On the Newton and Covering Radii of Linear Codes*

Ernst Gabidulin† Torleiv Kløve‡

Abstract

The Newton radius of a code is the largest weight of a uniquely correctable error. The covering radius is the largest distance between a vector and the code. Two relations between the Newton radius and the covering radius are given.

Index terms: error correction, covering radius, Newton radius, MDS codes.

1 Introduction

In [3], the name *Newton radius* of a binary linear code was introduced for the largest weight of a uniquely correctable error. It was shown that for a code of dimension k, the Newton radius ν is at least $r-k$, where r is the covering radius of the code. In [2], the upper bound $n-k$ on $r+\nu$ for binary linear codes without zero-positions was given. The main goal of this paper is to generalize these relations to linear codes over arbitrary alphabets.

*The research was supported by the Russian Foundation for Basic Research and The Norwegian Research Council.

†Ernst Gabidulin is with the Moscow Institute of Physics and Technology, Institutskii per. 9, 141700 Dolgoprudnyi, Russia.

‡Torleiv Kløve is with the Department of Informatics, University of Bergen, HIB, N-5020 Bergen, Norway.

2 Notations

The notations and definitions below (for general q) are the direct generalization of the definitions given in [3] in the binary case.

Let $\mathcal{C}$ be a linear $[n, k; q]$ code, that is, a code of length n and dimension k over $GF(q)$. Consider a coset $\mathbf{z} + \mathcal{C}$. A *coset leader* is a vector in the coset of minimal (Hamming) weight. The *weight of the coset* is the weight of a coset leader.

A coset leader $\mathbf{x}$ is *unique* if it is the only coset leader in the coset. This means that $w(\mathbf{x}) < d(\mathbf{x}, \mathbf{c})$ for all non-zero code words $\mathbf{c}$, where w is the (Hamming) weight and d the (Hamming) distance.

An error $\mathbf{e}$ is (uniquely) correctable if and only if it is the unique coset leader in its coset.

The *Newton radius* $\nu(\mathcal{C})$ of $\mathcal{C}$ is the largest weight of a uniquely correctable error:

$$\nu(\mathcal{C}) = \max\Big\{ w(\mathbf{x}) \;\Big|\; w(\mathbf{x}) < d(\mathbf{x}, \mathbf{c}) \text{ for all } \mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\} \Big\},$$

where $\mathbf{0}$ is the all zero vector. The *covering radius* $r(\mathcal{C})$ is defined as the maximal distance of a vector from the code:

$$r(\mathcal{C}) = \max\Big\{ w(\mathbf{x}) \;\Big|\; w(\mathbf{x}) \le d(\mathbf{x}, \mathbf{c}) \text{ for all } \mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\} \Big\}.$$

In [3] it was shown that if $\mathcal{C}$ is a binary $[n, k]$ code, and we create an $[n+1, k]$ code by adding a position which is zero for all codewords, then both the covering radius and the Newton radius will increase by one. The same is true for non-binary codes, as can easily be seen. Therefore, we will from now on only consider codes without zero-positions, that is, for each position there exists at least one codeword which is non-zero in that position.

Lemma 1 *Let $\mathcal{C}$ be an $[n, k; q]$ code without zero-positions. Then*

$$r(\mathcal{C}) \le n - \frac{n}{q}. \tag{1}$$

and

$$\nu(\mathcal{C}) < n - \frac{n}{q}. \tag{2}$$

Proof: Since the code is linear without zero-positions, for any element $s \in GF(q)$ and any position, $q^{k-1}(q-1)$ of the q^k code words have the value s in that position. Hence, for any vector $\mathbf{x}$, the average distance between $\mathbf{x}$ and a codeword is $n(q-1)/q = n - n/q$. In particular, this implies (1). Moreover, if $\mathbf{x}$ is a coset leader of weight $n - n/q$, then all vectors in the corresponding coset are coset leaders. In particular, this implies (2). □

Later in this paper we will determine the structure of the codes for which we have equality in (1). We will also give an improved upper bound on $\nu(\mathcal{C})$.

We end this introduction with a general simple lemma without proof.

Lemma 2 *If $\mathcal{C}$ and $\widetilde{\mathcal{C}}$ are equivalent codes, then*

$$r(\mathcal{C}) = r(\widetilde{\mathcal{C}}), \quad \textit{and} \quad \nu(\mathcal{C}) = \nu(\widetilde{\mathcal{C}}).$$

3 Codes of dimension 1

In this section we determine exactly the Newton and covering radii for codes of dimension 1. The main reason is that this will be needed as a basis for an induction later.

Lemma 3 *Let $\mathcal{C}$ be an $[n, 1; q]$ code without zero-positions. Then*

$$\begin{aligned} r(\mathcal{C}) &= n - \left\lceil \frac{n}{q} \right\rceil, \\ \nu(\mathcal{C}) &= n - 1 - \left\lceil \frac{n-1}{q} \right\rceil = \begin{cases} r(\mathcal{C}) & \textit{if } n \equiv 1 \pmod{q}, \\ r(\mathcal{C}) - 1 & \textit{if } n \not\equiv 1 \pmod{q}. \end{cases} \end{aligned}$$

Proof: By Lemma 2, we may assume, without loss of generality, that $\mathcal{C}$ has generator matrix $(1, 1, \ldots, 1) = \mathbf{1}$, that is

$$\mathcal{C} = \{s \cdot \mathbf{1} \mid s \in GF(q)\}.$$

Consider a vector $\mathbf{x} \in GF(q)^n$. For each $s \in GF(q)$, let a_s be the number of occurrences of s as an element of $\mathbf{x}$. Then

$$d(\mathbf{x}, s \cdot \mathbf{1}) = n - a_s.$$

Hence, $\mathbf{x}$ is a coset leader if and only if

$$a_0 \geq a_s \text{ for all } s \neq 0.$$

In particular, this implies that

$$a_0 \geq \left\lceil \frac{n}{q} \right\rceil .$$

On the other hand, we can find $\mathbf{x} \in GF(q)^n$ such that

$$a_0 = \left\lceil \frac{n}{q} \right\rceil \geq a_s$$

for all $s \neq 0$. This proves the expression for $r(\mathcal{C})$. A similar argument shows that $\mathbf{x}$ is a unique coset leader if and only if

$$a_0 - 1 \geq a_s \text{ for all } s \neq 0$$

which is possible if and only if

$$a_0 - 1 \geq \left\lceil \frac{n-1}{q} \right\rceil$$

and the expression for $\nu(\mathcal{C})$ follows. □

4 An upper bound on the Newton radius

In [2] we showed that for a binary $[n, k]$ code $\mathcal{C}$ without zero-positions we have $r(\mathcal{C}) + \nu(\mathcal{C}) \leq n - k$. Here we give the following generalization to non-binary codes.

Theorem 1 *Let $\mathcal{C}$ be an $[n, k; q]$ code without zero-positions. Then*

$$r(\mathcal{C}) + (q-1)\nu(\mathcal{C}) \leq (q-1)n - k - (q-2). \tag{3}$$

To prove Theorem 1, we generalize the approach used in [2] for binary codes. The proof is by induction.

For $k = 1$, (3) is verified by straightforward calculation of the left side using the known values of $r(\mathcal{C})$ and $\nu(\mathcal{C})$ given in Lemma 3.

Induction step. Let $k > 1$, and suppose that the theorem is true for all codes of dimension $k - 1$. Let $\mathbf{x}$ be a coset leader of $\mathcal{C}$ of weight $r = r(\mathcal{C})$

and $\mathbf{y}$ be a unique coset leader of $\mathcal{C}$ of weight $\nu = \nu(\mathcal{C})$. Permuting positions if necessary, we may assume w.l.o.g. that $\mathbf{x}$ and $\mathbf{y}$ are of the following form:

$$\mathbf{x} = (\overbrace{* \ldots *}^{\rho} | \overbrace{* \ldots *}^{r-\rho} | \overbrace{0 \ldots 0}^{\nu-\rho} | \overbrace{0 \ldots \ldots 0}^{n-r-\nu+\rho}),$$

$$\mathbf{y} = (\overbrace{* \ldots *}^{\rho} | \overbrace{0 \ldots 0}^{r-\rho} | \overbrace{* \ldots *}^{\nu-\rho} | \overbrace{0 \ldots \ldots 0}^{n-r-\nu+\rho}),$$

for some $\rho \leq \nu$, where $*$ denotes non-zero elements.

Consider the $q^k \times n$ matrix $M_{\mathcal{C}}$ with the code words of $\mathcal{C}$ as rows. By Lemma 1, we have

$$r(\mathcal{C}) + (q-1)\nu(\mathcal{C}) < (q-1)n$$

and so

$$\rho < (q-1)(n - r - \nu + \rho) + (q-2)(r - \rho). \tag{4}$$

For each vector $\mathbf{u} \in GF(q)^{q^k}$, let $s_1(\mathbf{u})$ denote the number of times some non-zero multiple of $\mathbf{u}$ appears as a column among the first part (of ρ columns) of $M_{\mathcal{C}}$. Similarly, let $s_2(\mathbf{u})$, $s_3(\mathbf{u})$, and $s_4(\mathbf{u})$ for the second, third, and forth parts of $M_{\mathcal{C}}$ respectively. Summing $s_1(\mathbf{u})$, $s_2(\mathbf{u})$, $s_3(\mathbf{u})$, and $s_4(\mathbf{u})$ over all $\mathbf{u} \in GF(q)^{q^k}$ and comparing with (4), we can conclude that there exists a non-zero $\mathbf{u} \in GF(q)^{q^k}$ such that

$$s_1(\mathbf{u}) < (q-2)s_2(\mathbf{u}) + (q-1)s_4(\mathbf{u}). \tag{5}$$

From now on we consider only this $\mathbf{u}$ and write $s_1 = s_1(\mathbf{u})$, etc. For any vector $\mathbf{z} \in GF(q)^n$, let $\mathbf{z}'$ be the vector obtained by puncturing those $s_1+s_2+s_3+s_4$ positions of $\mathbf{z}$ where the corresponding positions $M_{\mathcal{C}}$ contain multiples of $\mathbf{u}$. Let $\mathcal{D}$ be the $[n, k-1; q]$ subcode of $\mathcal{C}$ of codewords which are 0 in these $s_1 + s_2 + s_3 + s_4$ positions, and let $\mathcal{D}'$ be the $[n - s_1 - s_2 - s_3 - s_4, k-1; q]$ code

$$\mathcal{D}' = \{\mathbf{c}' \mid \mathbf{c} \in \mathcal{D}\}.$$

We have

$$d(\mathbf{x}', \mathbf{c}') - w(\mathbf{x}') = d(\mathbf{x}, \mathbf{c}) - w(\mathbf{x})$$

for all $\mathbf{c} \in \mathcal{D}$. Hence $\mathbf{x}'$ is a coset leader for $\mathcal{D}'$ and so

$$r(\mathcal{D}') \geq w(\mathbf{x}') = r - s_1 - s_2.$$

Similarly, $\mathbf{y}'$ is a unique coset leader for $\mathcal{D}'$ and

$$\nu(\mathcal{D}') \geq w(\mathbf{y}') = \nu - s_1 - s_3.$$

By the induction hypothesis

$$\begin{aligned}
&(r - s_1 - s_2) + (q-1)(\nu - s_1 - s_3) \\
&\leq r(\mathcal{D}') + (q-1)\nu(\mathcal{D}') \\
&\leq (q-1)(n - s_1 - s_2 - s_3 - s_4) - (k-1) - (q-2),
\end{aligned}$$

and so, using (5), we have

$$\begin{aligned}
r + (q-1)\nu \leq\ & (q-1)n - k - (q-2) \\
& +s_1 - (q-2)s_2 - (q-1)s_4 + 1 \\
\leq\ & (q-1)n - k - (q-2).
\end{aligned}$$

□

5 A lower bound on the Newton radius

In [3] it was shown that for binary codes $\mathcal{C}$ we have

$$\nu(\mathcal{C}) \geq r(\mathcal{C}) - k.$$

This relation is true also for non-binary codes. However, the proof given in [3] for the binary case does not immediately generalize to $q > 2$. We give an alternative proof valid for all q.

Lemma 4 *Let $\mathcal{C}$ be an $[n, k; q]$ code. If i is the weight of a coset, then there exists a coset with unique coset leader and weight at least $i - k$.*

Proof: Let $\mathcal{K}$ be a coset with coset leader $\mathbf{x}$ of weight i. We will construct a coset with unique coset leader $\mathbf{y}$ of weight at least $i - k$.

If $\mathbf{x}$ is the only coset leader of $\mathcal{K}$ we let $\mathbf{y} = \mathbf{x}$ and are finished. Otherwise, let $\mathcal{L} = \mathbf{x} + \mathcal{S}$ be the set of coset leaders in $\mathcal{K}$, where $\mathcal{S} \subseteq \mathcal{C}$ and $|\mathcal{S}| \geq 2$. Let $\mathcal{D}$ be the space spanned by $\mathcal{S}$. Then $\mathcal{D}$ is a subcode of $\mathcal{C}$ of dimension s, say, where $s \leq k$. Let $I = \{i_1, i_2, \ldots, i_s\}$ be an information set for $\mathcal{D}$. For any vector $\mathbf{z} \in GF(q)^n$, let

$$\mathbf{z}_I = (z_{i_1}, z_{i_2}, \ldots, z_{i_s}) \in GF(q)^s.$$

The vectors

$$\{\mathbf{c}_I \mid \mathbf{c} \in \mathcal{D}\}$$

are all distinct, since I is an information set, and so are the vectors

$$\{\mathbf{x}_I + \mathbf{c}_I \mid \mathbf{c} \in \mathcal{D}\}.$$

In particular, the vectors

$$\{\mathbf{z}_I \mid \mathbf{z} \in \mathcal{L}\}$$

are distinct. Let $\mathbf{z}' \in \mathcal{L}$ be such that

$$w(\mathbf{z}'_I) = m = \max\{w(\mathbf{z}_I) \mid \mathbf{z} \in \mathcal{L}\}.$$

Since $|\mathcal{L}| \geq 2,\ m > 0$. Let $\mathbf{u}$ be defined by

$$u_i = \begin{cases} z'_i & \text{if } i \in I, \\ 0 & \text{otherwise.} \end{cases}$$

Then $w(\mathbf{u}) = m$. Let $\mathbf{y} = \mathbf{z}' - \mathbf{u}$. We will show that $\mathbf{y}$ is the unique coset leader in $\mathbf{y}+\mathcal{C}$. Let $\chi(\mathbf{v})$ denote the support of $\mathbf{v}$, that is,

$$\chi(\mathbf{v}) = \{i \mid v_i \neq 0\}.$$

First, we note that

$$w\left(\mathbf{y}\right) = w\left(\mathbf{z}'\right) - w\left(\mathbf{x}'\right) = i - m.$$

Next, we note that if $\mathbf{z} \in \mathcal{L}$, then, by the maximality of $w(\mathbf{z}'_I)$,

$$\text{either } \chi(\mathbf{u}) \not\subseteq \chi(\mathbf{z}_I) \text{ or } \chi(\mathbf{u}) = \chi(\mathbf{z}_I).$$

If $\mathbf{z} \in \mathcal{L}$ such that $\chi(\mathbf{u}'_I) \not\subseteq \chi(\mathbf{z}_I)$, then there exists an $i \in I$ such that $u_i \neq 0$ and $z_i = 0$ and so

$$w(\mathbf{z} - \mathbf{u}) > w(\mathbf{z}) - m = i - m.$$

If $\mathbf{z} \in \mathcal{L}$ and $\chi(\mathbf{u}) = \chi(\mathbf{z}_I)$ but $\mathbf{z} \neq \mathbf{z}'$, then there exists an $i \in I$ such that $u_i \neq 0$ and $u_i \neq z_i$ and so again

$$w(\mathbf{z} - \mathbf{u}) > w(\mathbf{z}) - m = i - m.$$

Finally, if $\mathbf{z} \in \mathcal{K} \setminus \mathcal{L}$, then

$$w(\mathbf{z}-\mathbf{u}) \geq w(\mathbf{z}) - w(\mathbf{u}) > i - m.$$

Hence $\mathbf{y}$ is the unique coset leader of $\mathbf{y} + \mathcal{C}$ and

$$w(\mathbf{y}) = i - m \geq i - s \geq i - k.$$

□

Theorem 2 *If $\mathcal{C}$ is an $[n, k; q]$ code, then*

$$\nu(\mathcal{C}) \geq r(\mathcal{C}) - k.$$

Proof: Consider a coset of weight $r(\mathcal{C})$ and apply Lemma 4. □

For vectors $\mathbf{x}, \mathbf{z} \in GF(q)^n$, we say that $\mathbf{z}$ *covers* $\mathbf{x}$ if and only if

$$w(\mathbf{z}-\mathbf{x}) = w(\mathbf{z}) - w(\mathbf{x})$$

or, equivalently, $x_i \in \{0, z_i\}$ for all i.

Considering the proof above, a natural question is the following: Given a code $\mathcal{C}$; if $\mathbf{y}$ is a unique coset leader of weight $\nu(\mathcal{C})$, is there a vector $\mathbf{x}$ which covers $\mathbf{y}$ and which is a coset leader of weight $r(\mathcal{C})$.

We show by an example that this is not always the case. Let $\mathcal{C}$ be the binary $[5, 2]$ code whose codewords are the rows of the following matrix

$$\mathcal{C} = \begin{bmatrix} 00000 \\ 11110 \\ 11001 \\ 00111 \end{bmatrix}$$

For this code $r(\mathcal{C}) = 2$ and $\nu(\mathcal{C}) = 1$. There are 5 vectors which are unique coset leaders, namely the vectors of weight 1. There are 4 coset leaders of weight 2, namely 10100, 10010, 01010, 01100 (they belong to 2 distinct cosets). None of these covers the unique coset leader 00001.

6 Comparing the bounds

From (3) we get

$$\nu(\mathcal{C}) \leq \frac{(q-1)n - k - (q-2) - r(\mathcal{C})}{q-1} \tag{6}$$

and this gives an improvement of the trivial upper bound $\nu(\mathcal{C}) \leq r(\mathcal{C})$ if and only if

$$r(\mathcal{C}) > n - \frac{n}{q} - \frac{k+q-2}{q}.$$

Hence, if $r(\mathcal{C}) \leq n - \frac{n}{q} - \frac{k+q-2}{q}$, then the difference between the upper bound $r(\mathcal{C})$ and the lower bound $r(\mathcal{C}) - k$ is k.

If $n - \frac{n}{q} - \frac{k+q-2}{q} \leq r(\mathcal{C}) \leq n - \frac{n}{q}$, then the difference between the upper bound (6) and the lower bound $r(\mathcal{C}) - k$ is

$$\frac{(q-1)n + (q-2)k - (q-2) - qr(\mathcal{C})}{q-1}.$$

This decreases from k to $(q-2)(k-1)/(q-1)$ when $r(\mathcal{C})$ increases from $n - \frac{n}{q} - \frac{k+q-2}{q}$ to $n - \frac{n}{q}$. In particular, if $q = 2$, these is no gap between the bounds when $r(\mathcal{C}) = \frac{n}{2}$.

References

[1] G. Cohen, I. Honkala, S. Litsyn, A. Lobstein, *Covering Codes.* Amsterdam: Elsevier, 1997.

[2] E. M. Gabidulin and T. Kløve, "On the Newton radius", *Reports in informatics*, no. 130, Department of Informatics, University of Bergen, February 1997.

[3] T. Helleseth and T. Kløve, "The Newton radius of codes", *IEEE Trans. on Inform. Th.*, vol. 43, pp. 1820-1831, 1997.

[4] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes.* New York: North Holland, 1977.