Generic Decoding in the Cover Metric

Sebastian Bitzer, Julian Renner, Antonia Wachtler-Zeh, Violetta Weger
Technical University of Munich, Germany
{sebastian.bitzer, julian.renner, antonia.wachtler-zeh, violetta.weger}@tum.de

Abstract—Properties of random codes endowed with the cover metric are considered. We prove the NP-hardness of the decoding problem and then provide a generic decoder, following the information set decoding idea from Prange’s algorithm in the Hamming metric. Despite the cover metric lying between the Hamming and the rank metric, the complexity analysis of the algorithm reveals a significant difference between the metrics.

I. INTRODUCTION

The recent advances in quantum computers have accelerated the process of developing efficient and quantum-resilient public-key cryptosystems. Code-based cryptography is based on the hardness of decoding a random linear code. Originally the Hamming metric was utilized, but recently also the rank metric has shown large potential [1], [2].

In this paper, we consider a metric which lies in between these two: the cover metric. Similar to the rank metric, the words that we consider are now matrices instead of vectors as for the Hamming metric. The cover weight of a matrix is the minimum number of lines (rows and columns) that are needed to cover all non-zero elements of the matrix. The cover metric has so far mainly been used for crisscross error correction [3]–[7]. In order to evaluate the potential of the cover metric for cryptographic applications, it is important to investigate properties of random codes and the complexity of generic decoding, i.e., decoding in a general linear code.

In this paper we provide new density results of maximum cover-distance codes. We show the NP-completeness of the cover-metric decoding problem and provide a Prange-like generic decoder. We derive its complexity and compare it with generic decoding in the Hamming metric. This comparison shows a significant difference: in the Hamming metric, the complexity grows exponentially in the number of code symbols, whereas in the cover metric the complexity is exponential in the number of lines.

II. PRELIMINARIES

Throughout this paper, $p$ denotes a prime number and $\mathbb{F}_p$ denotes the finite field with $q$ elements. Let $m$ and $n$ be positive integers and denote by $\mathbb{F}_p^{m \times n}$ the space of $m \times n$ matrices over $\mathbb{F}_p$. By the term lines we denote rows and columns of a matrix. For a matrix $A \in \mathbb{F}_p^{m \times n}$ we denote by $\text{rk}(A)$ its rank and by $\langle A \rangle$ its rowspan. The identity matrix of size $m$ will be denoted by $I_m$. For a set $S$, we denote its cardinality by $|S|$. For a matrix $A \in \mathbb{F}_p^{m \times n}$ and a block $I \times J \subseteq \{1, \ldots, m\} \times \{1, \ldots, n\}$ of size $k_m \times k_n$ we denote by $A_{I \times J} \in \mathbb{F}_p^{k_m \times k_n}$ the matrix consisting of the entries of $A$, where the rows are indexed by $I$ and the columns are indexed by $J$. Similarly, for a matrix $A \in \mathbb{F}_p^{m \times n}$, respectively for a vector $a \in \mathbb{F}_p^n$ and a set $I \subseteq \{1, \ldots, n\}$ of size $k$ we denote by $A_I \in \mathbb{F}_p^{m \times k}$ the matrix consisting of the columns of $A$ indexed by $I$, respectively by $a_I \in \mathbb{F}_p^k$ the vector consisting of the entries of $a$ indexed by $I$. Thus, calligraphic letters are used to indicate a block, while normal letters indicate a subset of $\{1, \ldots, n\}$. We describe the asymptotic behaviour of functions using the Bachmann-Landau notation.

Let $A = (a_{i,j})_{1 \leq i \leq m, \ 1 \leq j \leq n} \in \mathbb{F}_p^{m \times n}$. We say that $\text{Cov}(A) \subseteq \{1, \ldots, m + n\}$ is a cover of $A$ if for all $i \in \{1, \ldots, m\}$ and for all $j \in \{1, \ldots, n\}$ we have that, if $a_{i,j} \neq 0$, then either $i \in \text{Cov}(A)$ or $j + m \in \text{Cov}(A)$. Observe that a cover of a matrix does not have to be unique. In fact, we call a cover minimal if it is a cover of minimal size, i.e., for $A \in \mathbb{F}_p^{m \times n}$, the cover $C \subseteq \{1, \ldots, m + n\}$ is a minimal cover of $A$, if $|C| = \min_{A} (|\text{Cov}(A)| : \text{Cov}(A) \text{ is a cover of } A)$.

The cover weight of $A$ is the size of a minimal cover of this matrix, i.e.,

$$\text{wt}_C(A) = \min_{A} (|\text{Cov}(A)| : \text{Cov}(A) \text{ is a cover of } A).$$

The cover distance between $A, B \in \mathbb{F}_p^{m \times n}$ is given by $d_C(A, B) = \text{wt}_C(A - B)$ and defines a metric on $\mathbb{F}_p^{m \times n}$. An $[m \times n, k]$ matrix code $C$ is a $k$-dimensional linear subspace of $\mathbb{F}_p^{m \times n}$ with generators $G_1, \ldots, G_k \in \mathbb{F}_p^{m \times n}$ if

$$C = \left\{ \sum_{i=1}^k u_i G_i \mid u_i \in \mathbb{F}_p \right\} = \langle G_1, \ldots, G_k \rangle.$$

The minimum cover distance of $C$ is defined as

$$d_C = \min_{A \in C, A \neq 0} (\text{wt}_C(A) \mid A \in C).$$

We refer to an $[m \times n, k]$ cover-metric code with minimum cover distance $d$ as an $[m \times n, k, d]$ cover-metric code.

Remark 1. Any code defined over $\mathbb{F}_q^m$ can be associated to an $[m \times n, k]$ matrix code. We consider codes over $\mathbb{F}_q$, as the decoding problem can be shown to be NP-hard in this case, see Section IV.

To describe the operations which are performed on the generators and the received matrix for generic decoding of a matrix code, it is more convenient when the associated vector code is considered. To this end, we define the bijective map

$$\varphi : \mathbb{F}_q^{m \times n} \to \mathbb{F}_q^{m \times n}, \ A \mapsto a,$$

which concatenates the rows of $A = (a_1^T, \ldots, a_m^T)^T$ into a single vector $a = (a_1, \ldots, a_m)$, where $a_i \in \mathbb{F}_q^n$. Then, we...
refer to $a$ as the row vector form of $A$. The map $\varphi$ is extended to

$$\varphi : (q^{mn})^{k} \rightarrow F_q^{k\times(mn)}, \ G_1, \ldots, G_k \mapsto \tilde{G},$$

by performing $\varphi$ matrix-wise on the input and stacking the resulting vectors. Then, it holds that $(G_1, \ldots, G_k)$ coincides with

$$\varphi^{-1} \left( \{ c = u\tilde{G} \ | \ u \in F_q^k \tilde{G} = \varphi(G_1, \ldots, G_k) \} \right).$$

Hence, $\varphi$ allows for an unambiguous representation of the matrix code in a vector form. The vector form allows the introduction of an information set for the matrix code.

**Definition 2** (Information Block). Let $C \subseteq F_q^{m \times n}$ be a code of dimension $k$ and $C \subseteq C$. Then, we refer to $I \times J \subseteq \{1, \ldots, m\} \times \{1, \ldots, n\}$ of size $k_m \cdot k_n$ as an information block of $C$, if $|\{C_{I \times J} \ | \ C \subseteq C\}| = |C|$.

Note that not all codes of dimension $k$ have the same minimal size of an information block. In particular, not every code has an information block of size $k$. The definition of information block then also gives rise to a definition of systematic form for the generators.

**Definition 3** (Systematic Vector Form). Let $G_1, \ldots, G_k \in F_q^{k \times m}$ be the generators of a code $C \subseteq F_q^{m \times n}$ of dimension $k$ and $G$ the associated generator matrix in row vector form. Let $I \times J$ be an information block for $C$ of size $k_m \times k_n$. Let $G_i \in F_q^{k \times k_{n_i}}$ denote the submatrix formed from $G_i$ by considering only the rows of $I$ and columns of $J$. We refer to the row vector form of $G_1, \ldots, G_k$ as $G \in F_q^{n \times k_m k_n}$. As $I \times J$ forms an information block, there exists a set $I \subseteq \{1, \ldots, k_m k_n\}$ of size $k$, such that $G_I$ has full rank. Then, the systematic row vector form of $G_1, \ldots, G_k$ is given by $G_s = G_I^{-1} G \in F_q^{n \times m n}$.

### III. BOUNDS AND DENSITY IN THE COVER METRIC

For $n \leq m$, the Singleton bound in the cover metric can be written as $d \leq n - \frac{1}{n} + 1$ [5]. Codes that achieve this bound with equality are referred to as **maximal cover distance**. Asymptotically, this implies $R \leq 1 - \delta$, where $R = \frac{k}{mn}$ denotes the rate and $\delta = \frac{d}{n}$ the relative minimum distance.

Let $F_C(n, m, q, w)$ denote the size of the cover-metric sphere, i.e.,

$$F_C(n, m, q, w) = |\{A \in F_q^{m \times n} \ | \ wt_C(A) = w\}|,$$

and $V_C(n, m, q, w)$ the size of the cover-metric ball, i.e.,

$$V_C(n, m, q, w) = |\{A \in F_q^{m \times n} \ | \ wt_C(A) \leq w\}|.$$

The size of the cover ball is then $V_C(n, m, q, w) = \sum_{w=0}^{\infty} F_C(n, m, q, w)$, which is needed for the analogue of the Gilbert-Varshamov bound in the cover metric. Unfortunately, there is no exact formula for the cover-metric sphere or ball. Instead, we need to work with a lower and upper bound on the size of the ball. Recall that for $q \geq 2$ and $p \in [0, 1]$ the $q$-ary entropy function is defined as

$$H_q(p) = p \log_q(q - 1) - p \log_q(p) - (1-p) \log_q(1-p).$$

**Lemma 4** ([8]). Let $n \leq m$ be positive integers and $q$ be a prime power. Let $0 < d \leq n$. Then

$$q^{-md} \leq V_C(n, m, q, d) \leq (d + 1) q^{(m-1) H_2(d/(m)+1) + 1}.$$

Let $A(q, m, n, d)$ denote the size of the largest code over $F_q^{n \times m}$ of minimum cover distance $d$.

**Theorem 5** (Gilbert-Varshamov Bound). Let $0 < d \leq n \leq m$ be positive integers, then

$$A(q, m, n, d) \geq V_C(q, m, n, q, d).$$

In the case $n \leq m$ (thus if we let $n$ go to infinity, $m$ does as well), we have that

$$\lim_{n \to \infty} \frac{1}{mn} \log_q \left( V_C(n, m, q, d) \right) = \delta,$$

where $\delta$ denotes the relative minimum distance, i.e., $\delta = d/n$. Let us consider the maximal information rate

$$R(n, m, d) := \frac{1}{mn} \log_q \left( A(q, m, n, d) \right),$$

for $0 \leq d \leq n$.

**Theorem 6** (Asymptotic Gilbert-Varshamov Bound). For $n \leq m$, it holds that

$$\lim_{n \to \infty} \left( 1 - \frac{1}{mn} \log_q \left( V_C(n, m, q, d) \right) \right) = 1 - \delta.$$

**Theorem 7**. For every prime power $q$, $\delta \in [0, 1)$, $0 \leq \epsilon < 1 - H_2(\delta)$ and sufficiently large positive integer $n \leq m$, let

$$k = \left( m - m \delta + \frac{m}{n} - m \frac{\delta n}{n} H_2(\frac{\delta n}{n} - \epsilon) n \right).$$

If we choose $G_1, \ldots, G_k \in F_q^{m \times n}$ uniformly at random, the linear code generated by $G_1, \ldots, G_k$ has rate at least $1 - \delta - \epsilon$ and relative minimum cover distance at least $\delta$ with probability $1 - e^{-\Omega(n)}$.

**Proof:** For the first statement on the rate, observe that $G_1, \ldots, G_k$ generate a code of dimension $k$, if $\sum_{i=1}^k \lambda_i G_i = 0$, with $\lambda_i \in F_q$ implies that $\lambda_i = 0$ for all $i \in \{1, \ldots, k\}$. Thus, for $G_1$, we have $q^{nm} - 1$ choices, that is all but the zero matrix, for $G_2$ we can choose any non-zero matrix which lies outside the span of $G_1$, thus we have $q^{nm} - q$ choices. Continuing in this manner, we get that the probability for $G_1, \ldots, G_k$ to generate a code of rate $\frac{k}{mn}$ is given by

$$\prod_{i=0}^{k-1} \left( q^{mn} - q \right) \geq 1 - e^{-\Omega(n)}.$$

For the second statement, we first note that for any non-zero $u \in F_q^n$, we have that the codeword $u_1 G_1 + \cdots + u_k G_k$ is uniformly distributed in $F_q^{mn}$. We now bound the counter probability, that is

$$P( wt_C(u_1 G_1 + \cdots + u_k G_k) \leq \delta n).$$

This probability is given due to the uniform distribution of the codewords and Lemma 4 by

$$\frac{V_C(n, m, q, \delta n - 1)}{q^{mn}} \leq \frac{q^{(\delta n - 1) H_2((\delta n - 1)/(m n))} \delta n}{q^{nm}}.$$
A union bound over all non-zero \( x \in \mathbb{F}_q^k \), to get all non-zero codewords, now gives
\[
q^k q^{m \delta n + (m+n) H_2((\delta n-1)/(m+n)) + \log_q(\delta n) - m - mn} = q^{1 - nz} \leq e^{-\Omega(n)}.
\]

Thus, we get the claim. 

Due to the asymptotic Singleton bound, Theorem 7 implies the following corollary.

**Corollary 8.** Let \( n \leq m \). The density of maximum cover distance codes in \( \mathbb{F}_q^{m \times n} \) is \( 1 \), for \( n \) going to infinity.

In addition, the density is also 1 if we let the field size grow.

**Lemma 9.** For fixed \( k \leq n \leq m \), the density of maximum cover distance codes is \( 1 \), for \( q \) going to infinity.

**Proof:** Let \( C \) be a random \([m \times n, k]\) cover-metric code and \( e > 0 \). Then, the probability that \( C \) has minimum distance smaller than \( d = n - k - e + 1 \) can be bounded as \( P(\exists C \in \mathcal{C} \setminus \{0\}) \) with \( wt_C(C) \leq d - 1 \) is at most
\[
d \cdot q^{m(d-1)} q^{(m+n) H_2(d/(m+n))} q^{mn},
\]
using the same arguments as in the proof of Theorem 7. We define \( c = d \cdot 2^{m+n} H_2(d/(m+n)) \), which is a constant in \( q \) and simplify \( m(d-1) - mn \), thus getting as an upper bound on the probability \( c^{-k+e} \). Then, the claim follows from the union bound, as
\[
P(\forall C \in \mathcal{C} \setminus \{0\}) \) holds that \( wt_C(C) \geq d \) = \( 1 - c \cdot q^{-e} \),
which tends to \( 1 \) for \( q \) going to infinity. 

**IV. COVER DECODING PROBLEM**

The decoding problem in the Hamming metric, stated in the following, is well known to be NP-complete [9].

**Problem 10** (Hamming Decoding Problem). Given \( G \in \mathbb{F}_q^{k \times n} \), \( r \in \mathbb{F}_q^n \), a positive integer \( t \leq n \), does there exist \( e \in \mathbb{F}_q^n \) such that \( r - e \in (G) \) and \( wt_H(e) \leq t \)?

The analog problem in the cover metric reads as follows.

**Problem 11** (Cover Decoding Problem). Given \( C \in \mathbb{F}_q^{m \times n} \), a positive integer \( t \leq \min\{m, n\} \), and \( Y \in \mathbb{F}_q^{m \times n} \), does there exist a matrix \( E \in \mathbb{F}_q^{m \times n} \) such that there exist \( C \in C \) with \( C + E = Y \), and \( wt_C(E) \leq t \)?

This problem is equivalent to the cover-metric syndrome decoding problem, in the same manner as this equivalence holds for other metrics and ambient spaces. An algorithm that solves the lowest-weight codeword problem can also solve the decoding problem, by adding \( Y \) as a generator to the random code. The error matrix \( E \) is the codeword of smallest cover weight of the new code. This provides a reduction from the decoding problem to the lowest-weight codeword problem. For more details on these problems see [10].

**Theorem 12.** The Cover Decoding Problem is NP-complete.

**Proof:** Let \((q, G, r, t)\) be a random instance of the Hamming Decoding Problem, which is known to be NP-complete [9] [11]. Let \( g_i \) denote the \( i\)-th row of \( G \). We define \( G_i \in \mathbb{F}_q^{(t+1) \times n} \) as the matrix which results from stacking \( g_i + t + 1 \) times and \( R \in \mathbb{F}_q^{(t+1) \times n} \) the matrix which results from stacking \( r + t + 1 \) times. Then, \((q, G_1, \ldots, G_k, R, t)\) is an instance of the Cover Decoding Problem with \( m = t + 1 \). The construction method guarantees that all \( t + 1 \) rows of \( R \) are identical and all rows of a codeword in \((G_1, \ldots, G_k)\) are identical, we must get that all rows of \( E \) are identical as well. Let us denote such a row by \( e \in \mathbb{F}_q^n \). Since \( E \) consists of \( t + 1 \) identical rows, any cover of weight \( \leq t \) can be formed by columns only, thus \( wt_H(e) \leq t \). Since \( e \) is such that \( r - e \in (G) \) by construction, we have that the answer to the Hamming-metric problem is also ‘yes’. On the other hand, if the answer to the cover-weight problem is ‘no’, every matrix \( E \in \mathbb{F}_q^{(t+1) \times n} \) is such that \( R - E \in (G_1, \ldots, G_k) \) has cover weight \( t \). As the rows of \( E \) are identical, each row \( e \), which are all the vectors with \( r - e \in (G) \), has \( wt_H(e) > t \). Thus, the answer to the Hamming-weight problem is also ‘no’. Since this problem clearly lives in NP, we get the claim.

**V. GENERIC DECODING IN THE COVER METRIC**

In this section, we introduce an algorithm for generic decoding in the cover metric.

**A. Error Model**

In order to evaluate the complexity of the decoding approaches, it is essential to specify the underlying error model. The most general one is given as follows.

**Definition 13** (General Error Model). An error \( E \) of cover weight \( t \) is created by choosing \( E \) at random from \( \{A \in \mathbb{F}_q^{m \times n} \mid wt_C(A) = t\} \).

Another error model [6] allows a simplified generation of error matrices, as well as a simplified analysis of the complexity of generic decoding:

**Definition 14** (Simple Error Model). An error \( E \) of cover weight \( t \) is created as follows: first pick \( t \) of the \( n \times m \) rows and columns at random. Then, create \( E \) by setting the elements in the picked rows and columns to random elements of \( \mathbb{F}_q \). All remaining elements are zero. The cover weight of \( E \) is checked. If \( wt_C(E) < t \), the process is repeated.

The error models are similar, but not identical. In the general error model, every matrix in the sphere of radius \( t \) is chosen with equal probability \( P(E) \mid \text{general model} = \mathbb{F}_q^{[n,m,q,t]} \) for all \( E \in \{A \in \mathbb{F}_q^{m \times n} \mid wt_C(A) = t\} \). This is not the case for the simple error model, for which some matrices are more likely than others. Nevertheless, the simple model can be used to accurately approximate the general error model in practice, as the following theorem shows.
Theorem 15 (Unique Minimal Cover). Let $E \in \mathbb{F}_q^{m \times n}$ be a matrix, created by choosing $t \leq \min\{m,n\}$ out of $m + n$ lines at random and filling the chosen rows and columns with random elements from $\mathbb{F}_q$. Then, for sufficiently large $n$, $E$ has a unique minimal cover of cardinality $t$ with high probability.

For the proof, the reader is referred to [10]. From Theorem 15 we get a lower bound on the size of the spheres, which is of a similar form as the upper bound given in [12].

Corollary 16. Let $t \leq \min\{m,n\}$ be positive integers. Then, $F_C(n,m,q,t)$ is at least

$$\sum_{t_m + t_n = t} \left( \binom{m}{t_m} \binom{n}{t_n} \right) q^{n-t_n} \left( q^{n-t_n} - (q-1)(n-t) - q^{m} \right)^t m \cdot \left( q^{m-t_n} - (q-1)(m-t) - q^{n} \right)^{t_n}.$$

B. Prange-like Decoding in the Cover Metric

The classical generic decoding algorithm in the Hamming metric by Prange [13], formulated via the generator matrix is such that, given a received word $r$, a generator matrix $G$ and a weight $t$, one chooses an information set $I$ and checks whether $r - r_I G^{-1} G$ has weight $t$. If the support of the error vector lies outside the information set, this procedure succeeds.

In the following, we introduce and analyze a simple Prange-like generic decoder in the cover metric. For this, we focus on instances with $m = n$, which are the hardest among all instances with a given rate $R$, since the minimum distance scales with $\min\{m,n\}$. Any instance with $m > n$ can be reduced to this case by puncturing $m - n$ rows. As this results in more readable formulae, we nevertheless denote the number of rows as $m$ in the following. Let $C = \{ \sum_{i=1}^{k} u_i G_i | u_i \in \mathbb{F}_q \}$ with $G_i \in \mathbb{F}_q^{m \times n}$. In order to recover $C \in C$ from $R = C + E$ with $wt_C(E) = t$, one can proceed according to Algorithm 1.

Algorithm 1 Cover-Metric Prange Algorithm

Input: $R = C + E$, with $C \in \langle G_1, \ldots, G_k \rangle$ and $wt_C(E) = t$.
Output: $C \in C$ with $wt_C(R - C) \leq t$.

1. Choose $k_m \leq m$ and set $k_n = \lfloor k/m \rfloor \leq n$.
2. Choose $I \times J \subset \{1, \ldots, m\} \times \{1, \ldots, n\}$ of size $k_m \times k_n$ at random.
3. $G \leftarrow \varphi(G_1, \ldots, G_k)$.
4. $\hat{G} \leftarrow \varphi(G_1(I \times J), \ldots, (G_k)_{I \times J}) \in \mathbb{F}_q^{k \times k_n k_m}$.
5. Choose $I \in \{1, \ldots, k_m k_n\}$ of size $k$, s.t. $rk(G_t) = k$.
6. $G_s \leftarrow G_t^{-1} G \in \mathbb{F}_q^{k \times k_m n}$.
7. $r \leftarrow \varphi(R_{I \times J}) \in \mathbb{F}_q^{k \times k_m}$.
8. $\hat{c} \leftarrow r_I G_s$.
9. if $wt_C(R - \varphi^{-1}(\hat{c})) \leq t$, then return $\hat{C} = \varphi^{-1}(\hat{c})$.
10. else return to Step 2.

Similar to the classical case, one iteration succeeds if the chosen information-block is such that $E_{I \times J} = 0$.

Remark 17. The number of selected columns in Step 2 is chosen such that $k_m \cdot k_n \geq k$. This guarantees that we obtain an information block with high probability. Let $\tilde{G}_i \in \mathbb{F}_q^{k_m \times k_n}$ for $i \in \{1, \ldots, k\}$ be chosen at random. Define $\tilde{C} = \{ u \cdot \varphi(\tilde{G}_1, \ldots, \tilde{G}_k) | u \in \mathbb{F}_q^k \}$. Then,

$$P(\tilde{C} = q^t) = \prod_{i=1}^{k} (1 - q^{-k_m k_n}).$$

This probability is at least as high as the probability that $k$ random positions of a random code form an information set. We conclude that the probability that a random block of size $k_m k_n \geq k$ is an information block is, for most codes, a constant in the same order of magnitude as 1.

Now, we analyze the average success probability of the Prange-like decoder and, in doing so, determine how $k_m$ should be chosen in order to obtain the maximum average success probability. Let $t_m$ be the number of rows in the minimum-size cover of $E$ and $t_n$ the number of columns. According to the definition of the cover weight, we have $wt_C(E) = t = t_m + t_n$. Except for a negligible number of cases, the Prange-like decoder only succeeds if indeed all rows and columns of $E$, which have non-zero weight, are erased. Therefore, the probability of the event that $\tilde{C}$ is equal to $C$ given $t_m$ and $k_m$ is tightly approximated by

$$P(S \mid t_m, k_m) = \left( \frac{m-k_m}{m} \right)^{t_m} \left( \frac{n-k_n}{n} \right)^{t_n}.$$

In order to enable a compact complexity analysis of the Prange-like decoder, we assume the simple error model introduced in Definition 14, which is justified by Theorem 15. Then, the distribution of $t_m$ is well approximated by the hypergeometric distribution, which means that its probability mass function is given by

$$P(t_m \mid t) = \binom{m}{t} \left( \frac{m-n}{t} \right)^{t_m} \left( \frac{n}{t} \right)^{t_n}.$$

Hence, the overall success probability is given by

$$P(S \mid k_m) = \sum_{t_m=0}^{t_n} P(S \mid t_m, k_m) \cdot P(t_m \mid t) = \left( \frac{m-n-k_m-k_n}{m} \right)^{t_n}.$$

For $n = m$, this optimum is achieved for $k_m \approx k_n \approx \sqrt{k}$. Hence, the success probability can be tightly approximated as

$$P(S) = \left( \frac{m+n-2 \sqrt{k}}{t} \right)^{t_n} \left( \frac{m+n}{t} \right)^{t_n}.$$

It is worth noting that this expression for the success probability is similar to the formula for the success probability of Prange’s algorithm in the Hamming metric, i.e.,

$$P(S_{Prange}) = \left( \frac{n-k}{t} \right)^{t_n}.$$

Let $\tau = t/n$ and $H_q(p)$ denote the $q$-ary entropy function. Then, asymptotically, Prange’s algorithm in the Hamming metric requires on average $2^{c_{Prange}(R, \tau) \cdot n}$ iterations, where

$$c_{Prange}(R, \tau) = H_2((1-R) \cdot H_2(\tau/(1-R)).$$

For $\tau_{GV} = \frac{d_{GV} - 1}{2m}$, the constant is given by

$$c_{PrangeGV}(R) = H_2\left( \frac{H_2^{-1}(1-R)}{2} \right) - (1-R) \cdot H_2\left( \frac{H_2^{-1}(1-R)}{2} \right).$$
A similar analysis can be carried out for the proposed Prange-like decoder in the cover metric.

**Theorem 18** (Asymptotic Decoding Complexity). Let \( m = n, \tau = t/n \) and \( R = k/(nm) \). Then, the number of iteration is asymptotically in the order of \( 2^{c_{\text{cover}}(R, \tau)} (n+m) \) with

\[
e_{\text{cover}}(R, \tau) = H_2\left( \frac{\tau}{2} \right) - \left( 1 - \sqrt{R} \right) \cdot H_2\left( \frac{\tau}{2(1-\sqrt{R})} \right),
\]

where \( H_2(p) \) denotes the binary entropy function. For \( \tau_{\text{coverGV}} = \frac{4 \log^{\alpha-1}}{2n} \), the constant simplifies to \( c_{\text{coverGV}}(R) = H_2\left( \frac{1-R}{R} \right) - \left( 1 - \sqrt{R} \right) H_2\left( \frac{1+\sqrt{R}}{2} \right) \).

The cost of each iteration is dominated by the required Gaussian elimination, i.e., it is in the order of \( n^3 \).

*Proof:* The average number of required iterations is given by \( P(S)^{-1} \). For \( m = n \to \infty \) and \( R = k/(nm) \), it holds that

\[
O\left(P(S)^{-1}\right) = O\left(\left(\frac{n+m}{t}\right)\left(\frac{n+m-2\sqrt{Rmn}}{t}\right)^{-1}\right).
\]

As we consider the case \( m = n \), it holds that \( \sqrt{m \cdot n} = \frac{m+n}{2} \), which simplifies the previous equation to

\[
O\left(P(S)^{-1}\right) = O\left(\left(\frac{n+m}{t}\right)\left(\frac{(n+m)(1-\sqrt{R})}{t}\right)^{-1}\right).
\]

Further, a well-known formula for binomial coefficients states that \( O\left(\binom{k}{j}\right) = O\left(2^{\frac{j}{k}}\right) \). Using this relation, one observes that \( O(P(S)^{-1}) \) is

\[
O\left(2^{(m+n)H_2\left(\frac{t}{n+m}\right) - (m+n)(1-\sqrt{R})H_2\left(\frac{t}{(n+m)(1-\sqrt{R})}\right)} \right),
\]

which proves (1). In the cover metric, the Gilbert-Varshamov bound states that \( \lim_{n \to \infty} \tau_{\text{coverGV}} \) is

\[
\lim_{n \to \infty} \frac{c_{\text{coverGV}}(R)}{n} = \lim_{n \to \infty} \frac{n(1-R)}{2n} = \frac{1-R}{2}.
\]

Thus, we get the claim. \( \square \)

**Remark 19.** It is worth noting that \( O(P(S)^{-1}) = O(2^{(n+m)c_{\text{coverGV}}(R)}) \) implies

\[
\lim_{m \to \infty} \log_2\left(\frac{P(S)^{-1}}{n-m}\right) = 0.
\]

This behaviour is different from generic decoding in other metrics. In the Hamming metric, generic decoding of a random binary code of length \( n \cdot m \) succeeds with a probability, for which it holds that

\[
\lim_{m \to \infty} \log_2\left(\frac{P(S)^{-1}}{n-m}\right) = c_H(R),
\]

where \( c_H(R) \) is a constant which varies only slightly between the decoding algorithms.

In the Hamming metric, multiple improvements over Prange’s algorithm have been proposed, e.g., Stern’s algorithm [14]. These improvements utilize the birthday paradox to efficiently enumerate all solution of a subproblem. Adapting this approach to the cover metric is possible. However, we have observed that the list sizes are considerably increased in comparison to the Hamming metric. Therefore, one cannot achieve a further complexity reduction of relevant code rates.

Since we have \( \text{wt}_R(E) \leq \text{wt}_C(E) \), we can apply generic decoders for the rank metric to solve an instance in the cover metric. However, the generic decoders in the rank metric are considerably less efficient than the proposed decoding algorithm. For example [15] has an asymptotic cost of \( q^{nJ(n)2^R} \), where \( f(n) \) denotes the function with which \( f(n) \) grows and

\[
R := \lim_{n \to \infty} \frac{k(n)}{n} \in (0, 1), \quad T := \lim_{n \to \infty} \frac{t(n)}{n} \in (0, 1).
\]

**VI. CONCLUSION**

We have provided a polynomial-time reduction from the decoding problem in the Hamming metric to the decoding problem in the cover metric and, hence, showed the NP-hardness of the decoding problem for \( \mathbb{F}_q \)-linear codes in the cover metric. This similarity to the Hamming metric and the rank metric could enable cryptographic applications. Random codes in the cover metric achieve the largest possible minimum distance with high probability. To assess the cost of the cover-metric decoding problem, we provided a generic decoder and analyzed its cost. An asymptotic analysis shows that the decoding complexity is exponential in the number of lines. This behaviour is completely different to the Hamming metric and the rank metric, which have a complexity that is exponential in the number of code symbols.

**REFERENCES**

[1] C. A. Melchor, N. Aragon, S. Bettaieb, L. Bidoux, O. Blazy, J.-C. Deneuville, and J.-C. Deneuville, “A method for finding codewords of small weight,” in *Int. Conf. on Information Theory and Applications*, 2005.

[2] E. M. Gabidulin and V. I. Korzhik, “Codes correcting lattice-pattern errors,” *Probl. Peredachi Inform.*, vol. 30, no. 3, pp. 23–28, 1994.

[3] R. M. Roth, “Maximum-rank array codes and their application to crisscross error correction,” *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 328–336, 1991.

[4] E. M. Gabidulin, “Optimal array error-correcting codes,” *Probl. Peredach. Inform.*, vol. 21, no. 2, pp. 102–106, 1985.

[5] E. M. Gabidulin and V. I. Korzhik, “Codes correcting lattice-pattern errors,” *Zvestiya VUZ. Radioelektronika*, vol. 4, no. 6, p. 7, 1972.

[6] ——, “Probabilistic crisscross error correction,” *IEEE Trans. Inf. Theory*, vol. 43, no. 5, pp. 1425–1438, 1997.

[7] A. Wachter-Zeh, “List Decoding of Crisscross Errors,” *IEEE Trans. Inf. Theory*, vol. 63, no. 1, pp. 142–149, Jan. 2017.

[8] S. Liu, C. Xing, and C. Yuan, “List decoding of cover metric codes up to the Singleton bound,” *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2410–2416, 2018.

[9] S. Tümer, J. Renner, A. Wachter-Zeh, and V. Weger, “Generic decoding in the cover metric,” arXiv preprint arXiv:2205.12738, 2022.

[10] A. Barg, “Some new NP-complete problems,” *Probl. Peredach. Informatissi*, vol. 30, no. 3, pp. 23–28, 1994.

[11] U. Martínez-Peñas, “Multilayer crisscross error and erasure correction,” *arXiv preprint arXiv:2203.07238*, 2022.

[12] E. Prange, “The use of information sets in decoding cyclic codes,” *IRE Trans. Inf. Theory*, vol. 8, no. 5, pp. 5–9, 1962.

[13] J. Stern, “A method for finding codewords of small weight,” in *Int. Coll. on Coding Theory and Appl.*. Springer, 1988, pp. 106–113.

[14] P. Gaborit, O. Ruatta, and J. Schrek, “On the complexity of the rank syndrome decoding problem,” *IEEE Trans. Inf. Theory*, vol. 62, no. 2, pp. 1006–1019, 2015.