On the distribution of linear codes

Toshiyuki Katsura* and Motoko Qiu Kawakita†

(Received December 2, 2004)

Abstract In this paper, we examine the distribution of binary linear codes in the sense of Manin. For this purpose, we introduce the notions of isolated ratius and complete isolatedness. As a typical example, we calculate the isolated radius of the $[7,4,3]$-Hamming code, and show that it is completely isolated. Using the program in the appendix, we also give a list of isolated radii of some binary linear codes.

1 Introduction

Let $\mathbf{F}_q$ be a finite field with q elements ($q = p^m$, p : a prime number, m : a positive integer). A linear code $C \subset \mathbf{F}_q^n$ is called an $[n,k,d]$-linear code if $\dim_{\mathbf{F}_q} C = k$ and the minimum distance of C is equal to d. For an $[n,k,d]$-linear code C, the relative distance d/n and the information rate k/n are important numerical values which reflect properties of the code C. In this paper, we introduce a new invariant, using these two values, which shows how different the linear code is from other linear codes.
We denote by LC_q the set of all linear codes over the finite field $\mathbf{F}_q$. We consider the mapping:

$$\begin{array}{rccc} \varphi : & LC_q & \longrightarrow & [0,1]^2 \\ & [n,k,d]\text{-code } C & \longmapsto & (d/n, k/n). \end{array}$$

The set U_q of the limit points of Im φ was investigated by Yu. I. Manin, and for the shape of U_q he showed the following:

Theorem 1.1 (Manin [3]) *There exists a continuous function*

$$\alpha_q : [0,1] \longrightarrow [0,1]$$

such that

$$U_q = \{(\delta, R) \mid 0 \leq R \leq \alpha_q(\delta)\}$$

and that

$$\alpha_q(0) = 1, \ \alpha_q(\delta) \leq \max\{1 - (q/(q-1))\delta, 0\}.$$

As is well-known, the function $\alpha_q(\delta)$ is strictly decreasing for $\delta \in [0, (q-1)/q]$ (cf. Tsfasman and Vlădut [4]), and is estimated from below by the Varshamov-Gilbert bound.
The objects of our interest here are linear codes C such that $\varphi(C) \notin U_q$. For such a code C, the point $\varphi(C)$ is an isolated point in $\varphi(LC_q)$ and the following two questions arise.

Question 1 Is there any linear code C' such that $\varphi(C') = \varphi(C)$ which is different from C?

Question 2 What are the linear codes C' such that the points $\varphi(C')$ are closest to $\varphi(C)$? What is the distance between $\varphi(C')$ and $\varphi(C)$?

The codes C' in Question 2 are called the closest codes to C, and the distance between $\varphi(C')$ and $\varphi(C)$ is called the isolated radius of C (for the precise definitions, see Section 3) . We will give answers to

*Partially supported by Grand-in-Aid for Scientific Research (A), JSPS and the 21st Century COE Program at Graduate School of Mathematical Sciences, the University of Tokyo.
†Partially supported by Grand-in-Aid for JSPS Fellows.

these two questions for some typical binary linear codes (cf. List in Section 4). In particular, we will show that for the $[7,4,3]$-binary Hamming code C there exists no linear code C' such that $\varphi(C') = \varphi(C)$ and $C' \neq C$. We also show that the $[5,3,2]$-linear code is the closest code to C, and so the isolated radius of the $[7,4,3]$-Hamming code is equal to $\sqrt{2}/5 \cdot 7$.

2 Some bounds

In this section, we recall some bounds for linear codes, and give a new bound which we will use later. To begin with, we give the precise definition of U_q:

$$U_q = \left\{ (\delta, R) \in [0,1] \times [0,1] \;\middle|\; \begin{array}{l} \exists \text{ linear code } C_i \text{ of type } [n_i, k_i, d_i] \\ \text{such that} \\ n_i \longrightarrow \infty \quad \text{as} \quad i \to \infty \\ \text{and} \\ (d_i/n_i, k_i/n_i) \longrightarrow (\delta, R) \quad \text{as} \quad i \to \infty \end{array} \right\}$$

We are mainly interested in points which are not contained in U_q. Denoting by $d(C)$ (resp. $k(C)$) the the minimum distance of the code C (resp. $\dim_{\mathbf{F}_q} C$), we regard, in this paper, two linear codes $C, C' \subset \mathbf{F}_q^n$ as the same codes if $d(C) = d(C')$ and $k(C) = k(C')$. We need the following well-known lemma (cf. Manin [3], Tsfasman and Vlădut [4]).

Lemma 2.1 (Spoiling lemma) *If there exists an $[n,k,d]$-linear code, then an $[n-1,k-1,d]$-linear code and an $[n-1,k,d-1]$-linear code also exist.*

From here on, we assume $q = 2$, unless otherwise mentioned.

Lemma 2.2 (Plotkin bound for $q = 2$) *If there exists an $[n,k,d]$-linear code, then $d/n \leq 2^{k-1}/(2^k - 1)$ holds.*

Using these two lemmas, we have the following bound.

Theorem 2.3 (Linear bound) *Assume that there exists an $[n,k,d]$-linear code with $k \geq 4$. Then, the following bound holds:*

$$k/n + (15/8)(d/n) \leq 1 + 4/n.$$

Proof Using the spoiling lemma $k-4$ times, we have an $[n-k+4, 4, d]$-linear code. Therefore, using the Plotkin bound, we have

$$d/(n-k+4) \leq 2^3/(2^4 - 1),$$

which gives our inequality. ∎

Remark 2.4 *We fix a positive integer α. Then, we can generalize Theorem 2.3 as follows: Assume that there exists an $[n,k,d]$-linear code with $k \geq \alpha$. Then, the following bound holds:*

$$k/n + (2 - 1/2^{\alpha-1})(d/n) \leq 1 + \alpha/n.$$

For our purpose, the case $\alpha = 4$ is most efficient. Note that this inequality contains only linear terms for k, d and n like the Singleton bound.

We will also use the following two famous bounds (cf. Tsfasman and Vlădut [4], for instance).

Theorem 2.5 *If there exists an $[n,k,d]$-linear code, then the following bounds hold:*

$$n \geq \sum_{i=0}^{k-1} \lceil d/2^i \rceil \quad (\textit{Griesmer bound}),$$
$$2^n \geq \sum_{i=0}^{[d/2]} \binom{n}{i} \quad (\textit{Hamming bound}).$$

Here, for a real number r, $\lceil r \rceil$ means the least integer which is greater than or equal to r, and $[r]$ means the greatest integer which is less than or equal to r.

3 Isolated codes

In this section, we introduce the notion of complete isolatedness for linear codes and give some examples of completely isolated linear codes.

Definition 3.1 *For $r \in \mathbf{R}$ and $(a,b) \in [0,1]^2$, we set*

$$B_r((a,b)) = \{[n,k,d]\text{-}linear\ code \mid (d/n-a)^2 + (k/n-b)^2 < r^2\}.$$

Definition 3.2 *Let C be an $[n,k,d]$-linear code. If there exists a positive real number r such that $\varphi(C') = \varphi(C)$ for $C' \in B_r((d/n,k/n))$, then C is said to be isolated. An isolated linear code is said to be completely isolated if there exists no linear code C' $(C' \neq C)$ such that $\varphi(C') = \varphi(C)$.*

Example 3.3 *Let C be a linear code such that $\varphi(C) \in U_q$. Then, by the definition of U_q, C is not isolated.*

Example 3.4 *Let $\tilde{C}$ be the $[8,4,4]$-extended binary Hamming code. Then, $\varphi(\tilde{C})$ is not contained in U_2. Therefore, C is isolated. We set*

$$C' = \mathbf{F}_2(1,0) \subset \mathbf{F}_2^2.$$

Then, it is clear that C' is a $[2,1,1]$-linear code. Since we have

$$\varphi(\tilde{C}) = \varphi(C') = (1/2,1/2),$$

the $[8,4,4]$-extended binary Hamming code is not completely isolated.

Using the Plotkin bound, we have a criterion of complete isolatedness.

Lemma 3.5 *Let C be an isolated $[n,k,d]$-binary linear code. Assume that n is prime to either k or d. Moreover, we assume $3d > 2n - 2k + 2$. Then, C is completely isolated.*

Proof Suppose there exists an $[n',k',d']$-linear code C' such that $\varphi(C') = \varphi(C)$. Since n is prime to either k or d, there exists a positive integer ℓ such that

$$n' = \ell n,\ k' = \ell k,\ d' = \ell d.$$

Using the spoiling lemma $(k-1)\ell$ times, we have a $[(n-k+1)\ell, \ell, d\ell]$-linear code. Applying the Plotkin bound to this code, we have an inequality

$$d\ell/(n-k+1)\ell \leq 2^{\ell-1}/(2^\ell - 1).$$

Suppose $\ell \geq 2$. Then, we have

$$d/(n-k+1) \leq 2/(4-(1/2^{\ell-2})) \leq 2/3,$$

which contradicts the inequality $3d > 2n - 2k + 2$. Therefore, we have $\ell = 1$. Hence, the type of the code C' coincides with the one of C. ∎

Corollary 3.6 *The $[7,4,3]$-Hamming code and the $[7,3,4]$-binary linear code are completely isolated.*

Proof Let C be the $[7,4,3]$-binary linear code. By Manin's theorem, it is clear that the point $\varphi(C) = (3/7,4/7)$ is not contained in the set U_2. Therefore, the code C is isolated. Hence, using Lemma 3.5, we see that the $[7,4,3]$-Hamming code C is completely isolated. We can prove the latter part in the same way. ∎

Lemma 3.7 *Let C be an isolated $[n,k,d]$-binary linear code. Assume $15d > 8(n-k+1)$. Then, there exist no $[n\ell, k\ell, d\ell]$-binary linear codes with positive integer $\ell \geq 4$.*

Proof The proof is similar to the one in Lemma 3.5. Let ℓ be an integer ≥ 4. Suppose there exists an $[n\ell, k\ell, d\ell]$-binary linear code. Then, using the spoiling lemma $(k-1)\ell$ times, we have a $[(n-k+1)\ell, \ell, d\ell]$-linear code. Applying the Plotkin bound to this code, we have an inequality

$$d\ell/(n-k+1)\ell \leq 2^{\ell-1}/(2^{\ell}-1).$$

Since $\ell \geq 4$, we have

$$d/(n-k+1) \leq 8/15,$$

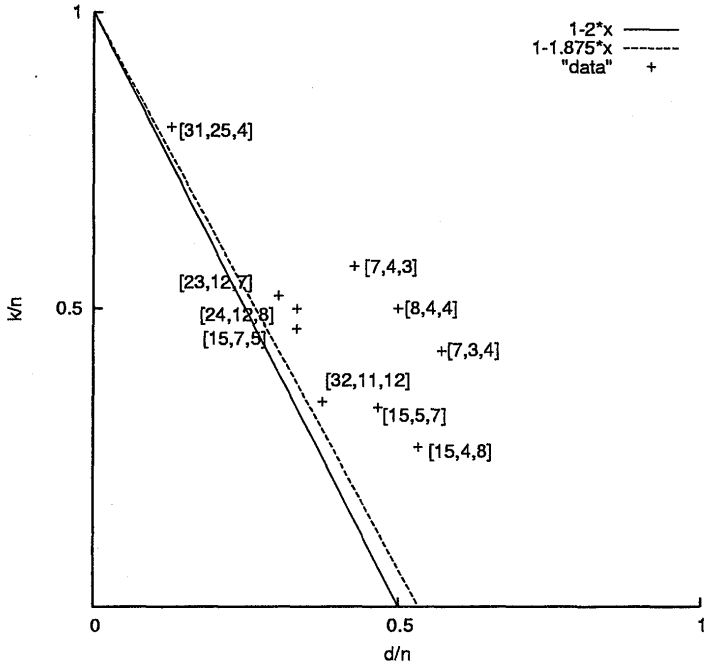
which contradicts the inequality $15d > 8(n-k+1)$. ■

Theorem 3.8 *The binary linear codes of types $[23,12,7]$, $[15,5,7]$, $[15,7,5]$, $[32,11,12]$, $[31,25,4]$ and $[15,4,8]$ are all completely isolated.*

Proof Suppose there exists an $[n',k',d']$-linear code C' such that $d'/n' = 7/23$ and $k'/n' = 12/23$. Then, as in Lemma 3.5, there exists a positive integer ℓ such that $n' = 23\ell$, $k' = 12\ell$, $d' = 7\ell$. Suppose $2 \leq \ell \leq 4$. Then, by A. E. Brouwer [1] we have no binary linear code of type $[23\ell, 12\ell, 7\ell]$. Hence, by Lemma 3.7, the $[23,12,7]$-binary linear code is completely isolated. We can prove the rest in the same way. ■

Remark 3.9 *Neither the $[8,4,4]$-extended Hamming code nor the $[24,12,8]$-Golay code is not completely isolated. This result follows from the fact that there exist the $[2,1,1]$ and the $[6,3,2]$ linear codes (cf. Example 3.4 and A. E. Brouwer [1]).*

Finally, we give a figure of the position in $[0,1]^2$ of the linear codes which we treated in this section.



4 Isolated radius

The following definition holds in any characteristic.

Definition 4.1 *Let C be an $[n,k,d]$-linear code. If there exists the greatest positive real number r such that $\varphi(C') = \varphi(C)$ for $C' \in B_r((d/n, k/n))$, then r is called the isolated radius of C. The linear codes C' such that the points $\varphi(C')$ are closest to $\varphi(C) = (d/n, k/n)$ with $\varphi(C') \neq \varphi(C)$ are called the closest codes to C.*

Now, we again assume $q = 2$. We look for the closest linear codes to the $[7,4,3]$-Hamming code C and calculate the isolated radius of C. For this purpose, we consider the extended linear code $\tilde{C}$ of C. As is well-known (or by an easy calculation), $\tilde{C}$ is an $[8,4,4]$-linear code. Since $\varphi(\tilde{C}) = (1/2, 1/2)$, the distance between $\varphi(C)$ and $\varphi(\tilde{C})$ is equal to $1/\sqrt{98}$. We examine the codes which are contained in $B_{1/\sqrt{98}}((3/7, 4/7))$.
Suppose that an $[n,k,d]$-code C' is contained in $B_{1/\sqrt{98}}((3/7,4/7))$. Then, we have

$$(\delta/n - 3/7)^2 + (k/n - 4/7)^2 < 1/98.$$

If $k \leq 3$, then we have $4/7 - 1/\sqrt{98} \leq k/n \leq 3/n$. Therefore, we have $n \leq 7$. Now, we assume $k \geq 4$. Then, by Proposition 2.3 we have an inequality $k/n + (15/8)(d/n) \leq 1 + 4/n$. We consider the line L and the circle Z defined as follows:

$$\begin{aligned} L: &\quad R + (15/8)\delta = 1 + 4/n, \\ Z: &\quad (\delta - 3/7)^2 + (R - 4/7)^2 = 1/98. \end{aligned}$$

The point $\varphi(C') = (d/n, k/n)$ exists in the circle Z and below the line L. Therefore, for the existence of such a point, it is necessary that part of the circle exists below the line L. Considering the condition that L and Z intersect each other, we conclude $n \leq 24$, which holds also in the case of $k \leq 3$. Thus, we have only finitely many candidates of linear codes in $B_{1/\sqrt{98}}((3/7,4/7))$.
Using the program in the appendix, we can choose the cases which satisfy both the Griesmer bound and the Hamming bound by computer search. Then, we have the following possibilities of the types of linear codes in $B_{1/\sqrt{98}}((3/7,4/7))$:

$$[5,3,2],[7,4,3],[8,4,3],[8,5,3],[9,5,3],[9,5,4],[10,5,4],[10,6,4],[11,6,4],$$

$$[11,7,4],[12,7,4],[16,8,6],[17,9,6],[18,10,6],[22,11,8],[23,12,8],[24,13,8].$$

By the list of linear codes in A. E. Brouwer [1], we have the following.

Lemma 4.2 *$B_{1/\sqrt{98}}((3/7,4/7))$ consists of the linear codes of the following types:*

$$[5,3,2],[7,4,3],[8,4,3],[9,5,3],[10,5,4],[11,6,4],[12,7,4].$$

Hence, we have the following.

Theorem 4.3 *The closest linear code to the $[7,4,3]$-Hamming code is the $[5,3,2]$-linear code. The isolated radius of the $[7,4,3]$-Hamming code is equal to $\sqrt{2}/5 \cdot 7 = 0.0404061\ldots$.*

Using the same method as in Theorem 4.3 and the results in Section 3, we have the following list.

Table. Closest codes, isolated radii and complete isolatedness

code	closest code	isolated radius	
Hamming code $[7,4,3]$	$[5,3,2]$	$\frac{\sqrt{2}}{5\cdot 7} = 0.0404061\ldots$	+
Extended Hamming code $[8,4,4]$	$[9,4,4]$	$\frac{\sqrt{2}}{2\cdot 3^2} = 0.0785674\ldots$	−
Dual of Hamming code $[7,3,4]$	$[5,2,3]$	$\frac{\sqrt{2}}{5\cdot 7} = 0.0404061\ldots$	+
Golay code $[23,12,7]$	$[17,9,5]$	$\frac{5}{17\cdot 23} = 0.0127877\ldots$	+
Extended Golay code $[24,12,8]$	$[22,11,7]$	$\frac{1}{2\cdot 3\cdot 11} = 0.0151515\ldots$	−
BCH code $[15,5,7]$	$[9,3,4]$,$[18,6,8]$	$\frac{1}{3^2\cdot 5} = 0.0222222\ldots$	+
BCH code $[15,7,5]$	$[24,11,8]$	$\frac{1}{2^3\cdot 3\cdot 5} = 0.0083333\ldots$	+
Extended BCH code $[32,11,12]$	$[27,9,10]$	$\frac{\sqrt{97}}{2^6\cdot 3^3} = 0.0113991\ldots$	+
Cyclic code $[31,25,4]$	$[16,13,2]$,$[32,26,4]$	$\frac{\sqrt{13}}{2^4\cdot 31} = 0.0072692\ldots$	+
Simplex code $[15,4,8]$	$[11,3,6]$	$\frac{\sqrt{5}}{3\cdot 5\cdot 11} = 0.0135519\ldots$	+

Here, + means that the code is completely isolated, and − means that the code is not completely isolated. The isolated radius of Golay code was also computed by a joint-work of the first author and J. Katsuta.

5 Appendix

We show here the program which we used to list the possibilities of the types of binary linear codes near our codes. The following program is for the $[7,4,3]$-Hamming code. We used the algebraic system KASH/KANT in [2].

Program.

```
#-------------------------------------------------------------------#
# Input:  [n0,k0,d0],t
# Output: [n,k,d]
# 1.(d/n,k/n) is in the ball with centre (d0/n0,k0/n0) and radius t;
# 2.[n,k,d] satisfies linear, Singleton, Griesmer and Hamming bound.
#-------------------------------------------------------------------#
n0:=7;
k0:=4;
d0:=3;
r0:=k0/n0;
delta0:=d0/n0;
t:=Sqrt((r0-4/8)^2+(delta0-4/8)^2);
kb:=Floor(32/(8*r0+15*delta0-8-17*t)); # linear bound for n
for n in [1..kb] do
  kmin:=Maximum(1,Ceil((r0-t)*n));
  kmax:=Minimum(n,Floor((r0+t)*n));
  for k in [kmin..kmax] do
    r:=k/n;
    dmin:=Maximum(1,Ceil((delta0-t)*n));
    dmax:=Minimum(n-k+1,Floor((delta0+t)*n));
    for d in [dmin..dmax] do
      delta:=d/n;
      # linear bound for (d/n,k/n) and region of ball #
      if r+15/8*delta<=1+4/n and (delta-delta0)^2+(r-r0)^2<t^2 then
        # Griesmer bound #
        g:=0;
```

```
        for i in [0..(k-1)] do
          g:=g+Ceil(d/2^i);
        od;
        if n>=g then
          # Hamming bound #
          h:=0;
          for j in [0..Floor(d/2)] do
            h:=h+Factorial(n)/(Factorial(n-j)*Factorial(j));
          od;
          if 2^n>=h then
            Print([n,k,d]);
          fi;
        fi;
      fi;
    od;
  od;
od;
```

References

[1] A. E. Brouwer, Bounds on the size of linear codes, Handbook of Coding Theory, Volume I, (V. S. Pless and W. C. Huffman, eds.), Elsevier, 1998, 295–461.

[2] M. Daberkow, C. Fieker, J. Kluners, M. Pohst, K. Roegner and K. Wildanger, KANT V4, J. Symbolic Comp. 24 (1997), 267-283.

[3] Yu. I. Manin, *What is the maximal number of points on a curve over* $\mathbf{F}_2$, J. Fac. Sci. Univ. Sect. Tokyo IA Math., 28 (1982), 715-720.

[4] M. A. Tsfasman and S. G. Vlădut, Algebraic-Geometric Codes, Kluwer Academic Publishers, 1991.

Toshiyuki Katsura
Graduate School of Mathematical Sciences,
The University of Tokyo
Tokyo, 153-8914 Japan
E-mail: tkatsura@ms.u-tokyo.ac.jp

Motoko Qiu Kawakita
Department of Information Sciences
Ochanomizu University
Tokyo, 112-8610 Japan
E-mail: kawakita@cc.ocha.ac.jp