A Lower Bound on the Greedy Weights of Product Codes and Projective Multisets

Hans Georg Schaathun[1]
Department of Informatics
University of Bergen
Høyteknologisenteret
N-5020 Bergen, Norway
e-mail: georg@ii.uib.no

Abstract — **We present the relation between product codes and projective multisets, and give a lower bound on the greedy weights of product codes.**

I. GREEDY WEIGHTS

The weight hierarchy has received a lot of attention after Victor Wei's paper [5]. Let C be an $[n, k]$ linear code. The support of a codeword $c \in C$ is the set $\chi(c)$ of non-zero coordinate positions. For a subcode $D \subseteq C$ we write $\chi(D) = \bigcup_{c \in D} \chi(c)$. The support size $\#\chi(D)$ is called the weight of D. The weight hierarchy of C is the sequence $(d_1, d_2, \ldots, d_k)$, where d_r is the least weight of an r-dimensional subcode.

When the code is applied on the Wire-Tap Channel of Type II, d_i is the number of channel symbols needed to acquire i information symbols.

The greedy weights are inspired by the following problem: Suppose the adversary uses a greedy approach. First he reads d_1 symbols to get one information symbol. After having got $i - 1$ information symbol, his top priority is to get the i-th bit as soon as possible. The total number of bits required to get i information symbols by this greedy approach is called the i-th greedy weight and denoted g_i; and g_2 has been studied in [1, 2].

The number g_i may equivalently be defined recursively from the code. Let a greedy 1-subcode be a subcode of dimension 1 and weight $g_1 = d_1$. Let a greedy i-subcode be a subcode of dimension i and as small weight as possible under the constraint that it contain a greedy $(i - 1)$-subcode. Then g_i is the weight of a greedy i-subcode.

II. PROJECTIVE MULTISETS

A q-ary $[n, k]$ code C is determined completely by its generator matrix G. The rows of G constitute a basis for C. The columns of G make the *projective multiset* γ_C corresponding to C. A projective multiset is a collection of projective points, not necessarily distinct, and it is often written as a map

$$\gamma_C : \mathsf{PG}(k - 1, q) \to \{0, 1, 2, \ldots\},$$

where the value $\gamma_C(x)$ of x is the number of times x occurs in the collection. The value of a set S as $\gamma_C(S) = \sum_{x \in S} \gamma_C(x)$.

It is well known that there is a one-to-one correspondence between subcodes $D \subseteq C$ of dimension i and subspaces $\Pi \subseteq \mathsf{PG}(k - 1, q)$ of codimension i, such that $\#\chi(D) = n - \gamma_C(\Pi)$.

The subspaces corresponding to greedy subcodes are called greedy subspaces. We can equivalently define a greedy subspace of codimension 1 to be a hyperplane of value $n - d_1 = $

n − g_1. Then we define a greedy subspace of codimension i to be a subspace of maximum value under the constraint that it be contained in a greedy subspace of codimension $i - 1$. The value of a greedy subspace of codimension i is $n - g_i$.

III. PRODUCT CODES

The product code $C = A \otimes B$ is the tensor product of A and B as vector spaces. In [3] we saw that γ_C is obtained by applying the Segre embedding on γ_A and γ_B. As a consequence we found a lower bound on the weight hierarchy of product codes and proved the Wei-Yang conjecture. These results have been generalised in [4]. Here we use the same technique to bound the greedy weights. The bound we find is quite similar to the existing one on the weight hierarchy, but the proof requires more care.

Define

$$\mathcal{M}_t := \{\mathbf{i} = (i_1, i_2, \ldots, i_{t-1}) \mid 1 \leq i_j \leq k_j, 1 \leq j < t\}.$$

Definition 1 *Let π be a map $\mathcal{M}_t \to \{0, 1, \ldots, k_t\}$ given by $\mathbf{i} \mapsto t_{\mathbf{i}}$. We call π a $(k_1, k_2, \ldots, k_t)$-partition of r if*

1. $\sum_{\mathbf{i} \in \mathcal{M}_t} t_{\mathbf{i}} = r$.

2. π is a decreasing function in each coordinate, i.e.
$$t_{i_1, \ldots, i_j, \ldots, i_{t-1}} \leq t_{i_1, \ldots, i_j - 1, \ldots, i_{t-1}} \text{ for } j = 1, \ldots, t - 1$$
and $1 < i_j$.

The set of all $(k_1, k_2, \ldots, k_t)$-partitions of r is denoted by $\mathcal{P}(k_1, \ldots, k_t; r)$.

Theorem 1 *If $C_1, C_2, \ldots, C_t$ are linear codes, then*

$$g_r(C_1 \otimes \ldots \otimes C_t) \geq \min \left\{ \nabla_E(\pi) \mid \pi \in \mathcal{P}(k_1, \ldots, k_t; r) \right\},$$

where

$$\nabla_E(\pi) := \sum_{\mathbf{i} \in \mathcal{M}_t} \prod_{j=1}^{t-1} (g_{i_j}(C_j) - g_{i_j - 1}(C_j)) g_{\pi(\mathbf{i})}(C_t).$$

It was proved in [2] that this bound holds with equality for $r = 2$.

REFERENCES

[1] Wende Chen and Torleiv Kløve. On the second greedy weight for linear codes of dimension 3. To appear in Discrete Mathematics.

[2] Gérard D. Cohen, Sylvia B. Encheva, and Gilles Zémor. Antichain codes. *Des. Codes Cryptogr.*, 18(1-3):71–80, 1999.

[3] Hans Georg Schaathun. The weight hierarchy of product codes. *IEEE Trans. Inform. Theory*, 46(7):2648–2651, November 2000.

[4] Hans Georg Schaathun and Wolfgang Willems. A lower bound for the weight hierarchy of product codes and projective multisets. In *Proc. IEEE Intern. Symp. Inform. Theory*, June 2001.

[5] Victor K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.