Thirteenth International Workshop on Algebraic and Combinatorial Coding Theory
June 15-21, 2012, Pomorie, Bulgaria *pp. 188–191*

Proper integers for search with a lie

Emil Kolev emil@math.bas.bg
Institute of Mathematica and Informatics
Bulgarian Academy of Sciences

Abstract. In this note we consider nonadaptive search with a lie for an unknown element from the set $A = \{1, 2, 3, \ldots, 2^k\}$. The question sets are all subsets of A of weight S for some positive integer S. A positive integer S is called proper if one can find the unknown element with minimum possible number of questions. We show that the problem of finding all proper S is connected to one error-correcting codes with 2^k codewords. In particular we show that when using Hamming code of length $n = 2^t - 1$ for t even there exist proper integers S_{min} and S_{max} such that S is proper if and only if $S_{min} \leq S \leq S_{max}$.

1 Introduction

Let $A = \{1, 2, 3, \ldots, 2^k\}$ and $x \in A$ be unknown element. To find x we can ask questions whether x is an element of a subset B of A where, for some positive integer S, the sum of elements of B equals S. We consider nonadaptive search, i.e. we ask all questions simultaneously and allow at most one lie in the answers received. Firstly, we wish to find the minimum number of questions needed to find x. It is straightforward that this minimum is equal to the minimum value of n for which there exists a binary code of length n, cardinality 2^k and minimum distance 3. Second, when this n is found, we want to determine all S for which there exists a collection $B_1, B_2, \ldots, B_n$ of subsets of A of weight S that determines x. Search with sets of given sum is considered in [3, 5]. For other search problems the reader is referred to [1, 2, 4].

We say that a vector $(v_1, v_2, \ldots, v_{2^k})$ is *characteristic vector* for a subset B of A if $v_i = 1$ when $i \in B$ and $v_i = 0$ otherwise. An $n \times 2^k$ matrix G is called *characteristic matrix* for a collection $B_1, B_2, \ldots, B_n$ of subsets if the rows of G are all characteristic vectors of $B_1, B_2, \ldots, B_n$.

Let n be the minimum number of questions needed to find x. Suppose there exists a collection $B_1, B_2, \ldots, B_n$ of question sets of weight S that determines x. By asking whether x belongs to B_i for $i = 1, 2, \ldots, n$ we obtain as answers a sequence of "yes" and "no" of length n. Note also that if the vector V_i is the $i-$th column of the characteristic matrix for this collection, then the element i gets as answer a binary vector V (1 meaning "yes" and 0 meaning "no") of length n and $d(V, V_i^t) \leq 1$. Therefore, if the unknown element can be

found by the collection $B_1, B_2, \ldots, B_n$ then the columns of the corresponding characteristic matrix form a binary one error-correcting code. Such a matrix is called *proper matrix* of weight S. Note that if G is a proper matrix of weight S then

$$G(1, 2, 3, \ldots, 2^k)^t = S(1, 1, 1, \ldots, 1)^t.$$

Let $V = (v_1, v_2, \ldots, v_n)^t$ be binary vector column of length n. Denote by π the cyclic shift of V by one position, i.e. $\pi(V) = (v_2, v_3, \ldots, v_n, v_1)^t$. It is well known that π partitions the set of all binary vectors of length n into orbits and the length of each orbit is a divisor of n. Also, the elements in one and the same orbit have equal weights. If the length of the orbit containing V where $\mathrm{wt}(V) = w$ equals l then call the matrix with columns $V, \pi(V), \pi^2(V), \ldots, \pi^{l-1}(V)$ (not necessarily in this order) *orbit matrix of weight w and length l*. Denote such matrix by $C_{w,l}$. It is easy to see that n divides lw and there are $\dfrac{lw}{n}$ ones in every row of $C_{w,l}$. The matrix obtained from $C_{w,l}$ by interchanging 0 and 1 is denoted by $\overline{C_{w,l}}$ and has weight $n - w$.

2 Using binary Hamming code

Consider one error-correcting cyclic code $\mathcal{C}$ of length n containing all-one vector. All codewords split into orbit matrices with respect to cyclic shift. Moreover if $C_{w,l}$ is an orbit matrix of codewords then $\overline{C_{w,l}}$ is also an orbit matrix of codewords. In particular we consider an $[n = 2^t - 1, k = 2^t - t - 1, 3]$ Hamming code.

Next Lemma shows how, using all orbit matrices of $\mathcal{C}$, one can construct a proper matrix.

Lemma 1. Let $C_1, C_2, \ldots, C_m$ be all orbit matrices of $\mathcal{C}$ such that for any $i, 1 \leq i \leq m$, $\overline{C_i}$ is also from this collection. The matrix $G = C_1 C_2 \ldots C_m$ is proper one.

Proof: First note that, since n is odd, for all w we have that $w \neq n - w$. Hence $C_{w,l}$ and $\overline{C_{w,l}}$ are distinct matrices.

Therefore it suffices to show that $C_{w,l}$ and $\overline{C_{w,l}}$ add one and the same amount in the scalar product of every row of G with $(1, 2, \ldots, 2^n)$. Let the first column of $C_{w,l}$ be on position p and the first column of $\overline{C_{w,l}}$ be on position q. Using that $C_{w,l}$ and $\overline{C_{w,l}}$ are complementary to each other it is easy to see that the amount added to the scalar product of each row with $(1, 2, \ldots, 2^k)$ equals

$$p + (p+1) + \cdots + (p+l-1) + (q-p)\frac{l(n-w)}{n} = \frac{l(l-1)}{2} + ql - (q-p)\frac{lw}{n}.$$

This completes the proof. $\diamond$

Remark 1. Note that Lemma 1 is true for any collection $D_1, D_2, \ldots, D_s$ where for any $i = 1, 2, \ldots, s$ the columns of D_i are any permutation of the columns of several orbit matrices and $\overline{D_i}$ is also from this collection.

Let H_1 be submatrix of a matrix G. If H_2 is a matrix having the same dimensions as H_1 then denote by $G(H_1 \to H_2)$ the matrix obtained from G by replacing H_1 by H_2. The next lemmas shows how, given a proper matrix, one can obtain new proper matrices by transformations of the type $H_1 \to H_2$.

Lemma 2. Consider proper matrix G and let $C_{p,t}$ and $C_{q,h}$ be neighboring orbit matrices in G. Then $G_1 = G(C_{p,t}C_{q,h} \to C_{q,h}C_{p,t})$ is a proper matrix of weight $\mathrm{wt}(G_1) = \mathrm{wt}(G) + \frac{th(p-q)}{n}$.

Remark 2. Lemma 2 is applicable not only for orbit matrices but in more general situation. Let C_1 and C_2 be neighboring matrices in G. If all rows of C_1 contain one and the the same number of 1's and all rows of C_2 also contain one and the same number of 1's then $G_1 = G(C_1C_2 \to C_2C_1)$ is proper matrix. The weight of G_1 depends on the size of C_1 and C_2 and the number of 1's in each row.

Lemma 3. Let V be a vector-column of weight w and let

$$C_{w,l} = \left(V\pi(V)\pi^2(V)\ldots\pi^{l-1}(V)\right)$$

be orbit matrix of weight w and length l. Also, set

$$T_{w,n-w} = \left(V\overline{V}\pi\left(V\right)\pi\left(\overline{V}\right)\ldots\pi^{l-1}\left(V\right)\pi^{l-1}\left(\overline{V}\right)\right)$$

and $T_{n-w,w} = \overline{T_{w,n-w}}$.

a) If G is a proper matrix having $C_{w,l}$ and $\overline{C_{w,l}}$ as neighboring matrices then $G_1 = G\left(C_{w,l}\overline{C_{w,l}} \to T_{w,n-w}\right)$ is proper and $\mathrm{wt}(G_1) = \mathrm{wt}(G) + (2w-n)\frac{l(l-1)}{2n}$;

b) Consider a proper matrix G having $T_{w,n-w}$ as submatrix. The matrix $G_2 = G\left(T_{w,n-w} \to T_{n-w,w}\right)$ is proper and $\mathrm{wt}(G_2) = \mathrm{wt}(G) + (2w-n)\frac{l}{n}$.

It follows from Lemma 1 that the maximal value of S_{max} is obtained when the orbit matrices are in increasing order of their weights (see also [3]). By ordering orbit matrices in decreasing order of their weights one finds the value of S_{min}.

As shown in [5] when using $[7, 4, 3]$ Hamming code not all integers in the interval $[S_{min} = 57, S_{max} = 79]$ are proper.

Theorem 1. For the binary Hamming code of length $n = 2^t - 1$, t even, all integers in the interval $[S_{min}, S_{max}]$ are proper ones.

Sketch proof. According to Lemma 1 we order the orbit matrices in increasing order of their weights and get a proper matrix G of weight S_{max}. Note that if G is a proper matrix of weight w then $\overline{G}$ is also a proper matrix of weight $2^k - w$. In particular $S_{max} + S_{min} = 2^k$. Therefore it suffices to prove that there exists a proper matrix of weight w for $w \in [2^{k-1}, S_{max}]$. The main idea is by using Lemma 2 and Lemma 3 to manipulate the orbit matrices from G in order to get a proper matrix of desired weight.

For example, to obtain a proper matrix of weight $S_{max} - 1$ we use the assertions of Lemma 1, Lemma 2 and the observation from Remark 1 and remark 2. According to Lemma 1 the matrix $G = C_0 C_{3,1} C_{3,2} \dots C_{3,r} \dots C_s$ is proper of weight S_{max}. Take $\frac{2^t-1}{3}$ codewords $V_1, V_2, \dots V_{\frac{2^t-1}{3}}$ of weight 3 with sum equals to all one vector (it is not difficult to be seen that such codewords exist). According to Remark 2 there exists a proper matrix G of weight S_{max} of the form $G = V_0^t V_1^t \dots V_{\frac{2^t-1}{3}}^t \dots$ where V_0 is the zero vector. It is clear now that $G_1 = V_1^t \dots V_{\frac{2^t-1}{3}}^t V_0^t \dots$ is a proper of weight $S_{max} - 1$.

Using Lemma 2 and Lemma 3 in a proper way one can find a proper matrix G of weight w for any $w \in [2^{k-1}, S_{max}]$.

References

[1] J. Czyzowicz, D. Mundici and A. Pelc, *Ulam's Searching Game With Lies*, J. Combin. Theory Ser. A 52(1989), 62-76.

[2] R. Hill and J. P.Karim, *Searching With lies: the Ulam Problem*, Discrete Mathematics, 106-107(1992), 273-283.

[3] E. Kolev, *Nonadaptive Search With Sets of Given Sum*, Proc. ACCT'9, Tsarskoe selo, (2002), 159-162.

[4] E. Kolev and I.Landgev, *On a Two-Dimensional Search Problem* Serdica Math. J. 21(1995), 219-230.

[5] Nikolay Ditchev and Emil Kolev, *Nonadaptive Search with a lie*, Ninth International Workshop, Algebraic and Combinatorial Coding theory, Kranevo, June 19-25, 2004, 120-124.