

Some remarks on the Plotkin bound

Jörn Quistorff

Speckenreye 48
22119 Hamburg, Germany
joern.quistorff@hamburg.de

Submitted: Nov 24, 2001; Accepted: Jun 17, 2003; Published: Jun 27, 2003

MR Subject Classifications: 94B65

Abstract

In coding theory, Plotkin's upper bound on the maximal cardinality of a code with minimum distance at least d is well known. He presented it for binary codes where Hamming and Lee metric coincide. After a brief discussion of the generalization to q -ary codes preserved with the Hamming metric, the application of the Plotkin bound to q -ary codes preserved with the Lee metric due to Wyner and Graham is improved.

1 Introduction

Let K be a set of cardinality $q \in \mathbf{N}$ and $d^K : K \times K \rightarrow \mathbf{R}$ be a metric. Consider $R := K^n$ with $n \in \mathbf{N}$ and $d^R((v_1, \dots, v_n), (w_1, \dots, w_n)) := \sum_{i=1}^n d^K(v_i, w_i)$. Then (K, d^K) and (R, d^R) are finite metric spaces.

A subset $C \subseteq R$ is called a (block) code of length n . If $|C| \geq 2$ then its minimum distance is defined by $d(C) := \min\{d^R(v, w) \in \mathbf{R}^+ | v, w \in C \text{ and } v \neq w\}$. The observation of the metric properties of (R, d^R) and of its subsets is an essential part of coding theory. The value $u(R, d^R, d)$ (or briefly $u(d)$), defined as the maximal cardinality of a code $C \subseteq R$ with minimum distance $d(C) \geq d$, is frequently considered.

The determination of $u(d)$ is a fundamental and often unsolved problem but some lower and upper bounds are well known. This paper deals with the following condition on the parameters of a code which gives Plotkin's upper bound on $u(d)$. Similar formulations are given by Berlekamp [1] and Răduică [8].

Let $d > 0$ and $u \in \mathbf{N} \setminus \{1\}$. Put $J := \{0, \dots, u-1\}$. If $u(d) \geq u$ then

$$d \binom{u}{2} \leq n \max \left\{ \sum_{\{j,k\} \subseteq J} d^K(v_1^{(j)}, v_1^{(k)}) | (v_1^{(0)}, \dots, v_1^{(u-1)}) \in K^u \right\} =: nP_{(K, d^K)}(u). \quad (1)$$

This condition is easy to prove by estimating $\sum_{\{v,w\} \subseteq C} d^R(v, w)$.

If instead of $P_{(K,d^\kappa)}(u)$ an upper bound $Q_{(K,d^\kappa)}(u)$ is known then inequality (1) can be replaced by

$$d\binom{u}{2} \leq nQ_{(K,d^\kappa)}(u). \quad (2)$$

The most common finite metric spaces in coding theory are the (n -dimensional q -ary) Hamming spaces (R, d_H) . Here, the Hamming metric can be introduced by

$$d_H((v_1, \dots, v_n), (w_1, \dots, w_n)) = \sum_{i=1}^n d_H(v_i, w_i)$$

and

$$d_H(v_i, w_i) = \begin{cases} 0 & \text{if } v_i = w_i \\ 1 & \text{if } v_i \neq w_i. \end{cases}$$

Furthermore, $A_q(n, d)$ is usually used instead of $u(R, d_H, d)$.

Other common finite metric spaces in coding theory consider $R = K^n$ with $K = \mathbf{Z}/q\mathbf{Z}$ together with the Lee metric d_L which can be introduced by

$$d_L((v_1, \dots, v_n), (w_1, \dots, w_n)) = \sum_{i=1}^n d_L(v_i, w_i)$$

and

$$d_L(v_i, w_i) = \min\{|v_i - w_i|, q - |v_i - w_i|\}. \quad (3)$$

Whenever, like on the right-hand side of equation (3), an order \leq is used in $\mathbf{Z}/p\mathbf{Z}$, their elements have to be represented by elements of $\{0, \dots, p-1\} \subseteq \mathbf{Z}$. The spaces (R, d_L) should be called Lee spaces.

In case of $q \leq 3$, the metrics d_H and d_L are identical. Lee [3] noticed that also the case $((\mathbf{Z}/4\mathbf{Z})^n, d_L)$ can be reduced to $((\mathbf{Z}/2\mathbf{Z})^{2n}, d_H)$, using the transformation $0 \mapsto (0, 0)$, $1 \mapsto (0, 1)$, $2 \mapsto (1, 1)$, $3 \mapsto (1, 0)$. The pathological case $q = 1$ is usually omitted.

After a brief discussion of the Plotkin bound in Hamming spaces, the paper considers this bound in Lee spaces.

2 Hamming Spaces

Plotkin [6] introduced his bound in case of $q = 2$ where Hamming and Lee metric coincide. In terms of condition (1), he used $P_2^H(u) := P_{(\{0,1\}, d_H)}(u) = \lfloor \frac{u+1}{2} \rfloor (u - \lfloor \frac{u+1}{2} \rfloor)$ and proved the existence of an $m \in \mathbf{N}$ with

$$A_2(n, d) \leq 2m \leq \frac{2d}{2d - n} \quad (4)$$

if $2d > n$. MacWilliams/Sloane [5] mentioned in this case the equivalent bound

$$A_2(n, d) \leq 2 \left\lfloor \frac{d}{2d - n} \right\rfloor. \quad (5)$$

Berlekamp [1] considered the generalization to q -ary Hamming spaces. In terms of $P_q^H := P_{(\mathbf{Z}/q\mathbf{Z}, d_H)}$ and Q_q^H , he showed $P_q^H(u) \leq Q_q^H(u) = \frac{u^2(q-1)}{2q}$. This result yields the bound

$$A_q(n, d) \leq \frac{dq}{dq - n(q-1)} \quad \text{if } dq > n(q-1).$$

Quistorff [7] determined

$$P_q^H(u) = \binom{u}{2} - b \binom{a+1}{2} - (q-b) \binom{a}{2} \quad (6)$$

if $u = aq + b$ with $a, b \in \mathbf{N}_0$ and $b < q$. An equivalent statement can be found in Bogdanova et al. [2]. The results (1) and (6) imply e.g. the tight upper bound $A_3(9, 7) \leq 6$. Vaessens/Aarts/Van Lint [9] formerly mentioned this and similar examples for $q = 3$ as an implication of Plotkin [6] and also solved the case $a = b = 1$ in (6) with arbitrary $q \in \mathbf{N} \setminus \{1\}$. Mackenzie/Seberry's [4] bound on $A_3(n, d)$ with $3d > 2n$ is incorrect. The adequate use of their method leads to

$$A_3(n, d) \leq \max \left\{ 3 \left\lfloor \frac{d}{3d-2n} \right\rfloor, 3 \left\lfloor \frac{d}{3d-2n} - \frac{2}{3} \right\rfloor + 1 \right\} \quad \text{if } 3d > 2n$$

which is equivalent to the application of (6).

3 Lee Spaces

Put $P_q^L(u) := P_{(\mathbf{Z}/q\mathbf{Z}, d_L)}(u)$. Wyner/Graham [10] proved

$$P_q^L(u) \leq Q_q^L(u) := \begin{cases} \frac{u^2(q^2-1)}{8q} & \text{if } q \text{ is odd} \\ \frac{u^2}{8}q & \text{if } q \text{ is even} \end{cases}$$

as an application of the Plotkin bound in Lee spaces, cf. also Berlekamp [1]. The stronger inequality

$$P_q^L(u) \leq \lfloor Q_q^L(u) \rfloor \quad (7)$$

follows by definition. In order to improve formula (7), some preparation is necessary.

Lemma 1 *Let $q, u \in \mathbf{N} \setminus \{1\}$ and $m \in \{1, \dots, u-1\}$. Let $J := \mathbf{Z}/u\mathbf{Z}$ and $v^{(j)} \in \mathbf{Z}/q\mathbf{Z}$ with $j \in J$ and $v^{(j)} \leq v^{(k)}$ for $j < k$. Then*

$$\sum_{j \in J} d_L(v^{(j)}, v^{(j+m)}) \leq mq \quad (8)$$

and equality holds in estimation (8) iff

$$d_L(v^{(j)}, v^{(j+m)}) = \begin{cases} v^{(j+m)} - v^{(j)} & \text{if } j < u-m \\ q + v^{(j+m)} - v^{(j)} & \text{if } j \geq u-m \end{cases} \quad (9)$$

is valid.

Proof:

$$\sum_{j \in J} d_L(v^{(j)}, v^{(j+1)}) \leq q + v^{(0)} - v^{(u-1)} + \sum_{j \in J \setminus \{u-1\}} v^{(j+1)} - v^{(j)} = q$$

and hence

$$\begin{aligned} \sum_{j \in J} d_L(v^{(j)}, v^{(j+m)}) &\leq \sum_{j \in J} \sum_{l=0}^{m-1} d_L(v^{(j+l)}, v^{(j+l+1)}) \\ &\leq \sum_{l=0}^{m-1} \sum_{j \in J} d_L(v^{(j)}, v^{(j+1)}) \\ &\leq mq. \end{aligned}$$

All estimates turn out to be equalities iff condition (9) is valid. □

Put

$$N_q^L(u) := \begin{cases} \frac{u^2-1}{8}q & \text{if } u \text{ is odd} \\ \frac{u(u-2)}{8}q + \frac{u}{2} \left\lfloor \frac{q}{2} \right\rfloor & \text{if } u \text{ is even} \end{cases}$$

with $u \in \mathbf{N} \setminus \{1\}$. Clearly, $\frac{u^2-1}{8} \in \mathbf{N}$ if u is odd and $\frac{u(u-2)}{8} \in \mathbf{N}_0$ if u is even.

Theorem 2 *Let $q, u \in \mathbf{N} \setminus \{1\}$. Then $P_q^L(u) \leq N_q^L(u)$ holds true.*

Proof: Let $v^{(j)} \in \mathbf{Z}/q\mathbf{Z}$ with $j \in J := \mathbf{Z}/u\mathbf{Z}$. Without loss of generality, let $v^{(j)} \leq v^{(k)}$ for $j < k$.

(i) Let u be odd. Then

$$\begin{aligned} \sum_{\{j,k\} \subseteq J} d_L(v^{(j)}, v^{(k)}) &= \sum_{m=1}^{\frac{u-1}{2}} \sum_{j \in J} d_L(v^{(j)}, v^{(j+m)}) \\ &\leq \sum_{m=1}^{\frac{u-1}{2}} mq = N_q^L(u) \end{aligned}$$

follows by Lemma 1.

(ii) Let u be even. Then

$$\begin{aligned} \sum_{\{j,k\} \subseteq J} d_L(v^{(j)}, v^{(k)}) &= \sum_{m=1}^{\frac{u}{2}-1} \sum_{j \in J} d_L(v^{(j)}, v^{(j+m)}) + \sum_{j \in J; j < \frac{u}{2}} d_L(v^{(j)}, v^{(j+\frac{u}{2})}) \\ &\leq \sum_{m=1}^{\frac{u}{2}-1} mq + \frac{u}{2} \left\lfloor \frac{q}{2} \right\rfloor = N_q^L(u) \end{aligned}$$

follows by Lemma 1.

Hence, in both cases $P_q^L(u) \leq N_q^L(u)$ is valid. \square

Theorem 2 improves formula (7) in many cases. E.g. $N_8^L(3) = 8 < 9 = \lfloor Q_8^L(3) \rfloor$ and $N_9^L(6) = 39 < 40 = \lfloor Q_9^L(6) \rfloor$ hold true.

The following statements will prove coincidence between $P_q^L(u)$ and $N_q^L(u)$ if q is odd or u is small, relative to q . Put $f(u) := 1$ if u is odd and $f(u) := 2$ if u is even.

Lemma 3 *Let $q, u \in \mathbf{N} \setminus \{1\}$. Let q be even or $f(u)q \geq u - 1$. Let $\lfloor \frac{jq}{u} \rfloor, \lfloor \frac{kq}{u} \rfloor \in \mathbf{Z}/q\mathbf{Z}$ with $j, k := j + m \in \mathbf{Z}/u\mathbf{Z}$ and $1 \leq m \leq \lfloor \frac{u-1}{2} \rfloor$ as well as $0 \leq j, k < u$. Put*

$$\left\lfloor \frac{\widetilde{kq}}{u} \right\rfloor := \begin{cases} \lfloor \frac{kq}{u} \rfloor & \text{if } j < u - m \\ q + \lfloor \frac{kq}{u} \rfloor & \text{if } j \geq u - m. \end{cases}$$

Then $d_L(\lfloor \frac{jq}{u} \rfloor, \lfloor \frac{kq}{u} \rfloor) = \lfloor \frac{\widetilde{kq}}{u} \rfloor - \lfloor \frac{jq}{u} \rfloor \leq \lfloor \frac{q}{2} \rfloor$ is valid.

Proof: It holds true that $\lfloor \frac{\widetilde{kq}}{u} \rfloor \leq \frac{(j + \lfloor \frac{u-1}{2} \rfloor)q}{u}$ and $\lfloor \frac{jq}{u} \rfloor \geq \frac{jq - (u-1)}{u}$.

(i) Let u be odd. Then $\lfloor \frac{\widetilde{kq}}{u} \rfloor - \lfloor \frac{jq}{u} \rfloor \leq \lfloor \frac{\frac{u-1}{2}q + (u-1)}{u} \rfloor = \lfloor (\frac{q}{2} + 1)(1 - \frac{1}{u}) \rfloor$. If q is even then $\lfloor \frac{\widetilde{kq}}{u} \rfloor - \lfloor \frac{jq}{u} \rfloor \leq \lfloor \frac{q}{2} \rfloor$. If $q \geq u - 1$ then $\lfloor \frac{\widetilde{kq}}{u} \rfloor - \lfloor \frac{jq}{u} \rfloor \leq \lfloor (\frac{q}{2} + 1) \frac{q}{q+1} \rfloor = \lfloor \frac{q+1}{2} - \frac{1}{2(q+1)} \rfloor \leq \lfloor \frac{q}{2} \rfloor$.

(ii) Let u be even. Then $\lfloor \frac{\widetilde{kq}}{u} \rfloor - \lfloor \frac{jq}{u} \rfloor \leq \lfloor \frac{(\frac{u}{2}-1)q + (u-1)}{u} \rfloor = \lfloor (\frac{q}{2} + 1) - \frac{q+1}{u} \rfloor$. If q is even then $\lfloor \frac{\widetilde{kq}}{u} \rfloor - \lfloor \frac{jq}{u} \rfloor \leq \lfloor \frac{q}{2} \rfloor$. If $2q \geq u - 1$ then $\lfloor \frac{\widetilde{kq}}{u} \rfloor - \lfloor \frac{jq}{u} \rfloor \leq \lfloor \frac{q+1}{2} - \frac{2(q+1)-u}{2u} \rfloor \leq \lfloor \frac{q}{2} \rfloor$.

Hence, $d_L(\lfloor \frac{jq}{u} \rfloor, \lfloor \frac{kq}{u} \rfloor) = \lfloor \frac{\widetilde{kq}}{u} \rfloor - \lfloor \frac{jq}{u} \rfloor$. \square

In case of $q = 3, u = 5, j = 3, m = 2$, Lemma 3 can not be applied. Here, $k = 0, \lfloor \frac{jq}{u} \rfloor = 1, \lfloor \frac{kq}{u} \rfloor = 0, \lfloor \frac{\widetilde{kq}}{u} \rfloor = 3, \lfloor \frac{\widetilde{kq}}{u} \rfloor - \lfloor \frac{jq}{u} \rfloor = 2 > 1 = \lfloor \frac{q}{2} \rfloor$ and $d_L(\lfloor \frac{jq}{u} \rfloor, \lfloor \frac{kq}{u} \rfloor) = 1$. A similar example is $q = 3, u = 8, j = 5, m = 3$.

Lemma 4 *Let $q, u \in \mathbf{N} \setminus \{1\}$ and u be even. Let $\lfloor \frac{jq}{u} \rfloor, \lfloor \frac{kq}{u} \rfloor \in \mathbf{Z}/q\mathbf{Z}$ with $j, k := j + \frac{u}{2} \in \mathbf{Z}/u\mathbf{Z}$ and $0 \leq j < \frac{u}{2} \leq k < u$. Then $d_L(\lfloor \frac{jq}{u} \rfloor, \lfloor \frac{kq}{u} \rfloor) = \lfloor \frac{q}{2} \rfloor$ is valid.*

Proof: It holds true that $\frac{(j + \frac{u}{2})q - (u-1)}{u} \leq \lfloor \frac{kq}{u} \rfloor \leq \frac{(j + \frac{u}{2})q}{u}$ and $\frac{jq - (u-1)}{u} \leq \lfloor \frac{jq}{u} \rfloor \leq \frac{jq}{u}$. Hence, $\lfloor \frac{kq}{u} \rfloor - \lfloor \frac{jq}{u} \rfloor \leq \lfloor \frac{q}{2} + \frac{u-1}{u} \rfloor \leq \lfloor \frac{q+1}{2} \rfloor$ and $q - \lfloor \frac{kq}{u} \rfloor + \lfloor \frac{jq}{u} \rfloor \leq \lfloor \frac{q}{2} + \frac{u-1}{u} \rfloor \leq \lfloor \frac{q+1}{2} \rfloor$. This yields $d_L(\lfloor \frac{jq}{u} \rfloor, \lfloor \frac{kq}{u} \rfloor) = \lfloor \frac{q}{2} \rfloor$. \square

Theorem 5 *Let $q, u \in \mathbf{N} \setminus \{1\}$. Let q be even or $f(u)q \geq u - 1$. Then $P_q^L(u) = N_q^L(u)$.*

Proof: Put $v^{(j)} := \lfloor \frac{jq}{u} \rfloor$ for $j \in J := \mathbf{Z}/u\mathbf{Z}$ with $0 \leq j < u$.

(i) Let u be odd. Then

$$\begin{aligned} P_q^L(u) &\geq \sum_{\{j,k\} \subseteq J} d_L(v^{(j)}, v^{(k)}) = \sum_{m=1}^{\frac{u-1}{2}} \sum_{j \in J} d_L(v^{(j)}, v^{(j+m)}) \\ &= \sum_{m=1}^{\frac{u-1}{2}} mq \\ &= N_q^L(u) \end{aligned}$$

by Lemma 1 and 3.

(ii) Let u be even. Then

$$\begin{aligned} P_q^L(u) &\geq \sum_{\{j,k\} \subseteq J} d_L(v^{(j)}, v^{(k)}) \\ &= \sum_{m=1}^{\frac{u}{2}-1} \sum_{j \in J} d_L(v^{(j)}, v^{(j+m)}) + \sum_{j \in J; j < \frac{u}{2}} d_L(v^{(j)}, v^{(j+\frac{u}{2})}) \\ &= N_q^L(u) \end{aligned}$$

by Lemma 1, 3 and 4.

Theorem 2 completes the proof. \square

If u is considerable greater than q , the Plotkin bound is usually weak and other well known upper bounds, e.g. the Hamming bound, give stronger results. Hence, it seems not to be fatal that $P_q^L(u)$ is not determined in all these cases. The final theorem gives at least a lower bound on $P_q^L(u)$. According to Theorem 5, it is sufficient to consider only odd values of q . The following convention is used. Extending inequality (1) by $u \in \{0, 1\}$, one gets $P_{(K,d\kappa)}(u) = 0$ and hence $P_q^L(0) = P_q^L(1) = 0$.

Theorem 6 *Let $q, u \in \mathbf{N} \setminus \{1\}$ and q be odd. Let $u = aq + b$ with $a, b \in \mathbf{N}_0$ and $b < q$. Then*

$$P_q^L(u) \geq a(u+b) \frac{q^2-1}{8} + P_q^L(b) \quad (10)$$

Proof: Put $J_s := \{0, \dots, q-1\} \times \{s\}$ with $s \in \{0, \dots, a-1\}$ as well as $J_a := \{(\lfloor \frac{iq}{b} \rfloor, a) | j \in \{0, \dots, b-1\}\}$. Put $v^{(r,s)} := r$ for all $(r, s) \in J := \bigcup_{s=0}^a J_s$. Using the proof of Theorem 5, it follows that

$$\sum_{\{j,k\} \subseteq \bigcup_{s=0}^{a-1} J_s} d_L(v^{(j)}, v^{(k)}) = a^2 \sum_{\{j,k\} \subseteq J_0} d_L(v^{(j)}, v^{(k)}) = a^2 P_q^L(q)$$

and

$$\sum_{\{j,k\} \subseteq J_a} d_L(v^{(j)}, v^{(k)}) = P_q^L(b)$$

as well as

$$\sum_{j \in \bigcup_{s=0}^{a-1} J_s; k \in J_a} d_L(v^{(j)}, v^{(k)}) = 2ab \sum_{i=0}^{\frac{q-1}{2}} i = ab \frac{q^2 - 1}{4}.$$

Hence,

$$P_q^L(u) \geq \sum_{\{j,k\} \subseteq J} d_L(v^{(j)}, v^{(k)}) = a(u+b) \frac{q^2 - 1}{8} + P_q^L(b)$$

is valid. □

One might conjecture equality in (10). The combination of the formulas (7) and (10) proves e.g. $P_3^L(5) = \lfloor Q_3^L(5) \rfloor = 8 < 9 = N_3^L(5)$ and $P_3^L(8) = \lfloor Q_3^L(8) \rfloor = 21 < 22 = N_3^L(8)$.

For some applications, let $u(d) \geq u \in \mathbf{N} \setminus \{1\}$.

- (i) Let $u = 3$. Inequality (2) and Theorem 2 imply the condition $3d \leq qn$. Theorem 5 shows that inequality (1) cannot improve this condition.
- (ii) Let $u = 4$ and use (2). If q is even then $3d \leq qn$ follows again. If q is odd then the stronger condition $6d \leq (2q - 1)n$ follows. In both cases, an improvement by (1) is impossible.
- (iii) Let $u = 5$. Inequality (2) implies $10d \leq 3qn$. Only in case of $q = 3$, an improvement by (1) is possible: $5d \leq 4n$.
- (iv) Let q be even and u be odd. Then inequality (1) implies the same condition for u and $u + 1$, since $\binom{u}{2}^{-1} P_q^L(u) = \binom{u+1}{2}^{-1} P_q^L(u + 1)$.
- (v) Let q be even. Then $\binom{u}{2}^{-1} P_q^L(u) > \frac{q}{4}$ and $\lim_{u \rightarrow \infty} \binom{u}{2}^{-1} P_q^L(u) = \frac{q}{4}$. Hence, inequality (1) turns out to be a tautology iff $4d \leq qn$.

References

- [1] Berlekamp, E.R.: *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.
- [2] Bogdanova, G.T. / Brouwer, A.E. / Kapralov, S.N. / Östergård, P.R.J.: Error-Correcting Codes over an Alphabet of Four Elements, *Des. Codes Cryptogr.*, 23 (2001), 333-342.
- [3] Lee, C.Y.: Some Properties of Nonbinary Error-Correcting Codes, *IRE Trans. Inform. Theory*, 4 (1958), 77-82.
- [4] Mackenzie, C. / Seberry, J.: Maximal Ternary Codes and Plotkin's Bound, *Ars Comb.*, 17A (1984), 251-270.
- [5] MacWilliams, F.J. / Sloane, N.J.A.: *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, New York, Oxford, 1977.

- [6] Plotkin, M.: Binary Codes with Specified Minimum Distance, *Univ. Penn. Res. Div. Report* 51-20 (1951); *IRE Trans. Inform. Theory*, 6 (1960), 445-450.
- [7] Quistorff, J.: *Simultane Untersuchung mehrfach scharf transitiver Permutationsmengen und MDS-Codes unter Einbeziehung ihrer Substitute*, Habilitationsschrift, Univ. Hamburg, 1999; Shaker Verlag, Aachen, 2000.
- [8] Răduică, M.: Marginile Plotkin si Ioshi relativ la coduri arbitrar metrizzate, *Bul. Univ. Braşov*, C 22 (1980), 115-120.
- [9] Vaessens, R.J.M. / Aarts, E.H.L. / van Lint, J.H.: Genetic Algorithms in Coding Theory - a Table for $A_3(n, d)$, *Discrete Appl. Math.*, 45 (1993), 71-87.
- [10] Wyner, A.D. / Graham, R.L.: An Upper Bound on Minimum Distance for a k -ary Code, *Inform. Control*, 13 (1968), 46-52.