PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9939(XX)0000-0

A LIMIT THEOREM FOR THE SHANNON CAPACITIES OF ODD CYCLES II

TOM BOHMAN

ABSTRACT. It follows from a construction for independent sets in the powers of odd cycles given in the predecessor of this paper that the limit as k goes to infinity of $k + 1/2 - \Theta(C_{2k+1})$ is zero, where $\Theta(G)$ is the Shannon capacity of graph G. This paper contains a shorter proof of this limit theorem that is based on an 'expansion process' introduced in an older paper of L. Baumert, R. McEliece, E. Rodemich, H. Rumsey, R. Stanley and H. Taylor. We also refute a conjecture from the paper of Baumert et al using ideas from the predecessor of this paper.

1. INTRODUCTION

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

$$\Theta(G) = \lim_{d\to\infty} \left(\alpha(G^d)\right)^{1/d} = \sup_d \left(\alpha(G^d)\right)^{1/d}$$

where $\alpha(G)$ is the independence number of G and G^d is the d^{th} power of G, the graph having vertex set $V(G)^d$ and an edge between distinct vertices $(x_1, \dots, x_d)$ and $(y_1, \dots, y_d)$ if and only if $\{x_i, y_i\} \in E(G)$ or $x_i = y_i$ for $i = 1, \dots, d$. This graph invariant was introduced by Shannon in 1956 as a measure of the zero-error capacity of a noisy communication channel [11]. For an excellent introduction to and survey of zero-error information theory see [9]; for a survey of recent progress on questions regarding the powers of graphs see [1].

The odd cycles on 7 or more vertices and their complements are the simplest graphs for which the Shannon capacity is not known. This follows from the following three facts:

(a) If G is a perfect graph then $\alpha(G) = \Theta(G)$ (this connection with Shannon capacity was part of the motivation for the perfect graph conjectures of Berge [3]),
(b) The Strong Perfect Graph Theorem (recently proved by Chudnovsky, Robertson, Seymour and Thomas [7]) which states that if G is an imperfect graph then G has an odd cycle or the complement of an odd cycle on 5 or more vertices as an induced subgraph, and
(c) $\Theta(C_5) = \Theta(\overline{C_5}) = \sqrt{5}$ (this was established in a celebrated paper of Lovász [10]).

1991 *Mathematics Subject Classification.* Primary 94A15, 05C35, 05C38.
Key words and phrases. Shannon capacity, odd cycles.
research supported in part by NSF Grant DMS-0100400.

The best known upper bounds on $\Theta(C_m)$ and $\Theta(\overline{C_m})$ for m odd and greater than 5 are given by the Lovász theta function (the theta function of graph G is denoted $\vartheta(G)$):

$$\Theta(C_{2k+1}) \leq \vartheta(C_{2k+1}) = \frac{(2k+1)\cos\left(\pi/(2k+1)\right)}{1+\cos\left(\pi/(2k+1)\right)} = k + \frac{1}{2} - O(1/k),$$
$$\Theta(\overline{C}_{2k+1}) \leq \vartheta(\overline{C}_{2k+1}) = \frac{1+\cos\left(\pi/(2k+1)\right)}{\cos\left(\pi/(2k+1)\right)} = 2 + O(1/k^2).$$

Bohman and Holzman recently showed that the Shannon capacities of the complements of odd cycles are all strictly greater than 2 [5].

Here we focus on the problem of determining $\alpha(C_m^d)$ for d fixed and m odd. This problem can be viewed as a packing problem (as is noted in [2]): How many cubes of side length 2 can be packed into a d-dimensional torus of side length m? For some values of m and d there is an elegant construction that gives the independence number of C_m^d.

Theorem 1.1 (BMRRST [2], Hales [8]). *For integers $\ell, d \geq 1$ we have*

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

The construction that achieves Theorem 1.1 is given in Section 2 and is the starting point for the ideas discussed below. The fact that this construction gives the actual independence number comes from consideration of $\alpha^*(C_m^d)$, the *fractional vertex packing number*, a graph invariant that can be viewed as a natural linear programming relaxation of the independence number and gives an upper bound on the independence number (for definitions and discussion see [4]).

Since

$$k = \alpha(C_{2k+1}) \leq \Theta(C_{2k+1}) \leq \vartheta(C_{2k+1}) = k + \frac{1}{2} - O(1/k),$$

it is natural to consider the behavior of the difference $k + 1/2 - \Theta(C_{2k+1})$ as k goes to infinity. It follows from Theorem 1.1 that

$$\liminf_{k\to\infty}\; k + 1/2 - \Theta(C_{2k+1}) = 0.$$

In [4] a construction is given that proves the following Theorem (resolving a conjecture made in [6]).

Theorem 1.2.

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

Here we give a simpler proof of Theorem 1.2 that uses a clever 'expansion process' given in a paper of Baumert, McEliece, Rodemich, Rumsey, Stanley and Taylor [2]. This proof is given in Section 3.

The expansion process is a centerpiece of an extensive study of the $\alpha(C_m^d)$ for d fixed and m odd given in [2]. A number of other intriguing results regarding these numbers are given in that paper, and the following unifying conjecture is made.

Conjecture 1.3 (BMRRST [2]). *Let $m = \ell 2^d + \beta + 1$ where $0 \leq \beta \leq 2^d - 2$ and β is even.*

$$\alpha\left(C_m^d\right) = \ell\left(\frac{m^d - \beta^d}{m - \beta}\right) + \alpha\left(C_{\beta+1}^d\right), \tag{1.1}$$

where we set $\alpha(C_1^d) = 0$.

It follows from Theorem 1.1 that this conjecture holds for $\beta = 0$. Baumert, McEliece, Rodemich, Rumsey, Stanley and Taylor also showed (using the expansion process mentioned above) that the conjecture holds for $\beta = 2$. The following result comes from a variation of the construction given in [4].

Theorem 1.4. *If $m = \ell 2^d + \beta + 1$ where $\beta = 2^{d-1}$ then we have*

$$\alpha\left(C_m^d\right) \geq \ell m^{d-1} + \left(\frac{m-1}{2}\right) m^{d-2}. \tag{1.2}$$

We note that the $d = 3$ case of Theorem 1.4 is proved in both [2] and [6]. For $d \geq 4$ fixed, the function in (1.1) is equal to

$$\ell m^{d-1} + \ell\beta m^{d-2} + \ell\beta^2 m^{d-3} + \ell\beta^3 m^{d-4} + O(\ell^{d-4}).$$

On the other hand, for d fixed and $\beta = 2^{d-1}$ the expression in (1.2) is

$$\begin{aligned}
\ell m^{d-1} + (\ell\beta + \beta/2)m^{d-2} &= \ell m^{d-1} + \ell\beta m^{d-2} + \beta/2(2\ell\beta + \beta + 1)m^{d-3} \\
&= \ell m^{d-1} + \ell\beta m^{d-2} + \ell\beta^2 m^{d-3} \\
&\quad + (\beta^2/2 + \beta/2)(2\ell\beta + \beta + 1)m^{d-4} \\
&= \ell m^{d-1} + \ell\beta m^{d-2} + \ell\beta^2 m^{d-3} + \ell\beta^3 m^{d-4} \\
&\quad + \ell\beta^2 m^{d-4} + O(\ell^{d-4}) \\
&= \ell m^{d-1} + \ell\beta m^{d-2} + \ell\beta^2 m^{d-3} + \ell\beta^3 m^{d-4} \\
&\quad + \ell^{d-3}\beta^{d-2}2^{d-4} + O(\ell^{d-4})
\end{aligned}$$

So, for $d \geq 4$ and $\beta = 2^{d-1}$ the function given in (1.1) grows too slowly for Conjecture 1.3 to hold.

It seems plausible that the bound given in Theorem 1.4 gives the actual independence numbers.

Conjecture 1.5. *If $m = \ell 2^d + \beta + 1$ where $\beta = 2^{d-1}$ then*

$$\alpha\left(C_m^d\right) = \ell m^{d-1} + \left(\frac{m-1}{2}\right) m^{d-2}.$$

Of course, it would be interesting to find a natural construction that unifies the $\beta = 2$ construction (which follows from the expansion process described in Section 3) and the $\beta = 2^{d-1}$ construction (i.e. Theorem 1.4) while providing good lower bounds on $\alpha(C_m^d)$ for other values of β. Such a construction would lend credence to the hypothesis that the sequence $\{\alpha(C_{2k+1}^d)\}_{k\geq 1}$ is a simple function of its first 2^{d-1} entries. This hypothesis seems to be a common theme of previous work on this subject: the hypothesis was stated formally in Conjecture 1.3 and dependence on the congruence class of m modulo 2^d is a feature of the construction given in [4].

The remainder of this paper is organized as follows. In the next section we give a proof of Theorem 1.1, which is the common starting point for the constructions in Sections 3 and 4. In Section 3 we introduce the expansion process of Baumert, McEliece, Rodemich, Rumsey, Stanley and Taylor and use it to give a short proof of Theorem 1.2. In Section 4 we prove Theorem 1.4.

2. The root construction

We begin with notational conventions. We henceforth identify the vertices of the graph C_m^d with the elements of the group $\mathbb{Z}_m^d$ in the natural way. We use the same symbol for both a vertex in the graph and the corresponding group element. We can express adjacency in the graph in terms of the group operation; to be precise, for $a \neq b$ we have

$$\{a,b\} \in E(C_m^d) \Leftrightarrow a - b \in \{-1,0,1\}^d. \tag{2.1}$$

We use the dot product notation $g \cdot h = g_1 h_1 + \cdots + g_d h_d$ for $g \in \mathbb{Z}^d$ and group element $h = (h_1, \ldots, h_d)$.

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

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

We extend the subgroup G_d to an independent set as follows:

$$\mathcal{H}_{d,\ell} = \{x + ie_1 : x \in G_d, i \in \{-\ell+1, -\ell+3, \ldots, \ell-1\}\}.$$

To show that $\mathcal{H}_{d,\ell}$ is an independent set we consider distinct $a, b \in \mathcal{H}_{d,\ell}$. We have $a - b = x + je_1$ where $x \in G_d$, $j \in \{-2\ell+2, \ldots, 2\ell-2\}$ and j is even. For

$$z \in \{-2\ell+1, -2\ell+2, \ldots, 2\ell-1\} \times \{-1,0,1\}^{d-1}$$

consider $z \cdot h_d$ over $\mathbb{Z}$. Since $|z \cdot h_d| \leq \ell 2^d - 1$ and $z \cdot h_d = 0$ implies $z = 0$ we have

$$G_d \cap \left(\{-2\ell+1, -2\ell+2, \ldots, 2\ell-1\} \times \{-1,0,1\}^{d-1}\right) = \{0\}.$$

It follows that

$$a - b \notin \{-1,0,1\}^d,$$

and $\mathcal{H}_{d,\ell}$ is an independent set.

3. An expansion process

The key idea in this proof of Theorem 1.2 is a counting argument (that can be viewed as an application of the basic probabilistic method) that, given a large independent set in C_m^d, proves the existence of a large independent set in $C_{m+\beta}^d$ for β even. In other words, we expand a large independent set in C_m^d to an independent set in the d^{th} power of a longer cycle. We prove Theorem 1.2 by applying this argument to the root construction (i.e. $\mathcal{H}_{d,\ell}$).

Theorem 3.1 (BMRRST). *If $m \geq 3$ and $\beta > 0$ is even then*

$$\alpha(C_{m+\beta}^d) \geq \alpha(C_m^d) \left(\frac{m+\beta}{m}\right)^d.$$

Proof. We begin with the map $\varphi : \mathbb{Z}_{m+\beta} \to \mathbb{Z}_m$ defined by

$$\varphi(a) = \begin{cases} a & \text{if } a \in \{0,1,\ldots,m-1\} \\ 0 & \text{if } a \in \{m, m+2, \ldots, m+\beta-2\} \\ m-1 & \text{if } a \in \{m+1, m+3, \ldots, m+\beta-1\} \end{cases}.$$

We also use φ to denote the map from $\mathbb{Z}_{m+\beta}^d$ to $\mathbb{Z}_m^d$ that takes $(x_1,\ldots,x_d)$ to $(\varphi(x_1),\ldots,\varphi(x_d))$. Note that

$$\varphi(x) \not\sim \varphi(y) \Rightarrow x \not\sim y \qquad \text{and} \qquad \varphi(x) = \varphi(y) \Rightarrow x \not\sim y.$$

Therefore, if X is an independent set in $\mathbb{Z}_m^d$ then

$$Y = \{y \in \mathbb{Z}_{m+\beta}^d : \varphi(y) \in X\}$$

is an independent set in $\mathbb{Z}_{m+\beta}^d$. We have

$$|Y| = \sum_{x\in X} \left(\frac{\beta}{2}+1\right)^{|\{i:x_i\in\{0,m-1\}\}|}. \tag{3.1}$$

So, $|Y|$ depends on the location of zero in our identification of $\mathbb{Z}_m^d$ and C_m^d. Averaging over the m^d such placements we see that there exists an independent set in $C_{m+\beta}^d$ of cardinality at least

$$\begin{aligned}
&\frac{1}{m^d}\sum_{z_1,\ldots,z_d=0}^{m-1}\sum_{x\in X}\left(\frac{\beta}{2}+1\right)^{|\{i:x_i\in\{z_i-1,z_i\}\}|} \\
&\qquad = \frac{1}{m^d}\sum_{x\in X}\sum_{j=0}^{d}\binom{d}{j}2^j(m-2)^{d-j}\left(\frac{\beta}{2}+1\right)^j \\
&\qquad = |X|\frac{(m+\beta)^d}{m^d}.
\end{aligned}$$

□

Recall Theorem 1.1:

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

For arbitrary k there exists $0 \le \beta < 2^d$ and $\ell \ge 0$ such that $2k+1 = \ell 2^d + 1 + \beta$. So, it follows from Theorem 3.1 that for arbitrary k we have

$$\begin{aligned}
\alpha(C_{2k+1}^d) &\ge \frac{2k-\beta}{2^d}(2k+1-\beta)^{d-1}\left(\frac{2k+1}{2k+1-\beta}\right)^d \\
&= \frac{(2k+1)^{d-1}}{2^d}\left(2k - \frac{\beta}{2k+1-\beta}\right)
\end{aligned}$$

for some β such that $0 \le \beta < 2^d$. Therefore, for d fixed we have

$$\alpha(C_{2k+1}^d) \ge k^d + \frac{d-1}{2}k^{d-1} + O(k^{d-2}). \tag{3.2}$$

Since we have an upper bound of the same form, in particular

$$\alpha(C_{2k+1}^d) \le \alpha(C_{2k+1})\alpha^*(C_{2k+1})^{d-1} = k\left(k+\frac{1}{2}\right)^{d-1},$$

we have

$$\lim_{k\to\infty} k + \frac{1}{2} - \left[\alpha(C_{2k+1}^d)\right]^{1/d} = \frac{1}{2d}.$$

Theorem 1.2 follows.

Remark. At first glance, this proof is nonconstructive: It depends on the location of zero in our identification of $V(C_m^d)$ and $\mathbb{Z}_m^d$, which was chosen at random. It turns out that, due to the symmetry of $\mathcal{H}_{d,\ell}$, this random choice is not necessary for the proof of Theorem 1.2. In particular, if we apply (3.1) to $X = \mathcal{H}_{d,\ell}$ with the canonical placement of zero then (after some careful counting) we get (3.2) directly.

4. Partitioning G_d

The expansion process discussed in the previous section can be viewed as a generalization of the root construction to cycles of length $m = \ell 2^d + \beta + 1$ where β is even, less than 2^d and nonzero. In this section we prove Theorem 1.4 and in so doing give a simple illustration of a different idea for such a generalization of $\mathcal{H}_{d,\ell}$. This idea, which was introduced in [4], takes advantage of the group structure of G_d directly.

Recall that $\mathcal{H}_{d,\ell}$ is formed by replacing every element g of G_d with a set of ℓ vertices centered at g. For $\beta \neq 0$, we would like to form an optimal independent set by placing a set of vertices around every element of G_d, but if $\beta \neq 0$ then $\alpha(C_m^d)$ is not a multiple of $|G_d| = m^{d-1}$, and the sets of vertices around elements of G_d cannot all have the same size. The construction uses the group structure of G_d to decide what should be done around particular elements, and the full construction (as given in [4]) uses many different types of sets of vertices. However, the $\beta = 2^{d-1}$ case (on which we focus here) admits a particularly interesting version of the construction. This version only requires two types of sets of vertices

Proof of Theorem 1.4. We partition G_d into two parts. Following the spirit of the construction in [4], we define this partition by way of the map

$$\varphi : \mathbb{Z}_m^{d-1} \to G_d$$

defined by

$$\varphi(x) = Ax$$

where

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

Let

$$G_d^1 = \{\varphi(x) : x \in \mathbb{Z}_m^{d-1} \text{ such that } x_{d-1} \in \{0, \dots, \ell 2^{d-1} + 2^{d-2} - 1\}\}$$
$$G_d^0 = G_d \setminus G_d^1.$$

Let

$$\mathcal{I}^1 = \{y + ie_1 : y \in G_d^1 \text{ and } i \in \{-\ell, -\ell+2, \dots, \ell\}\}$$
$$\mathcal{I}^0 = \{y + ie_1 : y \in G_d^0 \text{ and } i \in \{-\ell+1, -\ell+3, \dots, \ell-1\}\}$$
$$\mathcal{I} = \mathcal{I}^1 \cup \mathcal{I}^0.$$

Assume for the sake of contradiction that there exist distinct $a, b \in \mathcal{I}$ that are adjacent.

$$a - b = z + je_1$$

for some $z \in G_d$ and integer j such that $j \in \{-2\ell, \dots, 2\ell\}$. Since the set of vertices in $\mathcal{I}$ centered at any $w \in G_d$ is clearly an independent set, we may assume $z \neq 0$. Now,

$$z \in (G_d \setminus \{0\}) \cap \left(\{-2\ell - 1, -2\ell, \dots, 2\ell + 1\} \times \{-1, 0, 1\}^{d-1} \right)$$
$$\Rightarrow \qquad z_1 \in \{2\ell + 1, -2\ell - 1\} \quad \text{and} \quad \sum_{k=2}^{d} 2^{d-k} z_k = \pm 1.$$

It follows that $a = u + j_a e_1$ and $b = v + j_b e_1$ where $u, v \in G_d^1$ and the $(d-1)^{\text{st}}$ coordinate of

$$\varphi^{-1}(u) - \varphi^{-1}(v)$$

is $\pm(\ell 2^{d-1} + 2^{d-2})$. As no such $u, v \in G_d^1$ exist, we have a contradiction. $\square$

Acknowledgment. The author thanks Ron Holzman for helpful discussions and comments.

References

[1] N. Alon, Graph Powers, *Contemporary Combinatorics, (B. Bollobás, ed.)*, Bolyai Society Mathematical Studies, Springer 2002, pp. 11-28.

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

[3] C. Berge, Motivations and history of some of my conjectures *Discrete Mathematics* 165 (1997), 61-70.

[4] T. Bohman, A limit theorem for the Shannon capacities of odd cycles I, *Proceedings of the AMS*, to appear.

[5] T. Bohman, R. Holzman, A nontrivial lower bound on the Shannon capacities of the complements of odd cycles, *IEEE Transactions on Information Theory*, 49(3) (2003), 721-722.

[6] T. Bohman, M. Ruszinkó, 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.

[7] M. Chudnovsky, N. Robertson, P. Seymour, R. Thomas, The Strong Perfect Graph Theorem, submitted.

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

[9] J. Körner and A. Orlitsky, Zero-error information theory, *IEEE Transactions on Information Theory* 44(6) (1998), 2207-2229.

[10] L. Lovász, On the Shannon capacity of a graph, *IEEE Transactions on Information Theory* 25(1) (1979), 1-7.

[11] C. E. Shannon, The zero-error capacity of a noisy channel, *IRE Transactions on Information Theory*, 2(3) (1956), 8–19.

Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, PA 15213

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