

A generalization of Kung's theorem

Trygve Johnsen* Keisuke Shiromoto† Hugues Verdure‡

September 28, 2015

Abstract

We give a generalization of Kung's theorem on critical exponents of linear codes over a finite field, in terms of sums of extended weight polynomials of linear codes. For all $i = k + 1, \dots, n$, we give an upper bound on the smallest integer m such that there exist m codewords whose union of supports has cardinality at least i .

Keywords: linear code Kung's bound generalized Singleton bound
2010 Mathematics Subject Classification. 94B05 (05E40)

Acknowledgements

The first and third author are grateful to Thomas Britz and the second author for sharing early versions of the joint manuscript [2] with all of us. The material and results there gave the inspiration for writing the present article.

The second author was supported by JSPS KAKENHI Grant Number 14474695.

The first author wants to thank IMPA, Rio de Janeiro, where he stayed while this work was completed.

1 Introduction and main result

For a non-degenerate $[n, k]$ code C over a finite field \mathbb{F}_q , let c_j be the smallest integer m such that there exists a codeword of Hamming weight at least j in $C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$. In [6, 7], the authors show that there exist polynomials $P_j(x)$, only dependent on the matroid associated to (any parity check matrix of) C , such that the number of codewords of Hamming weight j in $C \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$ is $P_j(q^m)$ (see Theorems 5.4 and 5.9 of [7] for example).

We now recall the definition of these polynomials:

Definition 1.1 *Let M_C be the matroid associated to the parity check matrices of C , and n_{M_C} its nullity function. Set*

$$P_j(x) = (-1)^j \sum_{|\sigma|=j} \sum_{\gamma \subseteq \sigma} (-1)^{|\gamma|} x^{n_{M_C}(\gamma)} \text{ for } 0 \leq j \leq n.$$

Hence we see that c_j is the smallest integer m such that

$$P_j(q^m) + \dots + P_n(q^m) \neq 0.$$

*Dept. of Mathematics, University of Tromsø, N-9037 Tromsø, Norway, Trygve.Johnsen@uit.no

†Dept. of Mathematics and Engineering, Kumamoto University, 2-39-1 Kurokami, Kumamoto, 860-8555 Japan, keisuke@kumamoto-u.ac.jp

‡Dept. of Mathematics, University of Tromsø, N-9037 Tromsø, Norway, Hugues.Verdure@uit.no

In the special case $j = n$, we see that c_n is the smallest m such that $P_n(q^m) \neq 0$. The polynomials $P_j(x)$ can of course also be expressed in terms of functions obtained from the matroid of generator (instead of parity check) matrices of C . Then

$$P_n(x) = \sum_{A \subseteq E} (-1)^{|A|} x^{\rho(E) - \rho(A)},$$

where ρ is the rank function associated to the matroid of generator matrices of C , and $E = \{1, 2, \dots, n\}$. For simplicity, and in order to be in harmony with established notation, we will denote $P_n(x)$ by $p(M_C; x)$.

This makes it natural to quote the "Critical Theorem" by Crapo and Rota, [3]:

Theorem 1.1 *Let C be an $[n, k]$ code over \mathbb{F}_q . For any $X \subseteq E$ and any natural number m , the number of ordered m -tuples $(\mathbf{v}_1, \dots, \mathbf{v}_m)$ of codewords in C with $\text{supp}(\mathbf{v}_1) \cup \dots \cup \text{supp}(\mathbf{v}_m) = X$ is $p(M_{C/(E-X)}; q^m)$, where $C/(E-X)$ is the code shortened by $E-X$.*

Remark 1.1 *In particular the number of ordered m -tuples $(\mathbf{v}_1, \dots, \mathbf{v}_m)$ of codewords in C with $\text{supp}(\mathbf{v}_1) \cup \dots \cup \text{supp}(\mathbf{v}_m) = E$ is $p(M_C; q^m)$. Hence we see that the number of ordered m -tuples of codewords from \mathbb{F}_q with support E , as described in [3], is the same as the number of codewords over \mathbb{F}_{q^m} (with the same generator matrix) with support E , as counted above. The analogous statement holds, also for any subset X of E . This follows, for example, from Proposition 4 and Corollary 5 of [5]. In Proposition 4 one sets up an isomorphism between the set of ordered m -tuples over \mathbb{F}_q in question, and the set of codewords over \mathbb{F}_{q^m} in question, and in Corollary 5 one states that this isomorphism is support-preserving (since the union of the supports of m codewords over \mathbb{F}_q is the same as the support of the subspace (of dimension at most m over \mathbb{F}_q) generated by these words). Hence the formula in the Critical Theorem also counts the number of codewords over \mathbb{F}_{q^m} with support X , and we understand that for each j , the number $P_j(q^m)$ described above, also counts the number of ordered m -tuples of codewords from \mathbb{F}_q with support weight j , that is, the size of their union of supports. Moreover this number appears as a sum of contributions $p(M_{C/(E-X)}; q^m)$, where the sum is taken over all subsets X of cardinality j . These observations give:*

Corollary 1.1 *For $1 \leq j \leq n$, we have: c_j is the smallest integer m such that there exists m codewords over \mathbb{F}_q , whose union of supports has cardinality at least j .*

We now give:

Definition 1.2 *Let C be a non-degenerate $[n, k]$ code. For $1 \leq j \leq n$, let γ_j be the smallest integer m such that there exists a m -dimensional (over \mathbb{F}_q) subspace D of C with support weight at least j .*

We then have:

Proposition 1.1 *For each $1 \leq j \leq n$, we have $\gamma_j = c_j$.*

Proof The proof for the case $j = n$, as given in Lemma 3 of [2], immediately carries over to any j in question. ■

Moreover, if G is any generator matrix of C , then we have:

Proposition 1.2 *For $1 \leq j \leq n$ we have: $c_j = \gamma_j =$ the smallest positive integer m for which there exists a $(k-m)$ -dimensional subspace of \mathbb{F}_q^k that contains at most $n-j$ columns of G .*

Proof The proof for the case $j = n$, stated in Lemma 5 of [2], and originally in Lemma 2 of [8] carries over to any j in question. ■

Let C be an $[n, k]$ code over \mathbb{F}_q . For any i , $1 \leq i \leq k$, the i -th generalized Hamming weight of C is defined by

$$d_i = \min\{|\text{Supp}(D)| : D \text{ is an } [n, i] \text{ subcode of } C\},$$

where $\text{Supp}(D) = \bigcup_{\mathbf{x} \in D} \text{supp}(\mathbf{x})$. Then the following result is known as the *generalized Singleton bound* (cf. [10]).

Lemma 1.1

$$d_i \leq n - k + i, \quad i = 1, 2, \dots, k.$$

For $1 \leq i \leq n - k$, let s_i^\perp be the i -th Singleton defect $n - (n - k) + i - d_i^\perp = k + i - d_i^\perp$, where d_i^\perp is the i -th generalized Hamming weight of the dual code C^\perp . We now give the main result of the paper.

Theorem 1.2 (Main result) *For a non-degenerate $[n, k]$ code C over \mathbb{F}_q with $n > k$, we have*

$$c_i = \gamma_i \leq s_{n+1-i}^\perp + 2$$

for $i = k + 1, \dots, n$.

Remark 1.2 *We obviously have $\gamma_i = 1$ for all $i \leq k$, since the word Σ , being the sum of all rows in any generator matrix G , on standard form after a possible permutation of columns, has Hamming weight at least k .*

If we define $s_i^\perp = -1$ for $n - k + 1 \leq i \leq n$, then the theorem remains true for $1 \leq i \leq k$, and the bound is actually sharp for these i . We use this convention in the sequel.

Corollary 1.2 (Kung's theorem, [9]) *For a non-degenerate $[n, k]$ code C over \mathbb{F}_q , we have*

$$\gamma_n \leq k - d^\perp + 3,$$

where d^\perp is the minimum Hamming weight of the dual code C^\perp .

Proof (of the corollary): From the definition of the i -th Singleton defect, we have that

$$\begin{aligned} s_{(n+1)-n}^\perp + 2 &= s_1^\perp + 2 \\ &= (k + 1 - d_1^\perp) + 2 \\ &= k - d_1^\perp + 3 \\ &= k - d^\perp + 3. \end{aligned}$$

■

Remark 1.3 *In [4], one expresses the polynomials from the present Definition 1.1 in terms of the Betti numbers of the Stanley-Reisner rings of the matroid associated to the parity check matrix of the code in question, and so-called elongations of this matroid. The matroids are then thought of simplicial complexes with facets the bases of the matroids. Our main result is formulated in terms of properties of these polynomials. Hence the material in the present paper gives another link between coding theory properties, and algebraic topological properties of associated matroids appearing in a natural way.*

2 Proof of the generalization of Kung's bound

We now prove the main result of the article.

Proof (of Theorem 1.2): Let G be a generator matrix of C . Set $d_{n+1-i}^\perp := t$. Then it is known that the rank of any set of $(t-1)$ column vectors in G is at least $t - (n+1-i)$ and there exists a set of t column vectors whose rank is $t - (n+1-i)$ (see, for instance [10]). We assume that C has a generator matrix of the form $[I_k|A]$. From the generalized Singleton bound, it follows that

$$t \leq k + (n+1-i).$$

So we can take $\mathbf{e}_1, \dots, \mathbf{e}_{t-n-2+i}$ as linearly independent column vectors in G , where \mathbf{e}_i denotes the vector in \mathbb{F}_q^k with a 1 in the i th coordinate and 0's elsewhere.

Assume, for contradiction, that $c_i = \gamma_i > s_{n+1-i}^\perp + 2 = k + 3 + n - i - t$. By Proposition 1.2, this means that any $(k - (n+k-i-t+3)) = (t+i-3-n)$ -dimensional subspace of \mathbb{F}_q^k contains at least $n-i+1$ column vectors in G . Let $\alpha \in \mathbb{F}_q$ be non-zero. Then the $(t-n-3+i)$ -dimensional subspace D generated by $\mathbf{e}_1 + \alpha\mathbf{e}_{t-n-2+i}, \dots, \mathbf{e}_{t-n-3+i} + \alpha\mathbf{e}_{t-n-2+i}$, contains (at least) $n-i+1$ distinct column vectors of G , say

$$\begin{aligned} \mathbf{u}_1 &= (u_1^{(1)}, \dots, u_{t-n-2+i}^{(1)}, 0, \dots, 0)^t \\ &\vdots \\ \mathbf{u}_{n-i+1} &= (u_1^{(n-i+1)}, \dots, u_{t-n-2+i}^{(n-i+1)}, 0, \dots, 0)^t. \end{aligned}$$

None of these \mathbf{u}_j is equal to any \mathbf{e}_l , for $j = 1, \dots, n-i+1$ and $l = 1, \dots, t-n-2+i$. (Set a linear combination of $\mathbf{e}_1 + \alpha\mathbf{e}_{t-n-2+i}, \dots, \mathbf{e}_{t-n-3+i} + \alpha\mathbf{e}_{t-n-2+i}$ equal to \mathbf{e}_l , and derive the contradiction $\alpha = 0$.)

Therefore $\{\mathbf{u}_1, \dots, \mathbf{u}_{n-i+1}, \mathbf{e}_1, \dots, \mathbf{e}_{t-n-2+i}\}$ is a set of $(t-1)$ column vectors in G . We see any $t-n-1+i$ vectors of this set are linearly dependent, since they effectively are $t-n-1+i$ vectors in $(t-n-2+i)$ -space. Hence the rank of the subspace of \mathbb{F}_q^k spanned by these $t-1$ vectors is strictly less than $t - (n+1-i)$.

This is a contradiction, and the proof is complete. \blacksquare

3 An analysis of the sharpness of the new bound

Some initial observations are:

Inserting $i = k+1$ in the statement of Theorem 1.2, we get

$$\gamma_{k+1} = \gamma_{n+1-(n-k)} \leq s_{n-k}^\perp + 2.$$

If C^\perp is also non-degenerate, we have $s_{n-k}^\perp = 0$, so $\gamma_{k+1} \leq 2$.

It is well known that $s_1^\perp \geq s_2^\perp \dots \geq s_{n-k}^\perp$ for any linear code (cf. [10]), and it is clear from the definitions that $\gamma_i \leq \gamma_j$ if $i \leq j$.

We observe that for MDS codes, that is, an $[n, k]$ code over \mathbb{F}_q with $d_1 = d = n - k + 1$, the theorem gives $\gamma_i \leq 2$, for all $i \geq k+1$, but it is clear that there exist MDS codes with $n > k$ and individual codewords of Hamming weight n , and then $\gamma_i = 1$ for all i . Hence we do not claim that the bound given in the theorem is sharp, neither just for $i = n$, nor stronger: for all $i = k+1, \dots, n$, simultaneously.

In [2] one finds, to the contrary:

Theorem 3.1 ([2], Theorem 17) *Let C be a non-trivial $[n, k]$ code over \mathbb{F}_q , with q odd, and $d^\perp > 3$. Then $(c_n =) \gamma_n \leq k - d^\perp + 2$.*

One expects the result to be true also for $d^\perp = 3$ and q odd, with the extra assumption that C is not a simplex code. (We recall that a simplex code is the dual of a Hamming code, and that for these codes, $d^\perp = 3$.) Also for binary codes this result holds (see [2], Corollary 15, for a statement also involving most cases with $d^\perp = 3$).

Hence, at least for odd q , and $q = 2$, there are almost no linear codes with simultaneous sharpness for all $j \in \{k+1, \dots, n\}$ in Theorem 1.2, and $d^\perp \geq 3$, since there are almost no codes where the bound is sharp just for $j = n$. On the other hand, as pointed out in [2] (see also Corollary 3.1 below):

Proposition 3.1 *If an $[n, k]$ code C over \mathbb{F}_q is a simplex code, or an MDS code having no codewords of Hamming weight n , then $(c_n) \gamma_n = k - d^\perp + 3$.*

On the other hand again, if C is an MDS code having no codewords of weight n , it is easily shown, as in [2], that $\gamma_{n-1} = 1$, so the only possibility for simultaneous sharpness for all $j \geq k+1$ is $k+1 = n$, in other words an $[n, n-1]$ code. We will now, after a suitable definition valid for linear codes in general, take a closer look at simplex codes. We will study these codes in particular, since they serve as a demonstration of how good the bound in Theorem 1.2 after all is.

Definition 3.1 *For a non-degenerate $[n, k]$ code C over \mathbb{F}_q and $i = k+1, \dots, n$, we set $t_i = t_i(C) = s_{n+1-i}^\perp + 2 - \gamma_i$.*

One understands that $t_i(C)$ measures the lack of sharpness of the bound in Theorem 1.2 for each i .

Let \mathcal{H}^\perp be a $[(q^k - 1)/(q - 1), k, q^{k-1}]$ simplex code over \mathbb{F}_q . We set $\mu_s := (q^s - 1)/(q - 1)$. Then, for each $r = 1, \dots, k$, the number of r -dimensional subcodes of \mathcal{H}^\perp of support weight i is given by

$$A_i^{(r)}(\mathcal{H}^\perp) = \begin{cases} \begin{bmatrix} k \\ r \end{bmatrix}_q & , i = \mu_k - \mu_{k-r}; \\ 0 & , \text{otherwise} \end{cases}$$

where $\begin{bmatrix} k \\ r \end{bmatrix}_q$ denotes the Gaussian binomial coefficient (cf. [8]). In particular, all the subcodes of dimension r have support weight $d_r = \mu_k - \mu_{k-r}$. Therefore we can easily derive the following result.

Lemma 3.1 *For any r such that $1 \leq r \leq k$, $\gamma_i = r$ if and only if $\mu_k - \mu_{k-r+1} < i \leq \mu_k - \mu_{k-r}$.*

Proof Indeed, if $\mu_k - \mu_{k-r+1} < i$, then there is no subcode of dimension at most $r-1$ with weight support at least i , while for $i \leq \mu_k - \mu_{k-r}$, all subcodes of dimension r have weight support at least i . ■

Moreover the weight hierarchy of a Hamming $[n = (q^k - 1)/(q - 1), n - k, 3]$ code \mathcal{H} over \mathbb{F}_q is determined as follows (cf. [10]):

$$\begin{aligned} \{d_r(\mathcal{H}) : 1 \leq r \leq n - k\} &= \{1, 2, \dots, n\} \setminus \{n + 1 - (\mu_k - \mu_{k-i}) : 1 \leq i \leq k\} \\ &= \{1, 2, \dots, n\} \setminus \{\mu_{k-i} + 1 : 1 \leq i \leq k\}. \end{aligned}$$

Then it follows that:

Lemma 3.2 *Let $1 \leq r \leq n - k$. Then there exists a unique $2 \leq j \leq k$ such that $\mu_{j-1} - j + 2 \leq r \leq \mu_j - j$. Moreover,*

$$d_r(\mathcal{H}) = r + j.$$

Proof The first part is obvious, while the second part is a direct consequence of the description of the set $\{d_r(\mathcal{H}) : 1 \leq r \leq n - k\}$ above. \blacksquare

Proposition 3.2 *Let \mathcal{H}^\perp be a $[(q^k - 1)/(q - 1), k, q^{k-1}]$ simplex code over \mathbb{F}_q . For each $r, 1 \leq r \leq k$, if $i = \mu_k - \mu_{k-r+1} + l, l = 1, 2, \dots, q^{k-r}$, then*

$$t_i = \begin{cases} 0 & (l \leq k - r + 1) \\ 1 & (k - r + 2 \leq l). \end{cases}$$

Proof From Lemma 3.1, we have that $\gamma_i = r$. We set

$$s := n + 1 - i = \mu_k + 1 - (\mu_k - \mu_{k-r+1} + l) = \mu_{k-r+1} + 1 - l.$$

In the case of $r > 1$ and $l \leq k - r + 1$, it follows that

$$\mu_{k-r+1} - (k - r + 2) + 2 \leq s (\leq \mu_{k-r+2} - k - r + 2),$$

and so $d_s(\mathcal{H}) = s + (k - r + 2)$ by Lemma 3.2. Therefore we have that

$$\begin{aligned} t_i &= (k + (n + 1 - i) - d_s(\mathcal{H}) + 2) - \gamma_i \\ &= k + \mu_k + 1 - (\mu_k - \mu_{k-r+1} + l) - (\mu_{k-r+1} + 1 - l + k - r + 2) + 2 - r \\ &= 0. \end{aligned}$$

When $r = 1$ and $l \leq k - r + 1$, it follows from our convention in Remark 1.2 that in that case too,

$$t_i = s_{n+1-i}^\perp + 2 - \gamma_i = -1 + 2 - 1 = 0.$$

Similarly, in the case of $k - r + 2 \leq l$, it follows that $d_s(\mathcal{H}) = s + (k - r + 1)$. Thus we have that

$$\begin{aligned} t_i &= (k + (n + 1 - i) - d_s(\mathcal{H}) + 2) - \gamma_i \\ &= k + \mu_k + 1 - (\mu_k - \mu_{k-r+1} + l) - (\mu_{k-r+1} + 1 - l + k - r + 1) + 2 - r \\ &= 1. \end{aligned}$$

The proposition follows. \blacksquare

Example 3.1 *As an illustration, let us study the $[(q^k - 1)/(q - 1), k, q^{k-1}]$ simplex code for $q = 2$ and $k = 4$. Here $n = 15, k = 4$, and $(d_1, d_2, d_3, d_4) = (8, 12, 14, 15)$. This is a constant weight code, and then $\gamma_i = \min\{j | d_j \geq i\}$ for all i . The dual code has the following weight hierarchy:*

$$(d_1^\perp, \dots, d_{11}^\perp) = (3, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15).$$

We obtain the following table, where we only list the interesting values $i = k + 1 = 5, \dots, n = 15$. (Trivially $\gamma_i = 1$ for $i = 1, \dots, 4$ and strictly speaking, s_{n+1-i}^\perp is not defined for these values of i . See Remark 1.2.)

i	5	6	7	8	9	10	11	12	13	14	15
$s_{16-i}^\perp + 2$	2	2	2	2	2	2	2	3	3	3	4
$c_i = \gamma_i$	1	1	1	1	2	2	2	2	3	3	4
t_i	1	1	1	1	0	0	0	1	0	0	0

Remark 3.1 *We observe that even if our bound is not sharp in the example above, nor in any other simplex codes (Proposition 3.2), it is reasonably good; the t_i are 0 or 1, and 0 "quite often".*

But as one sees from Proposition 3.2, for all non-trivial cases of simplex codes there will be some i , with $k + 1 \leq i < n$ with $t_i = 1$, (see the case $i = 12$ in Example 3.1 above), so the generalization of Kung's bound in Theorem 1.2 will never be sharp for all j in the range $[k + 1, n]$, even for simplex codes.

On the other hand, we see that $t_{n+1-j} = 0$, so that our bound is sharp, for all $j = 1, q, q+1, q^2 + q - 1, q^2 + q, q^2 + q + 1, q^3 + q^2 + q - 2, q^3 + q^2 + q - 1, q^3 + q^2 + q, q^3 + q^2 + q + 1, \dots$, with $j \leq n - k$. The smallest integer j not of this form, for any prime power q , is 22. For MDS codes, it is trivially true that the t_i are 0 or 1 since all s_i^\perp in question are zero by definition, for $i = 1, \dots, n - k$, and the corresponding γ_{n+1-i} are 1 or 2.

Example 3.2 Quite "often" a linear code has a codeword of weight n , and then $c_i = 1$ for all i , and then there is of course no need to apply the bound in our Theorem 1.2 to determine the c_i . (See [1] where the authors discuss when a linear code might have a codeword of maximum weight.) So in such cases that bound is expected to be very unsharp, and our t_i fairly big. As a contrast to the examples above, where we looked at codes that are more "sparse" when it comes to non-zero elements, even for those codewords that have largest weight, we here give an example of a class of codes with codewords of weight n .

Let C be the Reed-Muller code of first order and rank r over \mathbb{F}_q . This is a $[q^{r-1}, r, q^{r-2}(q-1)]$ linear code. These codes are often given as examples alongside with simplex codes in articles and textbooks. But in the context we discuss here these classes are opposite extremes. The word $(1, \dots, 1)$ is a codeword of the Reed-Muller code, and therefore $c_i = 1$, for $1 \leq i \leq n = q^{r-1}$, for all r . The weight hierarchy of C is given by

$$d_i = \begin{cases} q^{r-1} - q^{r-i-1} & \text{if } 1 \leq i \leq r-1 \\ q^{r-1} & \text{if } i = r \end{cases}$$

By Wei duality, we can therefore find the weight hierarchy of the dual code. Namely,

$$\begin{aligned} (d_1^\perp, \dots, d_{q^{r-1}-r}^\perp) &= \{1, \dots, q^{r-1}\} \setminus \{q^{r-1} + 1 - d_i : 1 \leq i \leq r\} \\ &= \{2, \dots, q^{r-1}\} \setminus (\{q^{r-i-1} + 1 : 1 \leq i \leq r-1\}) \end{aligned}$$

From there, we get that

$$s_{n+1-j}^\perp = k + n + 1 - j - d_{n+1-j}^\perp = i - 1 \Leftrightarrow q^{r-1} - q^{r-i} + r - i + 2 \leq j \leq q^{r-1} - q^{r-i-1} + r - i.$$

We can then evaluate the sharpness of our bound and we get that

$$t_j = i \Leftrightarrow q^{r-1} - q^{r-i} + r - i + 2 \leq j \leq q^{r-1} - q^{r-i-1} + r - i.$$

In particular

$$t_{q^{r-1}} = r - 1.$$

An $[n, k]$ code C over \mathbb{F}_q is called an r -MDS code iff it attains the generalized Singleton bound $d_r = n - k + r$ from Lemma 1.1 for $i = r$. Note that if a code is r -MDS, then it also i -MDS for all $r < i$, and that a code is MDS if and only if it is 1-MDS. We denote the maximum Hamming weight of a single non-zero codeword in C by d_{\max} .

Proposition 3.3 Let C be an $[n, k]$ code over \mathbb{F}_q . If C^\perp is an $(n + 1 - i)$ -MDS code and $d_{\max} < i$, then C attains the bound for c_i in Theorem 1.2.

Proof Since C^\perp is an $(n + 1 - i)$ -MDS code, we have that the bound in Theorem 1.2 is:

$$c_i \leq (k + n + 1 - i - d_{n+1-i}^\perp) + 2 = 2.$$

Moreover C does not contain any codeword whose Hamming weight is greater than $i - 1$. Thus we find that $c_i \geq 2$ also, and so the proposition holds (with bound 2 in this case). \blacksquare

For the special case $d = n - k + 1$ and $i = n$, we obtain:

Corollary 3.1 *Let C be an MDS code over \mathbb{F}_q . If $d_{\max} < n$, then the bound in Theorem 1.2 is sharp for $i = n$ (with $c_n = \gamma_n = 2$).*

Example 3.3 *Another example of sharpness and the lack of it is provided a binary code given by the parity check matrix*

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Here $n = 9$, and $k = 6$, and the d_j^\perp are 3, 6, 9, so that $s_1^\perp = 4$, $s_2^\perp = 2$, and $s_3^\perp = 0$. Moreover we have $c_7 = c_8 = c_9 = 2$ since $d_{\max} = 6$ (and one easily finds two words whose support union is $\{1, 2, \dots, 9\}$). The upper bounds for the c_i given by Theorem 1.2 are $\{2, 4, 6\}$. So this is sharp for c_i only when $i = 7$ (in the "proper" range $[k + 1, n] = [7, 9]$). We observe that Proposition 3.3 gives sharpness for $i = 7$ since C^\perp is $n + 1 - i = 9 + 1 - 7 = 3$ -MDS, and $d_{\max} < 7$.

More generally, let H be a $m \times 3m$ parity check matrix with 3 consecutive 1's grouped together "on the diagonal" in an analogous pattern. It defines a $[3m, 2m]$ binary code C . It is easy to see that $d_{\max} = 2m$ and that we can cover the whole space with two codewords. Thus

$$c_{2m+1} = \dots = c_{3m} = 2.$$

We also have that the weight hierarchy of C^\perp is

$$(d_1^\perp, \dots, d_m^\perp) = (3, 6, \dots, 3m)$$

and that

$$(s_1^\perp, \dots, s_m^\perp) = (2m - 2, 2m - 4, \dots, 0).$$

Then the bound is sharp for $i = 2m + 1$ since

$$c_{2m+1} = 2 = s_{3m+1-(2m+1)}^\perp + 2,$$

while it is non-sharp for $i \geq 2m + 2$. The sharpness of the bound for $i = 2m + 1$ can be derived from Proposition 3.3 since $2m = d_{\max} < 2m + 1$ and C is $(3m + 1 - (2m + 1))$ -MDS.

There is an obvious further generalization of this example to the case of H with m rows with $2l + 1$ consecutive 1's grouped together "on the diagonal" in an analogous pattern, for any natural number l .

In Corollary 3.1 and Example 3.3 we show sharpness of the bound in Theorem 1.2 for the "extreme cases" $i = n$ or $i = k + 1$. Using the following corollary of Proposition 3.3 we finish with an example where we obtain sharpness for some intermediate values of i in many cases.

Corollary 3.2 *Let C be an $[n, k, d]$ code over \mathbb{F}_q . If $d_{\max} < k + d - 1$, then the bound in Theorem 1.2 is sharp for $i = k + d - 1$.*

Proof Set $s := n + 2 - k - d = n + 1 - i$. From the generalized Singleton bound, it follows that

$$d_s^\perp \leq k + (n + 2 - k - d) = n + 2 - d.$$

By Wei duality, this is in fact an equality, because of

$$(d_s^\perp, d_{s+1}^\perp, \dots, d_{n-k}^\perp) = (n + 2 - d, n + 3 - d, \dots, n).$$

Thus C^\perp is $n + 1 - i = s$ -MDS. Thus the result follows from Proposition 3.3 (and $c_i = \gamma_i = 2$). \blacksquare

Example 3.4 Let k and j be natural numbers, and let G be a $k \times n$ matrix over \mathbb{F}_q , where $n = j \frac{q^k - 1}{q - 1}$, and where we for each point of \mathbb{P}_n^{k-1} over \mathbb{F}_q use j of its representatives in \mathbb{F}_q^k as columns of G . Using G as generator matrix of a q -ary code C we get a simplex code for $j = 1$. For an arbitrary natural number j we get a constant weight code with weight $d(C) = d_1(C) = d_{\max}(C) = jq^{k-1}$. We assume $k \geq 2$ and conclude that $d_{\max}(C) < jq^{k-1} + k - 1 = k + d(C) - 1$. Hence Corollary 3.2 can be applied, and our bound for c_i in Theorem 1.2 is sharp for $i = jq^{k-1} + k - 1$. From the proof of that result we also know that that bound is 2. In the case $j = 4$, $k = q = 2$, we have $k + 1 = 3$, $n = 12$, while we obtain sharpness for the intermediate value $i = 9$ (in the table of Example 3.1 the value for the i in question is 11).

References

- [1] Ball, S., Blokhuis, A., *A bound for the maximum weight of a linear code*, SIAM J. Discrete Math. **27**(1), 575–583 (2013).
- [2] Britz, T., Shiromoto, K., *On the covering dimension of a linear code*, arXiv:1504.02357 (2015).
- [3] Crapo, H., Rota, G.-C. *On the Foundation of Combinatorial Theory: Combinatorial Geometries (Preliminary Edition)*, MIT Press, Cambridge (1970).
- [4] Johnsen, T., Roksvold, J.N., Verdure, H. *A generalization of weight polynomials to matroids*, arXiv:1311.6291 (2013).
- [5] Jurrius, R. *Weight enumeration of codes from finite spaces*, Des. Codes Cryptogr. **63**(3), 321–330 (2012).
- [6] Jurrius, R. *Codes, arrangements, matroids, and their polynomial links*, PhD thesis, Technische Universiteit Eindhoven (2012). Full text available at <http://alexandria.tue.nl/extra2/734704.pdf>
- [7] Jurrius, R., Pellikaan, R., *Codes, arrangements and matroids*, in: Algebraic geometry modeling in information theory, Ser. Coding Theory Cryptol., 8, World Sci. Publ., Hackensack, NJ, 219–325 (2013).
- [8] Kløve, T. *Support weight distribution of linear codes*, Discrete Math. **106/107**, 311–316 (1992).
- [9] Kung, J.P.S., *Critical problems*, in: Matroid Theory, Seattle, WA, 1995, Contemporary Mathematics, **197**, American Mathematical Society, Providence, RI, 1–127 (1996).
- [10] Wei, V.K., *Generalized Hamming weights for linear codes*, IEEE Trans. Inform. Theory **37**(5), 1412–1418 (1991).