PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 84, Number 2, February 1982

THE CAPACITY OF C_5 AND FREE SETS IN C_m^2

D. G. MEAD AND W. NARKIEWICZ

ABSTRACT. In a recent paper, S. K. Stein examined the problem of determining the cardinality, $\tau(C_m^k)$, of the largest subset S of the direct product C_m^k of k copies of C_m such that distinct sums of elements of S yield distinct elements of C_m^k. In this paper we show that $\tau^*(C_5) = \lim_{k\to\infty}(\tau(C_5^k)/k) = 2$, answering a question raised by Stein. We also produce an infinite set of m's such that $\tau(C_m^2) > 2[\log_2 m]$.

Introduction. In [3], S. K. Stein examined from an algebraic standpoint a problem in information theory raised by Shannon [2] in 1956. Stein says that a subset $\{b_1, \ldots, b_r\}$ of a group G is free if $\sum \varepsilon_i b_i = 0$, $\varepsilon_i = 0, \pm 1$ implies $\varepsilon_i = 0$ for all i. The number of elements, $\tau(G)$, in the largest free set in G, is also clearly equal to the cardinality of the largest subset S of G such that distinct sums of elements of S yield distinct elements of G. In [3], the free capacity of C_m, $\tau^*(C_m)$ is defined to be $\lim_{k\to\infty} \tau(C_m^k)/k$, where C_m is a cyclic group of order m. In this paper we show that $\tau^*(C_5) = 2$ and compute $\tau(C_m^2)$ for certain values of m.

The free capacity of C_5. With $E_i = (0, \ldots, 0, 1, \ldots, 0)$, the standard ith vector, we see that the set E_i, $2E_i$, $i = 1, \ldots, k$, is free in C_5^k, hence $\tau(C_5^k) \geqslant 2k$. Let $S = \{ g_i = (a_{1i}, \ldots, a_{ki}) | a_{ji} \in C_5, i = 1, \ldots, N\}$ be a free set in C_5^k. Since the only elements in Z_5 which are squares are $0, \pm 1$, the equation $\sum_{i=1}^N \varepsilon_i g_i = 0$ is equivalent to the system $\sum_{i=1}^N x_i^2 a_{ji} = 0$, $j = 1, \ldots, k$, to which the following corollary of the theorem of Chevalley-Warning [1] can be applied:

With $K = C_5$, let $\{f_j \in K[X_1, \ldots, X_N]\}$ be a set of homogeneous polynomials in N variables such that $\sum \deg f_j < N$. Then the f_j have a nontrivial common zero.

In our case, the degree of each f_j is 2. If $N > 2k = \sum \deg f_j$, the f_j have a nontrivial zero, i.e. the set S is not a free set. This is a contradiction and we can conclude that $\tau(C_5^k) = 2k$. Consequently, the free capacity of C_5, $\tau^*(C_5) = \lim_{k\to\infty} \tau(C_5^k/k) = 2$.

Free sets in C_m^2. Since $[\log_2 m] \leqslant \tau(C_m) \leqslant \log_2 m$ and $\tau(C_m^{k+l}) \geqslant \tau(C_m^k) + \tau(C_m^l)$, it follows that

$$2[\log_2 m] \leqslant 2\tau(C_m) \leqslant \tau(C_m^2) \leqslant [\log_2 m^2] \leqslant 2[\log_2 m] + 1.$$

When m is a power of 2, $\tau(C_m^k) = k \log_2 m$; we find $\tau(C_m^2)$ for certain other values of m.

THEOREM. *$\tau(C_m^2) = 2[\log_2 m] + 1$ if $3 \cdot 2^{a-1} < m < 2^{a+1}$ for $a \geqslant 2$.*

Received by the editors May 29, 1978 and, in revised form, April 17, 1981.
1980 *Mathematics Subject Classification.* Primary 05B40, 05C25; Secondary 15A03.

PROOF. It is sufficient to show that the following set of $2a + 1$ elements is free:

$$\{u_1 = (1, 0), u_2 = (0, 1), v_1 = (1, 2), v_2 = (1, -2), w_i = (3 \cdot 2^i, -3 \cdot 2^i),$$
$$i = 0, 1, \dots, a-3, z_j = (3 \cdot 2^j, 3 \cdot 2^j), j = 0, 1, \dots, a-2\}.$$

We first show that the set of u's, v's, w's, and z_j with $j \leqslant a - 3$ is free. Assume that

$$\Sigma\, b_i u_i + \Sigma\, c_i v_i + \Sigma\, d_i w_i + \sum^{a-3} e_i z_i = 0 \tag{1}$$

where the b_i, c_i, d_i, and e_i are chosen from $\{0, 1, -1\}$. Since

$$3 \sum^{a-3} 2^{i+1} = 3(2^{a-1} - 2) < m - 6,$$

it follows that the equation (1) must hold in $Z \times Z$. Thus

$$\begin{aligned} &b_1 + c_1 + c_2 + 3 \sum^{a-3} 2^i(d_i + e_i) = 0, \\ &b_2 2c_1 - 2c_2 + 3 \sum 2^i(-d_i + e_i) = 0. \end{aligned} \tag{2}$$

If not all of b_i, c_i, d_i, and e_i are zero, then some d_i or e_i is not zero. Assume some $e_i \neq 0$ and let t be the largest i for which $e_i \neq 0$. Adding the equations (2) we find

$$3 \cdot 2^{t+1} = \pm \left(b_1 + b_2 + 3c_1 - c_2 + 3 \cdot 2 \sum^{t-1} 2^i e_i\right)$$

which could only be true if $b_1 = b_2 = c_1 = -c_2 \neq 0$. Subtracting the second equation of (2) from the first, we see that some $d_i \neq 0$. With s representing the largest i such that $d_i \neq 0$, we have

$$3 \cdot 2^{s+1} = \pm \left(b_1 - b_2 - c_1 + 3c_2 + 3 \cdot 2 \sum^{s-1} 2^i d_i\right)$$

which could only occur if $b_1 = -b_2 \neq 0$. This is a contradiction and since the same sort of reasoning can be used if some d_i is assumed to be nonzero, we conclude that the set of u's, v's, w's, and z_j with $j \leqslant a - 3$ is free.

We will now show that the assumption that

$$0 = z_{a-2} + \sum b_i u_i + \sum c_i v_i + \sum d_i w_i + \sum^{a-3} e_i z_i \tag{3}$$

leads to a contradiction.

Let

$$A = 3 \cdot 2^{a-2} + b_1 + c_1 + c_2 + 3 \sum^{a-3} 2^i(d_i + e_i),$$

$$B = 3 \cdot 2^{a-2} + b_2 + 2c_1 - 2c_2 + 3 \sum^{a-3} 2^i(-d_i + e_i).$$

Since $-m < A, B < 2m$, equation (3) can hold only if A and B are in the set $\{0, m\}$.

Assume $A = B = m$. Then,

$$|A + B| \leqslant 3 \cdot 2^{a-1} + |b_1| + |b_2| + 3|c_1| + |-c_2| + 3 \cdot 2 \sum^{a-3} 2^i|e_i|$$
$$\leqslant 3 \cdot 2^{a-1} + 6 + 3 \cdot 2(2^{a-2} - 1) = 3 \cdot 2^a < 2m = A + B.$$

This contradiction shows that not both A and B can be m. Assume one of A and B is m and the other zero. Then,

$$|A - B| \leqslant |b_1| + |-b_2| + |-c_1| + 3|c_2| + 3 \cdot 2 \sum^{a-3} 2^i|d_i|$$
$$\leqslant 6 + 3 \cdot 2(2^{a-2} - 1) = 3 \cdot 2^{a-1} < m = |A - B|.$$

From this we can conclude that $A = B = 0$. Therefore

$$A + B = 3 \cdot 2^{a-1} + b_1 + b_2 + 3c_1 - c_2 + 3 \cdot 2 \sum^{a-3} 2^i e_i = 0,$$

whence

$$3 \cdot 2^{a-1} = \left| b_1 + b_2 + 3c_1 - c_2 + 3 \cdot 2 \sum^{a-3} 2^i e_i \right| \leqslant 6 + 3 \cdot 2(2^{a-2} - 1) = 3 \cdot 2^{a-1},$$

with equality only if $b_1 = b_2 = c_1 = -c_2 \neq 0$. However, if these conditions are satisfied, then

$$A - B = b_1 - b_2 - c_1 + 3c_2 + 3 \cdot 2 \sum^{a-3} 2^i d_i \neq 0.$$

From this final contradiction we conclude that the set of u's, v's, w's, and z's is a free set and that $\tau(C_m^2) = 2[\log_2 m] + 1$ if $3 \cdot 2^{a-1} < m < 2^{a+1}$ for $a \geqslant 2$. This completes the proof of the theorem.

References

1. Jean Pierre Serre, *A course in arithmetic*, Graduate Texts in Math., no. 7, Springer-Verlag, New York, 1973. MR **49** #8956.

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

3. S. K. Stein, *Modified linear dependence and the capacity of a cyclic graph*, Linear Algebra Appl. **17** (1977), 191–195. MR **57** #2983.

Department of Mathematics, University of California, Davis, California 95616

Department of Mathematics, University of Wroclaw, 50-137 Wroclaw, Poland