Contemporary Mathematics
Volume **634**, 2015
http://dx.doi.org/10.1090/conm/634/12692

Open Problems in Coding Theory

Steven Dougherty, Jon-Lark Kim, and Patrick Solé

Abstract. We present major open problems in algebraic coding theory. Some of these problems are classified as Hilbert problems in that they are foundational questions whose solutions would lead to further study. The remainder are classified as Fermat problems in that they are difficult problems in coding theory that have defied solution for a significant period of time.

1. Introduction

Coding theory began around 1950 to enable the detection and correction of errors in electronic communication. See Shannon seminal work [**68**] and Hamming's paper [**36**] for foundational work in this area. Soon after this, mathematicians began to treat the fundamental problems of coding theory as mathematical questions without necessarily being concerned with engineering applications. By the 1970s significant research had gone into both the practical and theoretical aspects of coding theory. Around this time, connections to finite geometry, combinatorics and lattice theory were made. Within 40 years of its birth, coding theory had become an important branch of algebra with numerous connections to other branches of mathematics and to applications in information theory and cryptography.

In the early 1990s, a connection was made between linear codes over $\mathbb{Z}_4$ and non-linear binary codes in the landmark paper [**37**]. This paper sparked an enormous amount of interest in codes over rings. Soon after this time, coding theory was studied over a variety of algebraic alphabets and the discipline broadened significantly. The notion of distance was also broadened at this time as serious study of non-Hamming metrics began. At present, coding theory concerns a wide variety of alphabets and metrics and it is in this setting that we shall present a collection of open problems. Some of these questions are fundamental to the study of coding theory and some of these questions are related to connections between coding theory and other objects.

We separate the problems into Hilbert problems and Fermat problems. A problem is a Hilbert problem if it is a large structural problem like Hilbert's famous problems from the International Congress of Mathematicians in 1900. A problem is a Fermat problem if it is like Fermat's last theorem, in that it is a very hard problem

2010 *Mathematics Subject Classification.* Primary 94B05.

J.-L. Kim would like to mention that this work was supported by Basic Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2005172).

that has withstood years of attempts to solve it and the usual techniques of the discipline seem not to work. For example, a Hilbert problem would be a question which pertains to the structure of coding theory, whereas a Fermat problem can simply be a very difficult problem within the discipline. We shall place each problem in its setting and explain partial results in the direction of the solution.

2. Definitions and Notations

We shall begin by giving some definitions and notations that will be used throughout the paper. Definitions that are specific to a particular problem will be given in the section pertaining to that particular problem.

A code C over an alphabet A is a simply a subset of A^n. If A is a ring, then we say that the code C is linear if it is a submodule of A^n. For codes over fields, this means that linear codes are vector spaces. We will assume that codes are linear codes over rings unless otherwise specified.

If A is a ring, then the ambient space A^n is equipped with an inner-product, specifically $[\mathbf{v}, \mathbf{w}] = \sum v_i \overline{w_i}$, where $\overline{w_i}$ is an involution on the ring. For example, if R is the field of order 4, often the involution sending ω to ω^2 is used. The usual properties hold in this setting, namely, $[\mathbf{v}_1 + \mathbf{v}_2, \mathbf{w}] = [\mathbf{v}_1, \mathbf{w}] + [\mathbf{v}_2, \mathbf{w}]$, $[\mathbf{v}, \mathbf{w}] = [\mathbf{w}, \mathbf{v}]$ and $[\alpha\mathbf{v}, \beta\mathbf{w}] = \alpha\beta[\mathbf{v}, \mathbf{w}]$. If $\overline{w_i} = w_i$ we say the inner-product is the Euclidean inner-product, otherwise we say it is a Hermitian inner-product. Often the application of the code determines which inner-product is used. We define the orthogonal to be $C^\perp = \{\mathbf{v} \mid [\mathbf{v}, \mathbf{w}] = 0, \ \forall \mathbf{w} \in C\}$. We note that $C^\perp$ is always a linear code. If $C \subseteq C^\perp$ we say that the code is self-orthogonal and if $C = C^\perp$ we say that the code is self-dual.

Given a metric D in A^n, we say d is the minimum distance of a code C with respect to D, if $d = min\{D(\mathbf{v}, \mathbf{w}) \mid \mathbf{v}, \mathbf{w} \in C, \mathbf{v} \neq \mathbf{w}\}$. The minimum weight of a code is $min\{D(\mathbf{v}, \mathbf{0}) \mid \mathbf{v} \in C, \mathbf{v} \neq \mathbf{0}\}$.

If C is a linear code in F^n where F is a field then we say that C is an $[n, k, d]$ code if the ambient space is F^n, the dimension of the code is k, and the minimum Hamming weight of the code is d. For codes over rings we shall avoid this notation since, in general, we do not have the same notion of dimension. We can however always use the notation (n, M, d) to indicate the code has length n, M elements and minimum distance d.

We define the complete weight enumerator of a code over an alphabet $\{a_0, a_1, \ldots, a_s\}$ by

$$cwe_C(x_0, x_1, \ldots, x_s) = \sum_{\mathbf{v} \in C} \prod x_i^{n_i(\mathbf{v})},$$

where there are $n_i(\mathbf{v})$ occurrences of a_i in $\mathbf{v}$. The Hamming weight enumerator of C is given by $W_C(x, y) = cwe(x, y, y, \ldots, y)$. For simplicity, we often set $x = 1$ when displaying this weight enumerator.

Hilbert Problems

3. Fundamental Problem of Coding Theory

The following is the original question of coding theory and remains the fundamental question of coding theory.

OPEN QUESTION 3.1. *For a fixed n, d and $\mathbb{F}_q$, find $A(n,d)$, the largest M such that there exists a code $C \subset \mathbb{F}_q^n$ with $|C| = M$.*

There are numerous known cases for given n and d over various small fields. However, the question remains unknown for most cases. The question can also be rephrased holding fixed any two parameters.

In general, more attention is paid to the linear version.

OPEN QUESTION 3.2. *For a fixed n, d and $\mathbb{F}_q$, find $k[n,d]$, the largest integer $k \leq n$ such that there exists a linear code $C \subseteq \mathbb{F}_q^n$ with $dim(C) = k$ and minimum weight d.*

We can state the fundamental question in its most general form.

OPEN QUESTION 3.3. *Given a finite metric space X^n and a metric D, fix n and d. Find the largest M such that there exists a code $C \subseteq X^n$, with minimum distance d, and $M = |C|$.*

Various forms of Open Problem 3.3 can be stated. For example, one might ask to find the optimal codes over $\mathbb{Z}_4$ with respect to the Lee metric or over $\mathbb{Z}_{2k}$ with the Euclidean metric.

The case of $X = J(n,w)$ the Johnson scheme with D equal to the Johnson distance leads to the definition of $A(n,d,w)$ the largest size of a constant weight code with given parameters. The case of $X = S_n$, the symmetric group, with the Hamming distance leads to the concept of permutation arrays. Both cases can be generalized further by looking at cartesian products with the sum of distances leading to the notions of multiple constant weight codes and multipermutation arrays respectively.

It seems very unlikely that a universal theoretical bound will be given in a closed form to solve this problem, since so many bounds exists which are often met. It seems also equally unlikely that the solution to Open Problem 3.1, Open Problem 3.2, Open Problem 3.3, will yield to an algorithmic approach, since all these problems are of the type of finding a maximum clique in some graphs, which is a notoriously difficult problem [**17**]. This begs the following problem.

OPEN QUESTION 3.4. *What is the complexity status of computing $A(n,d)$, $A(n,d,w)$, $k[n,d]$ and the above permutation analogues?*

While much work has been done in the area of the complexity of coding problems [**29**], these questions remain open.

4. Duality for non-Abelian groups

One of the foundations of coding theory is the use of an inner-product which gives rise to an orthogonal. The parity check matrix which generates the orthogonal is used in many decoding algorithms. The MacWilliams relations relate the weight enumerator of the code with its orthogonal and are one of the foundational theorems of coding theory.

One can generate an orthogonal for Abelian groups as follows. Let G be a finite abelian group and fix a duality of G, i.e. a character table. We have a bijective correspondence between the elements of G and those of $\widehat{G} = \{\pi | \pi \text{ a character of } G\}$. Note a character of G is a homomorphism from G to the multiplicative group

of the complex numbers. For each $\alpha \in G$ denote the corresponding character by χ_α.

A code C over G is a subset of G^n, the code is said to be linear if C is an additive subset of G^n.

DEFINITION 4.1. For C a code over G, $C^\perp = \{(g_1, g_2, \ldots, g_n) | \prod_{i=1}^n \chi_{g_i}(c_i) = 1$ for all $(c_1, \ldots, c_n) \in C\}$.

We associate an element of $\widehat{G}^n$ with an element of G^n with the natural correspondence and since $(\widehat{G})^n = \widehat{G^n}$ the code $C^\perp$ is associated with the set $\{\chi \in \widehat{G^n} | \chi(c) = 1 \quad \text{for all} \quad c \in C\}$. This gives that $|C^\perp| = \frac{|\widehat{G}|^n}{|C|} = \frac{|G|^n}{|C|}$ and that $C = (C^\perp)^\perp$.

Let $G = \{\alpha_i\}$ with α_0 the additive identity of the group.

Let T be defined as follows:

$$T_{\alpha_i, \alpha_j} = \chi_{\alpha_i}(\alpha_j).$$

Using the Poisson summation formula we have the following theorem.

THEOREM 4.2. *Let C be a code over G, $|G| = s$, with weight enumerator $cwe_C(x_0, x_1, \ldots, x_{s-1})$. Then the complete weight enumerator of the orthogonal is given by:*

$$cwe_{C^\perp} = \frac{1}{|C|} cwe_C(T \cdot (x_0, x_1, \ldots, x_{s-1})),$$

where $T \cdot \mathbf{v}$ indicates the matrix multiplication $T\mathbf{v}^t$, and

$$W_{C^\perp} = \frac{1}{|C|} W_C(x + (s-1)y, x - y).$$

This approach does not work for non-Abelian groups. This leads to our next open question.

OPEN QUESTION 4.3. *Is there a duality and MacWilliams formula for codes over non-Abelian groups? Is there a subclass of non-Abelian groups for which a duality and a MacWilliams formula exists?*

There are many difficulties in trying to solve this problem. For example, consider the non-Abelian Quaternion group of order 8. This group has elements $\{\pm 1, \pm i, \pm j, \pm k\}$. There are three subgroups of order 4 in this group, that is $\{\pm 1, \pm i\}$, $\{\pm 1, \pm j\}$ and $\{\pm 1, \pm k\}$. But there is only one group of order 2, that is $\{\pm 1\}$. If a linear code is defined as a subgroup (or even normal subgroup) of G^n then these are all linear codes. If we expect that $|C||C^\perp| = |G|^n$, then each subgroup of order 4 would need a subgroup of order 2 to be its orthogonal and the subgroup of order 2 would need a subgroup of order 4 to be its orthogonal. This would not be possible here, in other words we could not have $(C^\perp)^\perp = C$ in this scenario. Hence this problem may require a duality where some of the standard results are false, or we may restrict this to a subclass of non-Abelian groups where the theory can be reproduced. Alternatively, one might show that no such duality can exist for any non-Abelian group. This example is also important in that there is a Gray map from the Quaternion group to the binary Hamming space. Hence, it would be important to have an inner-product for this group that relates to this Gray map.

More generally, we have the following question.

OPEN QUESTION 4.4. *Find the largest class of algebraic structures A for which a duality and MacWilliams relations hold.*

An enormous step forward was given in [**76**]. It was shown there that the largest class of rings would be the class of Frobenius rings. In the proof given in [**76**], the fact that the underlying additive group is abelian is used so that the technique does not apply to the above question.

5. Designs and Codes

Since the beginning of the study of coding theory, there has been a very fruitful connection between the study of codes and the study of designs. A $t-(v,k,\lambda)$ design is a set of points and blocks, such that there are v points, each block contains k points, and through any t points there are exactly λ blocks. For example, a projective plane of order n is a $2-(n^2+n+1,n+1,1)$ design.

One of the most significant theorems relating codes and designs is the Assmus-Mattson theorem which first appeared in [**1**].

THEOREM 5.1. **Assmus-Mattson Theorem** *Let C be a code over $\mathbb{F}_q$ of length n with minimum weight d, and let $d^\perp$ denote the minimum weight of $C^\perp$. Let $w=n$ when $q=2$ and otherwise the largest integer w satisfying $w-(\frac{w+q-2}{q-1})<d$, define $w^\perp$ similarly. Suppose there is an integer t with $0<t<d$ that satisfies the following condition: for $W_{C^\perp}(Z)=B_iZ^i$ at most $d-t$ of $B_1,B_2,\ldots,B_{n-t}$ are non-zero. Then for each i with $d\le i\le w$ the supports of the vectors of weight i of C, provided there are any, yield a t-design. Similarly, for each j with $d^\perp\le j\le min\{w^\perp,n-t\}$ the supports of the vectors of weight j in $C^\perp$, provided there are any, form a t-design.*

One of the most fruitful uses of this theorem is to find 5-designs in the extremal doubly-even self-dual binary codes of length 24 and 48. There would also be 5-designs in the putative $[24k,12k,4k+4]$ codes, see Open Problem 7.1 and Open Problem 7.7

OPEN QUESTION 5.2. *Find a theoretical limit for t such that there exists t-designs via the Assmus-Mattson theorem applied to a linear code, or prove that no such limit exists by finding codes with t-designs for arbitrary t.*

Toward this very large question it would be interesting to solve the following.

OPEN QUESTION 5.3. *Find 5-designs that are not in $[24k,12k,4k+4]$ codes Type II codes or any 6-designs in codes.*

6. MDS Codes

One of the most important bounds on the size of the minimum distance is the following Singleton Bound. It first appeared in [**71**].

THEOREM 6.1. *Let C be a code over an alphabet A with length n, minimum distance d and size $k=log_{|A|}(C)$. Then $d\le n-k+1$.*

This bound assumes no algebraic structure for the code at all, in this sense it is a purely combinatorial bound. Codes meeting this bound are called Maximum Distance Separable (MDS) codes. Finding such codes is largely a combinatorial problem.

This combinatorial bound is equivalent to a number of interesting combinatorial questions involving mutually orthogonal Latin squares (and hypercubes) and arcs of maximal size in projective geometry. As an example, consider the following theorem. See [**38**] for a complete description and a proof of the theorem.

THEOREM 6.2. *A set of s mutually orthogonal Latin squares of order q is equivalent to an MDS $[s+2, q^2, s+1]$ code over $\mathbb{F}_q$.*

The question of determining exactly when a set of s MOLS exist has been largely open since 1782. While numerous cases are known, the vast majority of cases remains open.

When considering the algebraic structure of codes over rings, a stronger bound can be made for codes over a principal ideal ring.

THEOREM 6.3. *Let C be a linear code over a principal ideal ring, then*

$$d(C) \leq n - k + 1$$

where k is the rank of the code.

Codes meeting this bound are called Maximum Distance with respect to Rank (MDR). See [**27**] for a discussion of these codes. Of course, simply because a code is MDR does not imply that the code is MDS, in general, it will not be. In fact, showing a code is MDR (when it is not also MDS) indicates that the code is optimal and so there can be no linear MDS code with the same parameters.

OPEN QUESTION 6.4. *Find and classify all MDS and MDR codes over various classes of alphabets.*

For some results on MDR code see [**34**]. These bounds have been generalized to other weight for codes over rings of order 4 in [**25**].

THEOREM 6.5. *If C is a code of length n over any ring of order 4 with minimum Hamming weight d_H, minimum Lee weight d_L, minimum Euclidean weight d_E, and minimum Bachoc weight d_B then*

$$\left\lfloor \frac{d_L - 1}{2} \right\rfloor \leq n - \text{rank(C)}, \tag{1}$$

$$\left\lfloor \frac{d_E - 1}{4} \right\rfloor \leq n - \text{rank(C)}, \tag{2}$$

and

$$\left\lfloor \frac{d_B - 1}{2} \right\rfloor \leq n - \text{rank(C)}. \tag{3}$$

A code meeting bound (1) is a Maximum Lee Distance with respect to Rank (MLDR) Code, a code meeting bound (2) is a Maximum Euclidean Distance with respect to Rank (MEDR) Code, a code over meeting bound (3) is a Maximum Bachoc Distance with respect to Rank (MBDR) Code.

OPEN QUESTION 6.6. *Find and classify all MLDR, MEDR, MBDR codes over rings of order 4.*

Fermat Problems

7. Doubly-even binary codes

In this section, we shall describe one of the most fascinating open questions in coding theory. Namely, the question asks if extremal doubly-even binary self-dual codes exist of lengths a multiple of 24. It is one of the most studied open questions in coding theory. It is the quintessential Fermat type problem in that most coding theorists have tried to solve it, but the standard techniques do not seem to be able to solve it. Rather, they seem to find equally difficult problems to solve which would in turn solve this problem.

We say that a code is self-dual if $C = C^{\perp}$. It is self-orthogonal if $C \subseteq C^{\perp}$. If a binary self-dual code has all weights congruent to 0 (mod 4) then the code is said to be Type II, otherwise it is said to be Type I. Type II codes are said to have weights that are doubly-even.

The first open question is the following, it was first posed in [**69**] in 1973.

OPEN QUESTION 7.1. *Does there exist a Type II* $[72, 36, 16]$ *code?*

Some monetary prizes have been offered for its solution. Specifically, the following have been offered: N.J.A. Sloane \$10; S.T. Dougherty \$100 for the existence; M. Harada \$200 for the nonexistence. The usual conditions apply, namely that the prizes will be paid only once and a solution must be accepted by the mathematical community.

We shall show where the problem arises. If C is a self-dual code then the Hamming weight enumerator is held invariant by the MacWilliams relations and hence by the following matrix:

$$M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

If the code is doubly-even, that is the Hamming weights of all vectors are 0 (mod 4), then it is also held invariant by the following matrix:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

The group $G = \langle G, A \rangle$ has order 192. To this group we associate the series $\Phi(\lambda) = \sum a_i \lambda^i$, where there are a_i independent polynomials held invariant by the group G. Next, we apply the classic theorem of Molien.

THEOREM 7.2. *(Molien) For any finite group* G *of complex* m *by* m *matrices,* $\Phi(\lambda)$ *is given by*

$$\Phi(\lambda) = \frac{1}{|G|} \sum_{A \in G} \frac{1}{det(I - \lambda A)} \tag{4}$$

where I *is the identity matrix.*

This theorem allows us to compute the number of independent polynomials held invariant by the group.

For our group G we get

$$\Phi(\lambda) = \frac{1}{(1-\lambda^8)(1-\lambda^{24})} = 1 + \lambda^8 + \lambda^{16} + 2\lambda^{24} + 2\lambda^{32} + \dots \tag{5}$$

The generating invariants can be found. Specifically, we have:

$$W_1(x,y) = x^8 + 14x^4y^4 + y^8 \tag{6}$$

and

$$W_2(x,y) = x^4y^4(x^4 - y^4)^4. \tag{7}$$

Then we have the well known Gleason's Theorem first proven in [**33**].

THEOREM 7.3. *The weight enumerator of a Type II self-dual code is a polynomial in $W_1(x,y)$ and $W_2(x,y)$, i.e. if C is a Type II code then $W_C(x,y) \in \mathcal{C}[W_1(x,y), W_2(x,y)]$.*

It follows that if C is a Type II $[n,k,d]$ code then

$$d \leq 4\left\lfloor \frac{n}{24} \right\rfloor + 4. \tag{8}$$

Codes meeting this bound are called extremal. Notice that extremal codes are necessarily optimal in the sense that they are the best self-dual codes possible, whereas simply being optimal does not imply that the code is extremal. We investigate those with parameters $[24k, 12k, 4k+4]$. Using Gleason's Theorem stated above, if a code has parameters $[24k, 12k, 4k+4]$ then the code has a unique weight enumerator. It is not known whether these codes exist until $24k \geq 3720$, at which point a coefficient becomes negative.

For length 24, there is a $[24, 12, 8]$ code, namely the well known Golay code. This code is formed by adding a parity check coordinate from the perfect $[24, 12, 7]$ binary Golay code. For length 48, there is also a code, namely the extended quadratic residue code q_{48}. See Open Problem 9.1 for an open problem concerning this code. Hence the first unknown case is whether there exists a $[72, 36, 16]$ code.

We shall focus on the first case, namely when $k = 3$ realizing that there is a corresponding result for all k. Using Gleason's theorem it is easy to determine the weight enumerator for a putative $[72, 36, 16]$ Type II code. It is given in Table 1.

TABLE 1. The Weight Enumerator for a Type II $[72, 36, 16]$ Code

C_i	i
1	0, 72
249849	16, 56
18106704	20, 52
462962955	24, 48
4397342400	28, 44
16602715899	32, 40
25756721120	36

We shall show that the existence of the extremal Type II codes of length $24k$ are intimately related to the existence of certain Type I codes of length $24k-2$. In particular, the existence of a $[72, 36, 16]$ Type II code is equivalent to the existence of a $[72, 35, 24]$ Type I code.

Let C be a self-dual code with C_0 the subcode of doubly-even vectors. If the code C is Type I then $C_0 = C$, otherwise the subcode C_0 is linear and of codimension 1. Hence, we shall now assume that C is Type I. Then $C_0^{\perp} = C_0 \cup C_1 \cup C_2 \cup C_3$ with $C = C_0 \cup C_2$. We define the shadow to be

$$S = C_1 \cup C_3 = C_0^{\perp} - C. \tag{9}$$

Note that the shadow is a non-linear code. We shall show how to determine the weight enumerator of the shadow from the weight enumerator of the code.

Given the above situation we have:

$$W_{C_0}(x,y) = \frac{1}{2}(W_C(x,y) + W_C(x,iy)) \tag{10}$$

where i is the complex number with $i^2 = -1$. This follows simply by noting that replacing y with iy will hold fix monomials representing doubly-even vectors and will put a minus sign in front of a monomial representing singly-even vectors.

The following appears in [**20**].

LEMMA 7.4. *Let C be a Type I self-dual code with S its shadow then*

$$W_S(x,y) = W_C\left(\frac{x+y}{\sqrt{2}}, \frac{i(x-y)}{\sqrt{2}}\right). \tag{11}$$

The following theorem appears in [**11**], it shows how to construct a larger self-dual code from a smaller one.

THEOREM 7.5. *Let C be a self-dual code of length n, C_0 be any subcode of codimension 1, and S be the shadow with respect to that subcode, with $C_0^{\perp} = C_0 \cup C_1 \cup C_2 \cup C_3$ as described above. Then if $\boldsymbol{j} \notin C_0$, where $\boldsymbol{j}$ is the all-one vector, the code $C' = (0,0,C_0) \cup (1,1,C_2) \cup (1,0,C_1) \cup (0,1,C_3)$ is a self-dual code of length $n+2$ with weight enumerator: $W_{C'} = x^2 W_{C_0}(x,y) + y^2 W_{C_2}(x,y) + xy W_S(x,y)$. If $\boldsymbol{j} \in C_0$ then the code $C' = (0,0,0,0,C_0) \cup (1,1,0,0,C_2) \cup (1,0,1,0,C_1) \cup (0,1,1,0,C_3)$ is self-orthogonal and the code $C^* = \langle v, C' \rangle$, where $v = (1,1,1,1,0,\ldots,0)$, is a self-dual code of length $n+4$ with weight enumerator: $(x^4+y^4)W_{C_0}(x,y) + (2x^2y^2)(W_{C_1}(x,y) + W_{C_2}(x,y) + W_{C_3}(x,y))$.*

Using this theorem, it is then a simple matter to show that the existence of the length 72 code is equivalent to the the existence of a $[70, 35, 14]$ Type I which we call the child code. We give its weight distribution in Table 2. We give the weight distribution of its shadow in Table 3.

TABLE 2. The Weight Distribution of a [70,35,14] Code

Weight	Frequency
0, 70	1
14, 56	11730
16, 54	150535
18, 52	1345960
20, 50	9393384
22, 48	49991305
24, 46	204312290
26, 44	650311200
28, 42	1627498400
30, 40	3221810284
32, 38	5066556495
34, 36	6348487600

Let $\mathbf{v}$ be a vector of weight 4 with C a putative $[72, 36, 16]$ code. Then let $E_0 = \{\mathbf{w} \mid \mathbf{w} \in C, [\mathbf{w}, \mathbf{v}] = 0\}$. Then let $E = \langle E_0, \mathbf{v} \rangle$. The code E is a Type II code with minimum weight 4. Using the design properties of the vectors in C, it is possible to determine the weight enumerator of of its length 68 child as given in Theorem 7.5. Both of these weight enumerators are given in Table 4.

TABLE 3. The Weight Distribution of the Shadow of a [70,35,14] Code

Weight	Frequency
15, 55	87584
19, 51	7367360
23, 47	208659360
27, 43	2119532800
31, 39	8314349120
35	13059745920

TABLE 4. The Weight Distribution of the Weight 4 Neighbor and its Subcode

	C_0	C'
Weight	Frequency	Frequency
0, 72	1	1
4, 68	0	1
12, 60	0	442
16, 56	134521	264673
20, 52	9284176	18589296
24, 48	232444043	464824659
28, 44	2196187840	4392509606
32, 40	8298695163	16597183691
36	12886246880	25772731998

Other weight enumerators can also be used to understand codes and have been used in connection to this problem. We shall give the definition of higher weights, introduced by Wei [**75**], following the notation in [**73**]. Let $D \subseteq \mathbb{F}_2^n$ be a linear subspace, then

$$||D|| = |Supp(D)|, \tag{12}$$

where

$$Supp(D) = \{i \mid \exists v \in D,\ v_i \neq 0\}. \tag{13}$$

For a linear code C define

$$d_r(C) = min\{||D|| \mid D \subseteq C,\ \dim(D) = r\}. \tag{14}$$

The higher weight spectrum is defined as

$$A_i^r = |\{D \subseteq C \mid \dim(D) = r,\ ||D|| = i\}|. \tag{15}$$

and then we define the higher weight enumerator by

$$W^r(C; y) = W^r(C) = \sum A_i^r y^i. \tag{16}$$

In [**24**] a Gleason's theorem for higher weight enumerators is given and the second higher weight enumerator for the putative length 72 code is given and follows in Table 5.

In [**26**], the higher weight enumerators are given for $i = 12$ to 36. No contradiction has been found in investigating these weight enumerators nor have they been useful in constructing a code. It would be of interest to compute the remaining open higher weight enumerators. There is a possibility, of course, that a contradiction can be found in these weight enumerators.

Another technique used in investigating this code is the automorphism group of the code. The automorphism group of a code C denoted by $Aut(C)$ is the set of all permutations of the coordinates that preserves the code.

TABLE 5. The Second Higher Weight Enumerator

coefficient of y^i	weight i
96191865	24
4309395552	26
119312891460	28
2379079500864	30
37327599503964	32
466987648992480	34
4687779244903412	36
37810235197002240	38
244777798274765679	40
1269000323938260672	42
5251816390965277320	44
17262594429823645056	46
44763003632389491540	48

The number of codes that are equivalent to a binary code C is $\frac{n!}{|Aut(C)|}$. If a Type II $[72, 36, 16]$ code exists then there are two possible explanation as to why it is difficult to find. The first is that $|Aut(C)|$ is very large and hence there are very few codes equivalent to the code to find. The second is that $|Aut(C)|$ is very small and even though there are many equivalent copies of the code it remains hard to find because its structure is not interesting.

Several results about the automorphism group are known. In [**19**], it was shown 23 is the largest odd prime dividing the order of the automorphism group of this code. In [**65**], it was shown that 23 also does not divide the order and 11 was eliminated in [**41**]. Hence the only possible primes that remained that could divide the order of the automorphism group of a putative $[72, 36, 16]$ Type II code were $2, 3, 5$ and 7. From the papers [**9**], [**10**],[**59**],[**63**], and [**77**], it is known that the order of the automorphism group is either 5 or divides 24. In [**7**], is was shown that any automorphism of order 2 cannot have any fixed points.

The following Open Problem is certainly folklore.

OPEN QUESTION 7.6. *Show that the automorphism group of a putative* $[72, 36, 16]$ *Type II code is trivial.*

Recently, it was proved that the code, if it exists, cannot be $\mathbb{Z}_4-$linear [**42**].

Another technique used to study this problem is the theory of designs. Using the Assmus-Mattson theorem it follows that if the code exists, then 5-$(72, 16, 78)$ designs exist coming from the supports of the minimum weight vectors. One could show that the code does not exist by showing that this design does not exist.

The more general version of this question is the following.

OPEN QUESTION 7.7. *For which* k *does there exists a doubly-even self-dual binary* $[24k, 12k, 4k + 4]$ *code?*

As before we have the following theorem which gives an equivalent open problem of finding the smaller code.

THEOREM 7.8. *The existence of a Type II* $[24k, 12k, 4k + 4]$ *Type II code is equivalent to the existence of a Type I* $[24k - 2, 12k - 1, 4k + 2]$ *Type I code.*

8. Codes and Lattices

In this section, we shall describe some open questions in the relationship between codes and lattices. Specifically, the open questions ask about extremal self-dual codes over rings that can be used to construct extremal unimodular lattices.

The Euclidean weight $wt_E(x)$ of a vector in $\mathbb{Z}_{2k}^n$ $(x_1, x_2, \ldots, x_n)$ in $\mathbb{Z}_{2k}^n$ is $\sum_{i=1}^n \min\{x_i^2, (2k - x_i)^2\}$. The following is shown in [**2**].

THEOREM 8.1. *Suppose that C is a self-dual code over $\mathbb{Z}_{2k}$ which has the property that every Euclidean weight is a multiple of a positive integer c. Then the largest positive integer c is either $2k$ or $4k$.*

A self-dual code over $\mathbb{Z}_{2k}$ where every vector has weight a multiple of $4k$ is said to be Type II, otherwise it is said to be Type I.

Let $\mathbb{R}^n$ be an n-dimensional Euclidean space with the standard inner product. An n-dimensional lattice Λ in $\mathbb{R}^n$ is a free $\mathbb{Z}$-module spanned by n linearly independent vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$. A matrix whose rows are the vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is called a generator matrix G of the lattice Λ. The fundamental volume $V(\Lambda)$ of Λ is $|\det G|$. The dual lattice Λ^* is given by $\Lambda^* = \{\mathbf{v} \in \mathbb{R}^n \mid \mathbf{v} \cdot \mathbf{w} \in \mathbb{Z} \text{ for all } \mathbf{w} \in \Lambda\}$. We say that a lattice Λ is *integral* if $\Lambda \subseteq \Lambda^*$ and that an integral lattice with $\det \Lambda = 1$ (or $\Lambda = \Lambda^*$) is unimodular. If the norm $\mathbf{v} \cdot \mathbf{v}$ is an even integer for all $\mathbf{v} \in \Lambda$, then Λ is said to be even. Unimodular lattices which are not even are called odd. The minimum norm of Λ is the smallest norm among all nonzero vectors of Λ.

It is well known that except for $n = 23$, the minimum norm of a unimodular lattice of length n is bounded above by $2\lfloor \frac{n}{24} \rfloor + 2$.

The following is proven in [**2**].

THEOREM 8.2. *Let ρ be a map from $\mathbb{Z}_{2k}$ to $\mathbb{Z}$ sending $0, 1, \ldots, k$ to $0, 1, \ldots, k$ and $k+1, \ldots, 2k-1$ to $1-k, \ldots, -1$, respectively. If C is a self-dual code of length n over $\mathbb{Z}_{2k}$, then the lattice*

$$\Lambda(C) = \frac{1}{\sqrt{2k}}\{\rho(C) + 2k\mathbb{Z}^n\},$$

is an n-dimensional unimodular lattice, where $\rho(C) = \{(\rho(c_1), \ldots, \rho(c_n)) | (c_1, \ldots, c_n) \in C\}$. The minimum norm is $\min\{2k, d_E/2k\}$ where d_E is the minimum Euclidean weight of C. Moreover, if C is Type II then the lattice $\Lambda(C)$ is an even unimodular lattice.

In [**59**], G. Nebe solves the existence of a unimodular lattice of length 72. Harada et al, [**52**], finds a Type II code of length 72 over $\mathbb{Z}_8$ with minimum Euclidean weight 64. The existence of this code implies the existence of an extremal Type II lattice of dimension 72.

OPEN QUESTION 8.3. *In length n, a multiple of 8, find a Type II self-dual code over $\mathbb{Z}_{2k}$, $2k \geq 2s + 2$ such that $\frac{d_E}{2k} = 2s + 2$. Such an extremal code will give an extremal lattice using Theorem 8.2.*

The question is solved for $n \leq 72$ in [**52**]. The next case would be to find a $\mathbb{Z}_{16}$ code with $d_E = 160$. This would given an extremal lattice at length 96.

In [**4**], the following conjecture is made, motivated by the analysis of the Gaussian wiretap channel.

The **secrecy ratio** of a lattice L is the ratio $r_L(y) = \frac{\theta_{\mathbb{Z}^n}(y)}{\theta_L(y)}$, where the theta series is defined as

$$\theta_L(y) = \sum_{x \in L} q^{x.x},$$

with $q = \exp(-\pi y)$.

OPEN QUESTION 8.4. *If L is a unimodular lattice prove that $r_L(y)$ is unimodal for $y \geq 0$ with a maximum in $y = 1$.*

The motivation for this conjecture besides extensive numerical evidence is the symmetry $r_L(y) = r_L(1/y)$, an immediate consequence of the Poisson-Jacobi formula. The Conjecture is proved in many special cases like e.g.

- unimodular lattices in dimension ≤ 23 [**55**],
- *even* unimodular lattices in dimension ≤ 72 [**30**],
- lattices obtained by Construction A from Type II codes of length ≤ 40 [**64**].

9. Self-Dual Codes

In this section, we shall list several open problems relating to self-dual codes. The classification of self-dual codes (especially binary self-dual codes) has been one of the major areas of coding theory for decades. Numerous papers have been written on their classification. We shall state some problems that remain open in this area.

The following problem concerns the extremal length 48 Type II code described earlier.

OPEN QUESTION 9.1. *Prove without a lengthy computer search that a Type II $[48, 24, 12]$ code is unique (i.e., equivalent to the q_{48}). Prove or disprove that q_{48}* is a unique $[48, 24, 12]$ code.

We do know that the only Type II $[48, 24, 12]$ code with an *automorphism of odd order* is equivalent to q_{48}, [**40**]. Using an exhaustive computer search, Houghten, Lam, Thiel and Parker [**39**] showed that q_{48} is the *only* $[48, 24, 12]$ *Type II code.*

The next question concerns a gap in the known optimal self-dual codes.

OPEN QUESTION 9.2. *Does there exist a Type I $[56, 28, 12]$ code?*

The highest minimum distances of self-dual codes of lengths up to 68 are known except $n = 56$.

Only one weight enumerator exists:

$$W_{56}(y) = 1 + 4606y^{12} + 45,056y^{14} + 306,922y^{16} + \cdots$$

There exist at least five Type II $[56, 28, 12]$ codes from Hadamard matrices of order 28 and at least one thousand such codes. The weight enumerator is

$$W = 1 + 8190y^{12} + 622,314y^{16} + 11,699,688y^{20} + \cdots$$

We shall discuss some open question regarding extremal self-dual codes of length 48 and related codes.

There are two possible weight enumerators $W_{48,1}$ and $W_{48,2}$ for extremal singly-even self-dual $[48, 24, 10]$ codes. Namely,

$$\begin{aligned} W_{48,1} &= 1 + 704y^{10} + 8976y^{12} + 56896y^{14} + \cdots, \\ S_{48,1} &= y^4 + 44y^8 + 17021y^{12} + \cdots, \\ W_{48,2} &= 1 + 768y^{10} + 8592y^{12} + 57600y^{14} + \cdots, \\ S_{48,2} &= 54y^8 + 16976y^{12} + \cdots \end{aligned}$$

Gulliver-Harada-Kim [**35**] constructed ten inequivalent extremal singly-even self-dual $[48, 24, 10]$ codes with weight enumerator $W_{48,1}$. Harada-Kitazume-Munemasa-Venkov [**56**] showed that there are exactly ten inequivalent extremal singly-even

self-dual $[48, 24, 10]$ codes with weight enumerator $W_{48,1}$. The extended quadratic residue code of length 48 has exactly 74 inequivalent extremal singly-even self-dual $[48, 24, 10]$ neighbors [**56**]. This will imply that there are at least 64 singly-even self-dual $[48, 24, 10]$ codes with weight enumerator $W_{48,2}$. There exists an extremal singly even self-dual $[48, 24, 10]$ code with weight enumerator $W_{48,2}$, neither of whose doubly-even self-dual neighbors is an extremal doubly even self-dual $[48, 24, 12]$ code [**56**].

Open Question 9.3. *Classify all extremal singly-even self-dual* $[48, 24, 10]$ *codes with weight enumerator* $W_{48,2}$.

10. Decoding Algorithms

One of the most important aspects of applied coding theory is finding an efficient algorithm to decode vectors. Namely, how do you take a received vector and use the algebraic structure of the code to determine the error vector and in so doing the sent vector.

Open Question 10.1. *Find an efficient decoding algorithm for a family of self-dual codes or for all self-dual codes.*

It is rather mysterious that self-dual codes do not have a general decoding algorithm. Efficient decoding algorithms exist for the binary Golay $[24, 12, 8]$ code, four of the five Type II $[32, 16, 8]$ codes, and the Type II $[48, 24, 12]$ code q_{48}.

A similar question exists for another important class of codes, namely quasi-cyclic codes. A cyclic code is a code C such that if $\mathbf{v} = (v_1, \ldots, v_n) \in C$ then $\sigma(\mathbf{v}) = (v_n, v_1, \ldots, v_{n-1}) \in C$. A code C is quasi-cyclic of index k if $\mathbf{v} \in C$ implies $\sigma^k(\mathbf{v}) \in C$. Cyclic and quasi-cyclic codes are widely studied families of codes.

Open Question 10.2. *Give a universal decoding algorithm for quasi-cyclic codes.*

11. Bounds on Codes

One of the most useful and important aspects of coding is a bound placed on the minimum distance of a code. Specifically, these well known bounds aid in the search for optimal codes which is the fundamental question of coding theory.

Let $A_q(n, d)$ be the maximum size of a q-ary code C of length n and minimum distance n. Then

$$A_q(n, d) \left(\sum_{j=0}^{d-1} \binom{n}{j} (q-1)^j \right) \geq q^n.$$

This is known as the Varshamov-Gilbert bound.

The linear programming bound puts restrictions on the maximum dimension of a code given the length and minimum distance using the MacWilliams relations.

Open Question 11.1. *Bridge the gap between Varshamov-Gilbert (VG) and Linear Programming (LP) bound.*

It was shown by Samorodnitsky [**67**] that the best bound the LP can give is at least the average of the bound of the four americans also known as the JPL bound [**44**], and of the Varshamov-Gilbert bound. But it was conjectured by Barg and Jaffe [**12**], based on extensive computations, that the best LP bound for large n is the JPL bound.

OPEN QUESTION 11.2. *Is the VG bound tight for $q = 2$? It is not for $q > 49$ thanks to AG codes and the TVZ bound* [**72**].

It is a folklore theorem that almost all codes are on VG.

OPEN QUESTION 11.3. *Is there any BCH bound for cyclic $\mathbb{Z}_4$-codes?*

The arguments to bound below the Lee distance of codes in [**37**] are very ad hoc. An obvious approach is to apply the BCH bound to the residue code but that is insufficient in the interesting cases, i.e. when the Hensel lift increases the Hamming distance.

12. Covering Radius

The sphere packing bound is as follows. If C is a code over an alphabet of size p with minimum weight $2t + 1$ then

$$|C| \left(\sum_{s=0}^{t} C(n, s)(p-1)^s \right) \leq p^n. \tag{17}$$

When this bound is met the code is said to be perfect. The Hamming and Golay codes are well known examples of perfect codes.

The covering radius of a code is the smallest integer t such that balls of radii t centered about codewords cover the ambient space. The covering radius is always more than the error correcting capacity with equality if and only if the code is perfect. All perfect linear codes over fields are known.

The first two open questions concerns perfect codes.

OPEN QUESTION 12.1. *Are there perfect codes over non prime power size alphabets? (Folklore).*

A great deal of work has been done on the prime power case, since that is the size of finite fields, however much less has been done in completing the study of perfect codes over non prime power alphabets.

OPEN QUESTION 12.2. *Classify all perfect nonlinear single error correcting codes* [**18**].

The next two questions are concerned with the smallest size a code can be with given parameters for a given covering radius. The smallest dimension of a linear code of length n and covering radius R is denoted by $k(n, R)$. The smallest size of a covering code of length n and covering radius R is denoted by $K(n, R)$.

OPEN QUESTION 12.3. *Is $K(n + 2, R + 1) \leq K(n, R)$ for all $R \neq n$?*[**18**].

OPEN QUESTION 12.4. *Is $k(n + 2, R + 1) \leq k(n, R)$ for all $R \neq n$?*[**18**].

These questions are obviously related. However, as in most coding questions, allowing codes to be non-linear complicates the question considerably.

For a definition of normal see [**18**].

OPEN QUESTION 12.5. *Are all linear codes normal? See* [**18**] *for details.*

The next questions concern determining the covering radius for various important families of codes.

Open Question 12.6. *Find the covering radius of the first order Reed-Muller code $R(1,m)$ for m odd* [**57**]. *The problem for even m is solved by the existence of bent functions.*

Open Question 12.7. *Find the exact covering radius of K_m (Kerdock code) described in* [**37**].

Lower and upper bounds, based on respectively, the supercode lemma and a moment method can be found in [**14**].

Let R_m denote the binary repetition code of length m.

Open Question 12.8. *What is the covering radius of $(R_m \otimes R_m)^\perp$?*

This question is related to the Gale Berlekamp game [**18**, Example 1.2.7], which is an array of m by m lightbulbs with one switch per row and per column. The aim of the game is to find the brightest configuration over all possible initial configurations. As an optimization problem it was shown to be NP-hard in [**66**]. As a hardware model ($m = 10$) it could still be found in Bell Labs in the early nineties. The solution for $m = 10$ was claimed to be 34 in [**32**], and proved to be 35 in [**15**] where the exact values up to 12 are computed. This problem is also related to the covering radius of cocycle codes of graphs [**6**, **70**].

13. Cyclic Codes

There is a longstanding question which is to know whether the class of cyclic codes is asymptotically good. Let us recall that a sequence of linear binary $[n_i, k_i, d_i]$ codes C_i is asymptotically good if both

$$\liminf_{i\to\infty} \frac{k_i}{n_i} > 0,$$

and

$$\liminf_{i\to\infty} \frac{d_i}{n_i} > 0.$$

Although it is known that the class of BCH codes is not asymptotically good [**13**, **43**], (see [**57**] for a proof), we do not know if there is a family of asymptotically good cyclic codes.

Still on the negative side, Castagnoli [**16**] has shown that, if the length n_i goes to infinity with i while having a fixed set of prime factors, then there is no asymptotically good family of codes C_i of length n_i. Other negative results are in [**5**]. Known partial positive results are due to Kasami [**48**], for quasicyclic codes. Bazzi-Mitter [**3**] have shown that there exists an asymptotically good family of linear codes which are very close to cyclic codes. Also Willems and Martinez-Perez [**58**] have shown that if there exists an asymptotically good family of cyclic codes, then there exists an asymptotically good family of cyclic codes with with prime lengths. So, although some progress has been achieved, the question is still open.

Open Question 13.1. *Are cyclic codes asymptotically good?*

14. Optimal 2-error Correcting Codes

This question in this section can be found in [**46**, Open Problem 1]. The Hamming codes give, in some sense, the best 1-error-correcting codes (see Niven [**62**]). In particular, if $n = (q^r - 1)/(q-1)$ then there is no shorter 1-error-correcting

code of dimension $k = n - r$. However, for $e > 1$ the best e-error-correcting codes of length n is unknown for large n, provided we assume e is fixed[1], e.g., $e = 2$. The search for the best 2-error correcting codes lead to the discovery of the BCH codes around 1960. However, the BCH codes are not known, in general, to provide all the optimal 2-error correcting codes.

OPEN QUESTION 14.1. Find the best linear 2-error-correcting code of length n.

This is also related to "Ulam's game" (see [**74**] and [**62**]) or "searching with lies." There is an extensive literature on this topic. See for example the two sections on searching with lies in [**47**].

15. Virtually Self-Dual Weight Enumerator

This section is about virtually self-dual weight enumerator. See [**46**, Ch. 3] for details. A homogeneous polynomial $F(x, y) = x^n + \sum_{i=1}^{n} f_i x^{n-i} y^i$ of degree n with complex coefficients is called a *virtual weight enumerator* with *support* $\mathrm{supp}(F) = \{0\} \cup \{i \mid f_i \neq 0\}$. If $F(x, y) = x^n + \sum_{i=d}^{n} A_i x^{n-i} y^i$ with $A_d \neq 0$ then we call n the *length* of F and d the *minimum distance* of F. Such an F of even degree satisfying $F(x, y) = F(\frac{x+(q-1)y}{\sqrt{q}}, \frac{x-y}{\sqrt{q}})$, is called a *virtually self-dual weight enumerator over* $GF(q)$ (or more generally over a ring of cardinality q) having *genus*

$$\gamma(F) = n/2 + 1 - d.$$

If $b > 1$ is an integer and $\mathrm{supp}(F) \subset b\mathbb{Z}$ then the virtual weight enumerator F is called *b-divisible*.

The classification of non-trivial formally self-dual divisible codes into the four Types has a virtually self-dual weight enumerator analog. In other words, the Gleason-Pierce theorem has a strengthening where the hypothesis does not require the existence of a code, only a form with certain invariance properties.

THEOREM 15.1. *(Gleason-Pierce-Turyn)* Let F be a b-divisible virtually self-dual weight enumerator over a ring of cardinality q.

Then either

I. $q = b = 2$,
II. $q = 2$, $b = 4$,
III. $q = b = 3$,
IV. $q = 4$, $b = 2$,
V. q is arbitrary, $b = 2$, and $F(x, y) = (x^2 + (q-1)y^2)^{n/2}$.

For examples of Type IV codes over the four rings of order four see [**28**].

A virtual weight enumerator F is formally identified with an object we call a *virtual code* C subject only to the following condition: we formally extend the definition of $C \longmapsto A_C$ to all virtual codes by $A_C = F$. Of course, if F is the weight enumerator of an actual code, C' say, then we have $A_C = F = A_{C'}$. In other words, a virtual code is only well-defined up to formal equivalence. If C_1 and C_2 are virtual codes then we define $C_1 + C_2$ to be the virtual code associated to the virtual weight enumerator $A_{C_1}(x, y) + A_{C_2}(x, y)$.

[1]If $e > 1$ is allowed to vary with n then more can be said, but we omit that case.

The following question [**46**, Open Problem 18.] is really more a question of the classification of self-dual codes than of virtually self-dual weight enumerators. An excellent reference is the book [**60**].

Open Question 15.2. Given a virtually self-dual weight enumerator F, find necessary and sufficient conditions (short of enumeration) which determine whether or not F arises as the weight enumerator of some self-dual code C.

References

[1] E. F. Assmus Jr. and H. F. Mattson Jr., *New* 5*-designs*, J. Combinatorial Theory **6** (1969), 122–151. MR0272647 (42 #7528)

[2] E. Bannai, S. T. Dougherty, M. Harada, and M. Oura, *Type II codes, even unimodular lattices, and invariant rings*, IEEE Trans. Inform. Theory **45** (1999), no. 4, 1194–1205, DOI 10.1109/18.761269. MR1686252 (2000i:94091)

[3] L. M. J. Bazzi and S. K. Mitter, *Some randomized code constructions from group actions*, IEEE Trans. Inform. Theory **52** (2006), no. 7, 3210–3219, DOI 10.1109/TIT.2006.876244. MR2240009 (2007c:94255)

[4] J.C. Belfiore and P. Solé, Unimodular lattices for the Gaussian wiretap channel, *Proceedings of ITW* 2010, Dublin.

[5] S. D. Berman, *Semisimple cyclic and Abelian codes. II*, Cybernetics **3** (1967), no. 3, 17–23 (1970). MR0274185 (42 #9060)

[6] G. Bowlin, *Maximum frustration in bipartite signed graphs*, Electron. J. Combin. **19** (2012), no. 4, Paper 10, 13. MR3001647

[7] S. Buyuklieva, *On the binary self-dual codes with an automorphism of order* 2, Des. Codes Cryptogr. **12** (1997), no. 1, 39–48, DOI 10.1023/A:1008289725040. MR1462520 (98d:94028)

[8] C. Bachoc and P. Gaborit, *On extremal additive* $\mathbf{F}_4$ *codes of length 10 to 18* (English, with English and French summaries), J. Théor. Nombres Bordeaux **12** (2000), no. 2, 255–271. Colloque International de Théorie des Nombres (Talence, 1999). MR1823184 (2002b:94056)

[9] S. Bouyuklieva, *On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length* 24*m*, Des. Codes Cryptogr. **25** (2002), no. 1, 5–13, DOI 10.1023/A:1012598832377. MR1881338 (2003f:94084)

[10] S. Bouyuklieva, E. A. O'Brien, and W. Willems, *The automorphism group of a binary self-dual doubly even* $[72, 36, 16]$ *code is solvable*, IEEE Trans. Inform. Theory **52** (2006), no. 9, 4244–4248, DOI 10.1109/TIT.2006.880048. MR2298550 (2007m:94199)

[11] R. A. Brualdi and V. S. Pless, *Weight enumerators of self-dual codes*, IEEE Trans. Inform. Theory **37** (1991), no. 4, 1222–1225, DOI 10.1109/18.86979. MR1111828 (92f:94026)

[12] A. Barg and D. B. Jaffe, *Numerical results on the asymptotic rate of binary codes*, Codes and association schemes (Piscataway, NJ, 1999), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 56, Amer. Math. Soc., Providence, RI, 2001, pp. 25–32. MR1816385 (2001m:94066)

[13] P. Camion, *A proof of some properties of Reed-Muller codes by means of the normal basis theorem*, Combinatorial Mathematics and its Applications (Proc. Conf., Univ. North Carolina, Chapel Hill, N.C., 1967), Univ. North Carolina Press, Chapel Hill, N.C., 1969, pp. 371–376. MR0249172 (40 #2419)

[14] C. Carlet, *On Kerdock codes*, Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997), Contemp. Math., vol. 225, Amer. Math. Soc., Providence, RI, 1999, pp. 155–163, DOI 10.1090/conm/225/03217. MR1650612 (99m:94054)

[15] J. Carlson and D. Stolarski, *The correct solution to Berlekamp's switching game*, Discrete Math. **287** (2004), no. 1-3, 145–150, DOI 10.1016/j.disc.2004.06.015. MR2094708 (2005d:05005)

[16] G. Castagnoli, *On the asymptotic badness of cyclic codes with block-lengths composed from a fixed set of prime factors*, Applied algebra, algebraic algorithms and error-correcting codes (Rome, 1988), Lecture Notes in Comput. Sci., vol. 357, Springer, Berlin, 1989, pp. 164–168, DOI 10.1007/3-540-51083-4_56. MR1008500 (90e:94034)

[17] http://en.wikipedia.org/wiki/Clique_problem

[18] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering codes*, North-Holland Mathematical Library, vol. 54, North-Holland Publishing Co., Amsterdam, 1997. MR1453577 (99b:94059)

[19] J. H. Conway and V. Pless, *On primes dividing the group order of a doubly-even* (72, 36, 16) *code and the group order of a quaternary* (24, 12, 10) *code*, Discrete Math. **38** (1982), no. 2-3, 143–156, DOI 10.1016/0012-365X(82)90284-9. MR676531 (84g:94015)

[20] J. H. Conway and N. J. A. Sloane, *A new upper bound on the minimal distance of self-dual codes*, IEEE Trans. Inform. Theory **36** (1990), no. 6, 1319–1333, DOI 10.1109/18.59931. MR1080819 (91m:94024)

[21] D. B. Dalan, *New extremal type I codes of lengths 40, 42, and 44*, Des. Codes Cryptogr. **30** (2003), no. 2, 151–157, DOI 10.1023/A:1025476619824. MR2007207 (2004h:94055)

[22] L. E. Danielsen and M. G. Parker, *On the classification of all self-dual additive codes over* GF(4) *of length up to 12*, J. Combin. Theory Ser. A **113** (2006), no. 7, 1351–1367, DOI 10.1016/j.jcta.2005.12.004. MR2259065 (2007g:94083)

[23] L. E. Danielsen and M. G. Parker, *On the classification of all self-dual additive codes over* GF(4) *of length up to 12*, J. Combin. Theory Ser. A **113** (2006), no. 7, 1351–1367, DOI 10.1016/j.jcta.2005.12.004. MR2259065 (2007g:94083)

[24] S. T. Dougherty and T. A. Gulliver, *Higher weights and binary self-dual codes*, International Workshop on Coding and Cryptography (Paris, 2001), Electron. Notes Discrete Math., vol. 6, Elsevier, Amsterdam, 2001, pp. 12 pp. (electronic). MR1985267 (2004i:94056)

[25] S. T. Dougherty and K. Shiromoto, *Maximum distance codes over rings of order 4*, IEEE Trans. Inform. Theory **47** (2001), no. 1, 400–404, DOI 10.1109/18.904544. MR1820385 (2002b:94057)

[26] S. T. Dougherty and S. Han, *Higher weights and generalized MDS codes*, J. Korean Math. Soc. **47** (2010), no. 6, 1167–1182, DOI 10.4134/JKMS.2010.47.6.1167. MR2744205 (2011j:94182)

[27] S. T. Dougherty, J.-L. Kim, and H. Kulosman, *MDS codes over finite principal ideal rings*, Des. Codes Cryptogr. **50** (2009), no. 1, 77–92, DOI 10.1007/s10623-008-9215-5. MR2480670 (2010e:94282)

[28] S. T. Dougherty, P. Gaborit, M. Harada, A. Munemasa, and P. Solé, *Type IV self-dual codes over rings*, IEEE Trans. Inform. Theory **45** (1999), no. 7, 2345–2360, DOI 10.1109/18.796375. MR1725122 (2001b:94045)

[29] R. G. Downey, M. R. Fellows, A. Vardy, and G. Whittle, *The parametrized complexity of some fundamental problems in coding theory*, SIAM J. Comput. **29** (1999), no. 2, 545–570, DOI 10.1137/S0097539797323571. MR1744679 (2001g:94033)

[30] A. M. Ernvall-Hytönen, On a conjecture by Belfiore and Solé on some lattices, arXiv:1303.7460

[31] A.-M. Ernvall-Hytönen, *Some results related to the conjecture by Belfiore and Solé*, IEEE Trans. Inform. Theory **60** (2014), no. 5, 2805–2812. MR3200627

[32] P. C. Fishburn and N. J. A. Sloane, *The solution to Berlekamp's switching game*, Discrete Math. **74** (1989), no. 3, 263–290, DOI 10.1016/0012-365X(89)90141-6. MR992740 (90e:90151)

[33] A. M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities*, Actes du Congrès International des Mathématiciens (Nice, 1970), Gauthier-Villars, Paris, 1971, pp. 211–215. MR0424391 (54 #12354)

[34] K. Guenda and T. A. Gulliver, *MDS and self-dual codes over rings*, Finite Fields Appl. **18** (2012), no. 6, 1061–1075, DOI 10.1016/j.ffa.2012.09.003. MR3019184

[35] T. A. Gulliver, M. Harada, and J.-L. Kim, *Construction of new extremal self-dual codes*, Discrete Math. **263** (2003), no. 1-3, 81–91, DOI 10.1016/S0012-365X(02)00570-8. MR1955716 (2003m:94083)

[36] R. W. Hamming, *Error detecting and error correcting codes*, Bell System Tech. J. **29** (1950), 147–160. MR0035935 (12,35c)

[37] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The* $\mathbf{Z}_4$*-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 301–319, DOI 10.1109/18.312154. MR1294046 (95k:94030)

[38] R. Hill, *A first course in coding theory*, Oxford Applied Mathematics and Computing Science Series, The Clarendon Press, Oxford University Press, New York, 1986. MR853914 (87m:94024)

[39] S. K. Houghten, C. W. H. Lam, L. H. Thiel, and J. A. Parker, *The extended quadratic residue code is the only* $(48, 24, 12)$ *self-dual doubly-even code*, IEEE Trans. Inform. Theory **49** (2003), no. 1, 53–59, DOI 10.1109/TIT.2002.806146. MR1965886 (2004c:94114)

[40] W. C. Huffman, *Automorphisms of codes with applications to extremal doubly even codes of length* 48, IEEE Trans. Inform. Theory **28** (1982), no. 3, 511–521, DOI 10.1109/TIT.1982.1056499. MR672886 (84e:94016)

[41] W. C. Huffman and V. Y. Yorgov, *A* $[72, 36, 16]$ *doubly even code does not have an automorphism of order* 11, IEEE Trans. Inform. Theory **33** (1987), no. 5, 749–752, DOI 10.1109/TIT.1987.1057339. MR918202 (89a:94021)

[42] M. Kiermaier, *There is no self-dual* $\mathbb{Z}_4$*-linear code whose gray image has the parameters* $(72, 2^{36}, 16)$, IEEE Trans. Inform. Theory **59** (2013), no. 6, 3384–3386, DOI 10.1109/TIT.2013.2246816. MR3061253

[43] S. Lin and E. J. Weldon, Jr., Long BCH codes are bad, *Inform. Control,* vol. 11, no. 4, (October 1967), 445-451.

[44] R. J. McEliece, E. R. Rodemich, H. Rumsey Jr., and L. R. Welch, *New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities*, IEEE Trans. Information Theory **IT-23** (1977), no. 2, 157–166. MR0439403 (55 #12296)

[45] G. J. Janusz, *Overlap and covering polynomials with applications to designs and self-dual codes*, SIAM J. Discrete Math. **13** (2000), no. 2, 154–178 (electronic), DOI 10.1137/S0895480198341766. MR1760334 (2001m:94060)

[46] D. Joyner and J.-L. Kim, *Selected unsolved problems in coding theory*, Applied and Numerical Harmonic Analysis, Birkhäuser/Springer, New York, 2011. MR2838861 (2012i:94003)

[47] D. Joyner, R. Kreminski, and J. Turisco, *Applied abstract algebra*, Johns Hopkins University Press, Baltimore, MD, 2004. MR2378252

[48] T. Kasami, *A Gilbert-Varshamov bound for quasi-cyclic codes of rate* 1/2, IEEE Trans. Information Theory **IT-20** (1974), 679. MR0371494 (51 #7712)

[49] H. J. Kim, *Self-dual codes with automorphism of order 3 having 8 cycles*, Des. Codes Cryptogr. **57** (2010), no. 3, 329–346, DOI 10.1007/s10623-010-9370-3. MR2679151 (2011j:94184)

[50] P. Gaborit, W. C. Huffman, J.-L. Kim, and V. Pless, *On additive* GF(4) *codes*, Codes and association schemes (Piscataway, NJ, 1999), DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 56, Amer. Math. Soc., Providence, RI, 2001, pp. 135–149. MR1816395 (2002c:94046)

[51] P. Gaborit, J.-L. Kim, and V. Pless, *Decoding binary* $R(2, 5)$ *by hand*, Discrete Math. **264** (2003), no. 1-3, 55–73, DOI 10.1016/S0012-365X(02)00550-2. The 2000 Com^{2}MaC Conference on Association Schemes, Codes and Designs (Pohang). MR1972021 (2004f:94118)

[52] M. Harada and T. Miezaki, On the existence of extremal Type II $\mathbb{Z}_{2k}$ codes, `http://sci.kj.yamagata-u.ac.jp/ mharada/Paper/Z2k-32-64.pdf`.

[53] M. Harada and A. Munemasa, *Classification of self-dual codes of length 36*, Adv. Math. Commun. **6** (2012), no. 2, 229–235, DOI 10.3934/amc.2012.6.229. MR2924228

[54] G. Höhn, *Self-dual codes over the Kleinian four group*, Math. Ann. **327** (2003), no. 2, 227–255, DOI 10.1007/s00208-003-0440-y. MR2015068 (2004i:94063)

[55] F. Lin and F. Oggier, *A classification of unimodular lattice wiretap codes in small dimensions*, IEEE Trans. Inform. Theory **59** (2013), no. 6, 3295–3303, DOI 10.1109/TIT.2013.2246814. MR3061247

[56] M. Harada, M. Kitazume, A. Munemasa, and B. Venkov, *On some self-dual codes and unimodular lattices in dimension 48*, European J. Combin. **26** (2005), no. 5, 543–557, DOI 10.1016/j.ejc.2004.06.013. MR2126638 (2005m:94044)

[57] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North Holland, (1977).

[58] C. Martínez-Pérez and W. Willems, *Is the class of cyclic codes asymptotically good?*, IEEE Trans. Inform. Theory **52** (2006), no. 2, 696–700, DOI 10.1109/TIT.2005.862123. MR2236182 (2007a:94259)

[59] G. Nebe, *An even unimodular 72-dimensional lattice of minimum 8*, J. Reine Angew. Math. **673** (2012), 237–247. MR2999133

[60] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Self-dual codes and invariant theory*, Algorithms and Computation in Mathematics, vol. 17, Springer-Verlag, Berlin, 2006. MR2209183 (2007d:94066)

[61] G. Nebe, *An extremal* $[72, 36, 16]$ *binary code has no automorphism group containing* $Z_2 \times Z_4$*,* Q_8*, or* Z_{10}, Finite Fields Appl. **18** (2012), no. 3, 563–566, DOI 10.1016/j.ffa.2011.12.001. MR2899897

[62] I. Niven, *Coding theory applied to a problem of Ulam*, Math. Mag. **61** (1988), no. 5, 275–281, DOI 10.2307/2689543. MR979025 (90f:68035)

[63] E. A. O'Brien and W. Willems, *On the automorphism group of a binary self-dual doubly even* [72, 36, 16] *code*, IEEE Trans. Inform. Theory **57** (2011), no. 7, 4445–4451, DOI 10.1109/TIT.2011.2145850. MR2840465 (2012g:94135)

[64] J. Pinchak, Wiretap Codes: Families of Lattices Satisfying the Belfiore-Solé, Secrecy Function Conjecture, *Proceedings of ISIT*, 2013.

[65] V. Pless and J. G. Thompson, 17 *does not divide the order of the group of a* (72, 36, 16) *doubly even code*, IEEE Trans. Inform. Theory **28** (1982), no. 3, 537–541, DOI 10.1109/TIT.1982.1056503. MR672889 (83j:94022)

[66] R. M. Roth and K. Viswanathan, *On the hardness of decoding the Gale-Berlekamp code*, IEEE Trans. Inform. Theory **54** (2008), no. 3, 1050–1060, DOI 10.1109/TIT.2007.915716. MR2445050 (2010h:94267)

[67] A. Samorodnitsky, *On the optimum of Delsarte's linear program*, J. Combin. Theory Ser. A **96** (2001), no. 2, 261–287, DOI 10.1006/jcta.2001.3176. MR1864123 (2003g:94065)

[68] C. E. Shannon, *A mathematical theory of communication*, Bell System Tech. J. **27** (1948), 379–423, 623–656. MR0026286 (10,133e)

[69] N. J. A. Sloane, *Is there a* $(72, 36)d = 16$ *self-dual code?*, IEEE Trans. Information Theory **IT-19** (1973), no. 2, 251. MR0421849 (54 #9843)

[70] P. Solé and T. Zaslavsky, *A coding approach to signed graphs*, SIAM J. Discrete Math. **7** (1994), no. 4, 544–553, DOI 10.1137/S0895480189174374. MR1299082 (95k:94041)

[71] R. C. Singleton, *Maximum distance q-nary codes*, IEEE Trans. Information Theory **IT-10** (1964), 116–118. MR0164827 (29 #2118)

[72] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28, DOI 10.1002/mana.19821090103. MR705893 (85i:11108)

[73] M. A. Tsfasman and S. G. Vlăduţ, *Geometric approach to higher weights*, IEEE Trans. Inform. Theory **41** (1995), no. 6, 1564–1588, DOI 10.1109/18.476213. Special issue on algebraic geometry codes. MR1391017 (97m:94042)

[74] S. M. Ulam, *Adventures of a mathematician*, Charles Scribner's Sons, New York, 1976. MR0485098 (58 #4954)

[75] V. K. Wei, *Generalized Hamming weights for linear codes*, IEEE Trans. Inform. Theory **37** (1991), no. 5, 1412–1418, DOI 10.1109/18.133259. MR1136673 (92i:94019)

[76] J. A. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. **121** (1999), no. 3, 555–575. MR1738408 (2001d:94033)

[77] N. Yankov, *A putative doubly even* [72, 36, 16] *code does not have an automorphism of order 9*, IEEE Trans. Inform. Theory **58** (2012), no. 1, 159–163, DOI 10.1109/TIT.2011.2165829. MR2907709 (2012k:94219)

Department of Mathematics, University of Scranton, Scranton, Pennsylvania 18518
E-mail address: prof.steven.dougherty@gmail.com

Department of Mathematics, Sogang University, Seoul, 121-742, S. Korea
E-mail address: jlkim@sogang.ac.kr

Telecom Paris Tech, Paris, France – and – University King Abdul Aziz, Jeddah, Saudi Arabia
E-mail address: sole@enst.fr