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 \( n \to \infty \) 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:
\[
\Theta(G) = \limsup_{n \to \infty} \left( \frac{\alpha(G^n)}{n} \right)^{1/n} = \sup_n \left( \frac{\alpha(G^n)}{n} \right)^{1/n}
\]
where \( \alpha(G) \) is the independence number of \( G \) and \( G^n \) is the \( n^{th} \) 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
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 $n + 1/2 - \Theta(C_{2n+1})$. The best known upper bound on $\Theta(C_{2n+1})$ is given by the Lovász theta function:

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

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

$$\Theta(C_{2n+1}) \geq \sqrt{\alpha(C_{2n+1}^2)} = \sqrt{n^2 + \frac{n}{2}} = n + \frac{1}{4} - O(1/n).$$

While this general lower bound leaves a gap in the limit, Hales showed, by constructing a maximum independent set $H_d$ in $C_{2n+1}^d$, that the limit infimum as $n$ goes to infinity of $n + \frac{1}{2} - \Theta(C_{2n+1})$ is zero [7]. Bohman, Ruszinkó and Thoma recently improved the lower bound in [11] 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 $n + \frac{1}{2} - \Theta(C_{2n+1})$ is zero [4].

We construct nearly (in a sense made clear below) maximum independent sets in the $d^{th}$ powers of all odd cycles on $2^{d+2} + 1$ or more vertices. The construction is, in a sense, based on Hales’ $H_d$. 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 $\alpha(C_{2n+1}^d) \leq n(n + 1/2)^{d-1}$.

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

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

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

**Corollary 1.2.**

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

The remainder of the paper is organized as follows. In the next section we introduce Hales’ independent set $H_d$ 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 $n^d + O(n^{d-1})$
vertices in such a way that it leaves space for the placement of additional vertices during the formation of $I'_m \supseteq I_m$ in Phase II. The size of $I_m$ is determined in section 5.

2. Hales’ construction

We begin with notational conventions. We henceforth identify the vertices of the graph $C^n_r$ with the elements of the group $Z^n_r$ in the natural way. We use the same symbol for both a vertex in the graph and the corresponding group element. Define

\[ N = N_s = \{-1, 0, 1\}^s. \]

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

\[ \{a, b\} \in E(C^n_r) \iff a - b \in N. \]

We will make use of the following operations on sets of group elements: for subsets $X, Y$ of $Z^n_r$ 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 $a \in Z_r$ we define $\rho(a)$ to be the integer in the congruence class of $g$ modulo $r$ having the smallest absolute value. For $x = (x_1, \ldots, x_s) \in Z^n_r$ define $\rho(x) = (\rho(x_1), \rho(x_2), \ldots, \rho(x_s))$. Finally, we use the product notation $g \cdot h = g_1 h_1 + \cdots + g_s h_s$ for $g \in Z^n_r$ and group element $h = (h_1, \ldots, h_s)$.

We now turn to Hales’ construction of the independent set $H_d$ in $C^{d\ 2d+1}_r$. For $d = 2, 3, \ldots$ define

\[ h_d = (-2d-1, 2d-2, \ldots, 1) \]

and \[ H_d = \{ a \in Z^{d\ 2d+1}_r : h_d \cdot a = 0 \}. \]

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

3. Phase I

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

We begin with a subgroup of $Z^{d\ 2d+1}_r$ that corresponds to Hales’ $H_d$. Define

\[ H_m = \{ a \in Z^{d\ 2d+1}_r : h_d \cdot a = 0 \}. \]

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 $f : Z^{d\ 2d+1}_r \to H_m$ given by $f(x) = Ax$ where

\[ A = \begin{bmatrix} 1 & 1 & \ldots & 1 & 1 \\ 2 & 1 & \ldots & 1 & 1 \\ 0 & 2 & \ldots & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 2 & 1 \\ 0 & 0 & \ldots & 0 & 2 \end{bmatrix}. \]
Note that the inverse of \( f \) is given by \( f^{-1}(y) = By \) where
\[
B = \begin{bmatrix}
-1 & 1 & 0 & 0 & \cdots & 0 & 0 \\
-2 & 1 & 1 & 0 & \cdots & 0 & 0 \\
-4 & 2 & 1 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
-2^{d-2} & 2^{d-3} & 2^{d-4} & 2^{d-5} & \cdots & 1 & 1
\end{bmatrix},
\]
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 \( I_m \) 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
\[
I_x = f(x) + S_x + t_x
\]
where \( S_x \) is collection of multiples of \( e_1 = (1,0,\ldots,0) \) 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
\[
E_i = \{-(i-1)e_1, -(i-3)e_1, \ldots, (i-1)e_1 \} \quad \text{for} \quad i = l-3, l, l+1.
\]
The precise constraints that we place on \( S_x \) and \( t_x \) are as follows:
\[
S_x \subset \{E_i, E_{i+1}\} \quad \text{and} \quad t_x \subset \{\pm 1_A : A \subset \{2, \ldots, d-1\}\}.
\]
We then set
\[
I_m = \bigcup_{x \in \mathbb{Z}_m^{d-1}} I_x.
\]
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
\[
I_x \cup I_y \text{ is independent } \iff f(y-x) \notin S_x - S_y + t_x - t_y - \mathcal{N}.
\]
It follows from (3.2) that we have
\[
S_x - S_y + t_x - t_y - \mathcal{N} \subset \bigcup_{\xi=1}^1 [-2l-1, 2l+1] \times (\xi + [-2, 2])^{d-2} \times [-1, 1] =: B.
\]
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
\[
u_i \in \left\{ \left\lfloor \frac{km}{2^{d-i}} \right\rfloor, \left\lfloor \frac{km}{2^{d-i}} \right\rfloor, \left\lfloor \frac{km}{2^{d-i}} \right\rfloor, \left\lfloor \frac{km}{2^{d-i}} \right\rfloor + 1 \right\} \quad \text{for} \quad i = 1, \ldots, d-1.
\]

**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 \( |h_d \cdot z| \leq (l+2)^{d-2} < 2m \) and therefore there exists \( \kappa \in \{-1, 0, 1\} \) such that \( h_d \cdot z = \kappa m \). So, for \( i = 1, \ldots, d-1 \), we have
\[
2^{d-i}w_i - 2^{d-i-1}z_{i+1} + 2^{d-i-2}z_{i+2} + \cdots + z_d = h_d \cdot z = \kappa m,
\]
and therefore
\[
2^{d-i}w_i = \kappa m + 2^{d-i-1}z_{i+1} - 2^{d-i-2}z_{i+2} - \cdots - z_d.
\]
In order to define the collection of cubes we first define $x$ for each $i$.

For a pair of cubes $Z$ organized. This collection consists of three parts, each of which is a small ‘cube’ in $Z^{d-1}$.

Motivated by Claim 3.1, we partition $Z^{d-1}$ 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 $I_x$ constructed in this section to an independent set $I_m$ by assigning most of the elements of the ‘rest’ nonempty $I_x$’s).

In order to define the collection of cubes we first define

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

for $i = 0, \ldots, 2^{d-1} - 1$. In the definition of the interval $J_i$ we are working on the circle $Z_m$: 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 $Z_{2^{d-1}}$. Note that we have

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

and therefore this collection of intervals has the following property:

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

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

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

For a pair of cubes $C_j, C_k$ 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 $Z_{2^{d-1}}$). Since $J_{2^{\gamma - 1}j}$ and $J_{2^{\gamma - 1}k}$ are antipodes, the cubes $C_j$ and $C_k$ are disjoint. The indices of these cubes are also taken to be elements of $Z_{2^{d-1}}$. If $x \in C_k$ is fixed, then it follows from Claim 3.1 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

$$ y \in C_{k+\kappa} \quad \text{and} \quad h_d \cdot \rho(f(y - x)) = \kappa m. $$

We now turn to the definition of the expansion $S_x$ and translation $t_x$ used for each $x \in C_k$. 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 $k = 1, \ldots, 2^{d-1}$, define $\alpha_k$ and $\beta_k$ as follows:

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

and $\alpha_k = \alpha_{k-1} + \beta_{k-1} + \beta_k$.

This sequence has a number of important properties.

**Claim 3.2.**

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

**Proof.** We first note the following:

$$(3.8) \quad \beta_k = 0 \quad \Rightarrow \quad 2^{d-1}\alpha_k - kr' \geq -2^{d-1} + r'/2,$$

$$(3.9) \quad \beta_k = 1 \quad \Rightarrow \quad 2^{d-1}\alpha_k - kr' < r'/2.$$

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

$$(3.10) \quad 2^{d-1}\alpha_k - kr' \leq -2^{d-1} \quad \text{and} \quad 2^{d-1}\alpha_{k-1} - (k-1)r' > -2^{d-1}.$$ 

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 $k = 1, \ldots, 2^{d-1}$ we have

$$(3.11) \quad \alpha_k = 2 \sum_{j=0}^{k-1} \beta_j + \beta_k.$$ 

It follows that we have

$$(3.12) \quad \alpha_k \text{ is even} \iff \beta_k = 0.$$ 

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 $\mathbb{Z}^d_m$ of the form $\pm 1_A$ such that $A \subseteq \{2, \ldots, d-1\}$ and

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

For $x \in C_k$ we set

$$ S_x = \begin{cases} E_{t+1} & \text{if } \beta_k = 1, \\
E_l & \text{if } \beta_k = 0, 
\end{cases}$$

and $t_x = 1_{\alpha_k 2^{d-1} - kr'}$.

This completes the definition of $I_m$. 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: $x, y \in C_k$ and $h_d \cdot \rho(f(y-x)) = 0$, and $x \in C_k$, $y \in C_{k+1}$ and $h_d \cdot \rho(f(y-x)) = m$. In both cases we appeal to (3.3). If $x, y \in C_k$, then $t_x = t_y$ and

$$ S_x - S_y + t_x - t_y - N \subseteq [2l - 1, 2l + 1] \times [-1, 1]^{d-1} =: \mathcal{B}^1.$$
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 \( z = f(y - x) \in S_x - S_y + t_x - t_y - N \). We have

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

Therefore, \( I_m \) is an independent set.

4. Phase II

In this phase we expand our construction to \( I'_m \supseteq I_m \). As in the previous phase, we set \( I'_m = \bigcup_{x \in \mathbb{Z}^d_m} I_x \), where \( I_x \) is an independent set in \( \mathbb{Z}^d_m \) 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 \( \|t_x\| \leq 3 \) for arbitrary \( x, y \in \mathbb{Z}^d_m \). 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

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

We form a partition of \( \mathbb{Z}^{d-1} \setminus \mathcal{C} \). 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 \( x \in \mathbb{Z}^{d-1}_m \setminus \mathcal{C} \) 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 \( 2^{l-1}j + 2^{d-2} = 2^{l-1}k \), that \( J_{2^l-1} \) and \( J_{2^l-1} \) are antipodal, and that coordinate \( \gamma \) is the only coordinate in which \( \mathcal{C}_j \) and \( \mathcal{C}_k \) are antipodal. Define

\[
\mathcal{D}_{j,k} = (J_j \cap J_k)' \times \cdots \times (J_{2^{l_1}-1} \cap J_{2^{l_2}-1})' \times X_{2^{l_1}-1}
\]

\[
\times (J_{2^{l_1}} \cap J_{2^{l_2}})' \times \cdots \times (J_{2^{l_3}} \cap J_{2^{l_4}})'
\]

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 \( \gamma \)) and that we have

\[
i, j, k \quad \text{distinct and} \quad \gamma_{i,j} = \gamma_{j,k} \Rightarrow \gamma_{i,k} \neq \gamma_{i,j}.
\]

Claim 4.1. If \( (j, k) \neq (j', k') \), then \( \mathcal{D}_{j,k} + N \) 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 \( J'_{2^{\gamma'-1}j} \cdot X_{2^{\gamma'-1}j} \), \( J'_{2^{\gamma'-1}j'} \) and \( X_{2^{\gamma'-1}j} \) are not only pairwise disjoint but also nonadjacent on the circle \( \mathbb{Z}_m \). Since coordinate \( \gamma' \) of elements of \( D_{j,k} \) lie in the first two of these sets and coordinate \( \gamma' \) of elements of \( D_{j',k'} \) lie in the latter two of these sets, \( D_{j,k} + N \) and \( D_{j',k'} \) are disjoint.

Suppose \( j = j' \) and \( k \neq k' \). Let \( \gamma = \gamma_{j,k} \) and \( \gamma' = \gamma_{j,k'} \). It follows from (1.2) that if \( \gamma = \gamma' \), then there exists a coordinate other than \( \gamma \) in which \( C_k \) and \( C_{k'} \) are antipodal. In this case \( D_{j,k} + N \) and \( D_{j',k'} \) are clearly disjoint. If, on the other hand, \( \gamma \neq \gamma' \), then coordinate \( \gamma' \) of elements of \( D_{j,k} + N \) are contained in \( J_{2^{\gamma'-1}j} \) while coordinate \( \gamma' \) of elements of \( D_{j',k'} \) are contained in \( X_{2^{\gamma'-1}j} \).

Claim 4.2. If \( i,j,k \) are distinct, then \( D_{j,k} + N \) and \( C_i \) 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 (1.2)). The claim follows from the fact that \( C_i \) and \( C_j \) are antipodal in coordinate \( \gamma' \).

The cube \( D_{j,k} \) is, in a sense, isolated from most of the rest of \( \mathbb{Z}_m^{d-1} \). It follows from Claims 4.1 and 1.2 and 1.1 that if \( x \in D_{j,k} \), then \( I_x \cup I_y \) is a priori independent unless \( y \in D_{j,k} \cup C_j \cup C_k \).

We henceforth consider a fixed \( D_{j,k} \). Let \( t^j \) be the translation \( t \) assigned to \( x \in C_j \), and \( t^k \) be the translation assigned to elements of \( C_k \) and \( \gamma = \gamma_{j,k} \). We have, in \( \mathbb{Z}_m^{d-1} \),

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

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 \( t^k_\delta + t^j_\delta = t^k_{\delta+1} = \ldots = t^k_d = t^j_d = 0 \). Define

\[ t^{\beta;\gamma} = \left(0, \ldots, 0, t^j_{\gamma+1}, t^j_{\gamma+2}, \ldots, t^j_d \right) \]

We consider four cases. While the definition of the \( t^{\beta;\gamma} \)'s is very delicate, the proof of independence is based on very simple observations concerning \( f(y) \) for \( y \in N \). One of these simple observations is codified in the following claim (which is presented without proof).

Claim 4.3. If \( x = (x_1, \ldots, x_{d-1}) \in N \cap \mathbb{Z}_m^{d-1}, x_i \neq 0 \) 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 \( x \in D_{j,k} \) and \( y \in (x + N) \cap (C_j \cup D_{j,k} \cup C_k) \), \( y \neq x \). For such a pair we use the notation \( B_{x,y} = S_x - S_y + t_x - t_y + N \).

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

Here we set \( t_x = \{ t^{j;\gamma} \} \) for all \( x \in D_{j,k} \). We have

\[ B_{x,y} = \begin{cases} [-2l + 3, 2l - 3] \times [-2, 2]^{\gamma-1} \times [-1, 1]^{d-\gamma} & \text{if } y \in C_j \cup C_k, \\ [-2l + 7, 2l - 7] \times [-1, 1]^{d-1} & \text{if } y \in D_{j,k}. \end{cases} \]

If \( y \in D_{j,k} \), then it is clear that no nonzero \( z \in B_{x,y} \) satisfies \( h_d \cdot \rho(z) = 0 \). If \( y \in C_j \cup C_k \), then coordinate \( \gamma \) of \( y - x \) is nonzero and it follows from Claim 4.3 that \( f(y - x) \notin B_{x,y} \). Therefore \( I_x \cup I_y \) is an independent set.

Case 2. \( \delta \neq \gamma + 1 \).
Here we set $t_x = \{t^i : y\}$ for all $x \in D_{j,k}$. Define

$B^1 = [-2l + 3, 2l - 3] \times [-2, 2]^{\gamma - 1} \times [-1, 1]^{d - \gamma},$

$B^2 = [-2l + 7, 2l - 7] \times [-1, 1]^{d - 1}$ and

$B^3 = [-2l + 3, 2l - 3] \times [-2, 2]^{\gamma - 1} \times (-\eta + [-1, 1])^{\delta - \gamma - 1}$

$\times (-2\eta + [-1, 1]) \times [-1, 1]^{d - \delta}.$

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

Suppose $y \in C_k$. In this case $B_{x,y} \subseteq B^3$. Assuming that $y \in x + N$ and $f(y - x) \notin B^3$, we work backwards through the coordinates to attain conditions on $y$. Note first that $y_i = x_i$ for $i = d - 1, \ldots, \delta$. It then follows that $y_{\delta - 1} = x_{\delta - 1} + \eta$ and $y_i = x_i$ for $i = \delta - 2, \ldots, \gamma$. 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 $t_{\gamma + 1}^i = -1$ and $t_{\gamma + 1}^k = 1$. For $x = (x_1, \ldots, x_{d-1}) \in D_{j,k}$ we set

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

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

Since $x + N$ does not intersect $C_k$ we have $y \in C_j \cup D_{j,k}$. Define

$B^1 = [-2l + 3, 2l - 3] \times [-2, 2]^{\gamma - 1} \times [-1, 3] \times [-1, 1]^{d - \delta}.$

$B^2 = [-2l + 7, 2l - 7] \times [-1, 1]^{\gamma - 1} \times [-3, 3] \times [-1, 1]^{d - \delta}$, and

$B^3 = [-2l + 3, 2l - 3] \times [-1, 1]^{\gamma - 1} \times [-3, 1] \times [-1, 1]^{d - \delta}.$

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

Suppose $y \in D_{j,k}$ and $y_\gamma = x_\gamma$. In this case we have $B_{x,y} \subseteq B^2$. 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 $B^2$.

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

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

We may assume $y \in D_{j,k} \cup C_k$ and $y_\gamma \neq b_{\gamma - 1 - j} + 1$. We have

$B_{x,y} \subseteq \begin{cases} 
[-2l + 1, 2l - 1] \times [-2, 2]^{\gamma - 1} \times [-1, 1]^{d - \gamma} & \text{if } y \in C_k, \\
[-2l + 5, 2l - 5] \times [-1, 1]^{d - 1} & \text{if } y \in D_{j,k},
\end{cases}$

and the proof follows as in Case 1.

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


Note that $t_{\gamma+1}^j = 1$ and $t_{\gamma+1}^k = -1$. We set
\[ I_x = \begin{cases} f(x) + E_{l-3} - e_{\gamma+1} & \text{if } x_\gamma \neq b_{2\gamma-1j} + 1, \\ \emptyset & \text{if } x_\gamma = b_{2\gamma-1j} + 1. \end{cases} \]

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
\[ \mathcal{D} = \bigcup_{j \neq k} \mathcal{D}_{j,k} \quad \text{and} \quad \mathcal{X} = \bigcup_{i=0}^{2d-1-1} \hat{X}_i \]
where $[a, b] = [a - 1, b + 1]$. We count as follows:
\[ |\mathcal{I}'_m| = (l - 3) (|C| + |D|) + 3 |C_k| 2^{d-1} + |C_k| \cdot |\{i : \beta_i = 1\}|. \]

It follows from Claim 3.2 that $\alpha_{d-1} = r'$. It then follows from (3.11) that $\beta_{d-1} = 0$ and from (3.10) that the number of $\beta_i$'s that equal 1 is $r'/2$. The asymptotic behavior of $|C| + |D|$ follows from
\[ x = (x_1, \ldots, x_{d-1}) \in \mathbb{Z}^{d-1} \quad \text{and} \quad |\{i : x_i \in \mathcal{X}\}| \leq 1 \Rightarrow x \in C \cup D. \]

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

ACKNOWLEDGMENT

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

REFERENCES


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