References


Following are the two main results of this paper, that the Radius and the Covering Radius of a code are hard to compute.

**Theorem 3:** *The Minimum Radius Problem is NP-complete.*

**Proof:** First, note that this problem is in NP, as a center of a $k$-radius sphere which contains $C$ is a linear time verifiable witness to the fact that $R(C) \leq k$.

To show that the problem is NP hard, we reduce 3SAT to MR. Given a 3CNF formula $\Omega = \omega^1 \land \ldots \land \omega^t$, we define the following code of length $2(n + 1)$:

$$C_{\Omega} \triangleq \{00, \ldots, \widehat{00}\}.$$  

Observe that the code $C_{\Omega}$ is computable in polynomial time from the formula $\Omega$.

We now prove the following validity claim of the reduction:

$$\Omega \text{ is satisfiable } \iff R(C_{\Omega}) \leq n + 1.$$  

Let $v \in \{0, 1\}^n$ be a satisfying assignment for $\Omega$. Since $(\Pi(v)^00)$ is doubled, Lemma 2 implies that

$$Y_{2(n+1)} \subseteq B_{2(n+1)}((\Pi(v)^00, n + 1).$$

Claim 4 indicates that $\{\widehat{00}, \ldots, \widehat{00}\} \subseteq B_{2n}(\Pi(v), n + 1)$. Thus, by Fact 1

$$\{\widehat{00}, \ldots, \widehat{00}\} \subseteq B_{2(n+1)}((\Pi(v)^00, n + 1).$$

Hence, $C_{\Omega} \subseteq B_{2(n+1)}((\Pi(v)^00, n + 1)$, and $R(C_{\Omega}) \leq n + 1$.

For the other direction, let $b \in \{0, 1\}^{2(n+1)}$ be a center of a $(n + 1)$-radius sphere which contains $C_{\Omega}$. In particular, $Y_{2(n+1)} \subseteq B_{2(n+1)}(b, n + 1)$. Thus, Lemma 2 implies that $b$ is doubled. Therefore, there exists a vector $v \in \{0, 1\}^n$ such that $\Pi(v) = b^{2n}$. As

$$\{\widehat{00}, \ldots, \widehat{00}\} \subseteq B_{2(n+1)}(b, n + 1).$$

Fact 1 implies that

$$\{\widehat{00}, \ldots, \widehat{00}\} \subseteq B_{2n}(b^{2n}, n + 1) = B_{2n}(\Pi(v), n + 1).$$

Claim 4 implies that the assignment $v$ satisfies $\Omega$.

As a consequence of Corollary 2 and Theorem 3 we get:

**Theorem 4:** *The Maximum Covering Radius problem is NP-complete.*

**Acknowledgements** We would like to thank Shimon Even, Ronny Roth, Tuvi Etzion, Amos Beimel and Ofra Hod for helpful discussions.
The 3SAT Problem:
Input: A 3CNF formula \( F \).
Question: Is \( F \) satisfiable?

The 3SAT problem is known to be NP complete (see e.g. [GJ79]). In the following we present a polynomial reduction of the 3SAT problem to the MR problem. First, we present the reduction of a single 3-clause, and then extend it to a general 3CNF formula.

For a 3-clause \( \omega \) which is defined over the variables \( x_1, \ldots, x_n \), we define the vector
\[
\hat{\omega} = \hat{\omega}_1 \ldots \hat{\omega}_{2n} \in \{0,1\}^{2n}
\]
by:
\[
\forall i = 1, \ldots, n \quad \hat{\omega}_{2i-1} \hat{\omega}_{2i} \triangleq \begin{cases} 
00 & \text{if } \omega \text{ contains the literal } \neg x_i; \\
11 & \text{if } \omega \text{ contains the literal } x_i; \\
01 & \text{otherwise}.
\end{cases}
\]

Note that \( \hat{\omega} \) is defined via its blocks, and exactly three of its blocks are repetition ones. For example, the corresponding vector of the 3-clause \( \omega = x_1 \lor x_2 \lor \neg (x_3) \) is \( \hat{\omega} = 1111000101 \ldots 01 \).

Define \( \Pi : \{0,1\}^n \to \{0,1\}^{2n} \) by \( \Pi(v_1 v_2 \ldots v_n) = v_1 v_2 v_3 \ldots v_n v_n \). Observe that \( \Pi \) is a one to one map from \( \{0,1\}^n \) onto the set of all doubled vectors in \( \{0,1\}^{2n} \).

Claim 3: Let \( \omega \) be a 3-clause defined over the variables \( x_1, \ldots, x_n \), then for each \( v \in \{0,1\}^n \)
\[
\hat{\omega} \in B_{2n}(\Pi(v), n + 1) \iff \text{the assignment } v \text{ satisfies } \omega.
\]

Proof: Assume, without loss of generality, that the three literals of \( \omega \) are defined over the variables \( x_1, x_2 \) and \( x_3 \). Fact 1 implies that
\[
d(\Pi(v), \hat{\omega}) = d(\Pi(v)\hat{\omega}^0, \hat{\omega}^0) + d(\Pi(v)\hat{\omega}^0, \hat{\omega}^{2n}).
\]
As \( \Pi(v) \) is doubled and the last \( n-3 \) blocks of \( \hat{\omega} \) are non-repetition blocks,
\[
d(\Pi(v)\hat{\omega}^0, \hat{\omega}^{2n}) = n - 3.
\]
Since the first three blocks of \( \hat{\omega} \) are repetitions,
\[
d(\Pi(v)\hat{\omega}^0, \hat{\omega}^0) \leq 4 \iff \exists i \in \{1,2,3\} \text{ s.t. } (\Pi(v))(2i-1)(\Pi(v))2i = \hat{\omega}_{2i-1}\hat{\omega}_{2i}.
\]
By the definition of \( \hat{\omega} \), this happens iff there is an \( i \in \{1,2,3\} \) such that \( v_i = \hat{\omega}_{2i} \). This is equivalent to the fact that the assignment \( v \) satisfies the clause \( \omega \).

\[\square\]

The next claim characterizes the satisfying assignments of a 3-CNF formula. It is an immediate consequence of Claim 3.

Claim 4: Let \( \Omega = \omega^1 \land \ldots \land \omega^t \) be a 3CNF formula defined over the variables \( x_1, \ldots, x_n \), then for each vector \( v \in \{0,1\}^n \)
\[
\{\hat{\omega}^1, \ldots, \hat{\omega}^t\} \subseteq B_{2n}(\Pi(v), n + 1) \iff \text{the assignment } v \text{ satisfies the formula } \Omega.
\]
Let $S_i: \{0,1\}^{2n} \rightarrow \{0,1\}^{2n}$ denote the circular right shift of $2i-2$ bits. For $i = 2, \ldots, n$, define 
$$Y^i_{2n} \triangleq S_i(Y^1_{2n}).$$
Note that the equation $Y^i_{2n} = S_i(Y^1_{2n})$ holds.

Claim 2: If $Y^i_{2n} \subseteq B_{2n}(v,n)$ for $v = (v_1 \ldots v_{2n}) \in \{0,1\}^{2n}$, then $v_{2i-1} = v_{2i}$.

Proof: Note that $S_i$ is an isomorphism of the metric space $\langle \{0,1\}^{2n}, d \rangle$, i.e., a distances preserving one to one map from the metric space onto itself. Hence, for each $i$: $Y^i_{2n} \subseteq B_{2n}(v,n)$ iff $Y^i_{2n} \subseteq B_{2n}(S_i^{-1}(v),n)$. Moreover, for each $v \in \{0,1\}^{2n}$: $v_{2i-1} = v_{2i}$ iff $(S_i^{-1}(v))_1 = (S_i^{-1}(v))_2$. Thus, Claim 1 implies that if $v$ satisfies $Y^i_{2n} \subseteq B_{2n}(v,n)$ then $v_{2i-1} = v_{2i}$.

The following Lemma characterizes the doubled vectors in $\{0,1\}^{2n}$ as the centers of spheres of radius $n$ which contains a specific set of at most $4n$ vectors.

Lemma 2: For each positive integer $n$ there exists a set of vectors $Y_{2n} \subseteq \{0,1\}^{2n}$ such that $|Y_{2n}| \leq 4n$ and for every $v \in \{0,1\}^{2n}$
$$v \text{ is doubled } \iff Y_{2n} \subseteq B_{2n}(v,n).$$

Proof: Define $Y_{2n}$ by 
$$Y_{2n} \triangleq Y^1_{2n} \cup Y^2_{2n} \cup \ldots \cup Y^n_{2n}.$$ 
Clearly, $|Y_{2n}| \leq 4n$ (in fact, $|Y_{2n}| = 2n + 2$).

Let us assume that $Y_{2n} \subseteq B_{2n}(v,n)$. Since $Y^i_{2n} \subseteq B_{2n}(v,n)$ for each $i$, by Claim 2, $v_{2i-1} = v_{2i}$ for each $i$.

For the other direction, let $v$ be a doubled vector, and let $y \in Y_{2n}$. Any block of $y$ is a non repetition one, while any block of $v$ is a repetition. Hence $d(v_{2i-1},v_{2i},y_{2i-1},y_{2i}) = 1$ for each $i$. Multiple use of Fact 1 implies that $d(v,y) = n$. Thus $Y_{2n} \subseteq B_{2n}(v,n)$.

\[ \square \]

5 MR and MCR are NP complete

In this section we prove that the problems MR and MCR are both NP complete, via a reduction from the 3SAT problem to MR.

Definition 2: Let $X = \{x_1, \ldots, x_n\}$ be a set of boolean variables. Following are definitions of boolean formulas over $X$.

- A literal is either $x_i$ or $\neg x_i$ for some $i$.
- A 3-clause is a disjunction of three distinct literals, made of three different variables.
- A 3CNF formula is a conjunction of 3-clauses.
The following Theorem, proved in [Kar81], states that the Covering Radius and the Radius of a code are strongly related. We present a proof for the sake of completeness.

**Theorem 1:** For any code $C \subseteq \{0, 1\}^n$:

$$CR(C) + R(C) = n.$$  

**Proof:** Let $v \in \{0, 1\}^n$ be a vector such that $C \subseteq B_n(v, R(C))$. Lemma 1 implies that $C \cap B_n(v^c, n - R(C) - 1) = \emptyset$, which means that $d(v^c, c) > n - R(C) - 1$ for every $c \in C$. Thus $CR(C) > n - R(C) - 1$.

To complete the proof, let $r = R(C) - 1$. From the definition of $R(C)$, $C \not\subseteq B_n(v, r)$ for every $v \in \{0, 1\}^n$. Hence, by Lemma 1, $C \cap B_n(v^c, n - r - 1) \neq \emptyset$ for every $v$. Therefore, for each $v$ there exists $c \in C$ such that $d(v, c) \leq n - r - 1$. Thus, $CR(C) \leq n - r - 1 = n - R(C)$.

□

**Corollary 2:** The MR and the MCR problems are computationally equivalent.

4 Doubled Vectors

**Definition 1:** We say that a vector $v = (v_1v_2 \ldots v_{2n}) \in \{0, 1\}^{2n}$ is **doubled** if $v_{2i} = v_{2i-1}$ for each $i = 1, \ldots, n$.

We are about to present an intriguing characterization of all doubled vectors in $\{0, 1\}^{2n}$. We present a small set of vectors in $\{0, 1\}^{2n}$ and prove that all the centers of $n$-radius spheres that contain this set are exactly all doubled vectors in $\{0, 1\}^{2n}$ (Lemma 2 below).

Let $\lambda_k$ denote a $k$-times concatenation of 01, namely, $\lambda_k = 0101 \ldots 01 \in \{0, 1\}^{2k}$. We define a set of four vectors of length $2n$ as follows.

$$Y_{2n}^1 \triangleq \{\lambda_1, \lambda_1^c\} \cdot \{\lambda_{n-1}, \lambda_{n-1}^c\}.$$  

**Claim 1:** If $Y_{2n}^1 \subseteq B_{2n}(v, n)$ for $v \in \{0, 1\}^{2n}$ then the first two bits of $v$ are equal.

**Proof:** Assume, to the contrary of the claim, that $v_1 \neq v_2$. Let $\alpha = (v_1v_2)^c$. Since the two vectors, $(\alpha^c \lambda_{n-1})$ and $(\alpha^c \lambda_{n-1}^c)$, are in $Y_{2n}^1$:

$$2n \geq d(v, \alpha^c \lambda_{n-1}) + d(v, \alpha^c \lambda_{n-1}^c).$$

Fact 1 and the triangle inequality imply:

$$d(v, \alpha^c \lambda_{n-1}) + d(v, \alpha^c \lambda_{n-1}^c) = d(v_1v_2v_1^{2n}, \alpha^c \lambda_{n-1}) + d(v_1v_2v_1^{2n}, \alpha^c \lambda_{n-1}^c) =$$

$$4 + d(v_1^{2n}, \lambda_{n-1}) + d(v_1^{2n}, \lambda_{n-1}^c) \geq 4 + d(\lambda_{n-1}, \lambda_{n-1}^c) = 4 + 2(n - 1) = 2n + 2 > 2n,$$

in contradiction to the previous inequality.

□
2 Preliminaries

Let \( v \in \{0, 1\}^n \) be a binary vector. The \( i \)-th bit of \( v \) is denoted by \( v_i \). For \( 1 \leq i < j \leq n \), let \( v_{ij} \) denote the vector \( v_i \ldots v_j \). We write \( v^c \) for the 1's-complement of the vector \( v \) (we shall say ‘complement’ for short). We denote the length of a vector \( v \) by \( |v| \).

Throughout this paper we consider binary vectors of length \( 2k \), for some integer \( k \). Occasionally, such vector \( v \) is defined by presenting its consecutive pairs of bits, \( v_{2i-1}, v_{2i} \) for \( i = 1, \ldots, k \). We call such a pair the \( i \)-th block of \( v \). If \( v_{2i-1} = v_{2i} \) we shall call this block a repetition block or a repetition for short, otherwise we say that it is a non-repetition block. Finally, for two binary vectors \( w \in \{0, 1\}^k \) and \( z \in \{0, 1\}^\ell \), let \( w'z' \) denote the concatenation of \( w \) and \( z \). For two sets of vectors \( A \) and \( B \) we denote \( A \cup B = \{a'b' | a \in A, b \in B\} \).

In this paper we study the following two problems.

The Minimum Radius Problem (MR):
Input: A code \( C \subseteq \{0, 1\}^n \) and a positive integer \( k \).
Question: Is \( R(C) \leq k \) ?

The Maximum Covering Radius Problem (MCR):
Input: A code \( C \subseteq \{0, 1\}^n \) and a positive integer \( k \).
Question: Is \( CR(C) \geq k \) ?

3 \( R(C) \) and \( CR(C) \) are Related

We start by presenting two properties of the Hamming metric.

**Fact 1:** Let \( a_1, a_2 \) and \( b_1, b_2 \) be four binary vectors such that \( |a_1| = |a_2| \) and \( |b_1| = |b_2| \), then
\[
d(a_1b_1, a_2b_2) = d(a_1, b_1) + d(a_2, b_2).
\]

**Lemma 1:** Let \( a \in \{0, 1\}^n \), then the complement of \( B_n(a, r) \) in \( \{0, 1\}^n \) is \( B_n(a^c, n-r-1) \).

**Proof:** \( v \not\in B_n(a, r) \iff d(v, a) > r \iff a \text{ and } v \text{ differ in at least } r+1 \text{ components} \iff a^c \text{ and } v \text{ agree on at least } r+1 \text{ components} \iff d(a^c, v) \leq n-(r+1) \iff v \in B_n(a^c, n-(r+1)) \).
work of Berlekamp et. al. [BMT78], McLoughlin has shown that the problem of computing the Covering Radius of a linear code, where the code is given in some compact form, is complete for the class $\Pi_2^p$ in the polynomial hierarchy [McI84]. Hence, it is an NP-hard problem which is apparently not in NP. We address the problems of computing the Covering Radius and the Radius of a code in a different setting; we consider arbitrary code (i.e., not necessarily linear), and assume an explicit representation of the code, namely a list of all code words. We show that in this setting both problems are NP-complete.

To this end, we introduce an intriguing characterization of the following set of binary vectors of length $2n$: \( \{ v = v_1v_2 \ldots v_{2n} \mid v_{2i} = v_{2i-1} \ \forall i = 1, \ldots, n \} \) (“doubled vectors”). We show that these vectors are exactly the set of the centers of all $n$-radius spheres which contains a specific set of $O(n)$ vectors.
1 Introduction

In this paper we consider elements of \( \{0,1\}^n \), called vectors, and subsets of \( \{0,1\}^n \), called codes. For two vectors \( u, v \in \{0,1\}^n \), we write \( d(u,v) \) for the Hamming distance between them. The sphere in \( \{0,1\}^n \) of radius \( r \) with center \( a \in \{0,1\}^n \) is the set of all vectors \( v \in \{0,1\}^n \) such that \( d(v,a) \leq r \), and is denoted by \( B_n(a,r) \). The Covering Radius of a code \( C \), denoted by \( CR(C) \), is the smallest integer \( r \) such that each vector in \( \{0,1\}^n \) is at a distance at most \( r \) from some code word. The Packing Radius of a code \( C \), denoted by \( PR(C) \), is the largest integer \( r \) such that all spheres with radius \( r \) and centers in \( C \) are disjoint. The Radius of a code \( C \), denoted by \( R(C) \), is the smallest integer \( r \) such that \( C \subseteq B_n(v,r) \) for some vector \( v \). We use a result of Karpovsky [Kar81], that the Covering Radius and the Radius of a code are strongly related (Theorem 1 below).

The Covering Radius plays an important role in Coding theory. Suppose we would like to transmit messages on a noisy channel, where each message is a code word that is a member of a code \( C \subseteq \{0,1\}^n \). Since the channel is noisy, errors can occur, and the vector which arrives at the receiving end might differ from the original code word. The difference between those two vectors is called the error vector. The number of the non-zero bits of the error vector is the weight of the error. When the receiver gets a vector its goal is to reconstruct the original code word. This problem is the decoding problem.

One simple decoding strategy is to find the code word which is the one nearest to the received vector. This strategy is called Maximum Likelihood decoding and is based on the assumption that the smallest number of bit errors have occurred. This assumption is reasonable when the probability of a bit error on the channel is a constant smaller than \( \frac{1}{2} \), and all bit errors are independent. Both the Packing Radius and the Covering Radius are important parameters in this context, as the Maximum Likelihood decoding will correct all errors with weight up to the Packing Radius, none with weight more than the Covering Radius, and some with weight between the two.

The Minimum Distance of a code \( C \), denoted by \( DIST(C) \), is the smallest distance between two code words. Note that the Packing Radius and the Minimum Distance of a code satisfy the following simple equation: \( PR(C) = \lceil \frac{DIST(C)-1}{2} \rceil \). As mentioned above, the Packing Radius characterizes the error correctness capability of a code in the Maximum Likelihood decoding strategy. Therefore, one would like to have a code which consists of a large number of code words, with short length (to minimize transmission time), and large Packing Radius (i.e. large Minimum Distance). A maximal code is a code that has no proper super-code with the same Minimum Distance. Maximal codes are characterized by the fact that their Covering Radius is smaller than their Minimum Distance. This observation and other issues concerning the roles of the Covering Radius in Coding theory are surveyed in [CKMS84].

One extensively studied issue in Coding theory is the subject of linear codes. A linear code \( C \) is a vector space over \( GF[2] \). Such codes are easy to work with as they have compact representations and possess many nice features due to their algebraic simple structure.

In this paper we study the complexity of computing two parameters of a code, the Covering Radius and the Radius. As much as we know, previous work on this subject has been done only in the framework of linear codes. In that setting, a code is represented in some compact form (e.g., its parity check matrix or its generator matrix). Building on the
On Covering Problems of Codes

Moti Frances  Ami Litman
Department of Computer Science
Technion, Haifa 32000, Israel

Abstract

Let $C$ be a binary code of length $n$. The Radius of $C$ is the smallest integer $r$ such that $C$ is contained in an $r$-radius ball in the Hamming metric space $\langle \{0,1\}^n, d \rangle$. The Covering Radius of $C$ is the smallest integer $r$ such that each vector in $\{0,1\}^n$ is at a distance at most $r$ from some code word. We show that the problems of computing the Radius and the Covering Radius of an arbitrary binary code are both NP complete.

A central tool in our work is an intriguing characterization of the following set of binary vectors of length $2n$: $\{v = v_1v_2\ldots v_{2n} \mid v_{2i} = v_{2i-1} \forall i = 1, \ldots, n\}$ (doubled vectors). We show that there is a specific set $Y$ of $O(n)$ vectors such that the doubled vectors are exactly the centers of all $n$-radius spheres which contains $Y$. 