Energy bounds for codes and designs in Hamming spaces

Peter Boyvalenkov, Peter Dragnev, Douglas Hardin, Edward B. Saff, Maya Stoyanova

Energy bounds for codes and designs in Hamming spaces

Peter G. Boyvalenkov[1], Peter D. Dragnev[2], Douglas P. Hardin[3], Edward B. Saff[3], and Maya M. Stoyanova[4]

[1] Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 8 G Bonchev Str., 1113 Sofia, Bulgaria,
`peter@math.bas.bg` ⋆

[2] Department of Mathematical Sciences, Indiana-Purdue University Fort Wayne, IN 46805, USA,
`dragnevp@ipfw.edu` ⋆⋆

[3] Center for Constructive Approximation, Department of Mathematics, Vanderbilt University, Nashville, TN 37240, USA
`doug.hardin@vanderbilt.edu, edward.b.saff@vanderbilt.edu` ⋆⋆⋆

[4] Faculty of Mathematics and Informatics, Sofia University, 5 James Bourchier Blvd., 1164 Sofia, Bulgaria,
`stoyanova@fmi.uni-sofia.bg` †

Abstract. We apply linear programming techniques for obtaining lower and upper bounds on the energy of error-correcting codes and for designs in Hamming spaces $H(n,q)$. Our bounds are universal in the sense they hold for a large class of potential functions and allow unified treatment.

1 Introduction

Let $Q = \{0, 1, \ldots, q-1\}$ be the alphabet of q symbols and $H(n,q)$ be the set of all q-ary vectors $x = (x_1, x_2, \ldots, x_n)$ over Q. The Hamming distance $d(x,y)$ between points $x = (x_1, x_2, \ldots, x_n)$ and $y = (y_1, y_2, \ldots, y_n)$ from $H(n,q)$ is equal to the number of coordinates in which they differ. The use of q suggests that the alphabet is a finite field and most coding theory applications assume this but we will not make use of a field structure. In particular q is not necessarily a power of a prime.

⋆ The research of this author was supported, in part, by a Bulgarian NSF contract I01/0003.

⋆⋆ The research of this author was supported, in part, by a Simons Foundation grant no. 282207.

⋆⋆⋆ The research of these authors was supported, in part, by the U. S. National Science Foundation under grants DMS-1109266 and DMS-1412428.

† The research of this author was supported, in part, by the SF of Sofia University under contract "Discrete, algebraic and combinatorial structures", 2015.

It is convenient (cf. [12]) to use the inner product $\langle x, y\rangle := 1 - \frac{2d(x,y)}{n}$ instead of distances. Let $T_n = \{t_0, t_1, \ldots, t_n\}$, where $t_i := -1 + \frac{2i}{n}$, $i = 0, 1, \ldots, n$, are all possible values of inner products in $H(n, q)$, written in decreasing order. We refer to a finite set $C \subset H(n, q)$ as a *code*.

For a given function $h(t) : [-1, 1) \to (0, +\infty)$, we define the *h-energy* (or potential energy) of C by

$$E(n, C; h) := \frac{1}{|C|} \sum_{x,y \in C, x \neq y} h(\langle x, y\rangle).$$

At times we require h to be *absolutely monotone* on [-1,1); i.e., $h^{(k)}(t) \geq 0$ for all $k \geq 0$ and all $t \in [-1, 1)$. Thus our setting is different from the setting in Cohn-Zhao's paper [7] where the authors use the discrete version of absolute monotonicity in T_n. However, in the definition and proof of our universal bounds (Theorems 6 and 7 below) we need $h(t)$ to be defined and absolutely monotone in $[-1, 1)$ instead of T_n. In fact, the discrete version of the absolute monotonicity from [7] follows from the continuous one, and this can be used in a proof of Theorem 6. Furthermore, for the investigation of the asymptotic consequences (as $n \to \infty$) of our bounds, the assumption on the whole interval $[-1, 1)$ seems better suited.

A commonly arising problem (cf. [1–3, 7]) is to minimize the potential energy provided the cardinality $|C|$ of C is fixed; that is, to determine

$$\mathcal{E}(n, M; h) := \min\{E(n, C; h) : |C| = M\},$$

the minimum possible h-energy of a code $C \subset H(n, q)$ of cardinality M.

Energy minimizing codes $C \subset H(n, q)$ for the potential function $h(t) = [2/n(1-t)]^\alpha$, where $\alpha \to \infty$, are maximizing the minimum distance $d(C) := \min\{d(x, y) : x, y \in C, x \neq y\}$ for fixed cardinality $M = |C|$. Another interesting potential function is $f(t) = \gamma^{2/n(1-t)}$, where γ is Bhattacharyya parameter (cf. [13]). Further motivations are given in [1, 7].

In this paper we obtain universal lower bounds for $\mathcal{E}(n, M; h)$ where the universality can be seen in Levenshtein's sense (bounds hold for all dimensions and cardinalities, cf. [12]), as well as in expressions which are common for a large class of potential functions. Moreover, the method of deriving our bounds is based on Hermite interpolation at universally determined nodes that are independent on the particular potential. Our bounds are attained for many well known good codes (e.g. Hamming, Golay, MDS, or Nordstrom-Robinson codes) which are universally optimal in the sense of [7] (see also [1]).

2 Preliminaries

2.1 Designs in $H(n, q)$

We also need the notion of designs (see [9, 12]) in $H(n, q)$.

Definition 1. *Let τ and λ be positive integers. A τ-design $C \subset H(n, q)$ of strength τ and index λ is a code $C \subset H(n, q)$ of cardinality $|C| = M = \lambda q^\tau$ such that the $M \times n$ matrix obtained from the codewords of C as rows has the following property: every $M \times \tau$ submatrix contains all ordered τ-tuples of $H(\tau, q)$, each one exactly $\lambda = \frac{M}{q^\tau}$ times as rows.*

The notion of designs in $H(n, q)$ is a well studied topic in Coding theory since they are, in a certain sense, an approximation of the whole space $H(n, q)$. Here we obtain both lower and upper bounds for their potential energies, which are universal in the sense that the method is independent of the underlying potential function. In particular, the notion of designs is very important in our understanding of the energy problems in $H(n, q)$.

Denote by $\mathcal{L}(n, M, \tau; h) := \min\{E(n, C; h) : |C| = M, C \subset H(n, q)$ is a τ-design$\}$ the minimum possible h-energy of τ-designs in $H(n, q)$ of M points, and by $\mathcal{U}(n, M, \tau; h) := \max\{E(n, C; h) : |C| = M, C \subset H(n, q)$ is a τ-design$\}$ the maximum possible h-energy of τ-designs in $H(n, q)$ of M points. We also consider important to have energy estimates for codes with prescribed minimum distance instead of cardinality (the presence of the minimum distance allows upper bounds on energies as well). Denote by $\mathcal{F}(n, d; h) := \min\{E(n, C; h) : d(C) = d\}$ the minimum possible h-energy of a code $C \subset H(n, q)$ of fixed minimum distance d and by $\mathcal{G}(n, d; h) := \max\{E(n, C; h) : d(C) = d\}$ the maximum possible h-energy of a code $C \subset H(n, q)$ of fixed minimum distance d.

2.2 Rao's bound

For fixed strength τ and dimension n denote

$$B(n, \tau) = \min\{|C| : \exists \ \tau\text{-design } C \subset H(n, q)\}.$$

The classical universal lower bound on $B(n, \tau)$ is due to Rao [14] (see also [9, 8, 12])

$$B(n, \tau) \geq R(n, \tau) = \begin{cases} q \sum_{i=0}^{k-1} \binom{n-1}{i} (q-1)^i, & \text{if } \tau = 2k-1, \\ \sum_{i=0}^{k} \binom{n}{i} (q-1)^i, & \text{if } \tau = 2k. \end{cases}$$

We use the Rao bound to indicate which parameters must be chosen in order to obtain universal lower bounds on $\mathcal{E}(n, M; h)$, $\mathcal{L}(n, M, \tau; h)$ and $\mathcal{F}(n, d; h)$ and upper bounds for $\mathcal{U}(n, M, \tau; h)$ and $\mathcal{G}(n, d; h)$.

2.3 Krawtchouk polynomials

For fixed n and q, the (normalized) Krawtchouk polynomials are defined by

$$Q_i^{(n,q)}(t) := \frac{1}{r_i} K_i^{(n,q)}(n(1-t)/2),$$

where $r_i = (q-1)^i \binom{n}{i}$,

$$K_i^{(n,q)}(d) = \sum_{j=0}^{i} (-1)^j (q-1)^{i-j} \binom{d}{j} \binom{n-d}{i-j}, \quad i = 0, 1, \ldots, n,$$

are the (usual) Krawtchouk polynomials corresponding to $H(n, q)$.

If $f(t) \in \mathbb{R}[t]$ is a real polynomial of degree $m \leq n$, then $f(t)$ can be uniquely expanded in terms of the Krawtchouk polynomials as $f(t) = \sum_{i=0}^{n} f_i Q_i^{(n,q)}(t)$. The coefficients f_i can be found in (at least) two different ways – by direct comparison of the coefficients; or by using the orthogonality relations for the Krawtchouk polynomials.

2.4 Useful quadrature

Levenshtein [10] proves (see also [12, Section 5] and [11]) that for every fixed (cardinality) $M > R(n, 2k-1)$ there exist uniquely determined real numbers $-1 < \alpha_0 < \alpha_1 < \cdots < \alpha_{k-1} < 1$ and positive numbers $\rho_0, \rho_1, \ldots, \rho_{k-1}$, such that the equality

$$f_0 = \frac{f(1)}{M} + \sum_{i=0}^{k-1} \rho_i f(\alpha_i)$$

holds for every real polynomial $f(t)$ of degree at most $2k-1$.

The numbers α_i, $i = 0, 1, \ldots, k-1$, are the roots of the equation

$$P_k(t) P_{k-1}(\alpha_{k-1}) - P_k(\alpha_{k-1}) P_{k-1}(t) = 0,$$

where

$$P_i(t) = \frac{K_i^{(n-1,q)}(d-1)}{\sum_{j=0}^{i} \binom{n}{j} (q-1)^j},$$

$d = n(1-t)/2$. In fact, α_i, $i = 0, 1, \dots, k-1$, are the roots of a certain polynomial used by Levenshten for obtaining bounds on the maximum size of codes of prescribed length n and minimum distance d (see [10, 12]).

In what follows we take care where the cardinality M is located with respect to the Rao bound. We actually always associate M with the corresponding numbers:

$$\alpha_0, \alpha_1, \dots, \alpha_{k-1}, \rho_0, \rho_1, \dots, \rho_{k-1} \text{ when } M \in (R(n, 2k-1), R(n, 2k)]$$

or, analogously, with the corresponding

$$\beta_0, \beta_1, \dots, \beta_k, \gamma_0, \gamma_1, \dots, \gamma_k \text{ when } M \in (R(n, 2k), R(n, 2k+1)]$$

(see [10], [12, Section 5]).

3 General bounds for $\mathcal{E}(n, M; h)$, $\mathcal{F}(n, d; h)$, $\mathcal{L}(n, M, \tau; h)$, $\mathcal{U}(n, M, \tau; h)$ and $\mathcal{G}(n, d; h)$

The next assertion is well known (see [7], also [1, 2]).

Theorem 1. *Let n and h be fixed and $f(t)$ be a real polynomial such that:*

(A1) *$f(t) \le h(t)$ for every $t \in T_n$;*

(A2) *the coefficients in the expansion $f(t) = \sum_{i=0}^{n} f_i Q_i^{(n,q)}(t)$ satisfy $f_i \ge 0$ for every $i \ge 1$.*

Then $\mathcal{E}(n, M; h) \ge f_0 M - f(1)$ for every M.

The next four assertions are more or less immediate corollaries of results already obtained, but are not explicit in the literature. Indeed, the design's property allows relaxation of the conditions on the coefficients in the Krawtchouk expansion (Theorems 2 and 4), and the use of the minimum distance d allows formulations (Theorems 3 and 5) which involve the function $A_q(n, d)$ – the maximum possible cardinality of a code in $H(n, q)$ of minimum distance d.

Theorem 2. *Let n, h and τ be fixed and $f(t)$ be a real polynomial that satisfies* (A1) *and*

(A2′) *the coefficients in the expansion $f(t) = \sum_{i=0}^{n} f_i Q_i^{(n,q)}(t)$ satisfy $f_i \ge 0$ for every $i \ge \tau + 1$.*

Then $\mathcal{L}(n, M, \tau; h) \ge f_0 M - f(1)$ for every $M \ge R(n, \tau)$.

The quantity $\mathcal{F}(n, d; h)$ can be bounded from below in a similar way.

Theorem 3. *Let n, d and h be fixed and $f(t)$ be a real polynomial that satisfies* (A2) *and*

(A1$'$) *$f(t) \le h(t)$ for every $t \in T_n \setminus \{t_i : t_i > 1 - 2d/n\}$;*

Then $\mathcal{F}(n,d;h) \ge f_0 M - f(1)$, where M is a feasible size of a code of minimum distance d. In particular,

$$\mathcal{F}(n,d;h) \ge f_0 A_q(n,d) - f(1).$$

Denote by $A_{n,M;h}$ (respectively $A_{n,M,\tau;h}$ or $B_{n,d;h}$) the set of polynomials that satisfy the conditions (A1) and (A2) (respectively (A1) and (A2$'$) or (A1$'$) and (A2)).

One similarly obtains general upper bounds for $\mathcal{U}(n,M,\tau;h)$ and $\mathcal{G}(n,d;h)$.

Theorem 4. *Let n, M, τ and h be fixed and $g(t)$ be a real polynomial such that:*

(B1) *$g(t) \ge h(t)$ for every $t \in T_n \cap [-1,s]$, where s is such that no τ-design in $H(n,q)$ of M points can have inner products in $T \cap (s,1)$;*

(B2) *the coefficients in the expansion $g(t) = \sum_{i=0}^{n} g_i Q_i^{(n,q)}(t)$ satisfy $g_i \le 0$ for $i \ge \tau + 1$.*

Then $\mathcal{U}(n,M,\tau;h) \le g_0 M - g(1)$.

Theorem 5. *Let n, d and h be fixed and $g(t)$ be a real polynomial such that:*

(B1$'$) *$g(t) \ge h(t)$ for every $t \in T_n \setminus \{t_i : t_i > 1 - 2d/n\}$;*

(B2$'$) *the coefficients in the expansion $g(t) = \sum_{i=0}^{n} g_i Q_i^{(n,q)}(t)$ satisfy $g_i \le 0$ for every $i \ge 1$.*

Then $\mathcal{G}(n,d;h) \le g_0 M - g(1)$, where M is a feasible size of a code of minimum distance d. In particular,

$$\mathcal{G}(n,d;h) \le g_0 A_q(n,d) - g(1).$$

Denote by $B_{n,M,\tau;h}$ (respectively $C_{n,d;h}$) the set of polynomials satisfying the conditions (B1) and (B2) (respectively (B1$'$) and (B2$'$)).

The appearance of s in Theorem 4 is very natural not only from the error-correcting codes point of view. Indeed, good lower bounds on the minimum distance of designs in $H(n,q)$ can be proved.

Theorems 1–5 impose corresponding optimization problems. For example, one may consider the following.

Problem 1. Find polynomial(s) $f \in A_{n,M;h}$ ($f \in A_{n,M,\tau;h}$, $f \in B_{n,d;h}$, respectively) which give maximum value of $f_0 M - f(1) = f_0(M-1) - (f_1 + \cdots + f_n)$.

Problem 2. Find polynomial(s) $g \in B_{n,M,\tau;h}$ ($g \in C_{n,d;h}$, respectively) which give minimum value of $g_0M - g(1) = g_0(M-1) - (g_1 + \cdots + g_n)$.

One more general problem asks for universally optimal codes [2, 7]. Such codes attain the minimum possible energy with respect to all potential functions simultaneously.

4 Obtaining universal bounds

Utilizing Cohn-Zhao's [7] approach to finding good polynomials we use Lagrange interpolation in a set of inner products which correspond to what is called pair covering in [7].

We explain in more detail the odd case $\tau = 2k-1$. We first locate the nodes α_i, $i = 0, 1, \ldots, k-1$, with respect to the elements (the inner products) of T_n. In fact, the α_i's just say which pairs must be covered.

For every $i = 0, 1, \ldots, k-1$, let $t_{j(i)} \leq \alpha_i < t_{j(i)+1}$; i.e., $\alpha_i \in [t_{j(i)}, t_{j(i)+1})$. We assume that

$$t_{j(0)} < t_{j(0)+1} < t_{j(1)} < t_{j(1)+1} < \cdots < t_{j(k-1)} < t_{j(k-1)+1} \tag{1}$$

or adjust the inequalities to have pair covering. Then we apply Lagrange interpolation of $h(t)$ by a polynomial $f(t)$ of odd degree at most $2k-1$ in the points from (1) or its adjustment (which could become Hermite's interpolation at times). This construction implies that the condition (A1) is satisfied. The condition (A2$'$) is trivially satisfied for $\tau = 2k-1$ as well.

Theorem 6. *Let n and $\tau = 2k-1$ be fixed and h be absolutely monotone on $[-1, 1)$. Then*

$$\mathcal{L}(n, M, 2k-1; h) \geq M \sum_{i=0}^{k-1} \rho_i h(\alpha_i). \tag{2}$$

for every $M \in (R(n, 2k-1), R(n, 2k)]$.

Proof. It follows from the argument above that $f(t) \in A_{n,M,2k-1;h}$. We have

$$f_0 = \frac{f(1)}{M} + \sum_{i=0}^{k-1} \rho_i f(\alpha_i) \iff f_0M - f(1) = M \sum_{i=0}^{k-1} \rho_i f(\alpha_i)$$

Since $f(\alpha_i) \geq h(\alpha_i)$ from the interpolation, we obtain

$$f_0M - f(1) \geq M \sum_{i=0}^{k-1} \rho_i h(\alpha_i),$$

which implies the desired bound. $\square$

It can be similarly proved that

$$\mathcal{L}(n,M,2k;h) \geq M\sum_{i=0}^{k}\gamma_i h(\beta_i), \tag{3}$$

for every $M \in (R(n,2k), R(n,(2k+1)]$.

As in [4,5] we utilize the Hermite interpolant of $h(t)$ at the $\{\alpha_i\}$ nodes to derive the same bounds for $\mathcal{E}(n,M;h)$. The positive-definiteness of these Hermite interpolants (and condition (A2)) follows the framework of [6, Section 3], applied to discrete orthogonal polynomials.

Theorem 7. *Let n be fixed and h be absolutely monotone on $[-1,1)$. Then*

$$\mathcal{E}(n,M;h) \geq M\sum_{i=0}^{k-1}\rho_i h(\alpha_i) \tag{4}$$

for $\tau = 2k-1$ and every $M \in (R(n,2k-1), R(n,2k)]$, and

$$\mathcal{E}(n,M;h) \geq M\sum_{i=0}^{k}\gamma_i h(\beta_i) \tag{5}$$

for $\tau = 2k$ and every $M \in (R(n,2k), R(n,2k+1)]$.

Bounds (2)-(5) are not the best possible in particular cases since the pair covering bounds as explained above should be slightly better. However, their universality allows investigations in certain important situations, in particular, asymptotically as n and M tend to infinity.

We remark that all bounds in this section are discrete analogs of bounds on the potential energy of spherical codes and designs recently obtained by the authors [4,5].

5 Examples

There is a unique optimal (nonlinear) binary code of length 10 with 40 codewords and minimum distance 4. We have $q=2$, $n=10$, $N=40$ and $\tau=3$. Our bounds are very close, for example if $h=\frac{2}{10(1-t)}=\frac{1}{5(1-t)}$ then the actual energy is 8.125, the universal bound is ≈ 8.0722, the pair-covering bound is ≈ 8.0857, obtained by

$$\begin{aligned} f(t) &= 0.111t^3 + 0.200t^2 + 0.205t + 0.2 \\ &= 0.220Q_0^{10,2}(t) + 0.236Q_1^{10,2}(t) + 0.180Q_2^{10,2}(t) + 0.080Q_3^{10,2}(t) \end{aligned}$$

(here and below all numbers are truncated after the fourth digit).

There is a unique binary 5-design of 128 points in $H(9,2)$ (here $q=2$, $n=9$, $N=128$ and $\tau=5$). For the potentials $h(t)=\left(\frac{2}{9(1-t)}\right)^s$ and $s=0.1,0.25,0.5,0.75,1,2.5$, respectively, the actual energy is 109.861, 88.593, 62.284, 44.143, 31.546, 5.029, the corresponding universal bound (2) is $\approx$ 109.853, 88.571, 62.236, 44.066, 31.440, 4.828, and the pair-covering bound is $\approx$ 109.858, 88.584, 62.264, 44.111, 31.503, 4.953. For $h(t)=\exp(2t-2)$ the actual energy is 20.6017, the universal bound is ≈ 20.5968, the pair-covering bound is ≈ 20.5992.

All these bounds are valid for codes as well. For example, the above pair-covering bound of ≈ 31.503 (i.e. for $h(t)=\frac{2}{9(1-t)}$) is obtained by the polynomial

$$\begin{aligned} f(t) &= 0.183t^5+0.345t^4+0.284t^3+0.216t^2+0.216t+0.221 \\ &= 0.257Q_0^{9,2}(t)+0.330Q_1^{9,2}(t)+0.366Q_2^{9,2}(t)+0.306Q_3^{9,2}(t) \\ &\quad +0.159Q_4^{9,2}(t)+0.046Q_5^{9,2}(t) \end{aligned}$$

that satisfies the condition (A2) as well. Here, the best lower bound is 31.525 and can be obtained by a polynomial of degree 9

$$\begin{aligned} f(t) &= 0.540t^9-1.041t^7+0.773t^5+0.345t^4+0.171t^3+0.210t^2 \\ &\quad +0.222t+0.222 \\ &= 0.257Q_0^{9,2}(t)+0.330Q_1^{9,2}(t)+0.361Q_2^{9,2}(t)+0.296Q_3^{9,2}(t) \\ &\quad +0.159Q_4^{9,2}(t)+0.0394Q_5^{9,2}(t)+0.005Q_9^{9,2}(t) \end{aligned}$$

that also satisfies (A2).

Acknowledgement. The authors thank to anonymous referee for valuable remarks.

Keywords: Potential functions, h-energy of a code, error-correcting codes, τ-designs.

References

1. A. Ashikhmin, A. Barg, Binomial moments of the distance distribution: bounds and applications, *IEEE Trans. Inform. Theory* 45, 1999, 438-452.
2. A. Ashikhmin, A. Barg, S. Litsyn, Estimates of the distance distribution of codes and designs, *IEEE Trans. Inform. Theory* 47, 2001, 1050-1061.
3. S. Borodachov, D. Hardin, E. Saff, *Minimal Discrete Energy on the Sphere and other Manifolds*, manuscript.

4. P. Boyvalenkov, P. Dragnev, D. Hardin, E. Saff, M. Stoyanova, Universal lower bounds for potential energy of spherical codes, submitted.
5. P. Boyvalenkov, P. Dragnev, D. Hardin, E. Saff, M. Stoyanova, Universal upper and lower bounds on energy of spherical designs, manuscript.
6. H. Cohn, A. Kumar, Universally optimal distribution of points on spheres, *J. of AMS*, **20** no. 1, 2007, 99-148.
7. H. Cohn, Y. Zhao, Energy-minimizing error-correcting codes, arXiv:1212.1913v1, to appear in *IEEE Trans. Inform. Theory.*
8. P. Delsarte, V. I. Levenshtein, Association schemes and coding theory, *Trans. Inform. Theory* 44, 1998, 2477-2504.
9. A. Hedayat, N. J. A Sloane, J. Stufken, *Orthogonal Arrays: Theory and Applications*, Springer-Verlag, New York, 1999.
10. V. I. Levenshtein, Designs as maximum codes in polynomial metric spaces, *Acta Appl. Math.* 25, 1992, 1-82.
11. V. I. Levenshtein, Krawtchouk polynomials and universal bounds for codes and designs in Hamming spaces, *IEEE Trans. Infor. Theory* 41, 1995, 1303-1321.
12. V. I. Levenshtein, Universal bounds for codes and designs, *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds., Elsevier, Amsterdam, 1998, Ch. 6, 499-648.
13. R. J. McElliece, *The Theory of Information and Coding*, Reading MA, Addison-Wesley 1977; (2nd ed. Cambridge Univ. Press 2002).
14. C. R. Rao, Factorial experiments derivable from combinatorial arrangements of arrays, *J. Royal Stat. Soc.* 89, 1947, 128-139.