PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 131, Number 11, Pages 3559–3569
S 0002-9939(03)06495-5
Article electronically published on June 5, 2003

A LIMIT THEOREM FOR THE SHANNON CAPACITIES OF ODD CYCLES I

TOM BOHMAN

(Communicated by John R. Stembridge)

Abstract. This paper contains a construction for independent sets in the powers of odd cycles. It follows from this construction that the limit as n goes to infinity of $n + 1/2 - \Theta(C_{2n+1})$ is zero, where $\Theta(G)$ is the Shannon capacity of the graph G.

1. Introduction

The *Shannon capacity* of a simple graph G is defined as follows:

$$\Theta(G) = \limsup_{n\to\infty} \left(\alpha(G^n)\right)^{1/n} = \sup_n \left(\alpha(G^n)\right)^{1/n}$$

where $\alpha(G)$ is the independence number of G and G^n is the nth power of G, the graph having vertex set $V(G)^n$ and an edge between vertices $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$ if and only if $\{x_i, y_i\} \in E(G)$ or $x_i = y_i$ for $i = 1, \ldots, n$. This graph invariant was introduced by Shannon in 1956 as a measure of the zero-error capacity of a noisy communication channel [12]. For an excellent introduction to and survey of zero-error information theory see [8]; for recent progress on some long-standing conjectures concerning Shannon capacity that are not directly related to this paper see [1].

It is easy to see that $\alpha(G) \leq \Theta(G)$. Shannon showed that a linear programming relaxation of the independence number gives an upper bound on the capacity. A *fractional vertex packing* of a graph G is an assignment w of nonnegative weights to the vertices of G such that $\sum_{x\in V(K)} w(x) \leq 1$ for all cliques K. The *weighted independence number* of G, which is denoted by $\alpha^*(G)$, is the maximum taken over all fractional vertex packings of $\sum_{x\in V(G)} w(x)$. Shannon showed that $\Theta(G) \leq \alpha^*(G)$ [12] (this upper bound was later studied by Rosenfeld [11]). These bounds suffice to compute the capacity of any graph G whose vertex set can be covered

Received by the editors May 17, 2000 and, in revised form, June 21, 2000 and September 18, 2001.

2000 *Mathematics Subject Classification.* Primary 94A15, 05C35, 05C38.

Key words and phrases. Shannon capacity, odd cycles.

This research was supported in part by NSF Grant DMS-9627408.

While this paper was on its way to press, the author discovered *A combinatorial packing problem*, by L. Baumert et al., 1971, which contains an idea that yields an alternate (and shorter) proof of Theorem 1.1. The shorter proof together with some observations and questions that arise from comparing the two ideas are treated in the forth-coming manuscript *A limit theorem for the Shannon capacities of odd cycles II*.

by a collection of $\alpha(G)$ cliques. This class of graphs includes all perfect graphs; in particular, it includes all even cycles and all graphs on 5 or fewer vertices other than C_5, the cycle on 5 vertices.

The Shannon capacity of C_5 was not determined until 1979, when Lovász showed that $\Theta(C_5) = \sqrt{5}$ [9]. He achieved this celebrated result by showing that the umbrella function $\vartheta(G)$ (also known as the 'Lovász theta function') gives an upper bound on the capacity. Shortly thereafter Haemers [5], [6] and McEliece, Rodemich and Rumsey [10] gave other upper bounds on the capacity. The Shannon capacities of odd cycles on 7 or more vertices remain unknown (the capacity of C_7 is, perhaps, one of the most notorious open problems in extremal combinatorics). One indication of the importance of odd cycles is the following conjecture of Berge [3], known as the strong perfect graph conjecture: a graph is imperfect if and only if it contains an odd cycle or the complement of an odd cycle as an induced subgraph.

In this paper we establish a limit theorem for the Shannon capacities of odd cycles. Since $\alpha(C_{2n+1}) = n$ and $\alpha^*(C_{2n+1}) = n + 1/2$, the quantity of interest in the limit is the difference $n + \frac{1}{2} - \Theta\left(C_{2n+1}\right)$. The best known upper bound on $\Theta(C_{2n+1})$ is given by the Lovász theta function:

$$\Theta(C_{2n+1}) \leq \vartheta(C_{2n+1}) = \frac{(2n+1)\cos\left(\pi/(2n+1)\right)}{1+\cos\left(\pi/(2n+1)\right)} = n + \frac{1}{2} - O(1/n).$$

Hales [7] established a lower bound on $\Theta(C_{2n+1})$ by determining $\alpha(C_{2n+1}^2)$:

$$\Theta\left(C_{2n+1}\right) \geq \sqrt{\alpha(C_{2n+1}^2)} = \sqrt{n^2 + \left\lfloor \frac{n}{2} \right\rfloor} = n + \frac{1}{4} - O(1/n). \tag{1.1}$$

While this general lower bound leaves a gap in the limit, Hales showed, by constructing a maximum independent set $\mathcal{H}_d$ in $C_{2^d+1}^d$, that the limit infimum as n goes to infinity of $n + \frac{1}{2} - \Theta\left(C_{2n+1}\right)$ is zero [7]. Bohman, Ruszinkó and Thoma recently improved the lower bound in (1.1) to $n + 1/3 - O(1/n)$ by constructing large independent sets in the third powers of all odd cycles, and they went on to conjecture that the limit as n goes to infinity of $n + \frac{1}{2} - \Theta\left(C_{2n+1}\right)$ is zero [4].

We construct nearly (in a sense made clear below) maximum independent sets in the dth powers of all odd cycles on $2^{d+2} + 1$ or more vertices. The construction is, in a sense, based on Hales' $\mathcal{H}_d$. To see that the independent sets we construct are nearly maximum it will suffice to appeal to the bound $\alpha(G \times H) \leq \alpha^*(G)\alpha(H)$ (first noted by Hales [7]) from which it follows that $\alpha\left(C_{2n+1}^d\right) \leq n(n+1/2)^{d-1}$.

Theorem 1.1. *For $d \geq 3$ fixed we have*

$$\alpha\left(C_{2n+1}^d\right) = n^d + \frac{d-1}{2} n^{d-1} + O\left(n^{d-2}\right).$$

It follows from this that the limit as n goes to infinity of $n + \frac{1}{2} - \left(\alpha(C_{2n+1}^d)\right)^{1/d}$ is $1/(2d)$. Therefore, we have the limit theorem conjectured in [4].

Corollary 1.2.

$$\lim_{n\to\infty} n + \frac{1}{2} - \Theta\left(C_{2n+1}\right) = 0.$$

The remainder of the paper is organized as follows. In the next section we introduce Hales' independent set $\mathcal{H}_d$ and establish notational conventions. The construction that proves Theorem 1.1 is divided into two phases, which are presented in sections 3 and 4. Phase I yields an independent set $\mathcal{I}_m$ containing $n^d + O\left(n^{d-1}\right)$

vertices in such a way that it leaves space for the placement of additional vertices during the formation of $\mathcal{I}'_m \supseteq \mathcal{I}_m$ in Phase II. The size of $\mathcal{I}'_m$ is determined in section 5.

2. Hales' construction

We begin with notational conventions. We henceforth identify the vertices of the graph C_r^s with the elements of the group $\mathbb{Z}_r^s$ in the natural way. We use the same symbol for both a vertex in the graph and the corresponding group element. Define

$$\mathcal{N} = \mathcal{N}_s = \{-1, 0, 1\}^s.$$

We can express adjacency in the graph in terms of the group operation; to be precise, for $a \neq b$ we have

$$\{a, b\} \in E(C_r^s) \Leftrightarrow a - b \in \mathcal{N}. \tag{2.1}$$

We will make use of the following operations on sets of group elements: for subsets X, Y of $\mathbb{Z}_r^s$ let $X+Y = \{x+y : x \in X, y \in Y\}$ and $X-Y = \{x-y : x \in X, y \in Y\}$. For r odd and $g \in \mathbb{Z}_r$ we define $\rho(g)$ to be the integer in the congruence class of g modulo r having the smallest absolute value. For $x = (x_1, \ldots, x_s) \in \mathbb{Z}_r^s$ define $\rho(x) = (\rho(x_1), \rho(x_2), \ldots \rho(x_s))$. Finally, we use the product notation $g \cdot h = g_1h_1 + \cdots + g_sh_s$ for $g \in \mathbb{Z}^s$ and group element $h = (h_1, \ldots, h_s)$.

We now turn to Hales' construction of the independent set $\mathcal{H}_d$ in $C_{2^d+1}^d$. For $d = 2, 3, \ldots$ define

$$h_d = \left(-2^{d-1}, 2^{d-2}, \ldots, 1\right)$$
$$\text{and} \quad \mathcal{H}_d = \left\{a \in \mathbb{Z}_{2^d+1}^d : h_d \cdot a = 0\right\}.$$

To show that $\mathcal{H}_d$ is an independent set we first note that $\mathcal{H}_d$ is a subgroup of $\mathbb{Z}_{2^d+1}^d$. If there exist $a, b \in \mathcal{H}_d$ that are adjacent, then it follows from (2.1) that $a-b$ (which is a subgroup element) is in $\mathcal{N}$. However, it is easy to see that $\mathcal{H}_d \cap \mathcal{N} = \{\mathbf{0}\}$.

3. Phase I

Let $d \geq 3$ be fixed and suppose $2n+1 \geq 4\left(2^d\right)+1$. Our construction of a large independent set in C_{2n+1}^d depends on the residue of n modulo 2^{d-1}. So, we introduce the notation $2n+1 = m = l2^d + r$ where $1 \leq r \leq 2^d - 1$. The independent set in C_m^d that we produce in Phase I will be denoted $\mathcal{I}_m$.

We begin with a subgroup of $\mathbb{Z}_m^d$ that corresponds to Hales' $\mathcal{H}_d$. Define

$$H_m = \left\{a \in \mathbb{Z}_m^d : h_d \cdot a = 0\right\}.$$

We will find it useful to establish a notation for expressing elements of this subgroup in terms of a particular set of generators. We consider the map $f : \mathbb{Z}_m^{d-1} \to H_m$ given by $f(x) = Ax$ where

$$A = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 \\ 2 & 1 & \ldots & 1 & 1 \\ 0 & 2 & \ldots & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 2 & 1 \\ 0 & 0 & \ldots & 0 & 2 \end{bmatrix}.$$

Note that the inverse of f is given by $f^{-1}(y) = By$ where

$$B = \begin{bmatrix} -1 & 1 & 0 & 0 & \dots & 0 & 0 \\ -2 & 1 & 1 & 0 & \dots & 0 & 0 \\ -4 & 2 & 1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ -2^{d-2} & 2^{d-3} & 2^{d-4} & 2^{d-5} & \dots & 1 & 1 \end{bmatrix},$$

and that f is an isomorphism. In the remainder of this section both B and h_d will be viewed over both $\mathbb{Z}_m$ and $\mathbb{Z}$. It will be clear from context in which setting we are working.

We construct $\mathcal{I}_m$ by first assigning to each $x \in \mathbb{Z}_m^{d-1}$ an independent set I_x in $\mathbb{Z}_m^d$ of the form

$$I_x = f(x) + S_x + t_x \tag{3.1}$$

where S_x is collection of multiples of $e_1 = (1, 0, \dots, 0)$ that 'expands' $f(x)$ into a vertex set consisting of either l or $l+1$ vertices and t_x is a translation in coordinates 2 through $d-1$. Define

$$E_i = \{-(i-1)e_1, -(i-3)e_1, \dots, (i-1)e_1\} \quad \text{for} \quad i = l-3, l, l+1.$$

The precise constraints that we place on S_x and t_x are as follows:

$$S_x \in \{E_l, E_{l+1}\} \quad \text{and} \quad t_x \in \{\pm 1_A : A \subseteq \{2, \dots, d-1\}\}. \tag{3.2}$$

We then set

$$\mathcal{I}_m = \bigcup_{x \in \mathbb{Z}_m^{d-1}} I_x.$$

Since each I_x is clearly an independent set (as the same holds for each S_x), the crux of the proof will be in showing that $I_x \cup I_y$ is an independent set for $x \neq y$.

It follows from (2.1) that $I_x \cup I_y$ is both a disjoint union and an independent set if and only if $(I_x - I_y) \cap \mathcal{N} = \emptyset$. It then follows from (3.1) that we have

$$I_x \cup I_y \text{ is independent} \quad \Leftrightarrow \quad f(y-x) \notin S_x - S_y + t_x - t_y - \mathcal{N}. \tag{3.3}$$

It follows from (3.2) that we have

$$S_x - S_y + t_x - t_y - \mathcal{N} \subseteq \bigcup_{\xi=-1}^{1} [-2l-1, 2l+1] \times (\xi + [-2,2])^{d-2} \times [-1,1] =: \mathcal{B}. \tag{3.4}$$

The set $H_m \cap \mathcal{B}$ has a very well organized preimage under f.

Claim 3.1. If $u \in \mathbb{Z}_m^{d-1}$ and $f(u) \in \mathcal{B}$, then there exists $\kappa \in \{-1, 0, 1\}$ such that $h_d \cdot \rho(f(u)) = \kappa m$ and

$$u_i \in \left\{ \left\lfloor \frac{\kappa m}{2^{d-i}} \right\rfloor - 1, \left\lfloor \frac{\kappa m}{2^{d-i}} \right\rfloor, \left\lceil \frac{\kappa m}{2^{d-i}} \right\rceil, \left\lceil \frac{\kappa m}{2^{d-i}} \right\rceil + 1 \right\} \quad \text{for} \quad i = 1, \dots, d-1.$$

Proof. Let $v \in H_m \cap \mathcal{B}$, $u = Bv$, $z = \rho(v)$ and $w = Bz$. It follows from the definition of $\mathcal{B}$ that we have $|h_d \cdot z| \leq (l+2)2^d - 2 < 2m$, and therefore there exists $\kappa \in \{-1, 0, 1\}$ such that $h_d \cdot z = \kappa m$. So, for $i = 1, \dots, d-1$, we have

$$2^{d-i} w_i - 2^{d-i-1} z_{i+1} + 2^{d-i-2} z_{i+2} + \dots + z_d = h_d \cdot z = \kappa m,$$

and therefore

$$2^{d-i} w_i = \kappa m + 2^{d-i-1} z_{i+1} - 2^{d-i-2} z_{i+2} - \dots - z_d.$$

It follows (taking into account the three possible values of ξ) that we have

$$w_i \in \left\{ \left\lfloor \frac{\kappa m}{2^{d-i}} \right\rfloor - 1, \left\lfloor \frac{\kappa m}{2^{d-i}} \right\rfloor, \left\lceil \frac{\kappa m}{2^{d-i}} \right\rceil, \left\lceil \frac{\kappa m}{2^{d-i}} \right\rceil + 1 \right\} \quad \text{for} \quad i = 1, \ldots, d-1.$$

□

So, if we choose S_x's and t_x's that satisfy (3.2), then the collection of y's for which I_y *might* contain a vertex adjacent to a vertex in a fixed I_x is very well organized. This collection consists of three parts, each of which is a small 'cube' in $\mathbb{Z}_m^{d-1}$.

Motivated by Claim 3.1, we partition $\mathbb{Z}_m^{d-1}$ into $2^{d-1}+1$ sets. We define this partition by specifying a collection of 2^{d-1} large pairwise-disjoint cubes. The set S_x and vector t_x that define I_x will be constants over each of these cubes. The other part in the partition is (of course) the 'rest,' all vertices not contained in one of the cubes. We set $I_x = \emptyset$ for each vertex x in this extra part (in Phase II of this construction we enlarge the independent set $\mathcal{I}_m$ constructed in this section to an independent set $\mathcal{I}'_m$ by assigning most of the elements of the 'rest' nonempty I_x's). In order to define the collection of cubes we first define

$$a_i = \left\lfloor \frac{im}{2^{d-1}} \right\rfloor, \qquad b_i = a_i + n - 5 \qquad \text{and} \qquad J_i = [a_i, b_i]$$

for $i = 0, \ldots, 2^{d-1}-1$. In the definition of the interval J_i we are working on the circle $\mathbb{Z}_m$; that is, if $a > b$, the interval $[a, b]$ is taken to mean $[a, m-1] \cup [0, b]$. Furthermore, the indices of the J_i's are taken to be elements of $\mathbb{Z}_{2^d-1}$. Note that we have

$$a_{i+2^{d-2}} - b_i \in \{5, 6\}, \tag{3.5}$$

and therefore this collection of intervals has the following property:

$$J_i \cap J_{i+2^{d-2}} = \emptyset. \tag{3.6}$$

We say that interval $J_{i+2^{d-2}}$ is the *antipode* of J_i. We are now ready to define the cubes. Define

$$\mathcal{C}_k = J_k \times J_{2k} \times J_{4k} \times \cdots \times J_{2^{d-2}k} \quad \text{for} \quad k = 0, \ldots, 2^{d-1}-1.$$

For a pair of cubes $\mathcal{C}_j, \mathcal{C}_k$ such that $j \neq k$ we let $\gamma = \gamma_{j,k}$ be the unique element of $\{1, \ldots, d-1\}$ such that

$$2^{\gamma-1} j + 2^{d-2} = 2^{\gamma-1} k.$$

Note that $2^{d-1-\gamma}$ is the largest power of two that divides $j-k$ (and this notion is well defined because we are working over $\mathbb{Z}_{2^{d-1}}$). Since $J_{2^{\gamma-1}j}$ and $J_{2^{\gamma-1}k}$ are antipodes, the cubes $\mathcal{C}_j$ and $\mathcal{C}_k$ are disjoint. The indices of these cubes are also taken to be elements of $\mathbb{Z}_{2^{d-1}}$. If $x \in \mathcal{C}_k$ is fixed, then it follows from Claim 3.1, (3.6) and (3.5) that $I_x \cup I_y$ is a priori independent (assuming that we follow the guidelines set forth in (3.2)) unless there exists $\kappa \in \{-1, 0, 1\}$ such that

$$y \in \mathcal{C}_{k+\kappa} \quad \text{and} \quad h_d \cdot \rho(f(y-x)) = \kappa m. \tag{3.7}$$

We now turn to the definition of the expansion S_x and translation t_x used for each $x \in \mathcal{C}_k$. Let $r' = r-1$. We first define two auxiliary sequences: a sequence $\alpha_0, \ldots, \alpha_{2^{d-1}}$ of nonnegative integers and a sequence $\beta_0, \ldots, \beta_{2^{d-1}}$ of 0's and 1's.

These are defined recursively: set $\alpha_0 = \beta_0 = 0$, and, for $k = 1, \dots, 2^{d-1}$, define α_k and β_k as follows:

$$2^{d-1}\left(\alpha_{k-1} + \beta_{k-1}\right) - kr' \begin{cases} \geq -2^{d-1} + r'/2 \Rightarrow \beta_k = 0, \\ < -2^{d-1} + r'/2 \Rightarrow \beta_k = 1, \end{cases}$$
$$\text{and} \quad \alpha_k = \alpha_{k-1} + \beta_{k-1} + \beta_k.$$

This sequence has a number of important properties.

Claim 3.2.

$$-2^{d-1} < 2^{d-1}\alpha_k - kr' < 2^{d-1} \quad \text{for} \quad k = 0, \dots, 2^{d-1}.$$

Proof. We first note the following:

$$\begin{aligned} \beta_k = 0 \quad &\Rightarrow \quad 2^{d-1}\alpha_k - kr' \geq -2^{d-1} + r'/2, \\ \beta_k = 1 \quad &\Rightarrow \quad 2^{d-1}\alpha_k - kr' < r'/2. \end{aligned} \tag{3.8}$$

Assume for the sake of contradiction that k is an index for which

$$2^{d-1}\alpha_k - kr' \leq -2^{d-1} \quad \text{and} \quad 2^{d-1}\alpha_{k-1} - (k-1)r' > -2^{d-1}. \tag{3.9}$$

It follows from these inequalities that $2^{d-1}(\beta_{k-1} + \beta_k) - r' < 0$, and it follows from (3.8) that $\beta_k = 1$. Therefore, $\beta_{k-1} = 0$ and $r' > 2^{d-1}$. Since $\beta_{k-1} = 0$, (3.8) implies that $2^{d-1}\alpha_{k-1} - (k-1)r' > -2^{d-1} + r'/2$. This inequality and (3.9) give $2^{d-1}(\beta_k + \beta_{k-1}) - r' = 2^{d-1} - r' < -r'/2$, a contradiction. A similar argument establishes the upper bound. □

Also note that for $k = 1, \dots, 2^{d-1}$ we have

$$\alpha_k = 2\sum_{j=0}^{k-1} \beta_j + \beta_k. \tag{3.10}$$

It follows that we have

$$\alpha_k \text{ is even } \Leftrightarrow \beta_k = 0. \tag{3.11}$$

We included $\alpha_{2^{d-1}}$ and $\beta_{2^{d-1}}$ in this sequence because it will be important to note below (since the indices of the cubes are given by the elements of $\mathbb{Z}_{2^{d-1}+1}$) that $\beta_0 = \beta_{2^{d-1}}$. This observation follows from Claim 3.2 and (3.11).

We are now ready to define the S_x's and t_x's. Again, we need to introduce some new notation. For $-2^{d-1} < z < 2^{d-1}$ an even integer let 1_z be the vector in $\mathbb{Z}_m^d$ of the form $\pm 1_A$ such that $A \subseteq \{2, \dots, d-1\}$ and

$$\left(0, 2^{d-2}, 2^{d-3}, \dots, 2, 0\right) \cdot 1_z = z.$$

For $x \in \mathcal{C}_k$ we set

$$S_x = \begin{cases} E_{l+1} & \text{if } \beta_k = 1, \\ E_l & \text{if } \beta_k = 0, \end{cases}$$
$$\text{and} \quad t_x = 1_{\alpha_k 2^{d-1} - kr'}.$$

This completes the definition of $\mathcal{I}_m$. It remains to show that $I_x \cup I_y$ is an independent set for $x \neq y$. By (3.7) it suffices to consider two cases: $x, y \in \mathcal{C}_k$ and $h_d \cdot \rho(f(y-x)) = 0$, and $x \in \mathcal{C}_k$, $y \in \mathcal{C}_{k+1}$ and $h_d \cdot \rho(f(y-x)) = m$. In both cases we appeal to (3.3). If $x, y \in \mathcal{C}_k$, then $t_x = t_y$ and

$$S_x - S_y + t_x - t_y - \mathcal{N} \subseteq [2l-1, 2l+1] \times [-1, 1]^{d-1} =: \mathcal{B}^1.$$

However $h_d \cdot \rho(z) \neq 0$ for all nonzero $z \in \mathcal{B}^1$. Suppose, on the other hand, that $x \in \mathcal{C}_k$, $y \in \mathcal{C}_{k+1}$ and $z = f(y-x) \in S_x - S_y + t_x - t_y - \mathcal{N}$. We have

$$\begin{aligned} h_d \cdot \rho(z) &\leq (2l - 2 + \beta_k + \beta_{k+1})2^{d-1} + (\alpha_k 2^{d-1} - kr') \\ &\quad - (\alpha_{k+1}2^{d-1} - (k+1)r') + 2^d - 1 \\ &= l2^d + (\alpha_k + \beta_k + \beta_{k+1} - \alpha_{k+1})\, 2^{d-1} + r' - 1 \\ &= l2^d + r' - 1 \\ &< m. \end{aligned}$$

Therefore, $\mathcal{I}_m$ is an independent set.

4. Phase II

In this phase we expand our construction to $\mathcal{I}'_m \supseteq \mathcal{I}_m$. As in the previous phase, we set $\mathcal{I}'_m = \bigcup_{x \in \mathbb{Z}_m^{d-1}} I_x$, where I_x is an independent set in $\mathbb{Z}_m^d$ of the form $I_x = f(x) + S_x + t_x$. The set I_x is taken to be what was given in Phase I for x in

$$\mathcal{C} := \bigcup_{k=0}^{2^d-1} \mathcal{C}_k.$$

The general guidelines for forming I_x for $x \notin \mathcal{C}$ are as follows: $S_x = E_{l-3}$ and

$$t_x \in \{\{1_A\}, \{-1_A\}, \{1_A, -1_A\} : A \subseteq \{2, \ldots, d-1\}\}.$$

Note that, while t_x may now consist of more than one vector, we still have (3.4) for arbitrary $x, y \in \mathbb{Z}_m^{d-1}$. Furthermore, if $x \notin \mathcal{C}$, then, since we take S_x to be so small, the vertex set $I_x \cup I_y$ is a priori independent unless

$$y \in x + \{-1, 0, 1\}^{d-1} \quad \text{and} \quad h_d \cdot \rho(f(y-x)) = 0. \tag{4.1}$$

We form a partition of $\mathbb{Z}_m^{d-1} \setminus \mathcal{C}$. As noted above, we will always set $S_x = E_{l-3}$; the partition will be used to determine the t_x's (t_x is not a constant over every part in the partition). We define the partition by giving a collection of $2^{d-1}(2^{d-1}-1)$ parts. For $x \in \mathbb{Z}_m^{d-1} \setminus \mathcal{C}$ that do not lie in any of these parts we set $I_x = \emptyset$.

The partition contains one part for each ordered pair of cubes $(\mathcal{C}_j, \mathcal{C}_k)$ where $j \neq k$. Recall that $\gamma = \gamma_{j,k}$ is given by $2^{\gamma-1}j + 2^{d-2} = 2^{\gamma-1}k$, that $J_{2^{\gamma-1}k}$ and $J_{2^{\gamma-1}j}$ are antipodal, and that coordinate γ is the only coordinate in which $\mathcal{C}_j$ and $\mathcal{C}_k$ are antipodal. Define

$$\begin{aligned} \mathcal{D}_{j,k} = (J_j \cap J_k)' \times \cdots \times \left(J_{2^{\gamma-2}j} \cap J_{2^{\gamma-2}k}\right)' \times X_{2^{\gamma-1}j} \\ \times (J_{2^\gamma j} \cap J_{2^\gamma k})' \times \cdots \times \left(J_{2^{d-2}j} \cap J_{2^{d-2}k}\right)' \end{aligned}$$

where $[a,b]' = [a+1, b-1]$ and X_i is one of the short intervals that lie between J_i and its antipode:

$$X_i = [b_i + 1, a_{i+2^{d-2}} - 1] \quad \text{for} \quad i = 0, \ldots, 2^{d-1} - 1.$$

Note that we actually have $2^{i-1}j = 2^{i-1}k$ for $i > \gamma$ (i.e. the intersection symbol in the definition of $\mathcal{D}_{j,k}$ could technically be removed for all coordinates after coordinate γ) and that we have

$$i, j, k \quad \text{distinct and} \quad \gamma_{i,j} = \gamma_{j,k} \quad \Rightarrow \quad \gamma_{i,k} \neq \gamma_{i,j}. \tag{4.2}$$

Claim 4.1. If $(j,k) \neq (j',k')$, then $\mathcal{D}_{j,k} + \mathcal{N}$ and $\mathcal{D}_{j',k'}$ are disjoint.

Proof. Suppose $j' \neq j$. Let $\gamma' = \gamma_{j',j}$. Since the intervals $J_{2^{\gamma'-1}j}$ and $J_{2^{\gamma'-1}j'}$ are antipodal, the intervals $J'_{2^{\gamma'-1}j}$, $X_{2^{\gamma'-1}j}$, $J'_{2^{\gamma'-1}j'}$ and $X_{2^{\gamma'-1}j'}$ are not only pairwise disjoint but also nonadjacent on the circle $\mathbb{Z}_m$. Since coordinate γ' of elements of $\mathcal{D}_{j,k}$ lie in the first two of these sets and coordinate γ' of elements of $\mathcal{D}_{j',k'}$ lie in the latter two of these sets, $\mathcal{D}_{j,k} + \mathcal{N}$ and $\mathcal{D}_{j',k'}$ are disjoint.

Suppose $j = j'$ and $k \neq k'$. Let $\gamma = \gamma_{j,k}$ and $\gamma' = \gamma_{j,k'}$. It follows from (4.2) that if $\gamma = \gamma'$, then there exists a coordinate other than γ in which $\mathcal{C}_k$ and $\mathcal{C}_{k'}$ are antipodal. In this case $\mathcal{D}_{j,k} + \mathcal{N}$ and $\mathcal{D}_{j',k'}$ are clearly disjoint. If, on the other hand, $\gamma \neq \gamma'$, then coordinate γ' of elements of $\mathcal{D}_{j,k} + \mathcal{N}$ are contained in $J_{2^{\gamma'-1}j}$ while coordinate γ' of elements of $\mathcal{D}_{j',k'}$ are contained in $X_{2^{\gamma'-1}j}$. □

Claim 4.2. If i, j, k are distinct, then $\mathcal{D}_{j,k} + \mathcal{N}$ and $\mathcal{C}_i$ are disjoint.

Proof. Let $\gamma = \gamma_{j,k}$ and assume without loss of generality that $\gamma' := \gamma_{i,j} \neq \gamma$ (note that we have applied (4.2)). The claim follows from the fact that $\mathcal{C}_i$ and $\mathcal{C}_j$ are antipodal in coordinate γ'. □

The cube $\mathcal{D}_{j,k}$ is, in a sense, isolated from most of the rest of $\mathbb{Z}_m^{d-1}$. It follows from Claims 4.1 and 4.2 and (4.1) that if $x \in \mathcal{D}_{j,k}$, then $I_x \cup I_y$ is a priori independent unless $y \in \mathcal{D}_{j,k} \cup \mathcal{C}_j \cup \mathcal{C}_k$.

We henceforth consider a fixed $\mathcal{D}_{j,k}$. Let t^j be the translation t_x assigned to $x \in \mathcal{C}_j$, and t^k be the translation assigned to elements of $\mathcal{C}_k$ and $\gamma = \gamma_{j,k}$. We have, in $\mathbb{Z}_{2^{d-1}}$,

$$\left(0, 2^{d-2}, \ldots, 2, 0\right) \cdot \left(t^k - t^j\right) = jr' - kr'$$

and that $2^{d-\gamma}$ divides this difference. It follows that $t = (t_1, \ldots, t_d) = t^k - t^j$ has a very special form: either $t_{\gamma+1}, \ldots, t_d = 0$ or there exists $\delta \geq \gamma + 1$ and $\eta \in \{-1, 1\}$ such that $t_{\gamma+1}, \ldots, t_{\delta-1} = \eta$, $t_\delta = 2\eta$ and $t^j_{\delta+1} = t^k_{\delta+1} = \cdots = t^j_d = t^k_d = 0$. Define

$$t^{j,\gamma} = \left(0, \ldots, 0, t^j_{\gamma+1}, t^j_{\gamma+2}, \ldots, t^j_d\right).$$

We consider four cases. While the definition of the t_x's is very delicate, the proof of independence is based on very simple observations concerning $f(y)$ for $y \in \mathcal{N}$. One of these simple observations is codified in the following claim (which is presented without proof).

Claim 4.3. If $x = (x_1, \ldots, x_{d-1}) \in \mathcal{N} \cap \mathbb{Z}_m^{d-1}$, $x_i \neq 0$ and $v = (v_1, \ldots, v_d) = f(x)$, then there exists $j > i$ such that $v_j \in \{-2, 2\}$.

Throughout the cases we consider $x \in \mathcal{D}_{j,k}$ and $y \in (x + \mathcal{N}) \cap (\mathcal{C}_j \cup \mathcal{D}_{j,k} \cup \mathcal{C}_k)$, $y \neq x$. For such a pair we use the notation $\mathcal{B}_{x,y} = S_x - S_y + t_x - t_y + \mathcal{N}$.

Case 1. $t_{\gamma+1}, \ldots, t_d = 0$.

Here we set $t_x = \left\{t^{j,\gamma}\right\} = \left\{t^{k,\gamma}\right\}$ for all $x \in \mathcal{D}_{j,k}$. We have

$$\mathcal{B}_{x,y} \subseteq \begin{cases} [-2l+3, 2l-3] \times [-2,2]^{\gamma-1} \times [-1,1]^{d-\gamma} & \text{if } y \in \mathcal{C}_j \cup \mathcal{C}_k, \\ [-2l+7, 2l-7] \times [-1,1]^{d-1} & \text{if } y \in \mathcal{D}_{j,k}. \end{cases}$$

If $y \in \mathcal{D}_{j,k}$, then it is clear that no nonzero $z \in \mathcal{B}_{x,y}$ satisfies $h_d \cdot \rho(z) = 0$. If $y \in \mathcal{C}_j \cup \mathcal{C}_k$, then coordinate γ of $y - x$ is nonzero and it follows from Claim 4.3 that $f(y - x) \notin \mathcal{B}_{x,y}$. Therefore $I_x \cup I_y$ is an independent set.

Case 2. $\delta \neq \gamma + 1$.

Here we set $t_x = \{t^{j,\gamma}\}$ for all $x \in \mathcal{D}_{j,k}$. Define

$$\begin{aligned}\mathcal{B}^1 &= [-2l+3, 2l-3] \times [-2,2]^{\gamma-1} \times [-1,1]^{d-\gamma},\\ \mathcal{B}^2 &= [-2l+7, 2l-7] \times [-1,1]^{d-1} \quad \text{and}\\ \mathcal{B}^3 &= [-2l+3, 2l-3] \times [-2,2]^{\gamma-1} \times (-\eta + [-1,1])^{\delta-\gamma-1}\\ &\qquad \times (-2\eta + [-1,1]) \times [-1,1]^{d-\delta}.\end{aligned}$$

If $y \in \mathcal{C}_j$, then $\mathcal{B}_{x,y} \subseteq \mathcal{B}^1$ and $y_\gamma = x_\gamma - 1$. It then follows from Claim 4.3 that $f(y-x) \notin \mathcal{B}_{x,y}$. If $y \in \mathcal{D}_{j,k}$, then $\mathcal{B}_{x,y} \subseteq \mathcal{B}^2$, but there is clearly no nonzero $v \in \mathcal{B}^2$ such that $h_d \cdot \rho(v) = 0$.

Suppose $y \in \mathcal{C}_k$. In this case $\mathcal{B}_{x,y} \subseteq \mathcal{B}^3$. Assuming that $y \in x + \mathcal{N}$ and $f(y-x) \in \mathcal{B}^3$, we work backwards through the coordinates to attain conditions on y. Note first that $y_i = x_i$ for $i = d-1, \dots, \delta$. It then follows that $y_{\delta-1} = x_{\delta-1} + \eta$ and $y_i = x_i$ for $i = \delta-2, \dots, \gamma$. However, $y_\gamma = x_\gamma - 1$.

Thus, $I_x \cup I_y$ is an independent set.

Case 3. $\delta = \gamma + 1$ and $\eta = 1$.

Note that $t^j_{\gamma+1} = -1$ and $t^k_{\gamma+1} = 1$. For $x = (x_1, \dots, x_{d-1}) \in \mathcal{D}_{j,k}$ we set

$$t_x = \begin{cases} \{e_{\gamma+1}\} & \text{if } x_\gamma \neq b_{2^{\gamma-1}j} + 1,\\ \{e_{\gamma+1}, -e_{\gamma+1}\} & \text{if } x_\gamma = b_{2^{\gamma-1}j} + 1.\end{cases}$$

Subcase 3.1. $x_\gamma = b_{2^{\gamma-1}j} + 1$.

Since $x + \mathcal{N}$ does not intersect $\mathcal{C}_k$ we have $y \in \mathcal{C}_j \cup \mathcal{D}_{j,k}$. Define

$$\begin{aligned}\mathcal{B}^1 &= [-2l+3, 2l-3] \times [-2,2]^{\gamma-1} \times [-1,3] \times [-1,1]^{d-\delta}\\ \mathcal{B}^2 &= [-2l+7, 2l-7] \times [-1,1]^{\gamma-1} \times [-3,3] \times [-1,1]^{d-\delta}, \text{ and}\\ \mathcal{B}^3 &= [-2l+7, 2l-7] \times [-1,1]^{\gamma-1} \times [-3,1] \times [-1,1]^{d-\delta}.\end{aligned}$$

Suppose $y \in \mathcal{C}_j$. We have $\mathcal{B}_{x,y} \subseteq \mathcal{B}^1$ and $y_\gamma = x_\gamma - 1$. By Claim 4.3, if there exists $i > \gamma$ such that $x_i \neq y_i$, then $f(y-x) \notin \mathcal{B}^1$. On the other hand, if $x_i = y_i$ for $i = \gamma+1, \dots, d-1$, then coordinate $\gamma+1$ of $f(y-x)$ is -2 and $f(y-x) \notin \mathcal{B}^1$.

Suppose $y \in \mathcal{D}_{j,k}$ and $y_\gamma = x_\gamma$. In this case we have $\mathcal{B}_{x,y} \subseteq \mathcal{B}^2$. Let i be the largest index for which $x_i \neq y_i$. Since $i \neq \gamma$, the vector $f(y-x)$ is not in $\mathcal{B}^2$.

Finally, suppose $y \in \mathcal{D}_{j,k}$ and $y_\gamma = x_\gamma + 1$. We have $\mathcal{B}_{x,y} \subseteq \mathcal{B}^3$. If $z \in \mathcal{B}^3$ is nonzero and $h_d \cdot \rho(z) = 0$, then $z_{\gamma+1} = -2$ and $z_{\gamma+2}, \dots, z_d = 0$. However, $f(y-x)$ cannot be such a vector as $y_\gamma - x_\gamma = 1$.

Subcase 3.2. $x_\gamma \neq b_{2^{\gamma-1}j} + 1$.

We may assume $y \in \mathcal{D}_{j,k} \cup \mathcal{C}_k$ and $y_\gamma \neq b_{2^{\gamma-1}j} + 1$. We have

$$\mathcal{B}_{x,y} \subseteq \begin{cases} [-2l+1, 2l-1] \times [-2,2]^{\gamma-1} \times [-1,1]^{d-\gamma} & \text{if } y \in \mathcal{C}_k,\\ [-2l+5, 2l-5] \times [-1,1]^{d-1} & \text{if } y \in \mathcal{D}_{j,k},\end{cases}$$

and the proof follows as in Case 1.

Case 4. $\delta = \gamma + 1$ and $\eta = -1$.

Note that $t^j_{\gamma+1} = 1$ and $t^k_{\gamma+1} = -1$. We set

$$I_x = \begin{cases} f(x) + E_{l-3} - e_{\gamma+1} & \text{if } x_\gamma \neq b_{2^{\gamma-1}j} + 1, \\ \emptyset & \text{if } x_\gamma = b_{2^{\gamma-1}j} + 1. \end{cases}$$

The proof that $I_x \cup I_y$ is independent follows as in Case 1.

5. Counting

While a precise reckoning of the number of vertices in $\mathcal{I}'_m$ is possible, we opt for an estimate only precise enough to establish Theorem 1.1. Define

$$\mathcal{D} = \bigcup_{j \neq k} \mathcal{D}_{j,k} \quad \text{and} \quad \dot{\mathcal{X}} = \bigcup_{i=0}^{2^{d-1}-1} \dot{X}_i$$

where $[\dot{a, b}] = [a-1, b+1]$. We count as follows:

$$|\mathcal{I}'_m| = (l-3)\left(|\mathcal{C}| + |\mathcal{D}|\right) + 3\,|\mathcal{C}_k|\,2^{d-1} + |\mathcal{C}_k| \cdot |\{i : \beta_i = 1\}|\,.$$

It follows from Claim 3.2 that $\alpha_{2^{d-1}} = r'$. It then follows from (3.11) that $\beta_{2^{d-1}} = 0$ and from (3.10) that the number of β_i's that equal 1 is $r'/2$. The asymptotic behavior of $|\mathcal{C}| + |\mathcal{D}|$ follows from

$$x = (x_1, \ldots, x_{d-1}) \in \mathbb{Z}_m^{d-1} \quad \text{and} \quad |\{i : x_i \in \dot{\mathcal{X}}\}| \leq 1 \quad \Rightarrow \quad x \in \mathcal{C} \cup \mathcal{D}.$$

These observations imply that $|\mathcal{I}'_m| = n^d + (d-1)n^{d-1}/2 + O\left(n^{d-2}\right)$.

Acknowledgment

I would like to thank Ron Holzman for pointing out a number of errors in an earlier version.

References

[1] N. Alon, The Shannon capacity of a union, *Combinatorica*, 18 (1998), 301-310. MR **2000i:**05096

[2] L. Baumert, R. McEliece, E. Rodemich, H. Rumsey, R. Stanley, and H. Taylor, A Combinatorial Packing Problem, *Computers in Algebra and Number Theory*, American Mathematical Society, Providence, RI, 1971, pp. 97-108. MR **49:**2437

[3] C. Berge, *Balanced hypergraphs and some applications to graph theory. A survey of combinatorial theory,* North-Holland, Amsterdam and London, 1973. MR **51:**2970

[4] T. Bohman, M. Ruszinkó, and L. Thoma, Shannon capacity of large odd cycles, *Proceedings of the 2000 IEEE International Symposium on Information Theory*, June 25-30, Sorrento, Italy, p. 179.

[5] W. Haemers, On some problems of Lovász concerning the Shannon capacity of a graph, *IEEE Transactions on Information Theory*, 25(2) (1979), 231–232. MR **80g:**94040

[6] W. Haemers, An upper bound for the Shannon capacity of a graph, *Colloquia Mathematica Societatis János Bolyai, 25: Algebraic Methods in Graph Theory,* Szeged (Hungary), 1978, 267-272. MR **83m:**05098

[7] R. S. Hales, Numerical invariants and the strong product of graphs, *Journal of Combinatorial Theory – B*, 15 (1973), 146-155. MR **48:**177

[8] J. Körner and A. Orlitsky, Zero-error information theory, *IEEE Transactions on Information Theory* 44(6) (1998), 2207-2229. MR **99h:**94034

[9] L. Lovász, On the Shannon capacity of a graph, *IEEE Transactions on Information Theory* 25(1) (1979), 1-7. MR **81g:**05095

[10] R. J. McEliece, E. R. Rodemich, and H. C. Rumsey, The Lovász bound and some generalizations, *Journal of Combinatorics, Information and Systems Science* 3 (1978), 134-152. MR **80a:**05168

[11] M. Rosenfeld, On a problem of C. E. Shannon in graph theory, *Proceedings of the American Mathematical Society*, 18 (1967), 315-319. MR **34:**7405

[12] C. E. Shannon, The zero-error capacity of a noisy channel, *Institute of Radio Engineers Transactions on Information Theory*, 2(3) (1956), 8–19. MR **19:**623b

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

E-mail address: tbohman@moser.math.cmu.edu

Current address: Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213