On Weight Hierarchies of Product Codes The Wei-Yang Conjecture and more

Conchita Martínez-Pérez

Departamento de Matemáticas, Universidad de Zaragoza, 50009 Zaragoza, Spain. Email: ⟨conmar@posta.unizar.es⟩.

Hans Georg Schaathun

Institutt for Informatikk, Universitas Bergensis, Høyteknologisenteret, N-5020 Bergen, Norway. Email: ⟨georg@ii.uib.no⟩.

Wolfgang Willems

Fakultät für Mathematik, Otto-von-Guericke-Universität, D 39106 Magdeburg, Germany. Email: ⟨wolfgang.willems@mathematik.uni-magdeburg.de⟩.

Abstract

The weight of a code is the number of coordinate positions where no codeword is zero. The rth minimum weight d_r is the least weight of an r-dimensional subcode. Wei and Yang conjectured a formula for the minimum weights of some product codes. The conjecture is proved in two different ways, each with interesting side-results.

Key words: product code, projective multiset, weight hierarchy, Segre embedding, chain condition

1 Introduction

Generalised Hamming weights have received a lot of attention after Victor Wei's paper [14] in 1991. An early project by Victor Wei and Kyeongcheol Yang [15] attempted to determine the weight hierarchy of product codes, given the weight hierarchies for the component codes.

In the special case where both the component codes satisfy the chain condition they found an upper bound on the weight hierarchy. They conjectured that this bound is always satisfied with equality.

Two different proofs of the conjecture have appeared recently [11,9]. Each of the proofs give interesting generalisations of the Wei-Yang conjecture. In the sequel we will survey the results from both papers, as well as related results from the last decade. A new result appears in Theorem 8. Finally we suggest some open problems for further study.

2 Product Codes

An $[n, k]$ code is a k-dimensional subspace $C \leqq \mathbb{V}$ of some n-dimensional vector space $\mathbb{V}$. The support of a vector $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbb{V}$ is the set

$$\chi(\mathbf{c}) := \{i \mid c_i \neq 0\},$$

and the support of a subset $S \subseteq \mathbb{V}$ is the set

$$\chi(S) := \bigcup_{\mathbf{c} \in S} \chi(\mathbf{c}).$$

The weight hierarchy of the code $C \leqq \mathbb{V}$ is the sequence

$$(d_1(C), d_2(C), \ldots, d_k(C)),$$

where

$$d_r(C) := \min\{\#\chi(D) \mid D \leqq C, \dim D = r\}.$$

Clearly $d_1(C)$ is the minimum distance, and for convenience we put $d_0(C) = 0$.

The chain condition says that there exists a sequence of subcodes

$$\{0\} = D_0 < D_1 < \ldots < D_k = C,$$

such that D_i has dimension i and weight $d_i(C)$. Codes satisfying the chain condition are called chained codes.

Remark 1 *Almost all codes violate the chain condition [4]. However, a lot of interesting codes do satisfy the chain condition, such as the Hamming, Reed-Muller, MDS and extended Golay codes. In particular, codes with high generalised Hamming weights tend to satisfy the chain condition.*

Let C_1 be an $[n_1, k_1]$ code and C_2 an $[n_2, k_2]$ code over the same field $\mathbb{F}$. The product code $C_1 \otimes C_2$ is the tensor product of C_1 and C_2 as vector spaces over $\mathbb{F}$. In other words

$$C_1 \otimes C_2 = \langle a \otimes b \mid a \in C_1, b \in C_2 \rangle,$$

where

$$\begin{aligned} a \otimes b &= (a_i b_j \mid 1 \le i \le n_1, 1 \le j \le n_2), \\ a &= (a_1, a_2, \dots, a_{n_1}), \\ b &= (b_1, b_2, \dots, b_{n_2}). \end{aligned}$$

The product code is an $[n_1 n_2, k_1 k_2]$ code.

A (k_1, k_2)-partition of r is a non-increasing sequence $\pi = (t_1, t_2, \dots, t_{k_1})$ such that $t_1 + t_2 + \ldots + t_{k_1} = r$ and $t_i \le k_2$. Let $\mathcal{P}(k_1, k_2; r)$ denote the set of all (k_1, k_2)-partitions of r.

We define

$$\begin{aligned} \nabla(\pi) &:= \sum_{i=1}^{k_1} (d_i(C_1) - d_{i-1}(C_1)) d_{t_i}(C_2), \quad \pi \in \mathcal{P}(k_1, k_2; r), \\ d_r^*(C_1 \otimes C_2) &:= \min\{\nabla(\pi) \mid \pi \in \mathcal{P}(k_1, k_2; r)\}. \end{aligned}$$

The number d_r^* was first defined in [15], and the following theorem was proved.

Theorem 2 (Wei–Yang 1993) *If C_1 and C_2 are chained codes, then*

$$d_r(C_1 \otimes C_2) \le d_r^*(C_1 \otimes C_2) \quad \textit{for all } r.$$

The Wei-Yang conjecture says that $d_r(C_1 \otimes C_2) = d_r^*(C_1 \otimes C_2)$ for chained codes C_1 and C_2. This has been proved for $r \le 4$ by Barbero and Teña [1]. Following the conjecture, d_r^* has been determined for some linear codes by Helleseth and Kløve in [7]. It has also been proved that $d_r^*(C_1 \otimes C_2) = d_r^*(C_2 \otimes C_1)$. Jeng Yune Park [10] has computed d_r^* for products of certain classes of codes and shown that the conjecture holds for these classes.

Theorem 3 (Schaathun 2000) *If C_1 and C_2 are arbitrary linear codes, then*

$$d_r(C_1 \otimes C_2) \ge d_r^*(C_1 \otimes C_2) \quad \textit{for all } r.$$

The theorem has been proved in the language of projective multiset. Obviously Theorem 2 and 3 together prove the Wei-Yang conjecture.

A projective multiset is a collection of projective points which are not necessarily distinct. It is often presented as a map

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

where the value $\gamma(x)$ of a point x is the number of times x occurs in the collection. We also define the value of a subset $S \subseteq \mathsf{PG}(k-1, q)$ to be $\gamma(S) = \sum_{x \in S} \gamma(x)$.

There is a well-known one-to-one correspondence between equivalence classes of projective multisets on $\mathsf{PG}(k-1,q)$ and equivalence classes of linear q-ary codes of dimension k. See for instance [13,5,11]. The projective multiset γ corresponding to some $[n,k]$ code C is obtained by taking the columns of some generator matrix for C as projective points.

The largest value of any subspace of codimension r in $\mathsf{PG}(k-1,q)$ is $n-d_r(C)$. Hence the weight hierarchy can be computed in the language of projective multisets.

When a and b are projective points, the map $a,b \mapsto a \otimes b$ is known as the Segre embedding. The image under the Segre embedding is called the Segre variety. The proof of Theorem 3 is based on the following key fact.

Proposition 4 *Let γ_A, γ_B, and γ_C be the projective multisets corresponding to linear codes A, B, and $C = A \otimes B$, respectively. We have:*

$$\begin{aligned} \gamma_C(a \otimes b) &= \gamma_A(a) \cdot \gamma_B(b), && \forall a \in \mathbb{P}^{k_A-1}, \forall b \in \mathbb{P}^{k_B-1}, \\ \gamma_C(c) &= 0, && \forall c \notin Y, \end{aligned}$$

where Y is the Segre variety.

Theorem 5 *For any two linear codes C_1 and C_2, we have*

$$d_r^*(C_1 \otimes C_2) = d_r(C_1 \otimes C_2), \quad r \in \{0,1,2,k-2,k-1,k\}.$$

This is well known for $r = 0,1,k$. Wei and Yang proved it for $r = 2$. The proof for $r = k-2, k-1$ appears in [11], based on the language of projective multisets. For a six-dimensional product code $C_1 \otimes C_2$, we may or may not have $d_3^*(C_1 \otimes C_2) = d_3(C_1 \otimes C_2)$, see [11].

3 General Product Codes

Generalising the results from Section 2 we are lead to the following question: *Given a family $C_1, C_2, \ldots, C_t$ of linear codes, what can we say about the weight hierarchy of $C_1 \otimes C_2 \otimes \ldots \otimes C_t$?*

It is worth noting that the affirmative answer to the Wei-Yang conjecture has no implications for general product codes. Even if C_1 and C_2 are chained, $C_1 \otimes C_2$ may be non-chained.

To answer the question, we generalise the definition of (k_1,k_2)-partitions to $(k_1,k_2,\ldots,k_t)$-partitions.

Define

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

Note that $\mathcal{M}_2$ is just the set of integers from 1 through k_1. Hence an element $\pi \in \mathcal{P}(k_1, k_2; r)$ is a map $\pi : \mathcal{M}_2 \to \{0, 1, \dots, k_2\}$ where $\pi(i) = t_i$.

Definition 6 *Let π be a map $\mathcal{M}_t \to \{0, 1, \dots, k_t\}$ given by $\mathbf{i} \mapsto t_{\mathbf{i}}$. We call π a $(k_1, k_2, \dots, k_t)$-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.*

$$t_{i_1, \dots, i_j, \dots, i_{t-1}} \le t_{i_1, \dots, i_j - 1, \dots, i_{t-1}}$$

for $j = 1, \dots, t-1$ *and* $1 < i_j$.

We define the general expression for d_r^* as follows:

$$d_r^*(C_1 \otimes C_2 \otimes \dots \otimes C_t) := \min \Big\{ \nabla(\pi) \mid \pi \in \mathcal{P}(k_1, k_2, \dots, k_t; r) \Big\},$$

where

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

Theorem 7 (Martínez-Pérez–Willems 2000)
If $C_1, C_2, \dots, C_t$ are chained codes, then

$$d_r(C_1 \otimes C_2 \otimes \dots \otimes C_t) = d_r^*(C_1 \otimes C_2 \otimes \dots \otimes C_t).$$

The Wei-Yang conjecture is just the special case of the theorem with $t = 2$.

The original proof of Theorem 7 above uses only elementary facts from linear algebra. For each subspace $D \leqq C_1 \otimes C_2 \otimes \dots \otimes C_t$ there is a so-called *normal* subspace $\bar{D}$ such that $\dim D = \dim \bar{D}$ and $\#\chi(\bar{D}) \le \#\chi(D)$. Such a normal subspace $\bar{D}$ is naturally associated to a $(k_1, \dots, k_t)$-partition π and has support size $\nabla(\pi)$.

The following theorem is a new result. The proof is based on projective multisets, and it can also be extended to prove Theorem 7. We hope to publish the proof elsewhere.

Theorem 8 *If $C_1, C_2, \dots, C_t$ are arbitrary linear codes, then*

$$d_r(C_1 \otimes C_2 \otimes \dots \otimes C_t) \ge d_r^*(C_1 \otimes C_2 \otimes \dots \otimes C_t).$$

By Theorem 3, we can obtain a lower bound for general product codes by recursion, but the theorem above is stronger than that. There is an analogue of Theorem 8 [12] for the greedy weights, which was introduced in [2,3].

A Some Future Work

The support weight distribution was introduced in [8]. It was proved that if the support weight distribution for C is known, then one can also find the weight distribution of $C \otimes S$, where S is a simplex code. The support weight distribution is only known for a very few classes of codes. Is it possible to find the support weight distribution of some classes of product codes, such as the product of two simplex codes?

David Forney [6] proved that the generalised Hamming weights give a lower bound on the state complexity of a minimal trellis. It was proved that this bound is met with equality with some optimal bit ordering if and only if the code meets the so-called two-way chain condition. Is it possible to determine completely the state complexity of a product code, given the state complexities of the component codes?

References

[1] Angela I. Barbero and Juan G. Tena. Weight hierarchy of a product code. *IEEE Trans. Inform. Theory*, 41(5):1475–1479, September 1995.

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

[3] Wende Chen and Torleiv Kløve. On the second greedy weight for binary linear codes. In M. Fossorier et al., editor, *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, volume 1719 of *Springer Lecture Notes in Computer Science*, pages 131–141, 1999.

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

[5] S. Dodunekov and J. Simonis. Codes and projective multisets. *Electron. J. Combin.*, 5(1), 1998. Research Paper 37.

[6] G. David Forney, Jr. Dimension/length profiles and trellis complexity of linear block codes. *IEEE Trans. Inform. Theory*, 40(6):1741–1752, 1994.

[7] Tor Helleseth and Torleiv Kløve. The weight hierarchies of some product codes. *IEEE Trans. Inform. Theory*, 42(3):1029–1034, 1996.

[8] Tor Helleseth, Torleiv Kløve, and Johannes Mykkeltveit. The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l - 1)/n)$. *Discrete Math.*, 18:179–211, 1977.

[9] Conchita Martínez-Pérez and Wolfgang Willems. On the weight hierarchy of product codes. Preprint submitted to IEEE Trans. Inf. Theory, 2000.

[10] Jeng Yune Park. The weight hierarchies of some product codes. *IEEE Trans. Inform. Theory*, 46(6):2228–2235, November 2000.

[11] Hans Georg Schaathun. The weight hierarchy of product codes. *IEEE Trans. Inform. Theory*, 2000. To appear.

[12] Hans Georg Schaathun. A lower bound on the greedy weights of product codes. Submitted to ISIT, 2001.

[13] Michael A. Tsfasman and Serge G. Vlăduţ. Geometric approach to higher weights. *IEEE Trans. Inform. Theory*, 41(6, part 1):1564–1588, 1995. Special issue on algebraic geometry codes.

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

[15] Victor K. Wei and Kyeongcheol Yang. On the generalized Hamming weights of product codes. *IEEE Trans. Inform. Theory*, 39(5):1709–1713, 1993.