Generalized Hamming Weights

Ziquan Yang

August 22, 2014

1 Notes on Generalized Hamming Weights

Definition 1.1. Let D be a subcode of a linear code C, then

$$\mathrm{supp}(D) := \bigcup_{x \in D} \mathrm{supp}(x)$$

Definition 1.2.

$$d_r(C) := \min\{|\mathrm{supp}(D)| \mid D \subseteq C, \mathrm{rank}(D) = r\}$$

Remark 1.3. d_1 is the classical minimum distance of a code.

Notation 1.4. H_i denotes of a column vector of index i and R_i denotes a row vector of index i.

Definition 1.5. $P_I(C)$ denotes the *punctured* code of C with indices from $I \subset [n]$. Let $\pi_I : \mathbb{F}_2^n \mapsto \mathbb{F}_2^{|I|}$ be the projection map onto the indices set I. $P_I(C) = \pi_I(C)$. $\pi^{-1} : \pi(C) \mapsto$ is defined by filling in zeros in other coordinates: $\pi^{-1} \circ \pi : (x_i) \mapsto (x_j)$ where $x_j = x_i$ for $i \in I$ and $x_j = 0$ otherwise. $P_I^e(C)$ denotes $P_I(C)$ as "embedded" in $\mathbb{F}_2^n$, i.e. $P_I^e(C) = \pi^{-1} \circ \pi(C)$.

Definition 1.6. $S_I^e(C) = \mathrm{span}\,(\{\mathbf{x} \in C \mid \mathrm{supp}(\mathbf{x}) \subset I\})$. $S_I(C) = P_I(S_I^e(C))$ denotes the *shortened* code of C.

Remark 1.7. We have the following relationship between punctured code and shortened code:

$$P_I(C)^\perp = S_I(C^\perp) \text{ and } P_I(C^\perp) = S_I(C)^\perp$$

Theorem 1.8. (Monotinicity)
For an $[n, k]$ code C with $k > 0$, we have

$$1 \leq d_1(C) < d_2(C) < \cdots < d_k(C) \leq n$$

Proof. $d_{r-1}(C) \leq d_r(C)$ follows directly from definition. It remains to show the strict inequality holds. Let $D \subseteq C$ be a subcode with $\mathrm{rank}(D) = r$ and $|\mathrm{supp}(D)| = d_r(C)$. Let $i \in \mathrm{supp}(D)$. Consider the subcode $D_i = \{x \in D \mid x_i = 0\}$, then $\mathrm{rank}(D_i) = r - 1$, since $D_i^\perp = \mathrm{span}\,(D^\perp \bigcup \{e_i\})$ and $e_i \notin D^\perp$ for $i \in \mathrm{supp}(D)$. Thus $d_{r-1}(C) \leq |\mathrm{supp}(D_i)| = d_r(C) - 1$. □

Note there is a simple but non-trivial corollary of Monotinicity:

Corollary 1.9. *Let $D \subseteq C$ be a subcode of dimension r. Let $I = \mathrm{supp}(D)$. If $|I| = d_r(C)$, then $D = S_I^e(C)$.*

Proof. The inclusion $D \subseteq S_I^e(C)$ is clear. Suppose $\exists \mathbf{x} \in C$, such that $\text{supp}(\mathbf{x}) \subset I$ and $\mathbf{x} \notin D$, then $D' = \text{span}\,(D \bigcup \{\mathbf{x}\})$ is a $r+1$ dimensional subspace with $d_{r+1}(C) \leq |\text{supp}(D')| = |\text{supp}(D)| = d_r(C)$, contradicting with the monotinicity given in Theorem 1.8. Thus $S_I^e(C) \subseteq D$. □

Lemma 1.10. *For all $r \leq k$,*

$$d_r(C) = \min\{|I| | \dim P_I(C^\perp) = |I| - r, I \subset [n]\}$$

Proof. Notice that we have

$$P_I(C^\perp)^\perp = S_I(C)$$

Let $d = \min\{|I| | \dim P_I(C^\perp) = |I| - r\}$. Consider $I \subset [n]$, such that $|I| = d$. We have $\dim S_I(C) = r$, thus $d_r(C) \leq |\text{supp}(S_I(C))| \leq |I| = d$.
Now let $D \subseteq C$ be a subcode with $\dim D = r$ and $|\text{supp}(D)| = d_r(C)$. Let $I = \text{supp}(D)$, then by the corollary of Theorem 1.8 we see that $D = S_I(C)$. Thus $\dim P_I(C^\perp) = |I| - \dim P_I(C^\perp)^\perp = |I| - \dim S_I(C) = |I| - r$ and we have $d \leq |I| = d_r(C)$. □

Notation 1.11. We denote $\min\{|I| | \dim P_I(C) = |I| - r, I \subset [n]\}$ as $h_r(C)$, so Lemma 1.10 establishes $d_r(C) = h_r(C^\perp)$. Note that it is equivalent to define $h_r(C) = \min\{|I| | \dim P_I(C) \leq |I| - r, I \subset [n]\}$ since suppose $h_r(C)$ is achieved by $I \subset [n]$, then we have $\dim P_I(C) = |I| - r$. Otherwise we can delete a column and the rank remains the same.

Remark 1.12. Once the equality is established, all the inequalities in the proof are actually equalities. Thus we can observe the following: If $d_r(C)$ is achieved by a subcode D, then $h_r(C^\perp)$ is achieved by its support $\text{supp}(D)$. Conversely, if $h_r(C^\perp)$ is achieved by $I \subset [n]$, then $d_r(C)$ is achieved by $S_I^e(C)$.

This lemma has an equivalent formulation in [2]:

Corollary 1.13. *Let C be an $[n, k]$ code with parity check matrix H. Then $d_r(C) = d$, if and only if*

- *Every set of $d-1$ columns of H have rank at least $d - r$*
- *There exists d columns of H with rank $d - r$*

Theorem 1.14. (Duality)

$$\{d_r(C) | 1 \leq r \leq k\} \bigcap \{n + 1 - d_r(C^\perp) \mid 1 \leq r \leq n - k\} = \varnothing$$

or equivalently

$$\{d_r(C) | 1 \leq r \leq k\} \bigcup \{n + 1 - d_r(C^\perp) \mid 1 \leq r \leq n - k\} = [n]$$

Proof. It suffices to prove that for any r, where $1 \leq r \leq k$, we have $d_r(C) \notin \{n+1-d_t(C^\perp) \mid 1 \leq t \leq n - k\}$.
First we show that $d_t(C) < n + 1 - d_r(C^\perp)$ for $t = k + r - d_r(C^\perp)$. Now let $d_r(C^\perp)$ □

2 Notes on Griesmer Bound

The following are notes about Griesmer bound I took from [3].

Theorem 2.1. *Let C be an $[n, k, d]$ code over $\mathbb{F}_q$ and let $\boldsymbol{c}$ be a codeword of weight $w < (q/q-1)d$. Then $Res(C, \boldsymbol{c})$ is an $[n - w, k - 1, d']$ code, where $d' \geq d - w + \lceil w/q \rceil$.*

Proof. Without loss of generality, we can assume $\mathbf{c} = (c_i)$, where $c_i = 1$ for $0 \leq i \leq w-1$ and $c_i = 0$ otherwise. Clearly we have $\dim Res(C, \mathbf{c}) \leq k-1$. Now suppose $\dim Res(C, \mathbf{c}) < k-1$, then $\exists \mathbf{x} \in C$, $\mathbf{x} \notin \operatorname{span}\{\mathbf{c}\}$ is zero when projected onto $[n] - \operatorname{supp}(\mathbf{c})$. By Pigeon-Hole Principle, there exists a $\alpha \in \mathbb{F}_q$ that is repeated at least $\lceil w/q \rceil$ times in $\{x_i \mid 0 \leq i \leq w-1\}$. Therefore we have

$$d \leq wt(\mathbf{x} - \alpha\mathbf{c}) \leq w - \frac{w}{q} = w\frac{q-1}{q}$$

contradicting with our assumption on w. Hence $\dim Res(C, \mathbf{c}) = k-1$. Now consider any non-zero codeword $(x_w, \cdots, x_{n-1}) \in Res(C, \mathbf{c})$ and $\mathbf{x} \in C$ be the original codeword. Then by the above argument we have

$$d \leq wt(\mathbf{x} - \alpha\mathbf{c}) \leq w - \frac{w}{q} + wt((x_w, \cdots, x_{n-1}))$$

Thus we have $d' \geq d - w + \lceil w/q \rceil$. □

Applying the above theorem to a codeword of minimum weight then we have the following corollary:

Corollary 2.2. *Let C be an $[n, k, d]$ code over $\mathbb{F}_q$ and $\mathbf{c} \in C$ has weight d, then $Res(C, \mathbf{c})$ is an $[n-d, k-1, d']$ code, where $d' \geq \lceil d/q \rceil$.*

Theorem 2.3. (Griesmer Bound)
Let C be an $[n, k, d]$ code over $\mathbb{F}_q$, then

$$n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil$$

Proof. We induct on k. The conclusion is clear for $k = 1$. Now given $k > 1$, and $\mathbf{c} \in C$ has the minimum weight d. Then we apply induction hypothesis to $Res(C, \mathbf{c})$ a $[n-d, k-1, d']$ code, where $d' \geq \lceil d/q \rceil$, we get

$$n - d \geq \sum_{i=0}^{k-2} \lceil \frac{d'}{q^i} \rceil = \sum_{i=0}^{k-2} \lceil \frac{d}{q^{i+1}} \rceil$$

thus we have

$$n \geq d + \sum_{i=0}^{k-2} \lceil \frac{d}{q^{i+1}} \rceil = \sum_{i=0}^{k-1} \lceil \frac{d}{q^{i+1}} \rceil$$

□

Of course we can apply the bound to binary codes and give a bound on Hamming weights [1]:

$$d_r(C) \geq \sum_{i=0}^{r-1} \lceil \frac{d_1}{2^i} \rceil$$

References

[1] V. K. Wei, "Generalized Hamming weights for linear codes," *IEEE Trans. Inform. Theory*, vol. 37, pp.1412-1418, Sept. 1991

[2] G. L. Feng, K. K. Tzeng and V.K. Wei, "On the Generalized Hamming Weights of Several Classes of Cyclic Codes," *IEEE Trans. Inform. Theory*, vol. 38, pp.1125-1130, Sept. 1992

[3] W. C. Huffman and V. Pless *Fundamentals of Error-Correcting Codes*. Cambridge University Press, UK 2003.