Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 42 (2001), No. 2, 601-611.

On Codes with Given Minimum Distance and Covering Radius[1]

Jörn Quistorff

Speckenreye 48, D-22119 Hamburg, Germany
e-mail: Joern.Quistorff@Hamburg.de

Abstract. Codes with minimum distance at least d and covering radius at most $d-1$ are considered. The minimal cardinality of such codes is investigated. Herewith, their connection to covering problems is applied and a new construction theorem is given. Additionally, a new lower bound for the covering problem is proved. A necessary condition on an existence problem is presented by using a multiple covering of the farthest-off points.

1. Introduction

Coding theory, seen from the combinatorial point of view, considers often (block-)codes of finite order (i.e. alphabet size) and length provided with the Hamming metric, neither restricted to the binary nor to the linear case.

Prior reseach dealt usually with at most one of the following two problems.

On the one hand, packing problems were investigated in order to find (local) maximal, which means not extendable, codes with given minimum distance. Here, it is the aim to determine the maximal, more seldom the minimal, cardinality of such a code. Cf. MacWilliams/Sloane [15], Heise/Quattrocchi [10] and Quistorff [16].

On the other hand, covering problems were examined in order to find codes with given covering radius. There, it is the aim to determine the minimal cardinality of such a covering code. Cf. Cohen et al. [3], [4], [5], [6] and van Lint [14].

[1] **Editorial Remark:** This article replaces the version published by the same author in Beiträge zur Algebra und Geometrie 41, No. 2, 469-478 (2000). Due to an error in the files transmission the publication of that version was not based on the final TEX-file for the article. Hence some improvements suggested by the referee were missing.

Both problems were usually studied isolated. Cohen et al. [3] however remarked that in packing problems, also the covering radius plays an important role: A code with a minimum distance at least d is not extendable iff its covering radius is at most $d-1$.

The present work is mainly devoted to codes with given minimum distance and covering radius. It concentrates on the minimal cardinality of a code with minimum distance at least d and covering radius at most $d-1$, especially in case of $d=2$. Blokhuis/van Lint [1] started to treat the same problem independently. Additionally, a new lower bound for the covering problem is proved here.

In Section 2, the foundations of packing and covering problems are given.

Known results on the minimal cardinality $v(q,n,d)$ of a code of order q and length n with minimum distance at least d and covering radius at most $d-1$ are surveyed in Section 3. Some stem from Quistorff [16], where a code with the mentioned properties is called a local cardinal maximum code. Other findings, for example an implicit lower bound, were given in Quistorff [17], partially using the algebraic structure of an n-quasigroup.

The minimal cardinality of a code of order q and length n with covering radius at most t is called $K_q(n,t)$. Trivially, $K_q(n,d-1)$ is a lower bound on $v(q,n,d)$. Hence, some lower bounds and exact values on $K_q(n,t)$, for example the well-known sphere-covering bound, are mentioned in Section 4.

In Section 5, a new lower bound on $K_q(n,1)$ with $2 \leq n-1 < q \leq 2(n-1)$ is proved using ideas of Kalbfleisch/Weiland [13].

Section 6 presents a new construction of codes with minimum distance at least 2 and covering radius 1.

An open problem with relative small parameters is the determination of $v(4,4,2)$. Results of Sections 4 and 6 yield 24 and 32 as lower and upper bound, respectively. Blokhuis/van Lint [1] found 31 as an upper bound on $v(4,4,2)$.

In the final Section 7, a necessary condition on the existence of a code of a given cardinality u with minimum distance at least 2 and covering radius 1 is presented using the so-called multiple covering of the farthest-off points, cf. Hämäläinen et al. [9]. An example shows that this condition is satisfied in case of $q=n=4$ and $u=24$.

2. Foundations

Let $q,n \in \mathbf{N} = \{1,2,\ldots\}$. A set $C \subseteq K^n$ with $|K|=q$ is called a code of order q and length n (or q-ary code of length n). An element $w=(w_1,\ldots,w_n)$ of C is called codeword. The mapping

$$d : K^n \times K^n \to \mathbf{N}_0, (w,w') \mapsto |\{x \in \mathbf{Z}_n | w_x \neq w'_x\}|$$

with $\mathbf{N}_0 = \mathbf{N} \cup \{0\}$ and $\mathbf{Z}_n := \{x \in \mathbf{N} | x \leq n\}$ is called Hamming distance. It induces a metric on the space K^n, called the Hamming metric. If $|C| \geq 2$ and hence $q \geq 2$, the minimum distance of C is defined as

$$d(C) := \min\{d(w,w') \in \mathbf{N} | w,w' \in C \text{ with } w \neq w'\}.$$

If $|C| \geq 1$, the covering radius of C is introduced as

$$t(C) := \max\{\min\{d(v,w) \in \mathbf{N}_0 | w \in C\} | v \in K^n\}.$$

For $e \in \mathbf{N}_0$ and $v \in K^n$, the set

$$B(v,e) := \{v' \in K^n | d(v,v') \leq e\}$$

is called sphere around v with radius e (and respect to the Hamming metric). Its cardinality is $|B(v,e)| = \sum_{i=0}^{e} \binom{n}{i}(q-1)^i$.

The statement $B(w,e) \cap B(w',e) = \emptyset$ holds true for all $w, w' \in C$ with $w \neq w'$ iff $2e+1 \leq d(C)$ is valid. Furthermore, $\bigcup_{w \in C} B(w,t) = K^n$ (or, equivalently, $C \cap B(v,t) \neq \emptyset$ for all $v \in K^n$) holds true iff $t(C) \leq t$.

Because of these relations, questions referring to the minimum distance of codes are sphere-packing problems and questions referring to the covering radius are sphere-covering problems.

The minimum distance and the covering radius of any code with $|C| \geq 2$ are related by

$$d(C) \leq 2t(C) + 1, \tag{1}$$

cf. Graham/Sloane [7]. If the minimum distance of a code C is at least 2, bound (1) shows that in this case, $t(C) \leq 1$ is equivalent to $t(C) = 1$.

For $e \in \mathbf{N}_0$, a code $C \subseteq K^n$ with $e \leq n$ is called e-perfect iff the spheres around the codewords with radius e are disjoint and exhaust K^n, i.e.

$$\biguplus_{w \in C} B(w,e) = K^n.$$

In this case $t(C) = e$ and, if $|C| \geq 2$, clearly $d(C) = 2e+1$.

Let $q, n, d \in \mathbf{N}$ with $2 \leq q$ and $d \leq n$ as well as $C \subseteq K^n$ with $|K| = q$. Then C is called a (q,n,d)-cardinal maximum code iff $d(C) \geq d$ holds true and for every code $C' \subseteq K^n$ with $d(C') \geq d$, the statement $|C'| \leq |C|$ follows. The maximal cardinality of such a code is denoted by $u(q,n,d)$ (or by $A_q(n,d)$).

Weakening this notion, C is called a local (q,n,d)-cardinal maximum code iff $d(C) \geq d$ holds true and for every proper including set $C' \supset C$ the statement $d(C') < d$ follows. The minimal cardinality of such a code is denoted by $v(q,n,d)$.

Let $q, n, t \in \mathbf{N}$ with $t \leq n$ as well as $C \subseteq K^n$ with $|K| = q$. Then C is called a t-covering code iff $t(C) \leq t$. The minimal cardinality of such a code is denoted by $K_q(n,t)$.

Every local (q,n,d)-cardinal maximum code is a $(d-1)$-covering code, cf. Cohen et al. [3]. Hence,

$$v(q,n,d) \geq K_q(n,d-1). \tag{2}$$

If there exists an e-perfect code of order q and length n consisting of more than one codeword,

$$u(q,n,2e+1) = v(q,n,e+1) = K_q(n,e) = \frac{q^n}{\sum_{i=0}^{e} \binom{n}{i}(q-1)^i}$$

is valid. The existence of perfect codes is discussed e.g. by Heise/Quattrocchi [10].

3. Known results on $v(q,n,d)$

Trivially, $q \le v(q,n,d) \le u(q,n,d)$ holds true as well as $v(q,n,1) = q^n$.

As an example for an upper bound on $u(q,n,d)$ and hence also on $v(q,n,d)$, the (Joshi-) Singleton bound $u(q,n,d) \le q^{n-d+1}$ is mentioned. For further bounds on $u(q,n,d)$, cf. MacWilliams/Sloane [15], Heise/Quattrocchi [10], Quistorff [16] and their references.

In Quistorff [16], the inequalities $v(q,n,d) \ne q^{n-d+1} - 1 \ne u(q,n,d)$ were proved. Also, the statement $v(q,n,d) = q$ if $qd > n(q-1)$ was given. It yields especially $v(q,n,n) = q$.

Inspired by Stojaković/Ušan's [20] lower bound $v(q,3,2) \ge 2q-1$ if $q \ge 3$, Quistorff [17] proved the following implicit lower bound on $v(q,n,2)$ in the language of $(n-1)$-quasigroups.

If there exists a code $C \subseteq K^n$ of order q and cardinality u with minimum distance at least 2 as well as covering radius 1 and if $u = aq^{n-2} + b$ with $a, b \in \mathbf{N}_0$ as well as $b < q^{n-2}$, then

$$(n-1)(qu - b(a+1)^2 - (q^{n-2} - b)a^2) \ge (q^{n-1} - u)q \tag{3}$$

holds true. Using this implicit lower bound together with the construction of a suitable code, cf. also Kalbfleisch/Stanton [12] or Blokhuis/van Lint [1], the value of $v(q,3,2)$ was determined as follows.

$$v(q,3,2) = \left\lceil \frac{1}{2}q^2 \right\rceil . \tag{4}$$

($\lceil x \rceil$ denotes the least integer greater than or equal to x.)

Blokhuis/van Lint [1] showed $v(q,3,2) \ge \left\lceil \frac{1}{2}q^2 \right\rceil$ directly: Let $C \subseteq (\mathbf{Z}_q)^3$ be a code of cardinality u with minimum distance at least 2 as well as covering radius 1. Let G be a tripartite graph which corresponds to C in the following way. The three cocliques V_1, V_2 and V_3 of size q, each consist of vertices labeled by the elements of $\mathbf{Z}_q$. A triangle with edges from $w_1 \in V_1$ to $w_2 \in V_2$, from $w_2 \in V_2$ to $w_3 \in V_3$ and from $w_3 \in V_3$ to $w_1 \in V_1$ is contained in G iff $(w_1, w_2, w_3) \in C$.

Clearly, G consists of u edge-disjoint triangles since the minimum distance of C is at least 2. Let T_i denote the number of triples $w \in (\mathbf{Z}_q)^3$ that contain exactly i edges of G. Clearly, $T_0 = 0$ since C has covering radius 1.

By counting triples in $(\mathbf{Z}_q)^3$ as well as pairs of an edge and a triple where the edge is in the triple, one gets

$$\sum_i T_i = q^3 \tag{5}$$

and

$$\sum_i iT_i = 3uq. \tag{6}$$

Put $S_{ji} := |\{w \in (\mathbf{Z}_q)^3 | w_j = i\}|$ with $j \in \mathbf{Z}_3$ and $i \in \mathbf{Z}_q$. Hence, $\sum_i S_{ji} = u$ as well as $\sum_i S_{ji}^2 \ge \frac{u^2}{q}$ by Cauchy-Schwarz. By counting adjacent pairs of edges within triples, one obtains

$$T_2 + 3T_3 = \sum_{j,i} S_{ji}^2 \ge \frac{3u^2}{q}. \tag{7}$$

By (5), (6) and (7),

$$0 \le T_2 \le 9uq - 3q^3 - \frac{6u^2}{q}$$

follows. Hence,

$$0 \leq \left(2\frac{u}{q^2} - 1\right)\left(1 - \frac{u}{q^2}\right)$$

is valid. Since $u \leq q^2$, this proves $2\frac{u}{q^2} - 1 \geq 0$ and finally $u \geq \left\lceil \frac{1}{2}q^2 \right\rceil$. □

Quistorff [17] proved that $v(kq, n, d) \leq k^{n-d+1} v(q, n, d)$ if there exists an $(n, n-d+1)$-MDS-code of order k (i.e. a code which satisfies the Singleton bound with equality). Hence, the well-known existence of an $(n, n-1)$-MDS-code of every order yields

$$v(kq, n, 2) \leq k^{n-1} v(q, n, 2). \tag{8}$$

Furthermore, it was shown that

$$v(kp, p+1, 2) = k^p p^{p-1} \tag{9}$$

if p is a prime power and $k \in \mathbf{N}$.

4. Lower bounds and exact values on $K_q(n, t)$

Trivially, $K_q(n, 0) = q^n$ and $K_q(n, n) = 1$ holds true. Cohen et al. [6] mentioned also $K_q(n, n-1) = q$.

The best known lower bound on $K_q(n, t)$ is the sphere-covering bound:

$$K_q(n, t) \geq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i}. \tag{10}$$

Hence, from (2) and (10) follows

$$v(q, n, d) \geq \frac{q^n}{\sum_{i=0}^{d-1} \binom{n}{i} (q-1)^i}. \tag{11}$$

Equality holds in (10) iff there exists a t-perfect code of order q and length n, cf. Section 2. Several improvements of the sphere-covering bound (10) are known, cf. Chen/Honkala [2] and van Wee [22]. The latter proved e.g.

$$K_q(n, 1) \geq \frac{q^n}{n(q-1)} \text{ for even } q, n \in \mathbf{N}.$$

Trivially, (10) implies

$$K_q(n, t) \geq \left\lceil \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i} (q-1)^i} \right\rceil.$$

Habsieger [8] characterised all cases where this bound for $t = 1$ and a prime power q is attained: $K_q(n, 1) = \lceil \frac{q^n}{1+n(q-1)} \rceil$ iff there exists a $k \in \mathbf{N}$ with $n = \frac{q^{k-1}}{q-1}$ or $(q, n) = (2, 2)$ or $(q, n) = (2, 4)$.

Kalbfleisch/Stanton [12] mentioned

$$K_q(n+1,1) \leq qK_q(n,1), \tag{12}$$

they determined

$$K_q(3,1) = \left\lceil \frac{q^2}{2} \right\rceil \tag{13}$$

and proved $K_4(4,1) \geq 24$. Stanton et al. [19] improved the latter to

$$K_4(4,1) = 24 \tag{14}$$

by presenting a 1-covering code of order 4, length 4 and cardinality 24. They also proved

$$K_{kq}(n,1) \leq k^{n-1}K_q(n,1) \tag{15}$$

if $k, q \in \mathbf{N}$ with $q \geq 2$. Cohen et al. [6] mentioned

$$K_{kp}(p+1,1) = k^p p^{p-1} \tag{16}$$

if p is a prime power and $k \in \mathbf{N}$.

In the binary case, van Wee [21] showed $K_2(2^s,1) = 2^{2^s-s}$. Cohen et al. [4] proved e.g. $K_2(2t+2,t) \geq 4$ and $K_2(2t+3,t) = 7$.

Extensive tables of the known results on $K_q(n,t)$ were given by Cohen et al. [5], [6]. They include lower bounds on $K_q(n,1)$ with $2 \leq q \leq 5$ and $n \leq 33$, $n \leq 14$, $n \leq 10$ and $n \leq 9$, respectively. Using (2), these bounds force lower bounds on $v(q,n,2)$ which are, with one exception, as good as or better than the implicit lower bound (3). Only in case of $q = n = 5$, they mentioned $K_5(5,1) \geq 157$ referring to Kalbfleisch/Weiland [13] while (3) forces $v(5,5,2) \geq 164$. In the following section, $K_5(5,1) \geq 160$ will be shown.

It is not known whether there exist parameters with $v(q,n,d) > K_q(n,d-1)$. Considering the conformity of (4) and (13), of (8) and (15) and of (9) and (16), one might conjecture equality in (2), at least in case of $d = 2$. Additionally, a bound which is conformal to (12) is given in Section 6.

5. A new lower bound on $K_q(n,1)$

Kalbfleisch/Weiland [13] proved

$$K_q(n,1) \geq \left\lceil \frac{q^{n-1}}{n-1} \right\rceil \tag{17}$$

if $n-1 < q \leq 2(n-1)$. Rodemich [18] showed independently the validity of this bound if only $n \geq 2$.

Some notations are necessary in order to improve Kalbfleisch/Weiland's [13] argumentation in the scope of $2 \leq n-1 < q < 2(n-1)$.

Let $q, n \in \mathbf{N}$ with $q \geq 2$ and $n \geq 3$ as well as K a set with $|K| = q$. Let $v \in K^{n-1}$ and $j \in \mathbf{Z}_n$. Put

$$v\#_{(j)}y := (v_1, \ldots, v_{j-1}, y, v_j, \ldots, v_{n-1}) \in K^n$$

for $y \in K$ as well as $B_v^{(j)} := \{(v\#_{(j)}y) \in K^n | y \in K\}$. Let $w \in K^{n-2}$ and $j, k \in \mathbf{Z}_n$ with $j \neq k$. Put

$$w\#_{(j,k)}(y,z) := \begin{cases} (w_1, \ldots, w_{j-1}, y, w_j, \ldots, w_{k-2}, z, w_{k-1}, \ldots, w_{n-2}) \in K^n & \text{if } j < k, \\ (w_1, \ldots, w_{k-1}, y, w_k, \ldots, w_{j-2}, z, w_{j-1}, \ldots, w_{n-2}) \in K^n & \text{if } k < j, \end{cases}$$

for $y, z \in K$ as well as $R_w^{(j,k)} := \{(w\#_{(j,k)}(y,z) \in K^n | y, z \in K\}$. Clearly, $R_w^{(j,k)} = R_w^{(k,j)}$. For $C \subseteq K^n$ put $f_C(R_w^{(j,k)}) := (x,t) \in (\mathbf{N}_0)^2$ iff $|R_w^{(j,k)} \cap C| = x$ and $|\{v \in K^{n-1} | B_v^{(j)} \subseteq R_w^{(j,k)}$ and $B_v^{(j)} \cap C \neq \emptyset\}| = t$.

Lemma 1. *Let $(x,t) := f_C(R_w^{(j,k)})$ and $(x,t') := f_C(R_w^{(k,j)})$.*

(i) $t \leq x \leq qt$.

(ii) $t = 0 \iff x = 0 \iff t' = 0$.

(iii) *If $t = 1$ then $x = t'$.*

(iv) *If $t < x$ then $t' \geq 2$.*

Furthermore, let $h_C(j,k,x,t) := |\{w \in K^{n-2} | f_C(R_w^{(j,k)}) = (x,t)\}|$ for $j \neq k$ and $g_C(j,x,t) := \sum_{k \in \mathbf{Z}_n \setminus \{j\}} h_C(j,k,x,t)$ as well as $s(x,t) := (x - \frac{q}{n-1})(t-1)$. Using these notations, one gets

$$\sum_{x,t} h_C(j,k,x,t) = |K^{n-2}| = q^{n-2}$$

and hence

$$\sum_{x,t} g_C(j,x,t) = (n-1)q^{n-2} \tag{18}$$

as well as

$$\sum_{x,t} h_C(j,k,x,t)x = \sum_x x \sum_t h_C(j,k,x,t) = |C|$$

and hence

$$\sum_{x,t} g_C(j,x,t)x = (n-1)|C|. \tag{19}$$

Kalbfleisch/Weiland [13] proved

$$\sum_{x,t} g_C(j,x,t)s(x,t) \leq (q-1)((n-1)|C| - q^{n-1}) \tag{20}$$

if C is a 1-covering code. In case of $q \leq 2(n-1)$, each product $g_C(j,x,t)s(x,t)$ is nonnegative by Lemma 1 and thus $\sum_{x,t} g_C(j,x,t)s(x,t) \geq 0$. This proves (17).

In the following, the announced new lower bound is presented.

Theorem 1. *Let $q, n \in \mathbf{N}$ with $2 \leq n-1 < q \leq 2(n-1)$ and $b := 2(n-1) - q$. Then*

$$K_q(n,1) \geq \left\lceil \frac{2(q-1)q - b}{2(q-1)(n-1) - b} q^{n-2} \right\rceil.$$

Proof. Because of Lemma 1 (iii), the inequalities $h_C(j,k,x,1) \leq h_C(k,j,x,x)$ and hence $\sum_{j\in\mathbf{Z}_n} g_C(j,x,1) \leq \sum_{j\in\mathbf{Z}_n} g_C(j,x,x)$ are valid. Therefore, $\sum_{j\in\mathbf{Z}_n}\sum_{x\geq 2} g_C(j,x,1)s(x,x) \leq \sum_{x\geq 2} s(x,x)\sum_{j\in\mathbf{Z}_n} g_C(j,x,x) \leq \sum_{j\in\mathbf{Z}_n}\sum_{x,t} g_C(j,x,t)s(x,t)$ and thus there exists a $k \in \mathbf{Z}_n$ with

$$\sum_{x\geq 2} g_C(k,x,1)s(x,x) \leq (q-1)((n-1)|C| - q^{n-1}) \tag{21}$$

by inequality (20). Furthermore, $x \geq 2$ implies

$$x - \frac{q}{n-1} \geq \frac{b}{n-1}(x-1) \tag{22}$$

since $n-1<q$. After this preparation, one obtains

$$\begin{aligned}
(q-1)((n-1)|C|-q^{n-1}) &\geq \sum_{x,t\geq 2} g_C(k,x,t)s(x,x) \\
&\geq \sum_{x\geq 2;t\geq 1} g_C(k,x,t)\left(x-\frac{q}{n-1}\right) - \sum_{x\geq 2} g_C(k,x,1)\left(x-\frac{q}{n-1}\right) \\
&\geq \frac{b}{n-1}\sum_{x,t} g_C(k,x,t)(x-1) - \sum_{x\geq 2} g_C(k,x,1)s(x,x) \\
&\geq b|C| - bq^{n-2} - (q-1)((n-1)|C|-q^{n-1})
\end{aligned}$$

by (18), (19), (20), (21), (22) and Lemma 1. Finally,

$$(2(q-1)(n-1)-b)|C| \geq 2(q-1)q^{n-1} - bq^{n-2}$$

follows which proves the theorem. □

In case of $q = 2(n-1)$, Theorem 1 coincides with bound (17). In case of $2 \leq n-1 < q < 2(n-1)$, the rational number $\frac{2(q-1)q-b}{2(q-1)(n-1)-b}q^{n-2}$ is perceptibly greater than $\frac{q^{n-1}}{n-1}$. Therefore, Theorem 1 is in many cases stronger than (17).

Examples. Theorem 1 shows $K_5(5,1) \geq 160$ and $K_6(5,1) \geq 330$ as well as $K_7(5,1) \geq 606$ instead of the lower bounds 157, 324 and 601, respectively, given by (17).

6. A new construction

The following construction uses the notion of a quasigroup.

Theorem 2. *Every code $C \subseteq K^n$ with minimum distance $d(C) \geq 2$ and covering radius $t(C) = 1$ gives rise to a code $\overline{C} \subseteq K^{n+1}$ of cardinality $|\overline{C}| = |K| \cdot |C|$ with minimum distance $d(\overline{C}) \geq 2$ and covering radius $t(\overline{C}) = 1$. Hence, $v(q,n+1,2) \leq qv(q,n,2)$ for all $q,n \in \mathbf{N}\setminus\{1\}$.*

Proof. Clearly, $n \geq d(C) \geq 2$. Define an addition on K such that $(K,+)$ is a quasigroup. Put

$$\overline{C} := \{(w_1,\dots,w_{n+1}) \in K^{n+1} | (w_1,\dots,w_{n-1},w_n+w_{n+1}) \in C\}.$$

(I) Let $\overline{v}, \overline{w} \in \overline{C}$ with $(v_1, \ldots, v_{n+1}) := \overline{v} \neq \overline{w} =: (w_1, \ldots, w_{n+1})$. Put

$$d := d((v_1, \ldots, v_{n-1}), (w_1, \ldots, w_{n-1})).$$

In case of $d = 0$, the equality $v_n + v_{n+1} = w_n + w_{n+1}$ and, hence, $d(\overline{v}, \overline{w}) = 2$ follows. In case of $d = 1$, the statement $v_n + v_{n+1} \neq w_n + w_{n+1}$ and, hence, $d(\overline{v}, \overline{w}) \geq 2$ follows. In case of $d \geq 2$, trivially $d(\overline{v}, \overline{w}) \geq 2$ follows. Herewith, $d(\overline{C}) \geq 2$.

(II) Let $\overline{v} = (v_1, \ldots, v_{n+1}) \in K^{n+1}$. Put $v := (v_1, \ldots, v_{n-1}, v_n + v_{n+1})$. There exists a codeword $w = (w_1, \ldots, w_n) \in C$ with $d(v, w) \leq 1$. In case of $d(v, w) = 0$, clearly $\overline{v} \in \overline{C}$. So, let $d(v, w) = 1$. If there exists an index $x \in \mathbf{Z}_{n-1}$ with $v_x \neq w_x$, the equality $v_n + v_{n+1} = w_n$ is valid and therefore $\overline{w} := (w_1, \ldots, w_{n-1}, v_n, v_{n+1}) \in \overline{C}$ as well as $d(\overline{v}, \overline{w}) = 1$. If such an index does not exist, $v_n + v_{n+1} \neq w_n$. Let $z \in K$ be the unique solution of $v_n + z = w_n$. Then, $\overline{w} := (w_1, \ldots, w_{n-1}, v_n, z) = (v_1, \ldots, v_{n-1}, v_n, z) \in \overline{C}$ and $d(\overline{v}, \overline{w}) = 1$. On the whole, $t(\overline{C}) \leq 1$. By $d(\overline{C}) \geq 2$, this means $t(\overline{C}) = 1$.

(III) The cardinality of $\overline{C}$ is equal to $|K| \cdot |C|$ because the construction is based on a quasigroup. □

Connecting Theorem 2 with equation (4), one gets the following upper bound.

Corollary 1. *Let $q, n \in \mathbf{N}$ with $2 \leq q$ and $3 \leq n$. Then*

$$v(q, n, 2) \leq q^{n-3} \left\lceil \frac{1}{2} q^2 \right\rceil .$$

This corollary together with the lower bound (11) proves e.g. $v(2, 4, 2) = 4$.

7. A necessary condition

Considering all mentioned results on $v(q, n, 2)$, one can remark that the case $n = 2$, the case $n = 3$ and the case $n = 4$, $q \leq 3$ are solved. If $q = n = 4$, bound (2), equation (14) and Corollary 1 show

$$24 \leq v(4, 4, 2) \leq 32.$$

Blokhuis/van Lint [1] found

$$v(4, 4, 2) \leq 31.$$

No sharper bound is known. (The code which was used to establish equation (14) has minimum distance 1. Therefore, it cannot be applied here.)

This open problem motivates the development of a necessary condition on the existence of codes of given cardinality with minimum distance at least 2 and covering radius 1.

Hämäläinen et al. [9] and Honkala/Litsyn [11] dealt in the binary case with so-called multiple coverings of the farthest-off points (MCF). Extending this notion to the q-ary case, a code $C \subseteq K^n$ of order q and covering radius $t(C) \leq t$, satisfying

$$|B(v, t) \cap C| \geq \mu \text{ for all } v \in K^n \text{ with } \min\{d(v, w) | w \in C\} = t$$

is called an $(n, |C|, t, \mu)$ MCF of order q.

It is not difficult to prove the following application.

Theorem 3. *Let $C \subseteq K^n$ be a code of order q, length n, minimum distance at least* 2 *and covering radius $t(C) \leq t$. Then, C is an $(n, |C|, t, 1)$ MCF of order q and the puncturing*

$$C' := \{(w_1, \dots, w_{n-1}) \in K^{n-1} | \exists w_n \in K \text{ with } (w_1, \dots, w_n) \in C\}$$

of C is an $(n-1, |C|, t, q)$ MCF of order q.

This theorem is a slightly modified version of a theorem given by Hämäläinen et al. [9]. It yields that the existence of an $(n-1, u, 1, q)$ MCF of order q is necessary for the existence of a code of order q, length n, cardinality u, minimum distance at least 2 and covering radius 1.

In case of $q = n = 4$ and $u = 24$, the existence of the latter code is an open problem. But the necessary condition from above can be satisfied: The code

$$\begin{array}{llllll}
\{(1,1,1), & (1,1,2), & (1,2,1), & (1,2,2), & (1,3,3), & (1,4,4), \\
(2,1,1), & (2,1,2), & (2,2,1), & (2,2,2), & (2,3,4), & (2,4,3), \\
(3,1,4), & (3,2,3), & (3,3,2), & (3,3,4), & (3,4,1), & (3,4,3), \\
(4,1,3), & (4,2,4), & (4,3,1), & (4,3,3), & (4,4,2), & (4,4,4)\}
\end{array}$$

is a (3,24,1,4) MCF of order 4. (No puncturing of the code which was used to establish equation (14) is a $(3, 24, 1, 4)$ MCF.)

Acknowledgement. The author likes to thank J.H. van Lint for giving access to [1].

References

[1] Blokhuis, A.; van Lint, J.H.: *On Codes with Covering Radius* 1 *and Minimum Distance at least* 2. Internal Note, Eindhoven University of Technology, August 1999.

[2] Chen, W.; Honkala, I.S.: *Lower Bounds for q-ary Covering Codes.* IEEE Trans. Inform. Theory **36** (1990), 664–671.

[3] Cohen, G.D.; Karpovsky, M.G.; Mattson, H.F., Jr.; Schatz, J.R.: *Covering Radius – Survey and Recent Results.* IEEE Trans. Inform. Theory **31** (1985), 328–343.

[4] Cohen, G.D.; Lobstein, A.C.; Sloane, N.J.A.: *Further Results of the Covering Radius of Codes.* IEEE Trans. Inform. Theory **32** (1986), 680–694.

[5] Cohen, G.D.; Litsyn, S.N.; Lobstein, A.C.; Mattson, H.F., Jr.: *Covering Radius 1985–1994.* Appl. Algebra Eng. Comm. Comp. **8** (1997), 173–239.

[6] Cohen, G.; Honkala, I.; Litsyn, S.; Lobstein, A.: *Covering Codes.* North-Holland, Amsterdam 1997.

[7] Graham, R.L.; Sloane, N.J.A.: *On the Covering Radius of Codes.* IEEE Trans. Inform. Theory **31** (1985), 385–401.

[8] Habsieger, L.: *Lower Bounds for q-ary Coverings by Spheres of Radius One.* J. Comb. Th., Ser. A, **67** (1994), 199–222.

[9] Hämäläinen, H.O.; Honkala, I.S.; Litsyn, S.N.; Östergård, P.R.J.: *Bounds for Binary Codes that are Multiple Coverings of the Farthest-off Points.* SIAM J. Discr. Math. **8** (1995), 196–207.

[10] Heise, W.; Quattrocchi, P.: *Informations- und Codierungstheorie.* 3. Auflage, Springer, Berlin - Heidelberg 1995.

[11] Honkala, I.; Litsyn, S.: *Generalizations of the Covering Radius Problem in Coding Theory.* Bull. Inst. Comb. **17** (1996), 39–46.

[12] Kalbfleisch, J.G.; Stanton, R.G.: *A Combinatorial Problem in Matching.* J. London Math. Soc. **44** (1969), 60–64; *Corrigendum*, J. London Math. Soc., Second Ser., **1** (1969), 398.

[13] Kalbfleisch, J.G.; Weiland, P.H.: *Some New Results for the Covering Problem.* Recent Prog. Comb., Proc. Third Waterloo Conf. 1968, Academic Press, New York 1969.

[14] van Lint, J.H.: *Recent Results on Covering Problems.* In Mora, T. (ed.): Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Proc. 6th Intern. Conf. (Rome 1988), Springer, Berlin - New York 1989.

[15] MacWilliams, F.J.; Sloane, N.J.A.: *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam - New York - Oxford 1977.

[16] Quistorff, J.: *Simultane Untersuchung mehrfach scharf transitiver Permutationsmengen und MDS-Codes unter Einbeziehung ihrer Substitute.* Habilitationsschrift, Univ. Hamburg 1999; Shaker Verlag, Aachen 2000.

[17] Quistorff, J.: *On Full Partial Quasigroups of Finite Order and Local Cardinal Maximum Codes.* Beiträge Algebra Geom. **40** (1999), 495–502.

[18] Rodemich, E.R.: *Coverings by Rook Domains.* J. Comb. Th. **9** (1970), 117–128.

[19] Stanton, R.G.; Horten, J.D.; Kalbfleisch, J.G.: *Covering Theorems for Vectors with Special Reference to the Case of Four and Five Components.* J. London Math. Soc., Second Ser., **1** (1969), 493–499.

[20] Stojaković, Z.; Ušan, J.: *A Classification of Finite Partial Quasigroups.* Univ. u Novom Sadu Zb. rad. Prirod.-mat. fak., Serija za mat. **9** (1979), 185–190.

[21] van Wee, G.J.M.: *Improved Sphere Bounds on the Covering Radius of Codes.* IEEE Trans. Inform. Theory **34** (1988), 237–245.

[22] van Wee, G.J.M.: *Bounds on Packings and Coverings by Spheres in q-ary and Mixed Hamming Spaces.* J. Comb. Th., Ser. A, **57** (1991), 117–129.

Received July 1, 1999