

BOUNDS FOR CODES ON PENTAGON AND OTHER CYCLES

MARCO DALAI AND YURY POLYANSKIY

ABSTRACT. The capacity of a graph is defined as the rate of exponential growth of independent sets in the strong powers of the graph. In strong power, an edge connects two sequences if at each position letters are equal or adjacent. We consider a variation of the problem where edges in the power graphs are removed among sequences which differ in more than a fraction δ of coordinates. For odd cycles, we derive an upper bound on the corresponding rate which combines Lovász' bound on the capacity with Delsarte's linear programming bounds on the minimum distance of codes in Hamming spaces. For the pentagon, this shows that for $\delta \geq 1 - \frac{1}{\sqrt{5}}$ the Lovász rate is the best possible, while we prove by a Gilbert-Varshamov-type bound that a higher rate is achievable for $\delta < \frac{2}{5}$.

Communication interpretation of this question is the problem of sending quinary symbols subject to $\pm 1 \bmod 5$ disturbance. The maximal communication rate subject to the zero undetected-error equals capacity of a pentagon. The question addressed here is how much this rate can be increased if only a fraction δ of symbols is allowed to be disturbed.

1. INTRODUCTION

The problem we consider in this paper is the following. Given a graph G we define a semimetric on the vertex set $V(G)$

$$d(v, v') = \begin{cases} 0, & v = v', \\ 1, & v \sim v', \\ \infty, & \text{otherwise} \end{cases}.$$

We extend this semimetric additively to the Cartesian products $V(G)^n$ and define a graph $G(n, d)$ as follows

$$V(G(n, d)) = V(G)^n, E(G(n, d)) = \left\{ (x, x') : d(x, x') \triangleq \sum_{j=1}^n d(x_j, x'_j) \leq d \right\}.$$

The goal is to determine (bounds on)

$$R^*(G, \delta) \triangleq \limsup_{n \rightarrow \infty} \frac{1}{n} \log \alpha(G(n, \delta n)).$$

Note that $G(n, d)$ corresponds to the graph obtained by removing in the strong power graph G^n edges between sequences which differ in more than d positions. On one hand, this problem is a specialization of the general one considered in [1] (see Section V.D therein). On the other hand, it is a natural generalization of the two classically studied ones:

M. D. is with the Department of Information Engineering, University of Brescia, Italy, e-mail: marco.dalai@unibs.it. Y.P. is with the Department of EECS, MIT, Cambridge, MA, email: yp@mit.edu. This material is based upon work supported by the National Science Foundation under Grant No CCF-13-18620. The work was mainly completed while the authors were visiting the Simons Institute for the Theory of Computing at UC Berkeley, whose support is gratefully acknowledged.

- (1) Shannon capacity of a graph [2], which corresponds to $\delta = 1$. The best general upper bound is [3]

$$R^*(G, 1) \leq \log \theta_L(G), \quad (1)$$

where θ_L is the Lovasz's θ -function (see below).

- (2) Rate-Distance tradeoff in Hamming spaces corresponds to $G = K_q$ (the clique). Here the two bounds we mention are

$$R_{GV}(q, \delta) \leq R^*(K_q, \delta) \leq R_{LP1}(q, \delta), \quad (2)$$

where for $\delta < 1 - \frac{1}{q}$

$$R_{GV}(q, \delta) \triangleq \log q - H_q(\delta) \quad (3)$$

$$R_{LP1}(q, \delta) \triangleq H_q \left(\frac{(q-1) - (q-2)\delta - 2\sqrt{(q-1)\delta(1-\delta)}}{q} \right), \quad (4)$$

$$H_q(x) \triangleq x \log(q-1) - x \log x - (1-x) \log(1-x), \quad (5)$$

and for $\delta \geq 1 - \frac{1}{q}$ both R_{GV} and R_{LP1} equal zero. (Better bounds also exist: an improved upper bound for small δ 's was found by Aaltonen [4], and an improved lower bound for large q 's and some range of δ 's is shown via algebraic-geometric codes [5].)

The main contribution of this work is an upper bound on $R^*(G, \delta)$ for the case of $G = C_q$ (a q -cycle, $q \geq 3$ -odd). Namely, we prove:

$$R^*(C_q, \delta) \leq \log \theta_L(C_q) + R_{LP1}(q', \delta), \quad q' = 1 + \frac{1}{\cos \pi/q} \leq q. \quad (6)$$

Note that, for $q > 3$, q' is not an integer, and $R_{LP1}(q', \delta)$ can no longer be thought of as a rate upper bound for Hamming space. Also note that $\theta_L(C_q) = \frac{q}{q'}$ and so (informally speaking) the upper bound decomposes C_q^n into disjoint $\left(\frac{q}{q'}\right)^n$ copies of imaginary Hamming spaces with fractional q' , inside which one can additionally pack exponentially many points at minimum distance δ . As in the ordinary linear programming bound, the derivation of the bound goes through the use of Krawtchouk polynomials; to the best of our knowledge, this is the first appearance of these polynomials with a non-integer coefficient in coding theory or combinatorics.

We also give some lower bounds; in particular, for the pentagon we prove

$$\frac{1}{2} \log 5 + \frac{1}{2} R_{GV}(5, 2\delta) \leq R^*(C_5, \delta) \leq \frac{1}{2} \log 5 + R_{LP1}(\sqrt{5}, \delta). \quad (7)$$

2. MINIMUM DISTANCE OF CODES ON CYCLES

In the rest of the paper, we will focus on cycles. Let for ease of notation $C_q = \mathbb{Z}/q\mathbb{Z}$, be a ring and a graph (the q -cycle) simultaneously. A code $\mathcal{C}$ is a subset of C_q^n and its minimum distance is defined as usual

$$d_{\min}(\mathcal{C}) = \min_{c \neq c' \in \mathcal{C}} d(c, c'). \quad (8)$$

Let $M_q(n, d)$ be the size of the largest code of length n with minimum distance at least d , i.e. set $M_q(n, d) = \alpha(C_q(n, d-1))$.

2.1. Even Cycles. For even cycles, the problem is equivalent to the ordinary binary case with Hamming distance.

Proposition 1. *For even q , we have*

$$M_q(n, d) = (q/2)^n M_2(n, d). \quad (9)$$

and hence

$$R^*(C_q, \delta) = \log(q/2) + R^*(K_2, \delta). \quad (10)$$

Proof. For any $v \in \mathbb{Z}_{q/2}^n$, consider the sequence of edges indexed by v

$$\mathcal{E}_v = \bigtimes_{i=1}^n \{2v_i, 2v_i + 1\}. \quad (11)$$

There are $(q/2)^n$ such sets, and each codeword is contained in one of them. Hence, for a given q -ary code $\mathcal{C}$ which achieves $M_q(n, d)$, one of those sets contains at least $\lceil M_q(n, d)(q/2)^{-n} \rceil$ codewords. Since these codewords are all at finite distance with one another, they must differ in at least d positions, and they can be mapped to binary codewords preserving pairwise distances. Hence, $\lceil M_q(n, d)(q/2)^{-n} \rceil \leq M_2(n, d)$, implying $M_q(n, d) \leq (q/2)^n M_2(n, d)$.

Conversely, let $\mathcal{C}' \subseteq \{0, 1\}^n$ be any binary code achieving $M_2(n, d)$. Let $\mathcal{C} = \{0, 2, \dots, q-2\}^n$ and define the code

$$\mathcal{C}^+ = \mathcal{C} + \mathcal{C}' \quad (12)$$

Consider two distinct codewords $x^+ = x + x'$ and $y^+ = y + y'$ in $\mathcal{C}^+$. If $x' = y'$ then $x \neq y$ and $d(x^+, y^+) = \infty$. Otherwise, $x^+ - y^+$ contains at least d odd components and thus $d(x^+, y^+) \geq d$. Since $|\mathcal{C}| = (q/2)^n M_2(n, d)$, we deduce that $M_q(n, d) \geq (q/2)^n M_2(n, d)$. Note that the construction of $\mathcal{C}^+$ is a particular case of the general one discussed in Section 2.4 below. $\square$

2.2. Odd cycles. Proposition 1 relies on the fact that, for even n , the clique covering number of C_q^n equals its independence number. For odd cycles, a straightforward attempt along the same line only gives a much weaker result.

Proposition 2. *For odd q , we have*

$$\log((q-1)/2) + R^*(K_2, \delta) \leq R^*(C_q, \delta) \leq \log(q/2) + R^*(K_2, \delta). \quad (13)$$

Proof. The first inequality is trivial, since any δ -code for C_{q-1}^n is a δ -code for C_q^n . To prove the upper bound, let $\bar{\chi}(C_q^n)$ be the clique covering number of C_q^n . Any code achieving $M_q(n, d)$ has at least $\lceil M_q(n, d)/\bar{\chi}(C_q^n) \rceil$ codewords in the same clique and these codewords all lie in the same edge in each position. So, they can be mapped to a binary code and thus $\lceil M_q(n, d)/\bar{\chi}(C_q^n) \rceil \leq M_2(n, d)$. As $n \rightarrow \infty$, $\bar{\chi}(C_q^n)^{1/n}$ tends to $\bar{\chi}^*(C_q) = q/2$, the fractional clique covering number of the cycle. Taking logarithms and dividing by n we deduce $R_q(\delta) \leq \log(q/2) + R_2(\delta)$. $\square$

Remark 1. *Proposition 2 implies that, for large q ,*

$$R^*(C_q, \delta) = \log(q/2) + R^*(K_2, \delta) + \mathcal{O}(1/q). \quad (14)$$

Proposition 2 gives poor results for large values of δ . In particular, the upper bound becomes weaker than Lovász' result

$$R^*(C_q, 1) \leq \log \theta_L(C_q), \quad \theta_L(C_q) = \frac{q \cos(\pi/q)}{1 + \cos(\pi/q)}. \quad (15)$$

The first question we address is the following: Is it possible to show $R^*(C_q, \delta) \leq \log \theta_L(C_q)$ for some $\delta < 1$? That is, can we give a tighter bound on the ‘Plotkin’ point? The answer is yes and we can do so without the (heavier) machinery needed for (6).

Our upper bounds require computing θ -functions. We define three variations of those as follows (see [6], [3] and [7])

$$\theta_S(G) \triangleq \min\left\{\max_{v \in V(G)} D_{v,v} : D \succeq J, D|_{E(\bar{G})} \leq 0\right\} \quad (16)$$

$$\theta_L(G) \triangleq \min\left\{\max_{v \in V(G)} D_{v,v} : D \succeq J, D|_{E(\bar{G})} = 0\right\} \quad (17)$$

$$\theta_z(G) \triangleq \min\left\{\max_{v \in V(G)} D_{v,v} : D \succeq J, D|_{E(\bar{G})} = 0, D_{v,v'} \geq 0\right\}, \quad (18)$$

where D is $|G| \times |G|$ matrix and J is a matrix of all ones. These stand for the Schrijver, Lovász and Szegedy's θ -functions respectively.

Proposition 3. *We have*

$$\theta_S(G(n, d)) \leq \theta_z(G)^n \theta_S(K_{|G|}, d). \quad (19)$$

Proof. We prove a more general result: Let G and H be graphs with the same vertex sets $V(G) = V(H)$, then

$$\theta_S(G \cap H) \leq \theta_z(G) \theta_S(H), \quad (20)$$

where $G \cap H$ denotes a graph obtained by intersecting edge-sets $E(G) \cap E(H)$. Let D_1 and D_2 be solutions in (18) and (16) for the graphs G and H , respectively. Then,

$$D_{v,v'} \triangleq (D_1)_{v,v'} (D_2)_{v,v'},$$

i.e. $D = D_1 \odot D_2$, is a feasible choice for $\theta_S(G \cap H)$. Indeed, by property of Schur product of matrices

$$(D_1 - J) \odot (D_2 - J) \succeq 0,$$

and expanding the left-hand side we get $D \succeq J$ as required. The condition $D_{E(\overline{G \cap H})}$ is satisfied trivially.

To complete the proof of the proposition one only needs to notice that by taking tensor-power of a solution D for $\theta_z(G)$ we get $\theta_z(G^n) \leq \theta_z(G)^n$.

Finally, to derive (19) from (20) we note that

$$G(n, d) = G^n \cap K_{|G|}(n, \delta n),$$

where G^n denotes the strong-product power. □

Notice that for cycles

$$\theta_z(C_q) = \theta_L(C_q).$$

Therefore, Proposition 3 implies the following.

Corollary 1.

$$R^*(C_q, \delta n) \leq \log \theta_L(C_q) + R_{LP1}(q, \delta).$$

This shows that $R^*(C_q, \delta) \leq \log \theta_L(C_q)$ for $\delta \geq 1 - 1/q$, improving (15). While Proposition 2 is weak for large δ , Corollary 1 becomes quickly rather weak as δ decreases from $(q - 1)/q$. We next proceed to our main result, which improves Corollary 1 and gives a bound uniformly good at all values of δ .

Theorem 1.

$$R^*(C_q, \delta) \leq \log \theta_L(C_q) + R_{LP1}(q', \delta), \quad q' = 1 + \frac{1}{\cos \pi/q} \leq q. \quad (21)$$

Proof. The bound is based on θ functions and Delsarte's linear programming bound [8], but it is easier to describe in terms of Fourier transforms. To that end we identify C_q with the ring $\mathbb{Z}/q\mathbb{Z}$.

For any $f : C_q^n \rightarrow \mathbb{C}$ we define its Fourier transform as

$$\hat{f}(\omega) = \sum_{x \in C_q^n} f(x) e^{\frac{2\pi i}{q} \langle \omega, x \rangle}, \quad \omega \in C_q^n$$

where the non-degenerate C_q -valued bilinear form is defined as usual

$$\langle x, y \rangle \triangleq \sum_{i=1}^n x_i y_i.$$

We also define the inner product as follows

$$(f, g) \triangleq q^{-n} \sum_{x \in C_q^n} \bar{f}(x) g(x).$$

The starting point is a known rephrasing of linear programming bounds. Let $\mathcal{C}$ be a code with minimum distance at least d . Let f be such that $f(x) \leq 0$ if $d(x, 0) \geq d$, $\hat{f} \geq 0$ and $\hat{f}(0) > 0$. Then, consider the Plancherel identity

$$(f * 1_{\mathcal{C}}, 1_{\mathcal{C}}) = q^{-n} (\hat{f} \cdot \widehat{1_{\mathcal{C}}}, \widehat{1_{\mathcal{C}}}), \quad (22)$$

where 1_A is the indicator function of a set A . Upper bounding the left hand side by $|\mathcal{C}|f(0)$ and lower bounding the right hand side by the zero-frequency term $q^{-n}\hat{f}(0)|\mathcal{C}|^2$, one gets

$$|\mathcal{C}| \leq \min \left\{ q^n \frac{f(0)}{\hat{f}(0)} : f(x) \leq 0 \text{ for } d(x, 0) \geq d, \hat{f} \geq 0, \hat{f}(0) > 0 \right\}. \quad (23)$$

The proof of our theorem is based on an assignment f which combines Lovász' choice used to obtain (1) with the one used in [9] to obtain (2).

Observe first that Lovász assignment can be written in one dimension ($n = 1$) as

$$g_1(x) = 1_0(x) + \varphi 1_{\pm 1}(x), \quad x \in C_q,$$

where $\varphi = (2 \cos(\pi/q))^{-1}$. This gives

$$\hat{g}_1(\omega) = 1 + 2\varphi \cos(2\pi\omega/q), \quad \omega \in C_q. \quad (24)$$

Correspondingly, define the n -dimensional assignment

$$g(x) = \prod_{j=1}^n g_1(x_j), \quad \hat{g}(\omega) = \prod_{j=1}^n \hat{g}_1(\omega_j), \quad x, \omega \in C_q^n.$$

Note that $\hat{g}_1 \geq 0$ and, additionally, $\hat{g}_1(\omega) = 0$ for $\omega = \pm c$, with $c = (q-1)/2$. So, $\hat{g} \geq 0$, with $g(\omega) = 0$ if ω contains any $\pm c$ entry. Since $g(x) = 0$ for $x \notin \{0, \pm 1\}^n$, g satisfies all the properties required for f in the case $d = \infty$, and when used in (23) it gives Lovász' bound

$$|\mathcal{C}| \leq q^n \frac{g(0)}{\hat{g}(0)} \quad (25)$$

$$= q^n \left(\frac{\cos(\pi/q)}{1 + \cos(\pi/q)} \right)^n \quad (26)$$

for codes of infinite minimum distance.

For the case of finite $d \leq n$, we build a function f of the form $f(x) = g(x)h(x)$, for an appropriate $h(x)$. In particular, since $g(x)$ is non-negative and already takes care of setting $f(x)$ to zero if $x \notin \{0, \pm 1\}^n$, it suffices to choose h such that $h(x) \leq 0$ whenever $x \in \{0, \pm 1\}^n$ contains at least d entries with value ± 1 . We restrict

attention to h such that $\hat{h} \geq 0$, so that $\hat{f} = q^{-n} \hat{g} * \hat{h} \geq 0$. In particular, we consider functions h whose Fourier transform is constant on each of the following “spheres” in C_q^n

$$S_\ell^c = \{x : |\{i : x_i = \pm c\}| = \ell, |\{i : x_i = 0\}| = n - \ell\}, \quad \ell = 0, \dots, n,$$

and zero outside. This choice is motivated by the fact, observed before, that $\hat{g}_1(\pm c) = 0$. Restricting $\hat{h}$ to be null out of these spheres simplifies the problem considerably. We thus define

$$\hat{h}(\omega) = \sum_{\ell=0}^n \hat{h}_\ell 1_{S_\ell^c}(\omega), \quad h(x) = q^{-n} \sum_{\ell=0}^n \hat{h}_\ell \widehat{1_{S_\ell^c}}(x), \quad (27)$$

where $\hat{h}_\ell \geq 0$ and $\hat{h}_0 > 0$ will be optimized later. Since $\hat{g}(\omega) = 0, \omega \in S_\ell, \ell > 0$, setting $f(x) = g(x)h(x)$ gives $\hat{f}(0) = q^{-n}(\hat{g} * \hat{h})(0) = q^{-n}\hat{g}(0)\hat{h}_0$. So, the bound (23) becomes

$$|\mathcal{C}| \leq \left(q^n \frac{g(0)}{\hat{g}(0)} \right) \left(q^n \frac{h(0)}{\hat{h}_0} \right). \quad (28)$$

The first term above is precisely Lovász bound and corresponds the first term in the right hand side of (21). We now show that the second term corresponds to the linear programming bound of an imaginary “Hamming scheme” with a special non-integer alphabet size $q' = 1 + \cos(\pi/q)^{-1}$. To do this, define analogously to S_ℓ^c the spheres

$$S_u^1 = \{x : |\{i : x_i = \pm 1\}| = u, |\{i : x_i = 0\}| = n - u\}.$$

Our constraint is that $h(x) \leq 0$ if $x \in S_u^1, u \geq d$. Direct computation shows that for $x \in S_u^1$,

$$\widehat{1_{S_u^1}}(x) = \sum_{j=0}^u \binom{u}{j} \binom{n-u}{\ell-j} (-1)^j 2^\ell (\cos(\pi/q))^j, \quad (x \in S_u^1) \quad (29)$$

$$= (2 \cos(\pi/q))^\ell K_\ell(u; q'), \quad (q' = 1 + \cos(\pi/q)^{-1}), \quad (30)$$

where $K_\ell(u; q')$ is a Krawtchouck polynomial of degree ℓ and parameter q' in the variable u . Setting

$$H(u) = h(x), x \in S_u^1, \quad \hat{H}_\ell = q^{-n} (2 \cos(\pi/q))^\ell \cdot \hat{h}_\ell, \quad (31)$$

we have

$$q^n \frac{h(0)}{\hat{h}_0} = \frac{H(0)}{\hat{H}_0}, \quad (32)$$

where the conditions on h can be restated as

$$H(u) = \sum_{\ell=0}^n \hat{H}_\ell K_\ell(u; q'), \quad u = 0, \dots, n, \quad (33)$$

$$\hat{H}_\ell \geq 0, \quad \ell \geq 0, \quad (34)$$

$$H(u) \leq 0, \quad u \geq d. \quad (35)$$

So, the minimization of (32) is reduced to the standard linear programming problem for the Hamming space, though with a non-integer parameter q' . Since the construction of the polynomial used in [9] and [4] can be applied verbatim for non-integer values of q' (see also [10] for the position of the roots of $K_\ell(u; q')$), the claimed bound follows. $\square$

2.3. On improving bounds on the “Plotkin” point. We note that the bound (21) matches Lovasz’s (15) when $\delta > 1 - 1/q'$. Here we show that this threshold cannot be reduced with assignments of the type $f(x) = g(x)h(x)$ unless one chooses $h(x)$ to be a high degree polynomial. Indeed, going back to the proof of Theorem 1 we notice that (from symmetry) without loss of generality we can seek h among assignments of the type

$$h(x) = \sum_{u=0}^n H(u) 1_{S_u^1}(x), \quad \forall x \in \{0, \pm 1\}^n, \quad (36)$$

and the values at $x \notin \{0, \pm 1\}^n$ are immaterial. Here $H(u)$ is a degree $\leq n$ polynomial satisfying

$$H(u) \leq 0 \quad \forall u \in [\delta n, n] \cap \mathbb{Z} \quad (37)$$

and a set of linear constraints, encoded in

$$\hat{g} * \hat{h} \geq 0, \quad \hat{g} * \hat{h}(0) > 0. \quad (38)$$

For any such H we get the bound (after simple manipulations)

$$|C| \leq \theta_L(C_q)^n \cdot \frac{H(0)}{\mathbb{E}[H(U)]}, \quad U \sim \text{Bino}\left(n, 1 - \frac{1}{q'}\right). \quad (39)$$

Next, let us (as is done customarily) impose a stronger constraint on H namely that

$$H(u) \leq 0 \quad \forall u \in [\delta n, n]. \quad (40)$$

We want to show that every polynomial H of degree $\leq 2r$ satisfying (40) for $\delta < 1 - \frac{1}{q'}$ must have $\mathbb{E}[H(U)] \leq 0$ for $n \gg 1$ and thus will violate (38). This is a standard result in orthogonal polynomials, see [11, Lemma 2] for its appearance in regards to linear-programming bounds. Indeed, it is known since Gauss that there exists a discrete measure P_V with r atoms located in the roots of $K_r(\cdot; q')$ such that for any polynomial of degree $\leq 2r$ we have

$$\mathbb{E}[H(U)] = \mathbb{E}[H(V)].$$

Since all roots of K_r converge to $n\left(1 - \frac{1}{q'}\right) + o(n)$ as $n \rightarrow \infty$ we deduce from (40) that, if $\delta < 1 - \frac{1}{q'}$, $\mathbb{E}[H(U)] \leq 0$. Similarly, it can be shown that the MRRW choice used in Theorem 1 is optimal in the sense of minimizing the degree of H for a given distance, cf. [11].

As a closing remark, notice that a choice of H in Theorem 1 in addition to (38), (40) was further restricted to positive sums of Krawtchouk polynomials, cf. (34), which is stronger than (38). However, [11, Theorem 3] shows that this extra restriction does not affect the bounds, unless one goes beyond the minimal-degree (MRRW) choice. Further improvements may be more easily obtained by addressing constraint (37) via Elias-method (as is done in the second linear programming bounds, cf. [4]).

2.4. Achievability results. In this section we prove some lower bounds on $R^*(C_q, \delta)$ and in particular the left-hand side inequality (7). To that end we consider the following general method of producing new codes from old. We note that cycles C_q are in fact Cayley graphs on an abelian group, and so the next definitions are rather natural.

Let Γ be an abelian group with weight function $w : \Gamma \rightarrow \mathbb{R}_+ \cup \{+\infty\}$ s.t. $w(x) = 0 \iff x = 0$. We define the translation-invariant semi-metric $d(x, y) = w(x - y)$. ($d(\cdot, \cdot)$ is a metric when $w(-x) = w(x)$ and $w(a + b) \leq w(a) + w(b)$, which is the case for the Hamming weight on $\mathbb{F}_q^n$, for example.) We will say that (Γ_1, w_1) is isomorphic to (Γ_2, w_2) if there exists a surjective group isometry $\Gamma_1 \rightarrow \Gamma_2$.

Given a $\mathcal{C}$ that is a subgroup of Γ we form a *factor group* $\Gamma' = \Gamma/\mathcal{C}$ as a group of cosets of $\mathcal{C}$ and define a *factor-weight* on the space of cosets as

$$w'(\gamma' + \mathcal{C}) \triangleq \min_{\gamma \in \gamma' + \mathcal{C}} w(\gamma).$$

It is clear now that if $\mathcal{C}'$ is a code in (Γ', w') then the union of cosets $\mathcal{C}' + \mathcal{C}$ is a code of minimum distance (in (Γ, w)) equal to

$$d_{\min}(\mathcal{C}' + \mathcal{C}) = \min\{d_{\min}(\mathcal{C}), d_{\min}(\mathcal{C}')\}. \quad (41)$$

We now need the following result for the particular case of the pentagon.

Proposition 4. *Consider $\Gamma = \mathbb{F}_5^n$ with weight $w(x) = \infty$ if $x_j = \pm 2 \pmod{5}$ for any $j \in [n]$ and otherwise $w(x)$ is the Hamming weight of $x \in \mathbb{F}_5^n$. Let $n = 2k$ and take $\mathcal{C}$ to be the $\mathbb{F}_5$ -row span of the matrix $[1, 2] \otimes I_k$. The code $\mathcal{C}$ has rate $\frac{1}{2} \log 5$ and minimum distance ∞ . The factor-space (Γ', w') is isomorphic to the Hamming space $\mathbb{F}_5^k$ with Hamming weight.*

Proof. The minimum distance of $\mathcal{C}$ is verified easily: any non-zero $\mathbb{F}_5$ -multiple of $[1, 2]$ has an entry $\pm 2 \pmod{5}$. It is a standard fact that $\mathcal{C}$ is the code achieving the zero-error capacity of a pentagon.

To show the isomorphism, first consider the case $n = 2, k = 1$. Every vector in $\mathbb{F}_5^2$ can be written in coordinates

$$x = a[1, 2] + b[0, 1], \quad a, b \in \mathbb{F}_5.$$

Then for a factor weight of such x we have

$$w'(x + \mathcal{C}) \triangleq \min_{a_1 \in \mathbb{F}_5} w(a_1[1, 2] + b[0, 1]).$$

When $b = \pm 1$ we take $a_1 = 0$ and when $b = \pm 2$ we take $a = -b$. In this way, we get

$$w'(x + \mathcal{C}) = \begin{cases} 0, & x \in \mathcal{C} \\ 1, & x \notin \mathcal{C}. \end{cases}$$

Since there are 5 cosets, (γ', w') is isomorphic to a one-dimensional Hamming space $\mathbb{F}_5$. The general case of $k > 1$ follows by vectorizing this argument. $\square$

Equation (41) combined with Proposition 4 implies the following theorem, from which we get the bound (7) by application of the Gilbert-Varshamov bound for $\mathbb{F}_5^k$, see (2), to construct the code $\mathcal{C}'$ in the factor-space.

Theorem 2. *We have*

$$R^*(C_5, \delta) \geq \frac{1}{2} \log 5 + \frac{1}{2} R^*(K_5, 2\delta). \quad (42)$$

By a similar procedure, we can derive achievability bounds for other cycles. For example, when $q = 2^r + 1$, by using a maximal independent set in C_q^r presented in [12, Th. 3], we get the following estimation which generalizes Theorem 2.

Proposition 5. *For $q = 2^r + 1$, we have*

$$R^*(C_q, \delta) \geq \frac{r-1}{r} \log q + \frac{1}{r} R^*(K_q, r\delta). \quad (43)$$

Proof. For any n , consider the group C_q^n with weight $w(x) = \infty$ if $x \notin \{0, \pm 1\}^n$ and $w(x)$ is the Hamming weight of x if $x \in \{0, \pm 1\}^n$. We build a code of length $n = kr$ and show that, as $k \rightarrow \infty$, we can achieve (43). The construction is similar to the one used in Theorem 2 for the particular case $r = 2$, with the difference that we now only use the Hamming weight on the factor group as a lower bound for the factor-weight, since the factor groups is not isometric to a Hamming space for $r > 2$.

As shown in [12, Th. 3], the following set

$$\mathcal{C}_1 = \{(a_1, \dots, a_r) : a_i \in C_q, a_r = 2a_1 + 4a_2 + \dots + 2^{r-1}a_{r-1}\} \quad (44)$$

is a maximal independent set of C_q^r . Note that by maximality the factor weight on $C_q^r/\mathcal{C}_1$ is finite. Hence, we can consider an infinite distance code $\mathcal{C} \subset C_q^{rk}$ with rate $(1 - 1/r) \log q$ as the row-“span”¹ of the matrix

$$G = \begin{bmatrix} & 2I_k \\ & 4I_k \\ I_{(r-1)k}, & \vdots \\ & 2^{r-1}I_k \end{bmatrix}, \quad (45)$$

where I_m is again the $m \times m$ identity matrix. The factor group Γ' is homomorphic to C_q^k and admits the representation

$$[x'] = (0, 0, \dots, 0, x') + \mathcal{C}, \quad x' \in C_q^k, \quad (46)$$

where there are $(r-1)k$ concatenated zeros. We see that, using this representation, any $x' \in C_q^k$ with Hamming weight d gives a class $[x']$ with factor weight at least d . In fact, in the sum in (46), due to the structure of G above if a codeword in $\mathcal{C}$ cancels say t non-zero elements in x' , then it contains at least t non zero components in the first $(r-1)k$ positions. Hence, any q -ary code of length k and minimum Hamming distance d gives, under the representation in (46), a code $\mathcal{C}' \subset \Gamma'$ with factor weight at least d . Setting $d = \lceil r\delta \rceil$ and using the Gilbert-Varshamov bound for codes in C_q^k we get the statement of the theorem. $\square$

Note that Proposition 5 is not uniformly better than Proposition 2 with the Gilbert-Varshamov bound (see Figure 2 below). However, the bound can be improved for specific r using appropriate bounds for the minimum distance of codes in the factor group with the exact factor-weight. For example, in the case $r = 3$ (the 9-cycle), we have the following improved bound, also plotted in Figure 2 below.

Proposition 6. *For $q = 9$ (that is, $r = 3$), we have*

$$R^*(C_q, \delta) \geq \frac{r-1}{r} \log q + \frac{1}{r} R'(r\delta). \quad (47)$$

with $R'(\delta) = 0$ if $\delta > 10/9$ and otherwise $R'(\delta) = \log(9) - H(P)$, where P is the distribution defined by

$$P = \frac{(1, t, t, t^2, t, t, t^2, t, t)}{1 + 6t + 2t^2}, \quad (48)$$

t being the positive solution of the equation

$$2t^2(2 - \delta) + 6t(1 - \delta) - \delta = 0. \quad (49)$$

Proof. The proof is the same as for Proposition 5 but we use the exact factor-weight in the Gilbert-Varshamov bound for codes in the factor group $C_q^{rk}/\mathcal{C}$. In particular, for $r = 3$ it is not too difficult to see that the factor weight w' in $C_q^r/\mathcal{C}_1$ satisfies

$$w'(0) = 0, w'(1) = w'(2) = w'(4) = w'(5) = w'(7) = w'(8) = 1, w'(3) = w'(6) = 2. \quad (50)$$

Since $C_q^{rk}/\mathcal{C}$ is homomorphic to C_q^k (consider again representation (46)), we can build codes in the factor group using the standard Gilbert-Varshamov procedure with the exact factor-weight. Then one deduces (see for example [13] or [14])

¹Here the “span” is intended with coefficients in C_q , where multiplication is mod q , but q need not be a prime.

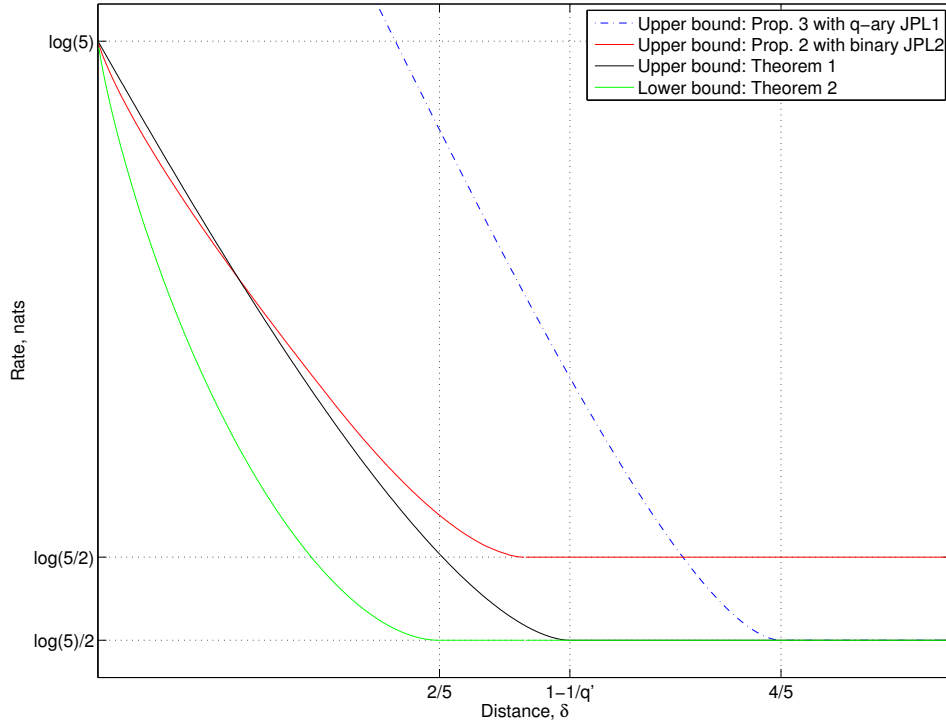


FIGURE 1. Comparison of different bounds for the pentagon.

the existence of codes with asymptotic minimum normalized distance $r\delta$ and rate $R \geq \log(9) - H(P)$, where P is the distribution with maximum entropy satisfying

$$\sum_{x \in C_q} P(x)w'(x) \leq r\delta. \quad (51)$$

Using Lagrange multipliers one deduces that the maximizing distribution is uniform if $r\delta \geq 10/9$ while for $r\delta < 10/9$ it has the form

$$P(x) = \frac{e^{-\lambda w'(x)}}{\sum_{x'} e^{-\lambda w'(x)}}, \quad (52)$$

where λ is chosen so that (51) is satisfied with equality. Simple algebraic manipulations then give the claimed bound. $\square$

3. EVALUATION AND DISCUSSION

Figures 1 and 2 compare various bounds obtained for the pentagon and for the 9-gon, respectively (all logs are to the base e). We observe that the upper bound derived from Proposition 2 with the use of a second linear programming bound outperforms Theorem 1 at low values of δ (a similar result is obtained even just using the Elias bound in Proposition 2, see also [1, Sec. V.D]). This is not surprising since Theorem 1 is based on the so called first linear programming bound of [9], which is known to be rather weak at high rates. It is an open question whether our technique (in particular working with non-integer q) can be extended to replace R_{LP1} in (7) with R_{LP2} derived by Aaltonen [4] for the q -ary Hamming scheme.

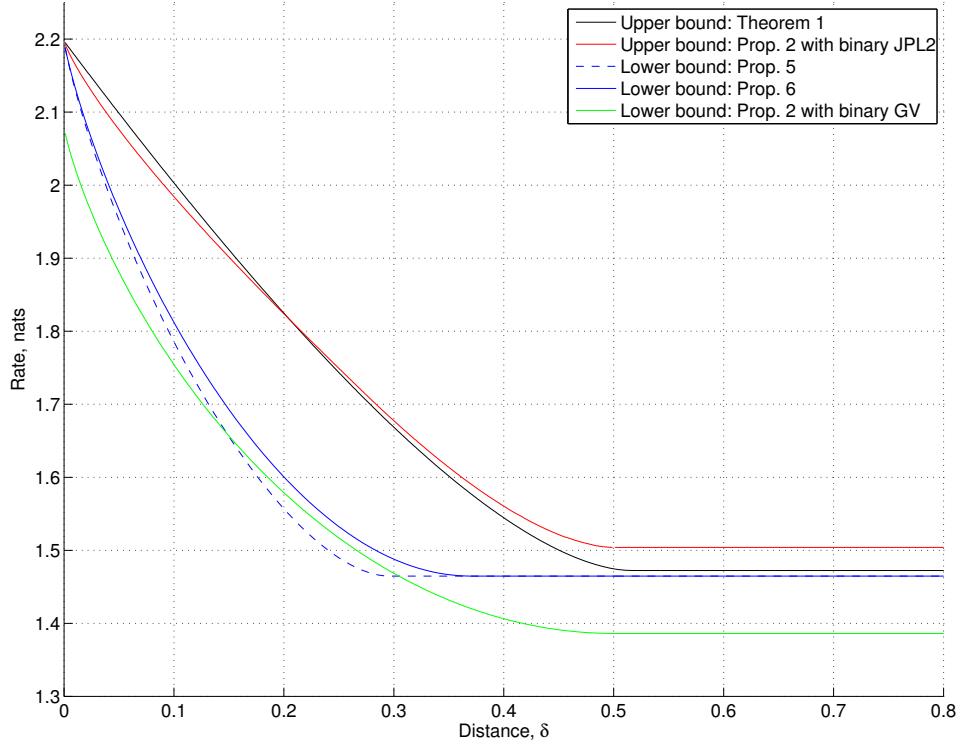


FIGURE 2. Comparison of different bounds for the 9-cycle.

REFERENCES

- [1] M. Dalai, “Elias Bound for General Distances and Stable Sets in Edge-Weighted Graphs,” *IEEE Trans. Inform. Theory*, vol. 61, no. 5, pp. 2335–2350, May 2015.
- [2] C. E. Shannon, “The Zero-Error Capacity of a Noisy Channel,” *IRE Trans. Inform. Theory*, vol. IT-2, pp. 8–19, 1956.
- [3] L. Lovász, “On the Shannon Capacity of a Graph,” *IEEE Trans. Inform. Theory*, vol. 25, no. 1, pp. 1–7, 1979.
- [4] M. Aaltonen, “A new upper bound on nonbinary block codes,” *Discrete Mathematics*, vol. 83, no. 2, pp. 139–160, 1990.
- [5] M. A. Tsfasman, S. Vlăduț, and T. Zink, “Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound,” *Mathematische Nachrichten*, vol. 109, no. 1, pp. 21–28, 1982.
- [6] A. Schrijver, “A comparison of the Delsarte and Lovász bounds,” *IEEE Trans. on Inform. Theory*, vol. 25, no. 4, pp. 425 – 429, jul 1979.
- [7] M. Szegedy, “A note on ϑ number of Lovász and the generalized delsarte bound,” in *35th Symposium on Foundations of Computer Science*, I. C. S. Press, Ed., 1994, pp. 36–39.
- [8] P. Delsarte, “An Algebraic Approach to the Association Schemes of Coding Theory,” *Philips Res. Rep.*, vol. 10, 1973.
- [9] R. McEliece, E. Rodemich, H. Rumsey, and L. Welch, “New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities,” *Information Theory, IEEE Transactions on*, vol. 23, no. 2, pp. 157 – 166, mar 1977.
- [10] M. E. H. Ismail and P. Simeonov, “Strong Asymptotics for Krawtchouk Polynomials,” *J. Comput. Appl. Math.*, vol. 100, no. 2, pp. 121–144, 1998.
- [11] V. Sidelnikov, “Extremal polynomials used in bounds of code volume,” (*in Russian*) *Probl. Peredachi Inform.*, vol. 16, no. 3, pp. 17–30, 1980.
- [12] L. D. Baumert, R. J. McEliece, E. Rodemich, R. H. C. Jr., R. Stanley, and H. Taylor, “A Combinatorial Packing Problem,” *Proc. SIAM AMS*, vol. 4, pp. 97–108, 1971.
- [13] E. Berlekamp, *Algebraic Coding Theory*, ser. McGraw-Hill series in systems science. Aegean Park Press, 1984.

- [14] P. Piret, “Bounds for Codes Over the Unit Circle,” *Information Theory, IEEE Transactions on*, vol. 32, no. 6, pp. 760–767, 1986.