] ———, *Secant spaces and Clifford's theorem over finite fields*, Finite Fields and Applications **4** (1998), 101–111.
[29] V. Wei, *Generalized Hamming weights for linear codes*, IEEE Trans. Inform. Theory **37** (1991), no. 5, 1412–1418.

Bell Labs, Lucent Technologies, 600 Mountain Ave., Rm. 2C-180, Murray Hill, NJ 07974
E-mail address: aea@research.bell-labs.com

Bell Labs, Lucent Technologies, 600 Mountain Ave., Rm. 2C-375, Murray Hill, NJ 07974
E-mail address: abarg@research.bell-labs.com

EE-Systems, Tel Aviv University, 69987 Ramat Aviv , Israel
E-mail address: litsyn@eng.tau.ac.il