9-1991

On Perfect Weighted Coverings with Small Radius

G. D. Cohen

S. N. Litsyn

H. F. Mattson Jr

SU-CIS-91-35

On Perfect Weighted Coverings with Small Radius

G. D. Cohen, S. N. Litsyn, and H.F. Mattson, Jr.

September 1991

School of Computer and Information Science
Syracuse University
Suite 4-116, Center for Science and Technology
Syracuse, New York 13244-4100

ON PERFECT WEIGHTED COVERINGS WITH SMALL RADIUS[1]

Gérard D. Cohen
Ecole Nationale Supérieure des Télécommunications
46 rue Barrault, C-220-5
75634 Paris cédex 13, France
Email: Cohen@inf.enst.fr

Simon N. Litsyn
Dept. of Electrical Engineering-Systems
Tel-Aviv University
Ramat-Aviv
69978, Israel
Email: litsyn@genius.tau.ac.il

H. F. Mattson, Jr.
School of Computer and Information Science
4-116 Center for Science & Technology
Syracuse, New York 13244-4100
Email: jen@SUVM.acs.syr.edu, jen@SUVM.bitnet

Abstract: We extend the results of our previous paper [8] to the nonlinear case: The Lloyd polynomial of the covering has at least R distinct roots among $1, \ldots, n$, where R is the covering radius. We investigate *PWC* with diameter 1, finding a partial characterization. We complete an investigation begun in [8] on linear *PMC* with distance 1 and diameter 2.

[1]This paper was presented at the French-Soviet Workshop in Algebraic Coding, ENST, Paris, 22–24 July 1991. It will appear in the Proceedings, to be published by Springer in the LNCS series.

1 Introduction

Much attention has been devoted to the problem of classifying perfect codes (See [13, 15]). Further generalizations of perfectness were introduced in [10, 2, 11, 14]. For all these codes the diameter of the covering spheres equals the covering radius of the code which by use of Delsarte's results leads to a very rigid set of possible parameters. This framework was broadened by introducing new types of perfect configurations [5, 6, 12, 16]. All these extensions fall under the concept of perfect weighted coverings (*PWC*) first considered in [8]. Although general, these definitions leave hope for a complete classification, at least for small diameter. The linear case with diameter at most 2 was considered in [8], where some motivation related to list decoding was given.

We are pleased to acknowledge that this problem arose in discussions with I. Honkala in Veldhoven in June, 1990.

2 Notations and known results

We denote by $\boldsymbol{F}^n$ the vector space of binary n-tuples, by $d(\cdot,\cdot)$ the Hamming distance, by $C(n, K, d)R$ a code C with length n, size K, minimum distance $d = d(C)$ and covering radius R [9], [7]. When C is linear, we write $C[n, k, d]R$, where k is the binary log of K. We denote the Hamming weight of $x \in \boldsymbol{F}^n$ by $|x|$.

For $x \in \boldsymbol{F}^n$, $A(x) = (A_0(x), A_1(x) \dots A_n(x))$ will stand for the distance distribution of C with respect to x; thus

$$A_i(x) := |\{c \in C : d(c, x) = i\}|.$$

For any $(n+1)$-tuple $M = (m_0, m_1, \dots, m_n)$ of weights, i.e., rational numbers, we define the *M-density* of C at x as

$$\theta(x) := \sum_{i=0}^{n} m_i \; A_i(x) = \langle M, A(x) \rangle. \tag{2.1}$$

We consider only *coverings*, i.e., codes C such that $\theta(x) \geq 1$ for all x.

(2.2) C is a *perfect M-covering* if $\theta(x) = 1$ for all x.

We define the *diameter* of an M-covering as

$$\delta := \max\{i : m_i \neq 0\}.$$

To avoid trivial cases, we usually assume that $m_i = 0$ for $i \geq n/2$, i.e., $\delta < n/2$.

Here are the known special cases.

(2.3) Classical perfect codes: $m_i = 1$ for $i = 0, 1, \dots \delta$.

(2.4) Perfect multiple coverings (*PMC*): $m_i = 1/j$ for $i = 0, 1, \dots \delta$ where j is a positive integer. See [16] and [5].

(2.5) Perfect L-codes: $m_i = 1$ for $i \in L \subseteq \{0, 1, \ldots \lfloor n/2 \rfloor\}$. See [12] and [6].

(2.6) Strongly uniformly packed codes:
$m_i = 1$ for $i = 0, 1, \ldots, e-1$
$m_e = m_{e+1} = 1/r$ for some integer r. See [14].

(2.7) Uniformly packed codes [2, 11]. For these codes $\delta(M) = R(C)$, and the m_i's are uniquely determined.

The following necessary and sufficient condition was already in [8] in the linear case. For a perfect M-covering C one gets from the definition:

$$\sum_{i=0}^{n} m_i \; A_i(x) = 1 \text{ for all } x.$$

Summing over all x in $\boldsymbol{F}^n$ and permuting sums, we get

$$\sum_{i=0}^{n} m_i \sum_{x \in F^n} A_i(x) = 2^n.$$

For $i = 0$, the second sum is $|C| = K$, for $i = 1$ it is Kn, and so on. For the converse we use the condition $\theta(x) \geq 1$. Hence we get the following analog of the Hamming condition.

Proposition 2.1 *A covering C is a perfect M-covering if and only if*

$$K \sum_{i=0}^{n} m_i \binom{n}{i} = 2^n . \tag{2.8}$$

□

3 A Lloyd theorem

In this section we prove

Theorem 3.1 *Let C be a perfect weighted covering with $M = (m_0, m_1, \ldots, m_\delta)$. Then the Lloyd polynomial of this covering,*

$$L(x) := \sum_{0 \leq i \leq \delta} m_i \; P_{n,i}(x)$$

has at least R distinct integral roots among $1, 2, \ldots, n$.

Proof. (Adapted from [1], Chapter II, Section 1, which records A. M. Gleason's proof of the classical Lloyd theorem.) The first part of the proof is identical to that of [8, Thm. 4.1].

We use the group algebra $\mathcal{A}$ of all formal polynomials

$$\sum_{a\in \boldsymbol{F}^n} \gamma_a X^a$$

with $\gamma_a \in \boldsymbol{Q}$, the field of rational numbers.

Define

$$S := \sum_{0\leq i\leq \delta} m_i \sum_{|a|=i} X^a. \tag{3.1}$$

We let the symbol C for our code also stand for the corresponding element in $\mathcal{A}$, namely,

$$C := \sum_{c\in C} X^c. \tag{3.2}$$

Then we find that

$$SC = \sum_{c\in C} X^c \cdot S \;=\; \boldsymbol{F}^n := \sum_{a\in \boldsymbol{F}^n} X^a. \tag{3.3}$$

Characters on $\boldsymbol{F}^n$ are group homomorphisms of $(\boldsymbol{F}^n,+)$ into $\{1,-1\}$, the group of order 2 in $\boldsymbol{Q}^{\times}$. All characters have the form χ_u for $u \in \boldsymbol{F}^n$, where χ_u is defined as

$$\chi_u(v) \;=\; (-1)^{u\cdot v} \text{ for } u,v \in \boldsymbol{F}^n.$$

We use linearity to extend χ_u to a linear functional defined on $\mathcal{A}$:
For all $Y \in \mathcal{A}$ if $Y = \sum_{a\in \boldsymbol{F}^n} \gamma_a X^a$, then $\chi_u(Y) := \sum \gamma_a \chi_u(a)$.
It follows that

$$\chi_u(YZ) \;=\; \chi_u(Y)\chi_u(Z) \text{ for all } Y,Z \in \mathcal{A}.$$

It is known [1, 9] that for any $u \in \boldsymbol{F}^n$, if $|u| = w$, then

$$\chi_u\left(\sum_{|a|=i} X^a\right) \;=\; P_{n,i}(w). \tag{3.4}$$

It follows that

$$\chi_u(S) \;=\; L(w). \tag{3.5}$$

From (3.3), furthermore, we see that

$$\chi_u(SC) \;=\; \chi_u(S)\chi_u(C) \;=\; 0$$

for all $u \neq 0$.

Let $u_0, u_1, \ldots, u_R$ be translate-leaders for C such that $|u_i| = i$. Define

$$C_i := X^{u_i}\, C.$$

Then

$$S\, C_i \;=\; \mathbf{F}^n. \tag{3.6}$$

Define the **symmetric subring** $\overline{\mathcal{A}}$ of $\mathcal{A}$ as the set of all elements Y of $\mathcal{A}$ in which the coefficient of X^a depends only on the weight of a:

$$Y \;=\; \sum_{a\in \mathbf{F}^n} \gamma_a\, X^a \;\in\; \overline{\mathcal{A}} \text{ iff } \forall a,b \in \mathbf{F}^n,\; |a| = |b| \rightarrow \gamma_a = \gamma_b. \tag{3.7}$$

The mapping $T : \mathcal{A} \to \overline{\mathcal{A}}$ defined by

$$T(Y) := \frac{1}{n!} \sum_{\varphi} \varphi(Y),$$

where φ runs over all $n!$ permutations of the n coordinates of $\boldsymbol{F}^n$, maps $\overline{\mathcal{A}}$ onto $\overline{\mathcal{A}}$. Furthermore, as the reader may easily verify,

$$\forall Y \in \overline{\mathcal{A}},\ \forall Z \in \mathcal{A},\ T(YZ) \;=\; YT(Z). \tag{3.8}$$

Define $\overline{C}_i := T(C_i)$. Applying (3.8) to (3.6), we see that

$$S\overline{C}_i = \mathbf{F}^n$$

since, of course, $S \in \overline{\mathcal{A}}$. Define also

$$K := \{Z;\ Z \in \overline{\mathcal{A}},\ SZ = 0\}. \tag{3.9}$$

Thus K is the kernel of the linear mapping from $\overline{\mathcal{A}}$ to $\overline{\mathcal{A}}$ defined by $Y \longmapsto SY$ for all $Y \in \overline{\mathcal{A}}$.

It follows from (3.8) that for any character χ_u such that $\chi_u(S) \neq 0$,

$$\forall Z \in K,\ \chi_u(Z) = 0.$$

Since $\overline{\mathcal{A}}$ has dimension $n+1$, its space of linear functionals also has dimension $n+1$. Since every linear functional on $\overline{\mathcal{A}}$ can be extended to one on $\mathcal{A}$, the $n+1$ linear functionals on $\overline{\mathcal{A}}$ obtained by restricting the χ_u to $\overline{\mathcal{A}}$, as

$$\chi_{u|_{\overline{\mathcal{A}}}} =: \chi_w \ \text{ for } \ |u| = w$$

$$w = 0, 1, \ldots, n,$$

are linearly independent.

Suppose that ρ is the exact number of values of $w \in \{0, 1, \ldots, n\}$ for which

$$\chi_w(S) \neq 0.$$

Since $\chi_w(S)\chi_w(K) = 0$ for all w, it follows that $\chi_w(K) = 0$ for ρ values of w. Since $S\overline{C}_i = \mathbf{F}^n$ for $i = 0, 1, \ldots, R$, we see that

$$S(\overline{C}_i - \overline{C}_0) = 0 \ \text{ for } \ i = 1, \ldots, R.$$

The elements $\overline{C}_i - \overline{C}_0$ are linearly independent because $\overline{C}_i$ contains elements of weight i but of no smaller weight. We find that

$$R \leq \dim_{\mathbf{Q}} K \leq n + 1 - \rho,$$

since K is included in the intersection of the t kernels of the χ_w mentioned above. But $n + 1 - \rho$ is the number of χ_w's which vanish on S; therefore $\chi_w(S) = 0$ for at least R values of w.

Notice now that

$$\chi_w(S) \;=\; \sum_{0 \leq i \leq \delta} m_i \, P_{n,i}(w).$$

This finishes the proof. $\square$

4 A construction

Definition 4.1 *Let $C(n,K,d)R$ and $C'(n',K',d')R'$ be two codes. Set*

$$\chi_C(x) = \begin{cases} 0 & \text{if } x \in C \\ 1 & \text{otherwise.} \end{cases}$$

We extend χ_C to a mapping $\chi : \boldsymbol{F}^{nn'} \to \boldsymbol{F}^{n'}$ by setting

$$\chi(x) := (\chi_C(x_1), \chi_C(x_2), \dots \chi_C(x_{n'}))$$

where the x_i's are in $\boldsymbol{F}^n$, for $1 \le i \le n'$, and $x = (x_1, x_2, \dots x_{n'})$ is their concatenation. We are now ready to define $C \otimes C'$ as follows:

$$C \otimes C' = \left\{ z \in \mathbf{F}^{nn'} : \chi(z) \in C' \right\}.$$

Proposition 4.1 *$C \otimes C'$ has length nn', minimum distance $\min\{d, d'\}$ and covering radius RR'.*

The proof is immediate. □

Proposition 4.2 *Let x and x' be such that $d(x,C) = R, d(x',C') = R'$. Suppose that $A_R(x)$ and $A'_{R'}(x')$ are independent of x. Then for $C \otimes C'$ the coefficient $A_{RR'}(z)$ is the same for any z such that $d(z, C \otimes C') = RR'$ and one has*

$$A_{RR'} = A_R A'_{R'}.$$

□

5 *PWC* with diameter 1

Let us denote such a *PWC* by (n, m_0, m_1). From (2.2), $A_1(x) = 1/m_1$ for any x not in C. Hence $m_1 = 1/p$, where p is an integer. This means that every two noncodewords have the same number of codewords at distance 1.

For $c \in C$, we get: $m_0 + A_1(c)/p = 1$, hence

$$A_1(c) = p\ (1 - m_0)$$

is a constant independent of c. Since $A_1(c)$ is an integer , so is $m_0 p$.

Now the Hamming analogue (2.9) gives

$$K\ (pm_0 + n) = p\ 2^n,$$

which implies

(5.1) $$n = p'\ 2^i - m_0 p, \text{ with } p' \mid p.$$

The case $m_0 = 1/p$ corresponds to the *PMC* mentioned in (2.4); it is solved in [16] and [8].

Let us give a few general constructions.

Proposition 5.1 *If there exists a PWC* $C(n, m_0, m_1)$, *then for any* $l \geq 0$ *there exists a PWC* $C'(n + l, m_0 - lm_1, m_1)$.

Proof. Let us define C' as the set of vectors (c, f) in $\boldsymbol{F}^{n+l}$, where $c \in C$ and $f \in \boldsymbol{F}^l$. Let A be the distance distribution for C_1 and A' that for C'. There are two possibilities for an arbitrary $(x, f) \in \boldsymbol{F}^{n+l}$:

(a) $x \in C$. Then $A'_1((x, f)) = A_1(x) + l$. Evidently $A'_0((x, f)) = 1$.

(b) $x \notin C$. Then $A'_0((x, f)) = 0$ by construction and $A'_1((x, f)) = A_1(x)$. □

Proposition 5.2 *If there exists a PWC* $C(n, m_0, m_1)$, *then there exists a PWC* $C'(ns, m_0, m_1/s)$.

Proof. Apply construction $\otimes$ (Def. 4.1) with outer code $C(n, m_0, m_1)$ and inner code the $[s, s-1]$ parity code. □

Proposition 5.3 *If there exists a PWC* $C(n, m_0, m_1)$, *then there exists a PWC* $C'(n, m_0/i, m_1/i)$, *for* i *a positive integer.*

Proof. Take the union of i cyclic shifts of code C. □

Let us now turn to the special case when $m_0 = 1$.

Proposition 5.4 *A PWC with* $\delta = m_0 = 1$ *exists for* $n = p(2^i - 1), m_1 = 1/p$. *It can be achieved by a linear code.* □

See [8] for a proof of this result. In contrast to the linear case, [8, Prop. 5.4], we cannot characterize *PWC* with $\delta = m_0 = 1$ here. However, we have a partial characterization:

Proposition 5.5 *A PWC* $(n, 1, 2^{-q})$ *exists if and only if for some* i $n = 2^q(2^i - 1)$. *Such a PWC can be achieved by a linear code.*

Proof. If $m_1 = 2^{-q}$, then $p' = 2^{q'}, q' \leq q$, and (5.1) gives $n = 2^q(2^{i+q'-q} - 1)$. The converse stems from Proposition 5.4. □

We would like to point out that for some parameters satisfying (5.1) there is no corresponding code.

Consider the case $m_0 = 1, \quad m_1 = 1/3$. Proposition 5.4 gives the sequence of lengths $n = 3 \cdot 2^i - 3$. The other possibility is $n = 2^i - 3$. The first code in this sequence would be a *PWC* with $n = 5$ and $K = 12$. Let us show its nonexistence.

Proposition 5.6 *A* $(5, 1, 1/3)$ *PWC does not exist.*

Proof. We may assume the code contains the zero vector. Furthermore, it does not contain vectors of weight 1, since the minimum distance is 2 for $m_0 = 1$. Every vector of weight 1 has to be covered by exactly two codewords of weight 2. There are exactly 5 codewords of weight 2, because if we consider the matrix of all such codewords, we see that each column has sum 2 (by the "coverage" condition just mentioned). Let x be any vector in $\mathbf{F}^5$ of weight 3. Each "1" in x is covered by two codewords of weight 2. That makes six codewords of weight 2. By the pigeonhole principle, two are equal, say to $c \in C$. Then x is at distance 1 from c.

So the code does not contain vectors of weight 1 and 3, and we cannot cover vectors of weight 2. □

6 Linear *PMC* with diameter 2 ($m_0 = m_1 = m_2 = 1/j$)

The purpose of this section is to summarize and extend results from [8].

6.1 The case $s = 1$

Proposition 6.1 [8] *The only PMC with $s = 1, d = 2$ is the $[2,1,2]$ code with $j = 2$.* □

We assume now that d is equal to 1. To set the stage, we repeat some material from [8]:

> We find that the only possibility for the check matrix is the t-fold repetition of $g(S_i)$ (generator matrix of a simplex code of length $2^i - 1$) with l zero-columns appended, yielding $n = t(2^i - 1) + l$. It amounts to appending all possible tails of length l to codewords described in Proposition 5.2. It is easy to check that there are 2 kinds of covering equalities (namely, vectors coinciding with, or being at distance 1 from, codewords on the first $t(2^i - 1)$ coordinates):
>
> $$\begin{aligned} m_0 + lm_1 &+ \binom{t}{2}(2^i - 1)m_2 + \binom{l}{2} m_2 = 1 \\ tm_1 &+ (2^{i-1} - 1)\, t^2 m_2 + tlm_2 = 1. \end{aligned}$$
>
> This implies
>
> (6.1) $$t^2 - t(2^i + 1 + 2l) + (l^2 + l + 2) = 0$$
>
> which has discriminant
>
> (6.2) $$D = (2^i + 1)^2 + 2^{i+2}l - 8.$$

We get a *PMC* iff $D = x^2$ has integer solutions. For example, the values $i = 3,\ l = 3,\ t = 14$ yield the *PMC* $[101, 98]$ with $j = 644$. Of course, for $i = t$ we get $8l + 1 = x^2$ having all odd x as solutions.

Now we can characterize the solutions of $D = x^2$. We need the following result:

Proposition 6.2 $(2^{i+1} - 7)$ *is a square mod* 2^{i+2}.

Proof. Proof by induction on i. If x is a solution for some i, i.e., for $\alpha \in \mathbf{N}$, $x^2 = \alpha\, 2^{i+2} + 2^{i+1} - 7$, then for any $\beta \in \mathbf{N}$ to be chosen later on, and $i \geq 3$:

$$\begin{aligned} (x + 2^{i+1}\beta + 2^i)^2 &= x^2 + 2^{i+2}(x\beta + \alpha) + 2^{i+1}x + 2^{i+1} - 7 + 2^{2i}(1 + 4\beta^2 + 4\beta) \\ &\equiv 2^{i+2}\left(x\beta + \alpha + \tfrac{x-1}{2}\right) + 2^{i+2} - 7 \bmod 2^{i+3}. \end{aligned}$$

Since x is odd, we can certainly find β to make $x\beta + \alpha + \frac{x-1}{2}$ even. Then $x + 2^{i+1}\beta + 2^i$ is a solution for $i + 1$. For $i \leq 2$, the proposition is easily checked. □

The first proof of this proposition was given by I. Shparlinski during the present Workshop.

Obviously, the congruence

$$x^2 \equiv 2^i - 7 \pmod{2^{i+2}}$$

has 4 roots. Denoting by a the one which lies in $[0, 2^{i+1}]$, they are

$$a,\ 2^{i+1} - a,\ 2^{i+1} + a,\ 2^{i+2} - a.$$

Now direct calculations lead to the solution of (6.2), giving the possible l. Then t is derived from (6.1).

Theorem 6.1 *Linear PMC with $m_0 = m_1 = m_2 = 1/j$, $d = 1$ exist only for the following sets of parameters:*

$$l = (\gamma^2 2^{2i+2} \pm 2^{i+2}\gamma a + a^2 - 2^{i+1} + 7 - 2^{2i})/2^{i+2}$$
$$t = (2^i + 1 + 2l \pm \sqrt{(2^i+1)^2 + 2^{i+2}l - 8})/2$$
$$n = t(2^i - 1) + l$$
$$k = n - i$$
$$j = (2^{i-1} - 1)t^2 + t(1 + l),$$

for $\gamma \in \mathbf{Z}$, provided $l \in \mathbf{N}$. □

6.2 The case $s = 2$

We have found the following *PMC* codes C in this case ($d = s = \delta = 2$); see [8] for constructions.

C		$C^\perp$
$[5,1;5]$	$j=1$	$[5,4;2,4]$
$[5,2,2]$	$j=2$	$[5,3;2,4]$
$[5,3,2]$	$j=4$	$[5,2;2,4]$
$[10,7,2]$	$j=7$	$[10,3;4,7]$
$[37,32,2]$	$j=22$	$[37,5;16,22]$
$[8282,8269,2]$	$j=4187$	$[8282,13;4096,4187]$

The first is a classical perfect code. The notation $[n,k;w_1,w_2,\ldots]$ stands for an $[n,k]$ code in which all nonzero weights are among $w_1, w_2, \ldots$. In the above codes $C^\perp$, since $s = 2$, both weights are present. All the above codes C are *PMC* codes.

Conjecture 6.1 *We conjecture the nonexistence of PMC with $d = s = \delta = 2$ other than those in the table.*

References

[1] E. F. Assmus, Jr., H. F. Mattson, Jr., R. Turyn, "Cyclic codes," Final Report, Contract no. AF 19(604)–8516, AFCRL, April 28, 1966. Sylvania Applied Research Laboratory, Waltham, Mass. (Document no. AFCRL–66–348.)

[2] L. A. Bassalygo, G. V. Zaitsev, V. A. Zinoviev, "On Uniformly Packed Codes," *Problems of Inform. Transmission*, vol. 10, no. 1, 1974, pp. 9–14.

[3] L. A. Bassalygo, G. V. Zaitsev, V. A. Zinoviev, "Note on Uniformly Packed Codes," *Problems of Inform. Transmission*, vol. 13, no. 3, 1977, pp. 22–25.

[4] A. R. Calderbank, J. M. Goethals, "On a Pair of Dual Subschemes of the Hamming Scheme $M_n(q)$, " *Europ. J. Combinatorics*, 6, 1985, pp. 133–147.

[5] R. F. Clayton, "Multiple Packings and Coverings in Algebraic Coding Theory," Thesis, Univ. of California, Los Angeles, 1987.

[6] G. D. Cohen, P. Frankl, "On tilings of the binary vector space,"*Discrete Math.*, 31, 1980, pp.271-277.

[7] G. D. Cohen, M. G. Karpovsky, H. F. Mattson, Jr., J. R. Schatz, "Covering Radius—Survey and Recent Results," *IEEE Trans. Inform. Theory* IT–31, 1985, pp. 328–343.

[8] G. D. Cohen, S. N. Litsyn, H. F. Mattson, Jr., "Binary Perfect Weighted Coverings," Sequences '91, Positano, 17–22 June 1991, *Springer-Verlag Lecture Notes in Computer Science.* To appear.

[9] P. Delsarte, "Four Fundamental Parameters of a Code and Their Combinatorial Significance," *Information and Control*, vol. 23, no. 5, 1973, pp. 407–438.

[10] J. M. Goethals, S. L. Snover, "Nearly Perfect Binary Codes," *Discrete Math.*, 3, 1972, pp. 65–88.

[11] J. M. Goethals, H. C. A. van Tilborg, "Uniformly packed codes," *Philips Res. Repts* 30, 1975, pp. 9–36.

[12] M. Karpovsky, "Weight distribution of translates, covering radius and perfect codes correcting errors of the given multiplicities," *IEEE Trans. Inform. Theory* IT-27, 1981, pp. 462–472.

[13] J. E. MacDonald, "Design methods for maximum minimum-distance error-correcting codes," *IBM J. Res. Devel.* vol. 4, 1960, pp. 43–57.

[14] N. V. Semakov, V. A. Zinoviev, G. V. Zaitsev, "Uniformly Packed Codes," *Problems of Inform. Transmission*, vol. 7, 1971, no. 1, pp. 38–50.

[15] Th. Skolem, P. Chowla, and D. J. Lewis, "The Diophantine equation $2^{n-2} - 7 = x^2$ and related problems," *Proc. Amer. Math. Soc.* 10 , 1959, pp. 663–669.

[16] G. J. M. van Wee, G. D. Cohen, S. N. Litsyn, "A note on Perfect Multiple Coverings of Hamming Spaces," *IEEE Trans. Inform. Theory*, IT – 37, no. 3, 1991, pp. 678–682.