Journal of Algebraic Combinatorics 2 (1993), 31–48

The Sperner Capacity of Linear and Nonlinear Codes for the Cyclic Triangle

A.R. CALDERBANK
Mathematical Sciences Research Center, AT&T Bell Laboratories, Murray Hill, NJ 07974

P. FRANKL*
CNRS, 15 Quai Anatole France, 75007 Paris, France

R.L. GRAHAM
Mathematical Sciences Research Center, AT&T Bell Laboratories, Murray Hill, NJ 07974

W.-C.W. LI**
Mathematics Department, Penn State University, University Park, PA 16802

L.A. SHEPP
Mathematical Sciences Research Center, AT&T Bell Laboratories, Murray Hill, NJ 07974

Received March 4, 1992; Revised October 29, 1992

Abstract. Shannon introduced the concept of zero-error capacity of a discrete memoryless channel. The channel determines an undirected graph on the symbol alphabet, where adjacency means that symbols cannot be confused at the receiver. The zero-error or Shannon capacity is an invariant of this graph. Gargano, Körner, and Vaccaro have recently extended the concept of Shannon capacity to directed graphs. Their generalization of Shannon capacity is called Sperner capacity. We resolve a problem posed by these authors by giving the first example (the two orientations of the triangle) of a graph where the Sperner capacity depends on the orientations of the edges.

Sperner capacity seems to be achieved by nonlinear codes, whereas Shannon capacity seems to be attainable by linear codes. In particular, linear codes do not achieve Sperner capacity for the cyclic triangle. We use Fourier analysis or linear programming to obtain the best upper bounds for linear codes. The bounds for unrestricted codes are obtained from rank arguments, eigenvalue interlacing inequalities and polynomial algebra.

The statement of the cyclic q-gon problem is very simple: what is the maximum size $N_q(n)$ of a subset S_n of $\{0, 1, \ldots, q-1\}^n$ with the property that for every pair of distinct vectors $x = (x_i)$, $y = (y_i) \in S_n$, we have $x_j - y_j \equiv 1 (\mathrm{mod}\ q)$ for some j? For $q = 3$ (the cyclic triangle), we show $N_3(n) \simeq 2^n$. If however S_n is a subgroup, then we give a simple proof that $|S_n| \leq \sqrt{3}^n$.

Keywords: information theory, directed graph, Sperner theorem, Shannon capacity

1. Introduction

The idea of zero-error capacity of a discrete memoryless channel was introduced by Shannon [18] in 1956. The input alphabet becomes the vertex set V of a graph G, and two vertices are joined if the action of noise cannot result in the

* Research carried out at AT&T Bell Laboratories.
** Supported in part by NSA grant No. MDA904-90-H-1021.

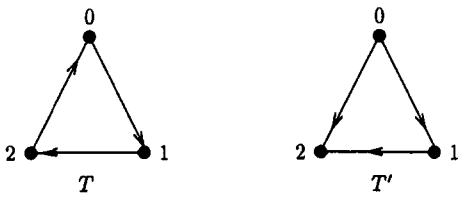

Figure 1. The two orientations of the triangle.

corresponding symbols being confused at the output of the channel. Distinct sequences $v = (v_1, \ldots, v_n)$, $v' = (v'_1, \ldots, v'_n)$ in V^n are then said to be *really different* if some pair (v_i, v'_i) is an edge in G. If $N(G, n)$ is the maximum size of a subset $S \subseteq V^n$ of pairwise really different sequences, then the zero-error capacity $C(G)$ is given by

$$C(G) = \lim_{n\to\infty} \frac{1}{n} \log N(G, n).$$

The problem of determining the capacity of the pentagon remained unsolved for some twenty years until the solution by Lovász [15].

Gargano, Körner and Vaccaro [7] have recently introduced the concept of the Sperner capacity $\sum(G)$ of a directed graph G. Here distinct sequences $v = (v_1, \ldots, v_n)$, $v' = (v'_1, \ldots, v'_n)$ in V^n are really different if there are indices i, j such that $v_i \to v'_i$ and $v'_j \to v_j$ are both edges in G. The *Sperner capacity* $\sum(G)$ is given by

$$\sum(G) = \lim_{n\to\infty} \frac{1}{n} \log N(G, n),$$

where $N(G, n)$ again denotes the maximum size of a code in V^n, that is a subset S of pairwise really different sequences. However Gargano, Körner and Vaccaro did not have any example of a directed graph for which the Sperner capacity depended on the orientation of the edges. Thus, it was not known whether Sperner capacity and Shannon (zero-error) capacity were different. The smallest candidate was the triangle, where the two orientations T and T' are shown in Figure 1. The Sperner capacity $\sum(T')$ is $\log 3$ (all logarithms are base 2), as may be seen by taking sequences with equally many 0s, 1s, and 2s. Gargano, Körner and Vaccaro raised the problem of determining the Sperner capacity $\sum(T)$, and it is this problem that we resolve here. We prove that

$$\frac{2^n}{c\sqrt{n}} \approx \binom{n}{\lfloor n/2 \rfloor} \leq N(T, n) \leq \begin{cases} \frac{1}{2}2^n + o(2^n), & \text{if } n \text{ is even,} \\ \frac{1}{3}2^n + o(2^n), & \text{if } n \text{ is odd,} \end{cases} \tag{1}$$

so that $\sum(T) = 1$. More accurate determination of $N(T, n)$ appears hard.

The term *Sperner capacity* is inspired by Sperner's theorem [19] on the size of a maximal antichain in the boolean lattice. We may restate this result as follows: if $V = \{0, 1\}$ and $G = 0 \to 1$, then $N(G, n) = \binom{n}{\lfloor n/2 \rfloor}$. The subsets of size $\lfloor n/2 \rfloor$ form a maximal antichain. Thus, $\sum(G) = 1$, and (1) shows that the extra symbol and edges in T do not increase the Sperner capacity. This is rather surprising, but it raises the question of identifying those transformations of directed graphs that preserve Sperner capacity.

Our results on the cyclic triangle problem also settle Problem 5 of Körner and Simonyi [14]. These authors consider a family $\mathcal{G}$ of graphs on a common vertex set V. A subset $S \subseteq V^n$ is said to be *$\mathcal{G}$-separated* if for every pair $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in S$, and every graph $G \in \mathcal{G}$, there is an index i such that (x_i, y_i) is an edge in G. The subset is said to be *symmetrically $\mathcal{G}$-separated* if for every pair $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in S$, and every graph $G \in \mathcal{G}$ there exist indices i and j such that $(x_i, y_i) = (y_j, x_j)$ is an edge in G. Let $N(\mathcal{G}, n)(N_\sigma(\mathcal{G}, n))$ be the maximum size of a $\mathcal{G}$-separated (symmetrically $\mathcal{G}$-separated) subset of V^n. Problem 5 asks if

$$\limsup_{n\to\infty} \frac{1}{n} \log N_\sigma(\mathcal{G}, n) = \limsup_{n\to\infty} \frac{1}{n} \log N(\mathcal{G}, n) \tag{2}$$

for all classes of graphs $\mathcal{G}$. An example for which equality does not hold is provided by the class $\mathcal{G}$ that consists of the undirected triangle. To make this clear, we use the main theorem of Gargano, Körner, and Vaccaro [6] to rewrite the left side of (2) as

$$\min \sum(G)$$

where the minimum is taken over all orientations of all graphs G in $\mathcal{G}$. The left side of (2) equals 1 and the right side equals $\log 3$, the Shannon capacity of the triangle. For more information about the fruitful interplay between information theory and extremal set theory, we refer the reader to [3], [5], [6], [7], [13], and [14].

In the next section we prove that the dimension of a linear code $S \subseteq \mathbb{Z}_3^n$ for the cyclic triangle problem satisfies $\dim S \leq n/2$. Since $(\log 3)/2 < 1$, we see that it is impossible to achieve the Sperner capacity of the directed triangle T using a linear code. This is strikingly different from classical information theory, where group codes achieve capacity on the Gaussian channel, and linear error-correcting codes meet the Gilbert-Varshamov bound (for details see [4] and [16]). It is interesting to contrast the cyclic triangle problem with that of constructing error-correcting ternary codes. The Hamming metric and the definition of two really different sequences are both invariant under translation by any fixed element of $\mathbb{Z}_3^n$, arbitrary coordinate permutations, and negation. However, the Hamming metric is also invariant under the full monomial group; all signed permutation matrices are symmetries. This raises an interesting question about

external problems involving the notion of pairwise really different sequences. Is it possible to quantify the power of group coding in a way that depends on the symmetry group of the notion of difference?

If a graph on q vertices is invariant under a q-cycle then it is possible to identify vertices with elements of $\mathbb{Z}_q$, so that the definition of two really different sequences is invariant under addition of any fixed element of $\mathbb{Z}_q^n$. This coordinatization goes through whenever the graph is invariant under a sharply transitive group H. Let A be the set of vertices not joined to the vertex 0. Then a code is a subset S of $\mathbb{Z}_q^n$ such that if $x \neq y$ belong to S, then $x \notin y + A^n$. Most cases of interest allow this group theoretic description.

One class of extensions of the cyclic triangle is the cyclic q-gon, where $x \to y$ if $y_j = x_j + 1 \bmod q$ for some j. Another way to generalize, more classical, is to use the complementary graph, where $x \to y$ if $y_j \neq x_j + 1 \bmod q$ for some j. For $q = 3$ these cases are isomorphic. A third class of extensions is when $x \to y$ if $y_j \neq x_j, x_j + 1, x_j - 1 \bmod q$ for some j. For $q = 5$ this is isomorphic to Lovász's problem mentioned above. We discuss each of these cases in the paper and determine, as far as we can, when linear codes are good and when not.

Our methods are linear and nonlinear. We obtain upper bounds for linear codes using Jamison's theorem [12] or linear programming. For nonlinear codes we use a technique of Haemers [9] based on eigenvalues of Kronecker products of matrices to obtain upper bounds. The examples of linear and nonlinear codes that appear in this paper do not involve random codes, and are elementary and constructive.

2. Linear methods for the cyclic triangle problem

In this section we use Fourier analysis on $\mathbb{Z}_3^n$ to derive upper bounds on the size of group codes for the cyclic triangle problem. *A group code* S is a subgroup of the additive group $\mathbb{Z}_3^n$ with the property that if $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ are distinct elements of S, then there are indices i, j such that $x_i \to y_i$ and $y_j \to x_j$ are edges in the triangle T. We then show how to use linear programming to derive bounds for arbitrary (nongroup) codes.

THEOREM 2.1. *If $H \subseteq \mathbb{Z}_3^n$ is a group code for the triangle T, then $|H| \leq 3^{n/2}$.*

Proof. Suppose H is a subgroup of $\mathbb{Z}_3^N$ and H has no word (except 0) with all 0s and 1s. We will show that $|H| \leq \sqrt{3}^n$. If $f : \mathbb{Z}_3^N \to \mathbb{C}$ define the Fourier transform of f, for $\alpha \in \mathbb{Z}_3^n$

$$\hat{f}(\alpha) = \frac{1}{3^n} \sum_{x \in \mathbb{Z}_3^N} f(x)\omega^{x \cdot \alpha}, \quad \omega = e^{\frac{2\pi i}{3}}. \tag{3}$$

It is easy to verify the inversion formula

$$f(x) = \sum_{\alpha} \hat{f}(\alpha)\omega^{-x\cdot\alpha} \tag{4}$$

and Parseval's formula,

$$\sum \hat{f}(\alpha)\overline{\hat{g}(\alpha)} = \frac{1}{3^n}\sum_{x} f(x)g(x), \tag{5}$$

where g is any function and $\bar{z}$ is z conjugate. Choose $f(x) = 1_E(x)(-1)^{x_1+\cdots+x_n}$ where $x_i = 0, 1, 2$ and $g(x) = 1_H(x)$, where 1_E is the indicator function of $E = \{0, 1\}^n$. Since no element x of H has all entries 0 and 1 except $x = 0$, the right side of (5) is $1/3^n$. But it is easy to verify that

$$\hat{f}(\alpha) = \frac{1}{3^n}(1-\omega)^{v_1(\alpha)}(1-\omega^2)^{v_2(\alpha)} \text{ if } v_0(\alpha) = 0;\ \hat{f}(\alpha) = 0 \text{ if } v_0(\alpha) \neq 0 \tag{6}$$

where $v_j(\alpha) = |\{i = 1, \ldots, n : \alpha_i = j\}|$, $j = 0, 1, 2$. Also if H has d linearly independent generators over $\{0, 1, 2\}$, $z^1, \ldots, z^d$, then

$$\hat{g}(\alpha) = \frac{1}{3^n}\prod_{i=1}^{d}\sum_{c_i=0,1,2}\omega^{c_i z^i} = 1_{H^\perp}(\alpha)\frac{1}{3^{n-d}}. \tag{7}$$

Then (5) becomes, after multiplication by 3^{2n-d},

$$\sum_{\alpha\in H^\perp, v_1(\alpha)=0}(1-\omega)^{v_1(\alpha)}(1-\omega^2)^{v_2(\alpha)} = 3^{n-d}. \tag{8}$$

But $v_1(\alpha) + v_2(\alpha) = n$ and $1 - \omega^2 = (-1/\omega)(1-\omega)$ so

$$\sum_{\alpha\in H^\perp, v_0(\alpha)=0}(-1/\omega)^{v_2(\alpha)} = 3^{n-d}/(1-\omega)^n. \tag{9}$$

The right side is $\sqrt{3}^n/3^d$ in magnitude while the left side is a sum of terms of the form $\pm\omega^l$ and, after reducing via $1 + \omega + \omega^2 = 0$, becomes $A + B\omega$ where A and B are integers. But if $d > n/2$ then $|A + B\omega| < 1$ in magnitude and is not zero, which is impossible since $\omega = \frac{1}{2} + \frac{\sqrt{3}i}{2}$ and the lattice $A + B\omega$ contains no points with magnitude < 1 except 0. This completes the proof. □

A second proof which extends to give a (tight) bound for primes $q \geq 3$ depends on a theorem of Jamison (see also [2]).

THEOREM 2.2. (Jamison [12]). *If $Z_q^k - \{0\}$ is a union of L flats of codimension 1 then $(q-1)k \leq L$.*

COROLLARY 2.1. *Let $H \leq \mathbb{Z}_q^n$ be a linear code where the zero vector is the only word with all entries in the set $\{s_1 = 0, s_2, \ldots, s_d\}$. Then*

$$|H| \leq q^{\frac{q-d}{q-1}n}. \tag{10}$$

Proof. Suppose $|H| = q^k$, i.e., there are k linearly independent generators $x_i, i = 1, \ldots, k$ of H

$$\begin{matrix} (x_{11}, \ldots, x_{1n}) \\ \vdots \qquad\quad \vdots \\ (x_{k1}, \ldots, x_{kn}) \end{matrix} \quad x_{ij} \in Z_q. \tag{11}$$

Consider the flats $F_{j,\xi} = \{u \in \mathbb{Z}_q^k : \sum_{i=1}^k u_i x_{ij} = \xi\}$ where $j = 1, \ldots, n$ and ξ takes one of the $q - d$ values which must occur in some coordinate of each element of H. Since each element u except $u \equiv 0$ belongs to one of $F_{j,\xi}$, the union of the flats $F_{j,\xi}$ is all of $\mathbb{Z}_q^k - \{0\}$, and there are $L = n(q - d)$ flats. By Jamison's theorem, $(q-1)k \leq n(q-d)$. The proof is complete since $|H| = q^k$. □

Remarks. For $q = 3$ and even n, we may take

$$H = \{x = \epsilon_1(1, -1, 0, \ldots, 0) + \epsilon_2(0, 0, 1, -1, 0, \ldots, 0) + \cdots + \epsilon_{n/2}(0, \ldots, 0, 1, -1)|$$
$$\epsilon_i = 0, 1, \text{ or } -1 \text{ for } i = 1, \ldots, n/2\}.$$

Then H is a group code of dimension $n/2$ and every nonzero vector in H has some entry equal to 1. This example shows that the bound provided by Theorem 2.1 is tight.

More generally, let H be a subgroup of $\mathbb{Z}_q^n$ with the property that no code word in H except 0 has every entry equal to 0 or 1. Then Theorem 2.2 implies dim $H \leq (q-2)n/(q-1)$. If n is divisible by $q-1$ then the rows of the Kronecker product

$$I_{n/q-1} \otimes \begin{bmatrix} 1 & & -1 \\ & \ddots & \vdots \\ & 1 & -1 \end{bmatrix}$$

generate a subgroup H with the required property that meets the bound provided by Jamison's theorem.

Linear programming bounds

We now follow Lovász [15] and use linear programming to derive bounds for arbitrary codes S. Let $\Omega = \{0,1\}^n \cup \{0,-1\}^n$ and let $p(z), z \in \mathbb{Z}_3^n$ be any function from $\mathbb{Z}_3^n$ to R for which $p(z) = 0$ if $z \notin \Omega$ and $p(z) = p(-z)$. The matrix E given by

$$E_{zz'} = p(z - z')$$

is symmetric, and it is positive semidefinite (psd) if all eigenvalues are nonnegative. Since E commutes with translation by any fixed element of $\mathbb{Z}_3^n$, the eigenvectors of E are the columns of the character matrix U of the additive group $\mathbb{Z}_3^n$. The eigenvalue corresponding to the column $U_\alpha(z) = \omega^{(\alpha,z)}$ is

$$3^n \hat{p}(\alpha) = \sum_{z \in \mathbb{Z}_3^n} p(z)\omega^{(\alpha,z)}.$$

Thus, E is psd if and only if $\hat{p}(\alpha) \geq 0$ for all $\alpha \in \mathbb{Z}_3^n$. Finally, we normalize E by taking $p(0) = 1$.

Henceforth we suppose $p(z) = 0$ if $z \notin \Omega$, $\sum_z p(z) \neq 0$, $\hat{p}(\alpha) \geq 0$ for all $\alpha \in \mathbb{Z}_3^n$, and $p(0) = 1$, so that E is psd. Since $U^* E U = \Lambda^2$ for some diagonal matrix Λ, we may write E as a gram matrix:

$$E = \langle \xi_z, \xi_{z'} \rangle, \quad \text{where } \xi_z \in \mathbb{C}^{3n}.$$

Define

$$\delta = \left(\sum_{z \in \mathbb{Z}_3^n} \xi_z \right) \Big/ \left(\sum_{z \in \mathbb{Z}_3^n} p(z) \right).$$

Then

$$(\delta, \xi_{z'}) = \left(\sum_z p(z - z') \right) \Big/ \left(\sum_z p(z) \right) = 1.$$

Let $S \subseteq \mathbb{Z}_3^n$ be a code for the cyclic triangle T. Then the vectors ξ_z, $z \in S$ are orthonormal, since $\langle \xi_z, \xi_z \rangle = p(0) = 1$, and $\langle \xi_z, \xi_{z'} \rangle = p(z - z') = 0$. Now Bessel's inequality gives

$$\begin{aligned} |S| &= \sum_{z \in S} |\langle \delta, \xi_z \rangle|^2 \\ &\leq \langle \delta, \delta \rangle \\ &= \left(\sum_{z \in \mathbb{Z}_3^n} \sum_{z' \in \mathbb{Z}_3^n} p(z - z') \right) \Big/ \left(\sum_{z \in \mathbb{Z}_3^n} p(z) \right)^2 \\ &= 3^n \Big/ \left(\sum_{z \in \mathbb{Z}_3^n} p(z) \right) \\ &= 1/\hat{p}(0). \end{aligned}$$

The linear programming problem is then to maximize $\hat{p}(0)$ given $p(z) = 0$ for $z \notin \Omega$, $\hat{p}(\alpha) \geq 0$ for all $\alpha \in \mathbb{Z}_3^n$, and $p(0) = 1$.

By averaging over the group of transformations that fixes Ω (which is the direct product of the symmetric group S_n with $\langle -I_n \rangle$) we may suppose $p(z)$ to be a constant p_i on the orbit $\{z \in \Omega \mid |z| = i\}$. For $n = 3$, 4, and 5 the optimal functions $p(z)$ are listed below:

	p_0	p_1	p_2	p_3	p_4	p_5	$1/\hat{p}(0)$
n = 3	1	2/5	1/5	2/5			5
n = 4	1	3/11	2/11	2/11	3/11		11
n = 5	1	2/7	1/7	1/7	1/7	2/7	21

If we adjoin the values of $1/\hat{p}(0)$ for $n = 1$, 2, to the table, namely 1, 3, it is tempting to conjecture that $1/\hat{p}(0) = (2^{n+1} + (-1)^n)/3$ since this holds for $n \leq 5$. However, for $n = 6, 7, \ldots$ solving the linear program (for which we are grateful to R. Vanderbei) gives $1/\hat{p}(0) = 48.6, 104.478, \ldots, 243, \ldots$. It thus appears that this method does not give the right constant. It is interesting that the use of rank inequalities in Section 3 gives the right constant while the linear programming bounds are so far from being tight. The latter method could perhaps be improved by using $\delta = \sum a_z \xi_z$ rather than a_z = constant, as above, but then the best choice of p and a involves nonlinear programming. Note that allowing $p(z, w)$ instead of $p(z - w)$ does not increase generality. The linear programming method needs symmetric inner products, whereas the rank method makes use of unsymmetric matrices even though the original problem is symmetric. This all seems both interesting and mysterious and calls for further investigation.

Let us apply a linear programming method to obtain upper bounds in the case of Lovász's problem and its extensions. Thus, suppose $G = \mathbb{Z}_q^n$ and H is a group code with the property that if $x \in H$ then $x_j \neq 0, \pm 1$ for some j. In this case the Jamison bound (10) gives $|H| \leq q^{(q-3)n/(q-1)}$ since $d = 3$. Here we will obtain a *better* bound (by Lovász's method, slightly extended) valid for *nonlinear* codes. Our proof is a variant of that of Lovász [15].

If we can find a positive-definite $q^n \times q^n$ matrix $\rho(x, y) = \rho_{x-y}$ where $x, y \in G = \mathbb{Z}_q^n$, then for any code S, we may obtain the bound

$$|S| \leq \frac{q^n}{\sum_{x \in G} \rho_x}, \tag{12}$$

provided that $\rho_x = 0$ for $x \notin N$ and $\rho_0 = 1$. To prove (12), observe by positive definiteness, there exist vectors $\xi_x \in \mathbb{R}^{q^n}$ for which

$$\rho_{x-y} = \langle \xi_x, \xi_y \rangle. \tag{13}$$

Now following Lovász, set

$$\eta = \sum_{x \in G} \xi_x \Big/ \sum_{x \in G} \rho_x, \tag{14}$$

note that $\langle \eta, \xi_y \rangle = 1$ for all $y \in G$ and that if $x \neq y \in S$ then ξ_x and ξ_y are orthogonal since $x-y \notin N$ and hence $\langle \xi_x, \xi_y \rangle = \rho_{x-y} = 0$. Also, $\langle \xi_x, \xi_x \rangle = \rho_0 = 1$, so by Bessel's inequality

$$|S| = \sum_{x \in S} \langle \eta, \xi_x \rangle^2 \leq \langle \eta, \eta \rangle = q^n \Big/ \sum_{x \in G} \rho_x \tag{15}$$

and (12) is proved.

Let us use

$$\rho_x = r_{x_1} r_{x_2} \cdots r_{x_n} \qquad r_{x_1} = \begin{cases} 1 & x_i = 0 \\ \theta & x_i = \pm 1 \end{cases} . \tag{16}$$

For ρ_{x-y} to be positive definite we need to check that the Fourier transform of ρ_x is nonnegative.

Now

$$\hat{\rho}(\alpha) = \frac{1}{q^n} \sum_{x \in G} \rho_x \omega^{x \cdot \alpha} = \hat{r}(\alpha_1) \cdots \hat{r}(\alpha_n) \geq 0, \tag{17}$$

for all $\alpha \in G$, if and only if

$$\hat{r}(\alpha_i) = 1 + 2\theta \cos \frac{2\pi \alpha_i}{q} \geq 0, \text{ for all } \alpha_i \in \mathbb{Z}_q. \tag{18}$$

If $q = 2p + 1$, then the worst value for α_i is p, so for this case, we need $\theta = -1/\cos((q-1)\pi/q) = 1/\cos(\pi/q)$. From (12) this gives the bound

$$|S| \leq \left(\frac{q}{1 + \frac{1}{\cos(\pi/q)}} \right)^n, \qquad q \text{ odd}, \quad q \geq 5. \tag{19}$$

For $q = 5$ this gives the value $\sqrt{5}^n$, which is the same as the bound (10), $|S| \leq 5^{(5-3)n/(5-1)}$, but for $q > 5$, the bound in (19) is better (smaller) even though it applies to nonlinear codes than Jamison's bound (10) valid only in the linear case. If (19) is achieved, it seems hard to see whether the achieving codes are linear or nonlinear. The problem remains open for $q = 7$ to our knowledge. We obtain the bound $(3.17667207394095)^n$ from (19), better than $(3.659305)^n$ from (10). For q even, the upper bound

$$|S| \leq (q/2)^n, \qquad q \text{ even}, \quad q \geq 2 \tag{20}$$

and this is achieved by the subgroup of Z_q^n of vectors all of whose components are even. Since for $q = 5$, and for even q, linear codes achieve capacity, it is tempting to conjecture that this is true also for $q = 7$, although, as Lovász points out there is no n for which the bound in (19) is an integer, so that in a sense (19) cannot be sharp and so $q = 7$ is essentially different from $q = 5$.

3. Eigenvalue interlacing inequalities

To begin, let G be any directed graph on q vertices. It will be convenient to label these vertices by the residue classes in $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$. The directed graph G distinguishes a class $\mathcal{B}$ of $q \times q$ matrices with real entries; the entries on the main diagonal are constrained to be 1, and the ijth entry is constrained to be zero when $i \to j$ is an edge in G. We shall be interested in choosing the unspecified entries so as to minimize the rank of a matrix B in the class $\mathcal{B}$.

Let $B \in \mathcal{B}$, and let $D = \otimes^n B$ be the Kronecker product of n copies of the matrix B. There is a natural labeling of rows and columns of D by vectors in $\mathbb{Z}_q^n$. For distinct vectors $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$, we have $D_{xy} = 0$ if there is an index i for which $y_i \to x_i$ is an edge in G. In order to apply eigenvalue interlacing inequalities, we need to work with a Hermitian matrix, so we consider $D + D^T$. Here $(D + D^T)_{xx} = 2$, and $(D + D^T)_{xy} = 0$ if there are indices i, j such that $x_i \to y_i$ and $y_j \to x_j$ are edges in G. The remaining entries depend on the representative B. If S is a code in $\mathbb{Z}_q^n$, then the vectors in S index the rows and columns of a principal submatrix of $D + D^T$, which is $2I_{|S|}$. The eigenvalues of this principal submatrix interlace the eigenvalues of $D + D^T$ as described in Theorem 3.1 below (for proofs of this theorem and similar results see Haemers [8] or Horn and Johnson [10]).

THEOREM 3.1. *Let E be an $M \times M$ Hermitian matrix, and let $\lambda_1(E) \geq \cdots \geq \lambda_M(E)$ be the eigenvalues of E. If P is an $m \times m$ principal submatrix of E with eigenvalues $\lambda_1(P) \geq \cdots \geq \lambda_m(P)$ then*

$$\lambda_i(E) \geq \lambda_i(P) \geq \lambda_{M-m+i}(E), \qquad \text{for } i = 1, \ldots, m.$$

We are now ready to give a universal upper bound on $N(G, n)$ for arbitrary directed graphs G.

THEOREM 3.2. *Given a directed graph G, let $\mathcal{B}$ be the class of matrices determined by G. For $B \in \mathcal{B}$, let $\Gamma^+(B)$ be the number of eigenvalues λ of $E = \otimes^n B + (\otimes^n B)^T$ for which $\lambda \geq 2$. Then*

(1) $N(G, n) \leq \min_{B \in \mathcal{B}} \{ \text{rank } (B)^n \}$, *and*

(2) $N(G, n) \leq \min_{B \in \mathcal{B}} \{\Gamma^+(B)\}$.

Proof. A code S determines a principal submatrix $I_{|S|}$ of $\otimes^n B$, so that rank $(\otimes^n B) = (\text{rank}(B))^n \geq |S|$. Part (2) follows directly from Theorem 3.1. □

Remarks.

(1) We may relax the definition of a code and allow ordered subsets S; if $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ are distinct elements of S, and if $x \geq y$,

then there exist an index j such that $y_j \to x_j$ is an edge in G. The code now determines a principal submatrix of $\otimes^n B$ that is lower triangular with all entries on the main diagonal equal to 1. Again we have $|S| \leq (\text{rank}(B))^n$.

(2) Lovász [15] used linear programming to determine the Shannon zero-error capacity of the pentagon. The rank argument appearing in part (1) of Theorem 3.2 was used by Haemers [8] to settle several problems left unresolved by Lovász.

In the remainder of this section, we assume $q \geq 3$ is odd, and we take G to be the q-cycle C_q with edges $0 \to 1 \to 2 \to \cdots \to q-1 \to 0$. We shall derive an upper bound for $N(C_q, n)$ by choosing an appropriate representative $B \in \mathcal{B}$. We begin with a preliminary observation.

LEMMA 3.1. *If $p > 1$ is a factor of q, then $N(C_q, n) \leq N(C_p, n)$.*

Proof. Consider the image $\tilde{S}$ of a code S in $\mathbb{Z}_q^n$ under the canonical homomorphism $\varphi : \mathbb{Z}_q^n \to \mathbb{Z}_p^n$ which sends each entry to its residue modulo p. Since C_p is the image of C_q mod p, the subset $\tilde{S}$ is a code in $\mathbb{Z}_p^n$. Finally observe that two distinct code words in S cannot be congruent mod p, so that $|S| = |\tilde{S}|$. □

Let e_i, $i = 1, \ldots, q$ be the standard basis vectors of $\mathbb{R}^q$, and let P be the permutation matrix that represents the linear transformation $e_1 \to e_2 \to \cdots \to e_q \to e_1$. Set $\epsilon = e^{2\pi i/q}$. Then the vector $z_i = (1, \epsilon^i, \epsilon^{2i}, \ldots, \epsilon^{(q-1)i})^T$ is a right eigenvector of P associated with the eigenvalue ϵ^{-i}. Let $q = 2m + 3$, and let

$$\begin{aligned} f(x) &= (x-1)(x-\epsilon)(x-\bar{\epsilon})\cdots(x-\epsilon^m)(x-\bar{\epsilon}^m) \\ &= x^{q-2} + a_{q-3}x^{q-3} + \cdots + a_1 x - 1, \end{aligned} \tag{21}$$

which is a polynomial with real coefficients. The q-cycle C_q determines a class of real $q \times q$ matrices, and from this class we select the representative

$$B = -f(P) = I - a_1 P - a_2 P^2 - \cdots - a_{q-3}P^{q-3} - P^{q-2}. \tag{22}$$

This matrix is diagonalizable, with $Bz_i = -f(\bar{\epsilon}^i)z_i$, for $i = 0, 1, \ldots, q-1$. Thus, $z_0, \ldots, z_m, z_{m+3}, \ldots, z_{q-1}$ are eigenvectors of B with eigenvalue 0, z_{m+1} is associated with the eigenvalue $-f(\bar{\epsilon}^{m+1})$, and z_{m+2} is associated with the eigenvalue $-f(\epsilon^{m+1})$.

Remarks.

(1) Since $\text{rank}(B) = 2$, we obtain $N(C_q, n) \leq 2^n$ by applying part (1) of Theorem 3.2. In the remarks following Theorem 3.2 we showed this bound holds when we relax the definition of a code by allowing ordered subsets of $\mathbb{Z}_q^n$. In this case it is possible to construct a code of size 2^n by suitably ordering the set of binary vectors.

(2) Let q be a prime, and let $\mathcal{B}$ be the class of matrices determined by an arbitrary cyclic tournament on q points with outdegree d. We relax the definition of $\mathcal{B}$ and allow complex matrices. The tournament determines $(q-d-1)$ powers P^{i_l} of the basic permutation matrix P, such that all linear combinations of the identity matrix and these powers belong to $\mathcal{B}$. Nonsingularity of the Vandermonde determinant implies that there exists a representative $B \in \mathcal{B}$ for which $\text{rank}(B) = d+1$. Now part (1) of Theorem 3.2 gives $N(G, n) \leq (d+1)^n$. When we relax the definition of a code by allowing ordered subsets it is often possible to achieve this bound by suitably ordering all vectors in W^n, where W is a subset of $\mathbb{Z}_q$.

(3) A. Blokhuis [1] has given an elementary proof of the bound $N(G, n) \leq (d+1)^n$ using elementary polynomial algebra, and avoiding Kronecker products.

We return to the matrix B given by (22). The transpose $B^T = -f(P^T) = -f(P^{-1})$, and

$$B^T z_i = -f(\epsilon^i) z_i, \qquad \text{for} \quad 0 \leq i \leq q-1.$$

In particular B^T vanishes at all eigenvectors except z_{m+1} and z_{m+2}, where the eigenvalues are $-f(\epsilon^{m+1})$ and $-f(\bar{\epsilon}^{m+1})$, respectively.

Let $D = \otimes^n B$ be the Kronecker product of n copies of B. The eigenvectors of D are obtained by taking Kronecker products of the eigenvectors z_i. The eigenvector $z_{i_1} \otimes \cdots \otimes z_{i_n}$ is associated with the eigenvalue $(-1)^n f(\bar{\epsilon}^{i_1}) \cdots f(\bar{\epsilon}^{i_n})$. Let U be the matrix of eigenvectors. Then

$$U^{-1} D U = \Lambda \quad \text{and} \quad U^{-1} D^T U = \overline{\Lambda}, \tag{23}$$

where Λ is diagonal. Hence,

$$U^{-1}(D + D^T)U = \Lambda + \bar{\Lambda}. \tag{24}$$

Let $\phi = -f(\bar{\epsilon}^{m+1})$. The nonzero eigenvalues of $D + D^T$ are $\phi^i \bar{\phi}^{n-i} + \bar{\phi}^i \phi^{n-i}$; for $0 \leq i < n/2$ the multiplicity is $\binom{n}{i} + \binom{n}{n-i}$, and for $i = n/2$ it is $\binom{n}{n/2}$. We need to study the relation between ϕ and $\bar{\phi}$ in order to find which eigenvalues are positive.

LEMMA 3.2. *If* $q = 2m + 3$, *then*

$$\phi = -f(\bar{\epsilon}^{m+1}) = -\bar{\epsilon}\bar{\phi} = \frac{q}{\epsilon - 1}.$$

Proof. For $1 \leq i \leq m$, we have

$$(\epsilon^{m+1} - \epsilon^i)(\epsilon^{m+1} - \bar{\epsilon}^i) = (\epsilon^{m+1-i} - 1)(\epsilon^{m+1+i} - 1), \quad \text{and}$$
$$(\bar{\epsilon}^{m+1} - \epsilon^i)(\bar{\epsilon}^{m+1} - \bar{\epsilon}^i) = \bar{\epsilon}^{2(m+1)}(1 - \epsilon^{m+1+i})(1 - \epsilon^{m+1-i}),$$

Since $\epsilon^q = 1$,

$$\phi = -f(\bar{\epsilon}^{m+1}) = \bar{\epsilon}^{(m+1)(q-2)} f(\epsilon^{m+1}) = -\bar{\epsilon}\bar{\phi}.$$

Further, the identity $\sum_{i=0}^{q-1} f(\epsilon^i) = q$ reduces to $\phi + \bar{\phi} = -q = (1-\epsilon)z$, so we obtain $z = q/(\epsilon - 1)$. □

For convenience, set $c = \phi\bar{\phi} > 0$ and $\mu(j) = \epsilon^j + \epsilon^{-j}$. Then $\mu(j)$ is real, nonzero and has period q. We distinguish two cases.

Case I. n is even.

Now $\phi^{n/2}\bar{\phi}^{n/2} = c^{n/2}$ so that $2c^{n/2}$ is an eigenvalue of $D + D^T$ with multiplicity $\binom{n}{n/2}$. By Lemma 3.2,

$$\phi^i\bar{\phi}^{n-i} = \phi^i\bar{\phi}^{n/2}\bar{\phi}^{n/2-i} = \phi^i\bar{\phi}^{n/2}(-\epsilon)^{n/2-i}\phi^{n/2-i} = c^{n/2}(-\epsilon)^{n/2-i}.$$

If $0 \le i < n/2$, then $c^{n/2}(-1)^{n/2-i}\mu(n/2-i)$ is an eigenvalue of $D + D^T$, and we rewrite the multiplicity of that eigenvalue as $\binom{n}{n/2-(n/2-i)} + \binom{n}{n/2+(n/2-i)}$. If the indices i are congruent modulo $2q$, then signs of the eigenvalues are identical. Note that the signs of $(-1)^{n/2-i}\mu(n/2-i)$ and $(-1)^{n/2-i+q}\mu(n/2-i+q)$ are opposite. We conclude that the number of positive eigenvalues of $D + D^T$ is equal to

$$\sum_{j\ge 0}\binom{n}{i_1+2qj} + \binom{n}{i_2+2qj} + \cdots + \binom{n}{i_q+2qj}$$

where $i_1, i_2, \ldots, i_q \in \{0, 1, \ldots, 2q-1\}$ are such that $(-1)^{n/2-i_l}\mu(n/2-i_l) > 0$.

Case II. n is odd.

In this case Lemma 3.2 gives

$$\begin{aligned}\phi^i\bar{\phi}^{n-i} = \phi^i\bar{\phi}^{(n-1)/2}\bar{\phi}^{(n+1)/2-i} &= \phi^i\bar{\phi}^{(n-1)/2}(-\epsilon)^{(n+1)/2-i}\phi^{(n+1)/2} \\ &= c^{(n-1)/2}\phi(-\epsilon)^{(n+1)/2-i},\end{aligned}$$

so that

$$\phi^i\bar{\phi}^{n-i} + \bar{\phi}^i\phi^{n-i} = c^{(n-1)/2}(-1)^{(n+1)/2-i}\left(\phi\epsilon^{(n+1)/2-i} + \bar{\phi}\bar{\epsilon}^{(n+1)/2-i}\right).$$

Substituting $\phi = q/(\epsilon - 1)$ we obtain

$$\begin{aligned}\phi\epsilon^{(n+1)/2-i} + \bar{\phi}\bar{\epsilon}^{(n+1)/2-i} &= \frac{q}{\epsilon-1}\epsilon^{(n+1)/2-i} + \frac{q}{\bar{\epsilon}-1}\bar{\epsilon}^{(n+1)/2-i} \\ &= \frac{q}{(\epsilon-1)(\bar{\epsilon}-1)}\left(\epsilon^{(n+1)/2-i}(\bar{\epsilon}-1)\right. \\ &\quad \left. + \bar{\epsilon}^{(n+1)/2-i}(\epsilon-1)\right) \\ &= \frac{q}{(\epsilon-1)(\bar{\epsilon}-1)}(\mu((n+1)/2-i-1) \\ &\quad -\mu((n+1)/2-i)).\end{aligned}$$

We conclude that the sign of $\phi^i\bar{\phi}^{(n-i)} + \bar{\phi}^i\phi^{(n-i)}$ equals the sign of

$$(-1)^{(n+1)/2-i}(\mu((n+1)/2 - i - 1) - \mu((n+1)/2 - i)),$$

when these quantities are nonzero.

Again the sign remains the same if i is replaced by $i + 2qj$, and the sign is reversed if i is replaced by $i + (2j+1)q$. We have $\mu(j) = \mu(j+1)$ if and only if $j \equiv (q-1)/2 (\mathrm{mod} q)$. Thus, we may conclude that the number of positive eigenvalues of $D + D^T$ is equal to

$$\sum_{j\geq 0}\binom{n}{i_1 + 2qj} + \binom{n}{i_2 + 2qj} + \cdots + \binom{n}{i_{q-1} + 2qj},$$

where $i_1, i_2, \ldots, i_{q-1} \in \{0, 1, \ldots, 2q-1\} \setminus \{(q-1)/2\}$ are such that $(-1)^{(n+1)/2-i_l}(\mu((n+1)/2 - i_l - 1) - \mu((n+1)/2 - i_l)) > 0$.

We need a final technical lemma.

LEMMA 3.3. *Let ξ be a primitive Mth root of unity, and let $i \in \{0, 1, \ldots, M-1\}$. Then*

$$M \sum_{\substack{j \equiv i (\mathrm{mod}\, M) \\ j\geq 0}} \binom{n}{j} = \sum_{l=1}^{M}(1 + \xi^l)^n \xi^{-li}.$$

Proof. We have

$$\sum_{l=1}^{M}(1 + \xi^l)^n \xi^{-li} = \sum_{l=1}^{M}\sum_{j=0}^{n}\binom{n}{j}\xi^{lj-li}$$

$$= M \sum_{\substack{j \equiv i (\mathrm{mod}\, M) \\ j\geq 0}} \binom{n}{j}.$$

□

THEOREM 3.3. *For n sufficiently large, we have*

$$N(C_q, n) \leq \begin{cases} \frac{1}{2}[2^n + (2p-1)(2 + 2\cos\pi/p)^{n/2}], & \text{if } n \text{ is even}, \\ \left(\frac{p-1}{2p}\right)[2^n + (2p-1)(2 + 2\cos\pi/p)^{n/2}], & \text{if } n \text{ is odd}, \end{cases}$$

where p is the smallest prime factor of q.

Proof. By Lemma 3.3, we may suppose q is prime. We have derived formulae for the number of positive roots of $D + D^T$. Applying Lemma 3.1 to these formulae, with $M = 2q$ and $\xi = -\epsilon$, we obtain

$$N(C_q, n) \le \frac{1}{2q} \sum_{l=1}^{2q} (1 + (-\epsilon)^l)^n \sum_{i \in I_n} (-\epsilon)^{-li},$$

where I_n consists of the elements i in $\{0, 1, \ldots, 2q-1\}$ such that $(-1)^{n/2-i}\mu(n/2-i) > 0$ for n even, and $(-1)^{(n+1)/2-i}(\mu((n+1)/2-i-1)-\mu((n+1)/2-i)) > 0$ for n odd. Since $|1 + (-\epsilon)^l| < (2 + 2\cos \pi/q)^{1/2}$ for $1 \le l \le 2q-1$, the dominant term on the right-hand side is that indexed by $l = 2q$, and the sum of the remaining terms is less than or equal to $|I_n|(2q-1)(2 + 2\cos \pi/q)^{n/2}$. □

4. Upper bounds for double-loop networks

In Section 3 we derived the upper bound $N(G, n) \le (d+1)^n$ for an arbitrary cyclic tournament G with outdegree d. Clearly eigenvalue interlacing inequalities can be used to improve this bound. The critical step is choosing the analog of the polynomial $f(x)$ that appears in Section 3. In this section we take G to be the double-loop network $G_q(1, 2)$, with vertex set the residue classes $\mathbb{Z}_q$ (where $q \ge 5$ is odd) and edges $i \to i+1$ and $i \to i+2$ for all $i \in \mathbb{Z}_q$. For more information about double-loop networks see Hwang and Li [11].

We write $q = 2m + 3$, $\epsilon = e^{2\pi i/q}$, and take

$$\begin{aligned} g(x) &= (x-\epsilon)(x-\bar{\epsilon})\cdots(x-\epsilon^m)(x-\bar{\epsilon}^m) \\ &= x^{2m} + b_{2m-1}x^{2m-1} + \cdots + 1; \end{aligned}$$

again the coefficients b_i are real. The representative matrix B is given by

$$B = g(P) = I + b_1 P + \cdots + b_{2m-1}P^{2m-1} + P^{2m}.$$

All entries on the main diagonal of B equal 1, and for $0 \le i \le q-1$, we have $B_{i(i+1)} = B_{i(i+2)} = 0$. The nonzero eigenvalues of B are $g(1) = \lambda$, $g(\bar{\epsilon}^{m+1}) = \psi$, and $g(\epsilon^{m+1}) = \bar{\psi}$. The eigenvalues of $D + D^T$ are $\lambda^a\psi^b\bar{\psi}^{n-a-b} + \lambda^a\bar{\psi}^b\psi^{n-a-b}$ with multiplicity $\binom{n}{a}\binom{n-a}{b}$. The following lemma is the counterpart of Lemma 3.2.

LEMMA 4.1. *If $q = 2m + 3$, then*

$$\psi = g(\bar{\epsilon}^{m+1}) = \epsilon^m\bar{\psi} = \frac{-q-\lambda}{1+\bar{\epsilon}^m}, \qquad \textit{and}$$

$$\lambda = g(1) = |(1-\epsilon)(1-\epsilon^2)\cdots(1-\epsilon^m)|^2 > 0.$$

Now we calculate the number of positive eigenvalues of $D + D^T$. Since λ is positive, we fix a, $0 \le a \le n$ and compute $\psi^b\bar{\psi}^{n-a-b} + \bar{\psi}^b\psi^{n-a-b}$. Again there are two cases.

Case I. $n - a$ is even.

Then for $0 \le b \le (n-a)/2$,

$$\psi^b\bar{\psi}^{n-a-b} + \bar{\psi}^b\psi^{n-a-b} = (\psi\bar{\psi})^{(n-a)/2}\mu(m((n-a)/2-b)).$$

Case II. $n-a$ is odd.

Then for $0 \le b < (n-a)/2$,

$$\psi^b\bar{\psi}^{n-a-b} + \bar{\psi}^b\psi^{n-a-b} = (\psi\bar{\psi})^{(n-a-1)/2}\frac{(-q-\lambda)}{|1+\epsilon^m|^2}$$
$$(\mu(m((n-a+1)/2-b)) + \mu(m((n-a-1)/2-b))).$$

Note that $gcd(m, q) = 1$ or 3, and $gcd(m, q) = 3$ if and only if 3 divides q. Let

$$q' = \begin{cases} q, & \text{if } 3 \nmid q, \\ q/3, & \text{if } 3 \mid q, \end{cases}, \quad \xi = \begin{cases} \epsilon, & \text{if } 3 \nmid q, \\ \epsilon^3, & \text{if } 3 \mid q, \end{cases}, \quad \text{and} \quad m' = \begin{cases} m, & \text{if } 3 \nmid q, \\ m/3, & \text{if } 3 \mid q. \end{cases}$$

Then $\epsilon^m = \xi^{m'}$, $gcd(m', q') = 1$, and $\mu(mj)$ has period q'. Define

$$J_{n-a} = \begin{cases} \{0 \le j < q' \mid \mu(m((n-a)/2-j)) > 0\}, \text{ if } n-a \text{ is even}, \\ \{0 \le j < q' \mid \mu(m((n-a+1)/2-j)) \\ \quad +\mu(m((n-a-1)/2-j)) > 0\}, \text{ if } n-a \text{ is odd}. \end{cases}$$

The next theorem now follows directly from Lemma 3.3.

THEOREM 4.1. *Let* $q = 2m+3$, *where* $m \ge 1$, *and let* q', ξ *and* J_{n-a} *be as defined above. Then*

$$N(G_q(1, 2), n) \le \frac{1}{q'}\sum_{a=0}^{n}\binom{n}{a}\sum_{l=1}^{q'}(1+\xi^l)^{n-a}\sum_{j\in J_{n-a}}\xi^{-lj}. \tag{25}$$

We need to know the cardinality of the set J_{n-a} in order to estimate the right-hand side of (25). We may suppose that $\xi^{m'} = e^{2\pi i/q'}$. Then $\mu(mj) > 0$ for $-q'/4 < j < q'/4$ and $\mu(mj) < 0$ for $q'/4 < j < 3q'/4$. Hence, $|J_{n-a}| = (q'+1)/2$ when $n-a$ is even.

Next we consider the sign of $\mu(mj) + \mu(m(j-1))$. If $s = \lceil q/4 \rceil$, then

$$\mu(mj) + \mu(m(j-1)) > 0 \quad \text{for} \quad 1 \le j \le s-1,$$

$$\mu(mj) + \mu(m(j-1)) < 0 \quad \text{for} \quad s+1 \le j \le (q'+1)/2,$$

and for all j,

$$\mu(mj) + \mu(m(j-1)) = \mu(m(q'-j)) + \mu(m(q'-j+1)).$$

The only uncertainty is $\mu(ms) + \mu(ms-1)$ and this depends on q' mod 4. More precisely, if $q' \equiv 1 (\bmod 4)$ then $s = (q'+3)/4$ and $\mu(ms) + \mu(m(s-1)) < 0$, whereas, if $q' \equiv 3 (\bmod 4)$ then $s = (q'+1)/4$ and $\mu(ms) + \mu(m(s-1)) > 0$. Thus, for $n-a$ odd we have

$$|J_{n-a}| = \begin{cases} (q'+1)/2, & \text{if } q' \equiv 1 (\bmod 4), \\ (q'-1)/2, & \text{if } q' \equiv 3 (\bmod 4). \end{cases} \tag{26}$$

THEOREM 4.2. *Let $q \geq 5$ be an odd integer and let*

$$q' = \begin{cases} q, & \text{if } s \nmid q, \\ q/3, & \text{if } 3|q. \end{cases}$$

Then

$$N(G_q(1,2), n) \leq \frac{(q'+1)}{2q'}(3^n + (q'-1)(2+\cos \pi/q)^n).$$

Proof. It follows from (26) that the dominant term on the right-hand side of (25) is at most

$$\frac{1}{q'}\left(\frac{q'+1}{2}\right)\sum_{a=0}^{n}\binom{n}{a}2^{n-a} = \left(\frac{q'+1}{2q'}\right)3^n,$$

and the sum of the remaining terms is no more than

$$\frac{1}{q'}\left(\frac{q'+1}{2}\right)(q'-1)\sum_{a=0}^{n}\binom{n}{a}(1+\cos \pi/q')^{n-a}$$
$$= \left(\frac{q'+1}{2q'}\right)(q'-1)(2+\cos \pi/q')^n.$$

□

Acknowledgments

The authors wish to thank Gabor Simonyi for pointing out that our results on the cyclic triangle problem settled problem 5 in [14]. We also thank Alon Orlitsky for many helpful discussions, Robert Vanderbei for the linear programming calculations mentioned in Section 2, A. Blokhuis and A.E. Brouwer for pointing out the usefulness of Jamison's theorem.

References

1. A. Blokhuis, "On the Sperner capacity of the cyclic triangle," *J. Algebraic Combin.*, to appear.

2. A. E. Brouwer and A. Schrijver, "The blocking number of an affine space," *J. Combinatorial Theory (A)* **24** (1978), 251–253.
3. G. Cohen, J. Körner, and G. Simonyi, "Zero-error capacities and very different sequences," in *Sequences: Combinatorics, Compression, Security and Transmission*, R.M. Capacelli, eds., Springer-Verlag, 1990, 144–155.
4. J.H. Conway and N.J.A. Sloane, *Sphere Packings, Lattices, and Groups*, Springer-Verlag, New York, 1988.
5. L. Gargano, J. Körner, and U. Vaccaro, "Capacities: from information theory to extremal set theory," *J. Amer. Math. Soc.*, to appear.
6. L. Gargano, J. Körner, and U. Vaccaro, "Sperner capacities," *Graphs and Combinatorics* to appear.
7. L. Gargano, J. Körner, and U. Vaccaro, "Sperner theorems on directed graphs and qualitative independence," *J. Combinatorial Theory (A)* **61** (1992), 173–192.
8. W. Haemers, *Eigenvalue Techniques in Design and Graph Theory*, Reidel, Dordrecht, The Netherlands, 1980. Thesis T.H. Eindhoven, 1979. Math. Centr. Tract 121, Amsterdam, 1980.
9. W. Haemers, "On some problems of Lovász concerning the Shannon capacity of a graph," *IEEE Trans. Inform. Theory* **25** (1979), 231–232.
10. R.A. Horn and C.R. Johnson, *Matrix Analysis*, Cambridge University Press, Cambridge, 1985.
11. F.K. Hwang and W.-C. W. Li, "Two-connectivities of extended double loop networks," submitted to *J. Graph Theory*.
12. R.E. Jamison, "Covering finite fields with cosets of subspaces," *J. Combinatorial Theory (A)*, **22**, (1977), 253–266.
13. J. Körner, "Intersection number and capacities of graphs," submitted to *J. Combinatorial Theory (B)*.
14. J. Körner and G. Simonyi, "A Sperner-type theorem and qualitative independence," *J. Combinatorial Theory (A)* **59** (1992), 90–103.
15. L. Lovász, "On the Shannon capacity of a graph," *IEEE Trans. Inform. Theory* **25** (1979), 1–7.
16. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1979.
17. R.J. McEliece, E.R. Rodemich, H. Rumsey, Jr., and L.R. Welch, "New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities," *IEEE Trans. Inform. Theory* **23** (1977), 157–165.
18. C.E. Shannon, "The zero-error capacity of a noisy channel," *IRE Trans. Inform. Theory* **2** (1956), 8–19.
19. E. Sperner, "Ein Satz über Untermengen einer endlichen Menge," *Math. Z.* **27** (1928), 544–548.