Integer Programming for Covering Codes

W. Lang
Faculty of Business and Economics
Berlin School of Economics
Badensche Str. 50/51
D-10825 Berlin, Germany
E-mail: wlang@fhw-berlin.de

J. Quistorff, E. Schneider
Department 4
FHTW Berlin (University of Applied Sciences)
D-10313 Berlin, Germany
E-mail: {J.Quistorff,E.Schneider}@fhtw-berlin.de

Abstract

The covering problem in the n-dimensional q-ary Hamming space consists of the determination of the minimal cardinality $K_q(n, R)$ of an R-covering code. It is known that the sphere covering bound can be improved by considering decompositions of the underlying space, leading to integer programming problems. We describe the method in an elementary way and derive about 50 new computational and theoretical records for lower bounds on $K_q(n, R)$.

1 Introduction

Let $Q = \{0, 1, ..., q-1\}$ be a finite set, consisting of q elements, and let $n \in \mathbb{N}$. Consider the n-dimensitional q-ary Hamming space, i.e. the Cartesian power $X := Q^n$, equipped with the Hamming distance: For words $y = (y_1, ..., y_n)$ and $y' = (y'_1, ..., y'_n)$ put

$$d_H(y, y') := |\{x \in \{1, ..., n\} \mid y_x \neq y'_x\}|.$$

A ball (or sphere) of radius R around $y \in X$ is the set of all words with a Hamming distance of at most R from the center y, i.e.

$$B_R(y) := \{y' \in X \mid d_H(y, y') \leq R\}.$$

JCMCC **66** (2008), pp. 279-288

It is easy to see that its volume is

$$V_R := |B_R(y)| = \sum_{k=0}^{R} \binom{n}{k} (q-1)^k.$$

A subset $C \subseteq X$ is called q-ary code of length n, its elements are called codewords. C is furthermore called R-covering, iff the union of balls with radius R around the codewords exhaust the whole space X, i.e. iff

$$\bigcup_{y \in C} B_R(y) = X.$$

The covering problem consists of the determination (or at least estimation) of the minimal cardinality $K_q(n, R)$ of a q-ary R-covering code of length n. Hence, three parameters are involved in this problem. Every explicit construction of an R-covering code implies an upper bound on $K_q(n, R)$. For every lower bound, theoretical or computational arguments are necessary. The standard work on covering codes is Cohen et al. [3]. The presently best known bounds are compiled by Kéri [8].

A very simple lower bound on $K_q(n, R)$ is the sphere covering bound. It is known, that it can be improved in several cases by considering decompositions of the underlying space, leading to integer programming problems. The aim of the present paper is to describe the method in an elementary way and to derive about 50 new computational and theoretical records for lower bounds on $K_q(n, R)$.

The paper is organized as follows: The sphere covering bound and its improvements by decompositions are recalled in Section 2, together with some remarks on the computation we applied throughout the paper. In Section 3, the decomposition of the space into q^2 subspaces, called blocks, is discussed. The induced integer programming problem is presented and 21 new computational records are compiled. Additionally, a new theorem, based on the same decomposition in certain cases, proves another 25 records. In the final section, the decomposition into q^s subspaces with $s \geq 3$ is briefly discussed and a few further computational records are presented.

2 The Sphere Covering Bound and its Improvements by Decompositions

Clearly, each single codeword covers V_R words of the space. If C is an R-covering code of cardinality $u := |C|$ then

$$\bigcup_{y \in C} B_R(y) = X,$$

implying

$$u \cdot V_R = \sum_{y \in C} |B_R(y)| \geq \left| \bigcup_{y \in C} B_R(y) \right| = |X| = q^n$$

and consequently

$$u \geq \left\lceil \frac{q^n}{V_R} \right\rceil .$$

Since these arguments hold for every R-covering code, the sphere covering bound

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

follows. It is possible to improve this bound by decompositions of the space into proper subspaces. This method was introduced by Kamps/Van Lint [6] and Stanton/Kalbfleisch [14]. It has been applied by Östergård et al. [12, 1, 9] and was recently discussed by Kaski/Östergård [7, Section 7.2.2] and, in a more general setting, by Quistorff [13].

If the space is decomposed into q subspaces

$$X_j := \{y \in X \mid y_1 = j\}$$

for $j \in Q$, which might be called bands, the following improvement can be achieved: Each codeword from X_j covers on the one hand

$$V_R^{(0)} := \sum_{k=0}^{R} \binom{n-1}{k} (q-1)^k$$

words of X_j and on the other hand

$$V_R^{(1)} := \sum_{k=0}^{R-1} \binom{n-1}{k} (q-1)^k$$

words of every band $X_{j'}$ with $j' \neq j$. Let C be an R-covering code with $|C| = u$. Put $u_j := |C \cap X_j|$. Clearly, $|C| = \sum_j u_j$. Since every band has to be covered, one gets the following q constraints:

$$u_j \cdot V_R^{(0)} + \sum_{j' \neq j} u_{j'} \cdot V_R^{(1)} \geq |X_j| = q^{n-1}$$

for every $j \in Q$. The pigeon hole principle proves the existence of a band with at most $\left\lfloor \frac{u}{q} \right\rfloor$ codewords, say $u_0 \leq \left\lfloor \frac{u}{q} \right\rfloor$, implying

$$u \cdot V_R^{(1)} + \left\lfloor \frac{u}{q} \right\rfloor \left(V_R^{(0)} - V_R^{(1)} \right) \geq u_0 \cdot V_R^{(0)} + (u - u_0) \cdot V_R^{(1)} \geq q^{n-1}.$$

Hence, we have the following implicit bound, which is due to Hämäläinen according to Chen/Honkala [2, Theorem 5]:

$$K_q(n,R) \cdot V_R^{(1)} + \left\lfloor \frac{K_q(n,R)}{q} \right\rfloor \left(V_R^{(0)} - V_R^{(1)} \right) \geq q^{n-1}. \tag{2}$$

A decomposition of the space into q^s proper subspaces with $2 \leq s \leq n$ leads to an integer programming problem. Solving this problem can imply further improvements of the sphere covering bound, i.e. sharpened lower bounds on $K_q(n,R)$. In case of $s = n$, the integer programming problem is equivalent to the determination of $K_q(n,R)$.

Some remarks on the computation we applied throughout the paper: To create the integer programs, we used a model generator written in Java and kept the generated models as MPS files. MPS is an industry standard, adopted by most commercial codes [11]. To solve the programs, we employed the mixed integer solver Cbc (Coin-or branch and cut) along with Clp (Coin-or linear programming) [4]. Cbc and Clp are projects of the COIN-OR Foundation (COmputational INfrastructure for Operations Research) [5], an open source initiative dedicated to advance open source for the operations research community. For further reading see [10]. The models have been solved on an Intel Core 2 Duo with 2.4 GHz and 4 GB RAM, running SUSE Linux 10.1. The solver runtime increased rapidly with the number q^s of problem variables. Models up to 32 variables were mostly solved within seconds. Larger problems used minutes or hours of cpu time and few problems with 100 or more variables could be solved within a preset time limit of eight hours.

3 Decomposition into Blocks

In this section, the case $s = 2$ is discussed. Let

$$X_{(j_1,j_2)} := \{y \in X \mid y_1 = j_1 \text{ and } y_2 = j_2\}$$

for all $(j_1, j_2) \in Q^2$. These subspaces might be called blocks. It is easy to see that each codeword from $X_{(0,0)}$ covers exactly

$$V_R^{(0)} := \sum_{k=0}^{R} \binom{n-2}{k} (q-1)^k$$

words of $X_{(0,0)}$, exactly

$$V_R^{(1)} := \sum_{k=0}^{R-1} \binom{n-2}{k} (q-1)^k$$

words of each of the $2(q-1)$ blocks $X_{(0,j)}$, $X_{(j,0)}$ with $j \neq 0$, and finally exactly

$$V_R^{(2)} := \sum_{k=0}^{R-2} \binom{n-2}{k} (q-1)^k$$

words of each of the $(q-1)^2$ blocks $X_{(j_1,j_2)}$ with $j_1 \neq 0 \neq j_2$. Similar statements hold for every codeword from any other block. Let C be an R-covering code. Put $u_{(j_1,j_2)} := |C \cap X_{(j_1,j_2)}|$. Clearly, $|C| = \sum_{j_1,j_2} u_{(j_1,j_2)}$. Since every block has to be covered, one gets q^2 constraints of the following type:

$$u_{(0,0)} \cdot V_R^{(0)} + \sum_{j \neq 0} \left(u_{(0,j)} + u_{(j,0)}\right) \cdot V_R^{(1)} + \sum_{j_1 \neq 0 \neq j_2} u_{(j_1,j_2)} \cdot V_R^{(2)} \geq q^{n-2}, \quad (3)$$

one for every $(j_1, j_2) \in Q^2$. Note that each $u_{(j_1,j_2)}$ is a non-negative integer $\leq q^{n-2}$. Together with the objective function

$$z := \sum_{j_1,j_2} u_{(j_1,j_2)} \to \min, \quad (4)$$

the constraints form an integer programming problem. Its solution $z^{(IP)}$ satisfies $K_q(n, R) \geq z^{(IP)}$.

Since the integer programming problem is non-trivial, it is worth to consider the linear programming problem (3), (4) with real $u_{(j_1,j_2)} \geq 0$ which can be solved easily as a consequence of the symmetry of the problem. Denote its solution by $z^{(LP)}$. Additionally, an upper bound on $z^{(IP)}$ is given in the following theorem.

Theorem 1.

$$\frac{q^n}{V_R} = z^{(LP)} \leq z^{(IP)} \leq q^2 \cdot \left\lceil \frac{q^{n-2}}{V_R} \right\rceil.$$

Proof. The sum of all q^2 inequalities of (3) shows on the one hand $z^{(LP)} = \sum_{j_1,j_2} u_{(j_1,j_2)} \geq \frac{q^n}{V_R}$. On the other hand, it is easy to see that $u_{(j_1,j_2)} = \frac{q^{n-2}}{V_R}$ for all (j_1, j_2) satisfies (3), leading to $z^{(LP)} \leq \frac{q^n}{V_R}$. Since the linear programming problem is a relaxation of the integer programming problem, $z^{(LP)} \leq z^{(IP)}$ follows. Clearly, $u_{(j_1,j_2)} = \left\lceil \frac{q^{n-2}}{V_R} \right\rceil \in \mathbb{N}$ for all (j_1, j_2) satisfies (3), yielding $z^{(IP)} \leq q^2 \cdot \left\lceil \frac{q^{n-2}}{V_R} \right\rceil$. □

In Table 1, our 21 new computational records are compiled. The case $q = 3$, $n = 11$, $R = 3$ is further improved in Section 4.

Table 1: New Computational Lower Bounds on $K_q(n,R)$ for $s=2$

q	n	R	Sphere Covering Bound (1)	Implicit Bound (2)	Old Bound [8]	New Bound $z^{(IP)}$	$q^2 \cdot \left\lceil \frac{q^{n-2}}{V_R} \right\rceil$
3	11	3	114	114	115	116	117
4	9	1	9363	9364	9365	9368	9376
4	9	2	745	747	748	751	752
5	5	2	18	20	20	21	25
5	8	2	813	815	815	821	825
5	8	3	97	98	98	99	100
5	8	4	18	20	20	21	25
5	9	4	52	53	53	55	75
5	10	3	1157	1160	1161	1163	1175
5	11	5	86	87	87	90	100
6	5	2	29	30	30	33	36
6	6	2	115	117	119	120	144
6	6	3	17	18	18	19	36
6	7	3	57	60	60	62	72
6	8	4	33	35	35	36	36
7	5	2	43	45	45	47	49
7	7	3	99	100	100	101	147
7	8	4	56	56	57	58	98
7	9	2	29870	29871	29871	29889	29890
8	9	5	55	56	57	58	64
8	10	6	37	39	39	40	64

If the number of problem variables is too large, solving the integer programming problem is not practical. In certain cases, the following new theorem is useful which is also based on decompostions into blocks. The results are at most as good as the integer programming. Note that $K_q(n,R) \geq q$ if $n > R$ is well-known, see Cohen et al. [3, Theorem 3.7.1].

Theorem 2. *Let $n > R$ and $u \in \mathbb{N}$ with $q \leq u < q^2$. Put $\alpha := \left\lfloor \frac{u}{q} \right\rfloor \geq 1$ and*

$$\beta := \left\lceil \frac{q^{n-2} - u \cdot V_R^{(2)}}{V_R^{(1)} - V_R^{(2)}} \right\rceil = \left\lceil \frac{q^{n-2} - u \cdot V_R^{(2)}}{\binom{n-2}{R-1}(q-1)^{R-1}} \right\rceil$$

as well as $\delta := \left\lfloor \frac{\min\{u-(q-\alpha)\cdot(\beta-\alpha),u\}}{\alpha} \right\rfloor$. If $u < (q-\alpha)\cdot(\beta-\alpha)$ or ($\delta < \min\{q,\beta\}$ and $u < (q-\delta)\cdot(\beta-\delta)$) then $K_q(n,R) \geq u+1$.

Proof. Let $C \subseteq Q^n$ with $|C| \leq u$ be an R-covering code. Put $u_{(i,\bullet)} := \sum_{j=0}^{q-1} u_{(i,j)}$ and $u_{(\bullet,j)} := \sum_{i=0}^{q-1} u_{(i,j)}$. The pigeon hole principle proves the existence of a horizontal band with at most $\alpha < q$ codewords, say $u_{(0,\bullet)} \leq \alpha$. W.l.o.g., let $u_{(0,\alpha)} = ... = u_{(0,q-1)} = 0$. For every $j \in \{\alpha, ..., q-1\}$, a constraint of type (3) implies

$$
\begin{aligned}
& 0 \cdot V_R^{(0)} + \left(u_{(0,\bullet)} + u_{(\bullet,j)}\right) \cdot V_R^{(1)} + \left(|C| - u_{(0,\bullet)} - u_{(\bullet,j)}\right) \cdot V_R^{(2)} \geq q^{n-2} \\
\Rightarrow \quad & u_{(\bullet,j)} \cdot \left(V_R^{(1)} - V_R^{(2)}\right) \geq q^{n-2} - |C| \cdot V_R^{(2)} - u_{(0,\bullet)} \cdot \left(V_R^{(1)} - V_R^{(2)}\right) \\
\Rightarrow \quad & u_{(\bullet,j)} \cdot \left(V_R^{(1)} - V_R^{(2)}\right) \geq q^{n-2} - u \cdot V_R^{(2)} - \alpha \cdot \left(V_R^{(1)} - V_R^{(2)}\right) \\
\Rightarrow \quad & u_{(\bullet,j)} \geq \beta - \alpha.
\end{aligned}
$$

Thus,

$$u \geq |C| = \sum_{j=0}^{q-1} u_{(\bullet,j)} \geq \sum_{j=\alpha}^{q-1} u_{(\bullet,j)} \geq (q-\alpha) \cdot (\beta - \alpha).$$

Let $\delta < \min\{q, \beta\}$. The pigeon hole principle also proves the existence of a vertical band, labeled by $j \in \{0, ..., \alpha - 1\}$, with at most $\delta < q$ codewords, say $u_{(\bullet,0)} \leq \delta$. W.l.o.g., let $u_{(\delta,0)} = ... = u_{(q-1,0)} = 0$. For every $i \in \{\delta, ..., q-1\}$, a constraint of type (3) implies

$$
\begin{aligned}
& 0 \cdot V_R^{(0)} + \left(u_{(i,\bullet)} + u_{(\bullet,0)}\right) \cdot V_R^{(1)} + \left(|C| - u_{(i,\bullet)} - u_{(\bullet,0)}\right) \cdot V_R^{(2)} \geq q^{n-2} \\
\Rightarrow \quad & u_{(i,\bullet)} \cdot \left(V_R^{(1)} - V_R^{(2)}\right) \geq q^{n-2} - |C| \cdot V_R^{(2)} - u_{(\bullet,0)} \cdot \left(V_R^{(1)} - V_R^{(2)}\right) \\
\Rightarrow \quad & u_{(i,\bullet)} \cdot \left(V_R^{(1)} - V_R^{(2)}\right) \geq q^{n-2} - u \cdot V_R^{(2)} - \delta \cdot \left(V_R^{(1)} - V_R^{(2)}\right) \\
\Rightarrow \quad & u_{(i,\bullet)} \geq \beta - \delta.
\end{aligned}
$$

Thus,

$$u \geq |C| = \sum_{i=0}^{q-1} u_{(i,\bullet)} \geq \sum_{i=\delta}^{q-1} u_{(i,\bullet)} \geq (q-\delta) \cdot (\beta - \delta).$$

The assumption follows by contraposition. □

Example: Consider $q = 7$, $n = 6$, $R = 3$, implying $V_3^{(1)} = 241$ and $V_3^{(2)} = 25$. In case of $u = 27$, we have $\alpha = 3$, $\beta = \left\lceil \frac{2401 - 27 \cdot 25}{241 - 25} \right\rceil = 8$, $\delta = 2$. Since $27 < 5 \cdot 6$, the bound $K_7(6,3) \geq 28$ follows.

Table 2: New Lower Bounds on $K_q(n, R)$ by Theorem 2

q	n	R	Old Bound	New Bound
6	9	5	23	24
7	6	3	27	28
7	7	4	17	19
7	10	6	26	27
8	6	3	37	40
9	6	3	50	52
9	7	4	31	35
10	6	3	66	70
10	7	4	41	42
11	7	4	55	56
12	7	4	67	71
13	7	4	84	87
13	8	5	57	60
14	7	4	99	107
14	8	5	69	70
15	7	4	123	125
15	8	5	80	88
16	7	4	144	147
16	8	5	96	100
17	8	5	114	120
18	8	5	133	141
19	7	4	233	234
19	8	5	152	158
20	8	5	180	184
21	8	5	204	210

4 Further Decompositions

In this section, the case $s \geq 3$ is briefly discussed, analogously to $s = 2$ in Section 3. Let

$$X_{(j_1,\ldots,j_s)} = \{y \in X \mid y_1 = j_1 \text{ and } \ldots \text{ and } y_s = j_s\}$$

for all $(j_1, \ldots, j_s) \in Q^s$. Each codeword from $X_{(0,\ldots,0)}$ covers exactly

$$V_R^{(0)} := \sum_{k=0}^{R} \binom{n-s}{k} (q-1)^k$$

words of $X_{(0,\ldots,0)}$, exactly

$$V_R^{(1)} := \sum_{k=0}^{R-1} \binom{n-s}{k} (q-1)^k$$

words e.g. of $X_{(1,0,\dots,0)}$, and so on. Similar statements hold for every codeword from any other block. Let C be an R-covering code. Put $u_{(j_1,\dots,j_s)} := |C \cap X_{(j_1,\dots,j_s)}|$. Clearly, $|C| = \sum_{j_1,\dots,j_s} u_{(j_1,\dots,j_s)}$. Since every $X_{(j_1,\dots,j_s)}$ has to be covered, one gets q^s constraints of the following type:

$$u_{(0,0)} \cdot V_R^{(0)} + \dots + \sum_{j_1 \neq 0,\dots,j_s \neq 0} u_{(j_1,\dots,j_s)} \cdot V_R^{(s)} \geq q^{n-s}.$$

The objective function is

$$z := \sum_{j_1,\dots,j_s} u_{(j_1,\dots,j_s)} \to \min .$$

Table 3 compiles four further computational records.

Table 3: New Computational Lower Bounds on $K_q(n, R)$ for $s \geq 3$

q	n	R	s	Old Bound	New Bound
3	9	3	3	25	27
3	11	3	3	116	117
3	13	3	3	611	612
2	14	2	4	157	159

References

[1] Bertolo, R. / Östergård, P.R.J. / Weakley, W.D.: An Updated Table of Binary/Ternary Mixed Covering Codes, *J. Combin. Des.*, 12 (2004), 157-176.

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

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

[4] COIN-OR Branch-and-Cut MIP Solver, `http://projects.coin-or.org/Cbc`.

[5] COmputational INfrastructure for Operations Research, `http://www.coin-or.org/`.

[6] Kamps, H.J.L. / van Lint, J.H.: The Football Pool Problem for 5 Matches, *J. Combin. Theory*, 3 (1967), 315-325.

[7] Kaski, P. / Östergård, P.R.J.: *Classification Algorithms for Codes and Designs*, Springer, Berlin, Heidelberg, New York, 2006.

[8] Kéri, G.: Tables for Covering Codes, http://www.sztaki.hu/~keri/codes/, download on November 24, 2006.

[9] Kéri, G. / Östergård, P.R.J.: Further Results on the Covering Radius of Small Codes, *Discrete Math.*, 307 (2007), 69-77.

[10] Lougee-Heimer, R.: The Common Optimization INterface for Operations Research, *IBM J. Res. Dev.*, 47 (2003), 57-66.

[11] MPS Input Format, http://www-fp.mcs.anl.gov/otc/Guide/OptWeb/continuous/constrained/linearprog/mps.html.

[12] Östergård, P.R.J. / Blass, U.: On the Size of Optimal Binary Codes of Length 9 and Covering Radius 1, *IEEE Trans. Inform. Theory*, 47 (2001), 2556-2557.

[13] Quistorff, J.: Improved Sphere Bounds in Finite Metric Spaces, *Bull. Inst. Combin. Appl.*, 46 (2006), 69-80.

[14] Stanton, R.G. / Kalbfleisch, J.G.: Intersection Inequalities for the Covering Problem, *SIAM J. Appl. Math.*, 17 (1969), 1311-1316.