Electronic Delivery Cover Sheet

NOTICE WARNING CONCERNING COPYRIGHT RESTRICTIONS

The copyright law of the United States (Title 17, United States Code) governs the making of photocopies or other reproductions of copyrighted materials.

Under certain conditions specified in the law, libraries and archives are authorized to furnish a photocopy or other reproduction. One of these specified conditions is that the photocopy or reproduction is not to be "used for any purpose other than private study, scholarship, or research." If a user makes a request for, or later uses, a photocopy or reproduction for purposes in excess of "fair use," that user may be liable for copyright infringement.

This institution reserves the right to refuse to accept a copying order if, in its judgment, fulfillment of the order would involve violation of copyright law.

This notice is posted in compliance with
Title 37 C. F. R., Chapter II, Part 201.14
Borrower: VPI

Lending String: "VA@,VA@,VGM,NOC,NOC

Patron: Chung, Woocheol ;DEPT; ;STAT;

Journal Title: Problems of control and information theory. Problemy upravlenièila i teorii informaètisii.

Volume: 12 Issue: 1
Month/Year: 1983 Pages: 3-10

Article Author:

Article Title: V.A. Zinoviev.; Cascade equal-weight codes and maximal packings

Imprint: Budapest, Akadáemiai Kiadó.

ILL Number: 7091545
PROBLEMS OF CONTROL AND INFORMATION THEORY

An international bi-monthly sponsored jointly by the Presidium of the Academy of Sciences of the USSR, of the Hungarian Academy of Sciences and of the Czechoslovak Academy of Sciences. The six issues published per year make up a volume of some 480 pp. It offers publicity for original papers and short communication of the following topics:

- theory of control processes
- general system theory
- information theory
- theory of decisions and estimates; queueing theory
- theory of adaptive systems, identification, learning and pattern recognition.

While this bi-monthly is mainly a publication forum of the research results achieved in the socialist countries, also papers of international interest from other countries are welcome.

Distributors

For the Soviet Union:

SOYUZPECHATY, Moscow 123 308 USSR

For Albania, Bulgaria, China, Cuba, Czechoslovakia, German Democratic Republic, Korean People's Republic, Mongolia, Poland, Romania, Vietnam and Yugoslavia
KULTURA Hungarian Foreign Trading Co.
P. O. Box 149 H–1389 Budapest, Hungary

For all other countries

PERGAMON PRESS LTD, Headington Hill Hall, Oxford OX3 OBW, England
or
PERGAMON PRESS INC, Maxwell House, Fairview Park, Elmsford, NY 10523, USA
1983 Subscription Rate US Dollars 140.00 per annum including postage and insurance.

ПРОБЛЕМЫ УПРАВЛЕНИЯ И ТЕОРИИ ИНФОРМАЦИИ

Международный журнал Академии наук СССР, Венгерской Академии наук и Чехословацкой Академии наук выходит 6 раз в год общим объемом 480 печатных страниц.
В журнале публикуются оригинальные научные статьи и статьи обзорного характера по следующим проблемам управления и теории информации:

- теория процессов управления,
- общая теория систем,
- теория информации,
- теория принятия решений и оценки;
- теория массового обслуживания,
- теория адаптивных систем, идентификации, обучения и распознавания образов.

Целью журнала является ознакомление научной общественности различных стран с важнейшими проблемами, имеющими актуальный и перспективный характер, научными достижениями ученых социалистических и других стран.
CASCADE EQUAL-WEIGHT CODES AND MAXIMAL PACKINGS

V. A. ZINOVIEV

(Received April 30, 1982)

The general method of construction of equal-weight codes with given weight and minimal distance is presented. The power of such code differs from upper Johnson bound only by the multiplicative constant which does not depend on the length of the code. This constant tends to unity when some conditions between the weight and distance are valid.

1. Introduction

Denote by \( A(n, d, w) \), \( d = 2\delta \), the maximal possible power of binary equal-weight code of length \( n \), Hamming distance \( d \) and weight of the code words \( w \). This value is studied also in combinatorics under the name maximal packing \( m(n, w, k) \), \( 1 \leq k \leq w \leq n \) \([1–5]\). Define this value. Let \( E^n \) be the set of all the binary vectors of length \( n \) and \( E^n_k \) be the subset of \( E^n \) containing all such vectors of weight \( w \). Say that the vector \( x = (x_1, \ldots, x_n) \), \( x \in E^n_k \), covers the vector \( y = (y_1, \ldots, y_n) \), \( y \in E^n_k \), \( k \leq w \), if the equality \( x_i - y_i = y_i \) is valid for all \( i = 1, \ldots, n \). Define

\[
m(n, w, k) = \max \{|V| : V \subseteq E^n_k\}
\]

and any vector \( y, y \in E^n_k \), is covered at most by one vector \( x, x \in V \). The problem consists in studying of the value \( m(n, w, k) \) as a function of parameters \( n, w, k \).

Firstly, let us note (it is known rather well) that the following equality is valid

\[
m(n, w, k) = A(n, 2(w - k + 1), w) \quad (1.1)
\]

It is necessary to note that in combinatorics this value is studied mainly for fixed (or slowly growing) parameters \( w \) and \( k \) and for growing \( n \), but in the coding theory (see, for example, references in [6]) this value is considered mainly for the cases, when \( w \) and \( k \) depend linearly on \( n \), when \( n \) grows to infinity. Nevertheless, the known results of error correcting codes allow us to obtain bounds for the value \( m(n, w, k) \) for fixed \( w \) and \( k \) which had been shown in \([5]\).

From the well-known Johnson upper bound \([7]\)

\[
m(n, w, k) \leq \binom{n}{k} / \binom{w}{k} \quad (1.2)
\]
Let us define

$$\mu(n, w, k) = m(n, w, k) \frac{w}{k} \left(\frac{n}{k}\right).$$

Erdős and Hanani [1] suggested that for fixed $w$ and $k$

$$\lim_{n \to \infty} \mu(n, w, k) = 1$$

and they proved it for the case $k = 2$ and all $w$ and for the case $k = 3$ and $w = q$ or $w = q + 1$, where $q$ is a prime power. Kuzurin [3] proved this conjecture for the case when $k = w - 1$. Furthermore, he proved it not only for fixed $w$ but for $w = 0(n)$ (he showed that in these cases usual limits also exist).

In [5] it was shown that

$$\lim_{n \to \infty} \mu(n, w, w - 2) = 1, \quad \text{when } w = 0(n)$$

and for $k \leq w - 3$ when $w - k$ is fixed

$$\lim_{n \to \infty} \mu(n, w, k) \geq 1/(w - k)!, \quad \text{when } w = 0(n). \quad (1.3)$$

In terms of codes the result obtained in [5] means: for length $n = 2^s - 1, s = 2, 3, \ldots$,

$$A(n, 2\delta, w) \geq \left(\frac{n}{w}\right) / (n + 1)^{\delta - 1}. \quad (1.4)$$

In [8], Graham and Sloane gave several constructions for equal-weight codes, using some mapping from $E^*_w$ to Galois fields GF$(q)$. In particular they proved, that if $q$ is a prime power such that $q \geq n$ then

$$A(n, 2\delta, w) \geq \left(\frac{n}{w}\right) / q^{\delta - 1}. \quad (1.5)$$

Note that bound (1.4) is coincident with (1.5) for the case $q = n + 1 = 2^s$ and they are good for the small $\delta$. It is possible to see from the following asymptotic expression of upper bound (1.2) and lower bounds (1.4) and (1.5) that, when $w$ is fixed and $n \to \infty$:

$$n^{w - \delta + 1} / w! \leq A(n, 2\delta, w) \leq n^{w - \delta + 1} (\delta - 1)! / w! . \quad (1.6)$$

We need also the result of Kuzurin [4]. Let $q = q(a)$ denote maximal prime power which is not more than $a$. From the number theory it is known [9] that for every $\varepsilon > 0$ it is possible to find $a_\varepsilon$ such as for any $a > a_\varepsilon$ the following inequality is valid:

$$|q(a) - a| \leq a^{7/12 + \varepsilon}.$$
Kuzurin proved the following result. Let \( w = w(n) \) and \( k = k(n) \) of positive integers have the properties:

1. \( w(n) \to \infty \), when \( n \to \infty \) and constant \( c, c > 7/12 \), exists such that for enough large \( n \) the following inequality is valid
   \[
   w^2 + n^2 - w^1 - c - (n - w) < 0;
   \]
2. \( k(n)/\sqrt{w(n)} \to 0 \) when \( n \to \infty \);
3. \( k(n)/(n/w(n))^{1-c} \to 0 \) when \( n \to \infty \).

Then

\[
\lim_{n \to \infty} m(n, w, k) w^k/n^k = 1. \quad (1.7)
\]

Let us emphasize that all lower bounds (1.4)–(1.6) and Kuzurin’s theorem are existence theorems stating that to construct corresponding codes it is necessary to make an overall choice over all possible vectors of \( E^n_w \).

The aim of this paper is to present a general and quite simple method of constructing of equal-weight codes with given weight and minimal distance. The power of such code differs from upper Johnson bound (1.2) only in a multiplicative constant, which does not depend from the length of the code. Unlike the codes satisfying lower bounds (1.4) and (1.5), this constant grows to unity when the weight of the code words grows and some conditions between length, weight and distance are valid. On the other side the codes and equivalent maximal packings obtained are good for some finite lengths. It is also essential that this method is constructive in such a sense that for the construction of code we have no overall choice in the set \( E^n_w \) and the complexity of the construction of the code is not more than \( c n^3 \) binary operations, where the constant \( c \) does not depend on \( n, w, \) and \( \delta \), and the binary operation is the arithmetic operation in GF(2). In particular, the result of Kuzurin mentioned above is obtained constructively.

The results of this paper have been partially published in [10] without proofs and presented at the International Symposium of Information Theory (Oberwolfach, FRG, 4–10 April, 1982). The author sincerely thanks V. I. Levenshtein and L. A. Bassalygo for their useful comments which helped much to improve the present paper.

2. The main construction

Theorem 1. Let \( q \) is a prime power such that \( q + 1 \geq w \). Then for any \( \delta, 1 \leq \delta \leq w \) and \( n = qw \)

\[
A(n, 2\delta, w) \geq (n/w)^{w-\delta+1}; \quad (2.1)
\]
bound (2.1) is better than bounds (1.4), (1.5) when \( \delta > 1/2 + w/\ln w \) and the complexity of the construction of such a code is not more than \( cn^2 \) binary operations, where \( c \) does not depend on \( n, w, \delta \).

**Proof.** Let \( w \) be given, \( \delta \) be any integer, \( 1 \leq \delta \leq w \), and \( q \) be prime power such that \( q + 1 \geq w \). Consider MDS code (see [6]) \( R \) over Galya field \( GF(q) \) with the following parameters: the length \( n' = w \), the number of information symbol \( k = w - \delta + 1 \), the code (Hamming) distance \( d' = n' - k + 1 = \delta \). The code \( R \) with parameters \( n', k, d' \) is denote by \( R = R(n', k, d') \). Now, construct the cascade constant weight code \([11]\) using the code \( R \) as outer code and the trivial constant weight code whose code words form the identity matrix \( I_q \) of order \( q \) as inner code. In other words, we perform the following transformation over all words of code \( R \). Denote by \( a_1, a_2, \ldots, a_q \) the elements of \( GF(q) \) ordered in some fixed manner. In the code word \((a_1, \ldots, a_w) \in R \) we replace each element \( a_i \) by the \( i \)-th row of matrix \( I_q \) (or by binary vector of length \( q \) and weight \( 1 \), where the unit is in the position with number \( i \)). It is clear that the resultant binary code (denote this code by \( C \)) has length \( n = n'q = qw \), each code word has weight \( w \), the distance between any two different words is not less then \( 2d' = 2\delta \) and the power of the code is equal \( q^w = q^{w-\delta+1} \). It corresponds to lower bound (2.1). Compare values (1.4), (1.5) and (2.1). We have

\[
\binom{n}{w} q^{\delta - 1} < n^{w-\delta+1}/w!,
\]

when \( w > 1 \). The condition

\[
(n/w)^{w-\delta+1} > n^{w-\delta+1}/w!
\]

is equivalent to

\[
w! > w^{w-\delta+1},
\]

and is valid, when \( \delta > 1/2 + w/\ln w \). The value of complexity of the construction follows immediately from [12]. According to our terms, this complexity is not more than \( cn^2 \). The theorem is proved.

**Theorem 2.** Let \( q = q_1 \cdots q_s \), where for each \( i, i = 1, \ldots, s \), \( q_i \) is a prime power such that \( q_i + 1 \geq w \). Then for every \( \delta, 1 \leq \delta \leq w \), and \( n = qw \), inequality (2.1) is valid.

**Proof.** Consider for each \( i, i = 1, \ldots, s \), the MDS code \( R_i = R_i(w, k, \delta) \), \( k = w + 1 - \delta \), over \( GF(q_i) \). Then the direct product of codes \( R_1, \ldots, R_s \) is MDS code \( R = R(w, k, \delta) \) over the alphabet of size \( q = q_1 \cdots q_s \), and further considerations are similar to the proof of theorem 1.

In terms of maximal packings, Theorems 1 and 2 can be formulated in the following manner. For any \( w \) and \( k \), \( 1 \leq k \leq w \), and for suitable \( n = qw \), where \( q \) satisfies the co

In the ne

on n and obt

In this p

and k, \( \delta \) are an

the values sim

Lemma.

Proof. F

using Theore

Lemma.

Proof. C

elements of GI

q - r elements

\( a_1, \ldots, a_{q-r-1} \)

vectors all suc:

elements. As a

length k over C

Conversion of

Theorem 1 (c)

alphabets of si

Lemma.

prime power s
satisfies the conditions of Theorem 1 or 2,

\[ \mu(n, w, k) \geq \frac{w-1}{w} \cdot \frac{w-2}{w} \cdot \ldots \cdot \frac{w-k+1}{w}. \]  

(2.2)

In the next paragraph we shall get rid of the discreteness of bounds (2.1) and (2.2) on \( n \) and obtain lower bounds for \( A(n, 2\delta, w) \) and \( m(n, w, k) \) which conform to \( n \).

3. Modification of the main construction

In this paragraph, for given \( w \) let the number \( q \) satisfy the conditions of theorem 1 and \( k, \delta \) are any numbers, \( 1 \leq k, \delta \leq w, k + \delta = w + 1 \). The following simple lemmas yield the values similar to (2.1) for any length \( n \).

**Lemma 1.** Let \( n = qw + \gamma \). Then

\[ A(n, 2\delta, w) \geq \left( \frac{n}{w} \right)^k \left( 1 - \frac{\gamma}{n} \right)^k, \quad k = w + 1 - \delta. \]

(3.1)

**Proof.** For \( n' = qw \) let us construct a cascade constant weight code satisfying (2.1), using Theorem 1. Addition to this code \( \gamma \) zero positions gives the value (3.1).

**Lemma 2.** Let \( n = qw - \gamma \), where \( \gamma < k(q-1) \) and \( \gamma = kr + t \), where \( 0 \leq t < k \). Then

\[ A(n, 2\delta, w) \geq \left( \frac{n}{w} \right)^k \left( 1 + \frac{\gamma}{n} \right)^k \left( 1 - \frac{r}{q} \right)^{k-t} \left( 1 - \frac{r+1}{q} \right)^k. \]

(3.2)

**Proof.** Consider MDS code \( R = R(w, k, \delta) \) over GF(q). Let \( x_1, \ldots, x_q \) denote elements of GF(q). Fix the first \( k \) positions of the code \( R \). In the first \( k-t \) positions fix \( q-r \) elements \( x_1, \ldots, x_{q-r} \) and in the following \( t \) positions fix \( q-r-1 \) elements \( x_{q-r}, \ldots, x_q \). Form the new code (denote it by \( R(\gamma) \)) of the same length \( w \), take as code vectors all such words from \( R \) which have in the first \( k \) positions only the fixed elements. As any \( k \) positions of MDS code \( R(w, k, \delta) \) (see [6]) contain each vector of length \( k \) over GF(q) exactly once, the power of code \( R(\gamma) \) is equal to \((q-r)^k - (q-r-1)^k\).

Conversion of the code \( R(\gamma) \) into cascade constant weight code, using the proof of Theorem 1 (considering only that the first \( k \) positions of the code \( R(\gamma) \) have the alphabets of sizes \( q-r \) and \( q-r-1 \), gives value (3.2).

**Lemma 3.** Let \( n = qw - \gamma = (q(v) - \Delta)w - \gamma \), where \( \gamma \leq w \) and \( q(v) \) is the minimum prime power such that \( q(v) \geq v \). Then

\[ A(n, 2\delta, w) \geq \left( \frac{n}{w} \right)^k \left( 1 - \frac{\Delta}{q(v)} \right)^{k-1} \left( 1 - \frac{1}{q(v) - \Delta} \right)^\gamma. \]

(3.3)
Proof. Let \( n = vw - \gamma = (q(v) - \Delta)w - \gamma \) and let \( q = q(v) \). Consider the partition of space all \( q^w \) vectors of length \( w \) over GF\( (q) \) on \( q^{w-k} \) cosets of MDS code \( R = R(w, k, \Delta) \). In the first \( \gamma \) positions of such vectors fix \( q - \Delta - 1 \) elements of GF\( (q) \) and in last \( w - \gamma \) positions of such vectors fix \( q - \Delta \) elements of GF\( (q) \). In every coset let’s consider all vectors over fixed elements of GF\( (q) \). As there are \( (q - \Delta - 1)(q - \Delta)^{w-\gamma} \) such vectors in all and they are distributed in \( q^{w-k} \) different cosets then there exists wittingly the code (denote it by \( R(D) \)) of length \( w \) with code distance \( \delta \) and of power \( (q - \Delta - 1)(q - \Delta)^{w-\gamma}/q^{w-k} \). This code \( R(D) \) has the alphabet of the size \( q - \Delta - 1 \) in the first \( \gamma \) positions and the alphabet of the size \( q - \Delta \) in the last \( w - \gamma \) positions. Conversion of the code \( R(D) \) into cascade code gives the value (3.3).

4. Asymptotic bounds of \( A(n, 2\delta, w) \)

In this paragraph, let \( w = w(n), k = k(n) \) denote the sequences of positive integers, which are growing if \( n \) grows. It is clear from (3.1) that if \( \gamma k = O(n) \) when \( n \to \infty \) then the lower bound \( A(n, 2\delta, w) \) has the order \( (n/w)^k \), \( k = w + 1 - \delta \). Let us estimate at growth of \( \gamma \) in Lemma 1. Theorem 1 is applied, when \( w(n) \) grows not more than \( \sqrt{n}/2 \). It means that the number \( v, v = [n/w] \), grows when \( n \) grows. It is known [9] that for any \( \varepsilon > 0 \) as small as possible it is possible to find \( v \), such that for any \( v > v \), the following inequality is valid: \( |q(v) - v| \leq q(v)^{5/12 - \varepsilon} \) where \( q(v) \) is the closest to \( v \) prime power such that \( q(v) \geq v \). So for \( n, n \leq v, v \longmapsto v, v \) large enough, the number \( \gamma \) in Lemma 1 satisfies the inequality \( \gamma \leq q(v)^{5/12 + \varepsilon} \), and the number \( \Delta \) in Lemma 3 satisfies the inequality \( \Delta < q(v)^{7/12 + \varepsilon} \). Thus from this considerations and Lemmas 1 and 3 we have the following results.

Lemma 4. Let (1) \( w(n) \leq \sqrt{n}/2 \); (2) \( k(n) = O\left(\left(\frac{n}{w(n)}\right)^{5/12 - \varepsilon}\right) \).

Then

\[
\lim_{n \to \infty} A(n, 2\delta, w) \left(\frac{w}{n}\right)^k \geq 1, \quad \delta = w + 1 - k,
\]

moreover the complexity of the construction for the length \( n \) is not more then \( cn^3 \) binary operations.

Lemma 5. Let (1) \( w(n) = O(\sqrt{n}) \); (2) \( w(n) - k(n) = O\left(\left(\frac{n}{w(n)}\right)^{5/12 - \varepsilon}\right) \).

Then the inequality (4.1) is valid.

Let us consider the asymptotic of the upper Johnson bound (1.2). From (1.2) we have

\[
A(n, 2\delta, w) \leq \left(\frac{n}{w}\right)^k \frac{w}{w-1} \frac{w}{w-2} \ldots \frac{w}{w-k+1},
\]

\[
k = w + 1 - \delta.
\]
and let \( q = q(v) \). Consider the partition of \( q^{w-\gamma} \) cosets of MDS code \( R = R(w, k, \delta) \) into \( \Delta - 1 \) elements of \( \text{GF}(q) \) and in last \( w-\gamma \) s of \( \text{GF}(q) \). In every coset let's consider all \( \gamma \) vectors \( (q-\Delta-1)^w(q-\Delta)^w \) such vectors in t cosets then there exists wittingly the code distance \( \delta \) and of power \( (q-\Delta-1)^w \) alphabet of the size \( q-\Delta-1 \) in the first \( \Delta \) in the last \( w-\gamma \) positions. Conversion of value (3.3).

The nds of \( A(n, 2\delta, w) \)

\( n = 0 \) denote the sequences of positive integers, \( n (3.1) \) that if \( n \rightarrow \infty \) then \( n = 0 \). Let us estimate at growth of \( n \) grows not more than \( \sqrt{n/2} \). It means that \( s \). It is known [9] that for any \( v > 0 \) as small it for any \( v > v \), the following inequality is closest to \( v \) prime power such that \( q(v) \geq v \).

\[ (n) = 0 \left( \frac{n}{w(n)} \right)^{5/12 - \varepsilon}, \]

\[ 
\geq 1, \quad \delta = w + 1 - k, \quad (4.1)
\]

\[ \text{wion for the length } n \text{ is not more then } cn^3 \]

\[ \text{wion for the length } n \text{ is not more then } cn^3 \]

\[ w(n) - k(n) = 0 \left( \frac{n}{w(n)} \right)^{5/12 - \varepsilon}, \]

\[ 
\text{upper Johnson bound (1.2). From (1.2) we}
\]

\[ \frac{w}{w - 2} \ldots \frac{w}{w + k - 1}, \]

\[ 1 - \delta. \quad (4.2) \]

So the following result is valid.

**Lemma 6.** Let \( k(n) = 0(\sqrt{w(n)}) \). Then

\[ \lim_{n \to \infty} A(n, 2\delta, w) \left( \frac{w}{n} \right)^k \leq 1, \quad k = w + 1 - \delta. \quad (4.3) \]

From Lemmas 4 and 6 we have the following result, which is coincident with the result of Kuzurin [4] and which is its constructive analog.

**Theorem 3.** Let

1. \( w(n) \to \infty \) if \( n \to \infty \) moreover \( w(n) \leq \sqrt{n/2} \);
2. \( k(n) = 0(\sqrt{w(n)}) \);
3. \( k(n) = 0(n/w(n))^{5/12 - \varepsilon} \). Then

\[ \lim_{n \to \infty} A(n, 2\delta, w) \left( \frac{w}{n} \right)^k = 1, \quad k = w + 1 - \delta, \quad (4.4) \]

moreover the complexity of the code construction for length \( n \) is not more then \( cn^3 \) binary operations.

**References**

Каскадные равновесные коды и максимальные упаковки
В. А. Зиновьев
(Москва)

В работе предложен каскадный метод построения широкого класса двоичных равновесных кодов или эквивалентных им максимальных упаковок. Мощность такого кода или соответствующей максимальной упаковки лишь на мультипликативную константу отличается от верхней границы Джонсона. Когда длина кода неограниченно возрастает, эта константа стремится к единице при соответствующих ограничениях на рост веса и расстояния.

В. А. Зиновьев
Институт проблем передачи информации АН СССР
СССР, 101447, Москва, ГСП-4
ул. Ермоловой, 19.

Several a coordinate parameter may either make the system parameter being described by variable systems these properties.
When the general form without using that loop, Ma increase the coordinate) of the system) in the equation with
When so differential equation along each solution the parameter.
Other a sliding mode equations un-