Modified Linear Dependence and the Capacity of a Cyclic Graph

S. K. Stein
Mathematics Department
University of California
Davis, California 95616

Submitted by Ky Fan

ABSTRACT

In 1956 Shannon raised a problem in information theory, which amounts to this geometric question: How many n-dimensional cubes of width 2 can be packed in the n-dimensional torus described by the nth power of the cyclic group C_m? The present paper examines this question in the special circumstance that the set of centers of the cubes form a subgroup—that is, a lattice packing. In this case, the machinery of vector spaces is available when m is a prime. This approach introduces a modified definition of linear independence, obtains some known results with its aid, and suggests a promising direction for future computation and theory. The paper concludes by showing that, in return, combinatorial information can yield results about finite vector spaces.

INTRODUCTION

A problem in information theory raised by Shannon [5] in 1956 has been the subject of several graph-theoretical, combinatorial, and geometrical investigations [1, 2, 4]. It is our purpose to examine it from an algebraic viewpoint, in particular, to show that a modified definition of linear dependence provides an explanation of some known results and possibly an approach to a general solution.

1. FREE SETS IN ABELIAN GROUPS

Let C_m be the cyclic group of order m, and let k be a positive integer. A set $B=\{b_1,b_2,\ldots,b_n\}\subset C_m^k$ is *free* if $\sum_{i=1}^{n}\epsilon_i b_i=0$, $\epsilon_i=0,\pm 1$ implies that

$\epsilon_i = 0$, $i = 1, 2, \ldots, n$. In case $m = 2$ or 3 this notion coincides with the usual linear independence in a vector space. If m is prime, C_m^k is a vector space over GF(m) but B may be free though not linearly independent. For instance, $B = \{1, 2\} \subset C_5$ is free but not linearly independent over GF(5).

Let $\tau(C_m^k)$ denote the number of elements in a largest free set in C_m^k. Since distinct subsets of a free set B have distinct sums,

$$\tau(C_m^k) \leqslant \log_2(m^k) = (\log_2 m)k.$$

On the other hand, as Erdös has pointed out in conversation,

$$\tau(C_m^k) \geqslant \log_3(m^k) = (\log_3 m)k,$$

since any free set with fewer than $\log_3(m^k)$ elements can be extended to a larger free set. Thus

$$(\log_3 m)k \leqslant \tau(C_m^k) \leqslant (\log_2 m)k.$$

Moreover, it is clear that $\tau(C_m^{k+l}) \geqslant \tau(C_m^k) + \tau(C_m^l)$. Now, for any numerical function f, defined on the positive integers, such that $f(k+l) \geqslant f(k) + f(l)$ and $f(k) \leqslant ak$ for all positive integers k and l and some constant a, there is a constant c such that $\lim_{k\to\infty} f(k)/k = c$ [3, p. 17]. Thus for a given group C_m, the quotient $\tau(C_m^k)/k$ approaches a limit as $k \to \infty$. This limit will be denoted by $\tau^*(C_m)$ and called the *free capacity* of C_m. From the above observations,

$$\log_3 m \leqslant \tau^*(C_m) \leqslant \log_2 m,$$

$\tau^*(C_2) = 1$, and $\tau^*(C_3) = 1$. In case m is a power of 2, it is easy to see that $\tau^*(C_m) = \log_2 m$, for $B = \{1, 2, 2^2, 2^3, \ldots, 2^{\log_2 m}/2\}$ is free in C_m. For no other values of m is $\tau^*(C_m)$ known.

2. INDEPENDENT SETS IN A LINEAR GRAPH

The set C_m^n may also be interpreted as a linear graph. Two distinct vertices of C_m^n are *adjacent* if their difference, as elements of the group C_m^n, is of the form $(\epsilon_1, \epsilon_2, \ldots, \epsilon_n)$, each $\epsilon_i = 0$, 1, or -1. A set of vertices, no two of which are adjacent, is called *independent*. Denote by $\beta(C_m^n)$ the largest number of vertices in an independent set in C_m^n. Moreover, for positive integers p and q clearly $\beta(C_m^{p+q}) \geqslant \beta(C_m^p)\,\beta(C_m^q)$. Define $f(n) = \log_2 \beta(C_m^n)$.

Again, by [3, p. 17], $f(n)/n$ has a limit as $n \to \infty$. Consequently $\sqrt[n]{\beta(C_m^n)}$ has a limit as $n \to \infty$. This limit, denoted $\theta(C_m)$, is called the *capacity* of the graph C_m.

For any $m \geqslant 4$, it is easy to show that $(m-1)/2 \leqslant \theta(C_m) \leqslant m/2$. If m is even, $\theta(C_m) = m/2$, for $\beta(C_m)$ is $m/2$. For odd $m \geqslant 5$, $\theta(C_m)$ is not known. However, it follows immediately from Theorem 1 in [1] that if $\theta(C_5) = \frac{5}{2}$, then $\theta(C_m) = m/2$ for all odd $m \geqslant 5$.

Incidentally, $\beta(C_m^n)$ may also be interpreted as the largest number of cubes of side 2 that can be packed in the n-dimensional toroid C_m^n (see [5]).

3. FREE SETS AND THE ALGEBRAIC CAPACITY OF A CYCLIC GRAPH

Let $\beta_L(C_m^n)$ be a largest independent set in C_m^n that form a subgroup. The *algebraic capacity* of C_m, denoted $\theta_L(C_m)$, is defined as

$$\lim_{n \to \infty} \sqrt[n]{\beta_L(C_m^n)} .$$

Clearly $\theta_L(C_m) \leqslant \theta(C_m)$. Trivially, for m even, $\theta_L(C_m) = \theta(C_m)$. We conjecture that $\theta_L(C_m) = \theta(C_m)$ for all m.

The relation between free sets and independent sets is expressed in the following two theorems.

THEOREM 1. *If there is a free set of n elements in C_m^k, then there is an independent subgroup in C_m^n with at least m^{n-k} elements.*

Proof. Let $\{b_1, b_2, \ldots, b_n\}$ be a free set in C_m^k. Define a homomorphism

$$f: C_m^n \to C_m^k$$

by

$$f(E_i) = b_i, \qquad i = 1, 2, \ldots, n.$$

[Here $E_i = (0, \ldots, 1, \ldots, 0)$, the standard ith unit vector.] Let K be the kernel of f. We assert that K is an independent set. For, let v_1 and v_2 be distinct vertices in K. If v_1 and v_2 were adjacent, there would exist integers ϵ_i, $i = 1, 2, \ldots, n$, $\epsilon_i = 0, 1, -1$, such that

$$v_2 = v_1 + \sum_{i=1}^{n} \epsilon_i E_i.$$

Application of f yields

$$0=0+\sum_{i=1}^{n}\epsilon_i b_i,$$

contradicting the freeness of the set $\{b_1,b_2,\ldots,b_n\}$. ∎

If m is prime, the argument for Theorem 1 is reversible and one has an equivalence between independent subgroups in C_m^n and free sets in C_m^k. This is expressed in the next theorem.

THEOREM 2. *Let m be prime and let k be a positive integer. Then there is a free set of n elements in C_m^k if and only if there is an independent subgroup of C_m^n that consists of m^{n-k} vertices.*

As an illustration of Theorem 1, note that $\{(0,1),(1,1),(1,3),(2,1),(3,6)\}$ is a free set in C_7^2. Hence

$$\beta_L(C_7^5)\geqslant 7^{5-2}=7^3,$$

and therefore

$$\theta_L(C_7)\geqslant 7^{3/5}\doteq 3.21.$$

This provides an alternative argument for the proof of Theorem 7 in [1]. Note that it is stronger than the result obtained in [2], namely $\theta(C_7)\geqslant\sqrt{10}\doteq 3.16$.

As a second illustration, since $B=\{1,2\}$ is a free set in C_5, there is an independent set in the graph C_5^2 consisting of 5 elements. Shannon [5] obtained this result by exhibiting an appropriate packing of the torus C_5^2.

The proof of the following corollary is straightforward.

COROLLARY 1. *Let $\tau(C_m^k)=\alpha\log_2 m^k$. Then $\theta_L(C_m)\geqslant m/2^{1/\alpha}$.*

Thus, showing that $\theta_L(C_5)=\frac{5}{2}$ is equivalent to showing that as $k\to\infty$, $\tau(C_5^k)/k\to\log_2 5\doteq 2.3$. It is not hard to show that for $1\leqslant k\leqslant 5$, $\tau(C_5^k)/k=2$, but $\tau(C_5^6)/6$ is not yet determined.

Independent sets, in return, can provide information about free sets, as the next corollary shows.

COROLLARY 2. *If m is odd, then*

$$\tau(C_m^k)\leqslant\left[\log_2\left(m^{k-1}(m-1)\right)\right].$$

Proof. Let $\tau(C_m^k)=n$. Then there is an independent set in C_m^n of m^{n-k} vertices. Thinking of the linear graph C_m^n as embedded in the n-dimensional toroid, note that a set of disjoint 2-by-2-by...-by-2 cubes meets each line parallel to an axis in at most $(m-1)/2$ such cubes. Independent vertices correspond to centers of disjoint 2-by-2-by-...-by-2 cubes. Hence

$$m^{n-k}\cdot 2^n \leqslant m^{n-1}(m-1)$$

or

$$2^n \leqslant m^{k-1}(m-1),$$

which completes the proof. ■

This corollary implies that $\tau(C_5^4)<9$; thus $\tau(C_5^4)=8$. The inequality $\tau(C_5^4)\leqslant \log_2 5^4$ implies merely that $\tau(C_5^4)\leqslant 9$.

REFERENCES

1 L. D. Baumert, et al. A combinatorial packing problem, Computers in Algebra and Number Theory, *SIAM/AMS Proc.* **4** (1971), 97–108.

2 R. S. Hales, Numerical invariants and the strong product of graphs, *J. Comb. Theory* **B(15)** (1973), 146–155.

3 G. Polyá and G. Szegö, *Aufgaben und Lehrsatze aus der Analysis*, Dover. New York, 1945, Problem 98, p. 17.

4 M. Rosenfeld, On a problem of C. E. Shannon in graph theory, *Proc. Am. Math. Soc.* **18**(1967), 315–319.

5 C. E. Shannon, The zero error capacity of a noisy channel, *IRE Trans. Inf. Theory*, **IT-2** (1956), 8–19; *MR* **19**, 623.

Received 15 September 1975; revised 1 February, 6 May 1976