A Note on the Newton Radius

Alex Samorodnitsky
Hebrew University
salex@cs.huji.ac.il

Sergey Yekhanin
Microsoft Research
yekhanin@microsoft.com

Abstract

The Newton radius of a code is the largest weight of a uniquely correctable error. We establish a lower bound for the Newton radius in terms of the rate. In particular we show that in any family of linear codes of rate below one half, the Newton radius increases linearly with the codeword length.

1 Introduction

Let $\mathcal{C}$ be a linear $[n,k]_q$ code, that is, a code of length n and dimension k over the finite field $\mathbb{F}_q$. Consider an arbitrary coset $\mathbf{v}+\mathcal{C}$. A *coset leader* is a vector of the minimal Hamming weight in the coset. An error $\mathbf{z}$ is uniquely correctable by the maximum likelihood decoder for the code $\mathcal{C}$ if and only if $\mathbf{z}$ is the unique coset leader in the coset containing $\mathbf{z}$. That is equivalent to saying that for all $\mathbf{c} \in \mathcal{C} \setminus \{0^n\}$ we have $\mathrm{wt}(\mathbf{z}) < d(\mathbf{z},\mathbf{c})$. The Newton radius $\nu(\mathcal{C})$ is defined as the largest weight of a uniquely correctable error

$$\nu(\mathcal{C}) = \max\{\mathrm{wt}(\mathbf{z}) \mid \mathrm{wt}(\mathbf{z}) < d(\mathbf{z},\mathbf{c}) \text{ for all } \mathbf{c} \in \mathcal{C} \setminus \{0^n\}\}.$$

The definition of the Newton radius strongly resembles that of the covering radius, i.e., the maximal distance of a vector from the code

$$\mathrm{rad}(\mathcal{C}) = \max\{\mathrm{wt}(\mathbf{z}) \mid \mathrm{wt}(\mathbf{z}) \leq d(\mathbf{z},\mathbf{c}) \text{ for all } \mathbf{c} \in \mathcal{C} \setminus \{0^n\}\}.$$

Newton radius has been introduced in [2] and further studied in [1, 3]. In particular in [1] it was shown that for any $[n,k]_q$ code $\mathcal{C}$

$$\nu(\mathcal{C}) \geq \mathrm{rad}(\mathcal{C}) - k. \tag{1}$$

In this note we present a lower bound (Corollary 2 and Theorem 3) for the Newton radius in terms of solely the rate of the code. Our bound is sometimes stronger than the bound above. In particular it allows us to conclude that in any family of linear codes of rate below one half, the Newton radius increases linearly with the codeword length.

Our bound can also be sometimes weaker than (1) since we use less information about the code. In particular we do not get any lower bounds for codes of rate above one half.

2 The result

In what follows we denote the set of all vectors of Hamming weight at most w in the space $\mathbb{F}_q^n$ by B_w. For sets $A, B \subseteq \mathbb{F}_q^n$ the sumset $A+B$ is defined by $\{a+b \mid a \in A, b \in B\}$.

Proposition 1 *Let $k \leq \frac{n}{2}$ be positive integers and q be a prime power. Let $\mathcal{C}$ be an $[n,k]_q$ linear code. There exists a $[n-k,k]_q$ linear code $\mathcal{D}$ such that*

$$\nu(\mathcal{C}) \geq \mathrm{rad}(\mathcal{D}).$$

Proof: Let $H \in \mathbb{F}_q^{(n-k)\times n}$ be a parity check matrix for $\mathcal{C} = \{\mathbf{x} \mid H\mathbf{x}^t = 0\}$. Without loss of generality after a permutation of coordinates we have $H = [I \mid M]$, for some matrix $M \in \mathbb{F}_q^{(n-k)\times k}$. Let $\mathcal{D} \subseteq \mathbb{F}_q^{n-k}$ be an arbitrary linear space of dimension k that contains the space spanned by the columns of the matrix M. Let $w = \mathrm{rad}(\mathcal{D})$ and let $\mathbf{x} \subseteq \mathbb{F}_q^{n-k}$ be a point that is w-far from the code $\mathcal{D}$. Let $\mathbf{v} = \mathbf{x} \circ 0^k$ be the n-dimensional vector obtained by padding $\mathbf{x}$ by k zeros. Observe that $H\mathbf{v}^t = \mathbf{x}^t$. We now argue that $\mathbf{v}$ is the unique vector of weight at most w in the coset

$$\mathcal{C}' = \{\mathbf{y} \in \mathbb{F}_q^n \mid H\mathbf{y}^t = \mathbf{x}^t\}.$$

Fix an arbitrary $\mathbf{y} \in \mathcal{C}'$, where $\mathrm{wt}(\mathbf{y}) \leq w$. Let $\mathbf{y} = \mathbf{y_1} \circ \mathbf{y}_2$, where $\mathbf{y}_1$ has dimension $n-k$ and $\mathbf{y}_2$ has dimension k. If $\mathbf{y_2} \neq 0^k$; then $\mathrm{wt}(\mathbf{y}_1) \leq w-1$ and we get

$$\mathbf{x}^t = H\mathbf{y}^t = \mathbf{y}_1^t + M\mathbf{y}_2^t \in B_{w-1} + \mathcal{D}$$

contradicting the fact that $\mathbf{x}$ is w-far from the space $\mathcal{D}$. Thus we have $\mathbf{y}_2 = 0^k$ and $\mathbf{x}^t = H\mathbf{y}^t = \mathbf{y}_1^t$, which implies $\mathbf{y} = \mathbf{v}$. ■

Proposition 1 allows one to translate lower bounds for the covering radius of $[n-k,k]_q$ codes to lower bounds for the Newton radius of $[n,k]_q$ codes. The following corollary combines Proposition 1 with the most basic lower bound for the covering radius. Let $B_q(n,t) = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathrm{wt}(\mathbf{x}) \leq t\}$ denote the Hamming ball of radius t. Clearly, $|B_q(n,t)| = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$.

Corollary 2 *Let $k \leq \frac{n}{2}$ be positive integers and q be a prime power. Let t be the smallest integer such that $|B_q(n-k,t)| \geq q^{n-2k}$. For all $[n,k]_q$ codes $\mathcal{C}$ we have $\nu(\mathcal{C}) \geq t$.*

Proof: For any $[n-k,k]_q$ code $\mathcal{D}$, the value of the product $q^k \cdot |B_q(n-k,\mathrm{rad}(\mathcal{D}))|$ has to be at least q^{n-k}. Thus $\mathrm{rad}(\mathcal{D}) \geq t$ holds. An application of Proposition 1 completes the proof. ■

We now obtain the asymptotic form of Corollary 2. It is well known that for prime power q, positive $\lambda \leq \frac{q-1}{q}$, and growing n we have $|B_q(n, \lfloor \lambda n \rfloor)| = q^{H_q(\lambda)n + o(n)}$, where where $H_q(\cdot)$ denotes the of the q-ary entropy function. See e.g., [4, Lemma 5.1.6]. Combining this asymptotic formula with Corollary 2 we get

Theorem 3 *Let $0 < r \leq \frac{1}{2}$ be a fixed rational number and q be a prime power. Let $\mathcal{C}$ be an $[n, rn]_q$ linear code. We have*

$$\nu(\mathcal{C}) \geq H_q^{-1}\left(\frac{1-2r}{1-r}\right)(1-r)n + o(n).$$

Remark 4 Corollary 2 and Theorem 3 give nontrivial lower bounds for the Newton radius of a rate r code $\mathcal{C}$ as long as $r < 1/2$. Observe that for larger values of the rate no such bounds exist. Indeed, for any $k \geq n/2$ the $[n,k]_q$ code

$$\mathcal{C} = \{\mathbf{x} \circ \mathbf{x} \circ \mathbf{y} \mid \mathbf{x} \in \mathbb{F}_q^{n-k}, \mathbf{y} \in \mathbb{F}_q^{2k-n}\}$$

satisfies $\nu(\mathcal{C}) = 0$. To see this consider an arbitrary vector $\mathbf{z} \in \mathbb{F}_q^n$. Let $\mathbf{z} = \mathbf{z}_1 \circ \mathbf{z}_2 \circ \mathbf{z}_3$, where $\mathbf{z}_1$ and $\mathbf{z}_2$ have dimension $n-k$, and $\mathbf{z}_3$ has dimension $2k-n$. Observe that the distance between $\mathbf{z}$ and the code $\mathcal{C}$ is given by $\mathrm{wt}(\mathbf{z}_1 + \mathbf{z}_2)$. Therefore assuming $\mathbf{z}_1 \neq \mathbf{z}_2$ we have two distinct elements $\mathbf{z}_1 \circ \mathbf{z}_1 \circ \mathbf{z}_3$ and $\mathbf{z}_2 \circ \mathbf{z}_2 \circ \mathbf{z}_3$ of $\mathcal{C}$ that are closest to the vector $\mathbf{z}$. Thus the code $\mathcal{C}$ cannot uniquely correct any pattern of one or more errors.

References

[1] Ernst Gabidulin and Torleiv Klove. On the Newton and covering radii of linear codes. *IEEE Transactions on Information Theory*, 45:2534–2536, 1999.

[2] Tor Helleseth and Torleiv Klove. The Newton radius of codes. *IEEE Transactions on Information Theory*, 43:1820–1831, 1997.

[3] Torleiv Klove. Relations between the covering and the Newton radii of binary codes. *Discrete Mathematics*, 238:81–88, 2001.

[4] J.H. van Lint. *Introduction to Coding Theory*. Springer-Verlag, Berlin, Heidelberg, 1982.