# Unique and Minimum Distance Decoding of Linear Codes with Reduced Complexity

Dejan Spasov and Marjan Gusev

University Ss. Cyrill and Methodious, Faculty of Natural Sciences and Mathematics, Institute of Informatics, Skopje, Macedonia
dejan@ii.edu.mk, marjangusev@gmail.com

**Abstract.** Given a linear $[n, Rn, \delta n]$ code, we show that for $R \geq \delta/2$ the time complexity of unique decoding is $O\left(n^2 q^{nRH(\delta/2/R)}\right)$ and the time complexity of minimum distance decoding is $O\left(n^2 q^{nRH(\delta/R)}\right)$. The proposed algorithms inspect all error patterns in the information set of the received message of weight less than $\delta n/2$ or $\delta n$, respectively.

**Keywords:** nearest neighbor decoding, unique decoding, bounded distance decoding, minimum distance decoding, syndrome decoding.

## 1 Introduction

Let $F_q$ be finite field of $q$ elements and let $F_q^n$ be $n$-dimensional vector space over $F_q$. Then a code $C$ is any subset of $F_q^n$ of $M$ elements. Elements of the code $c \in C$ are called codewords.

Let $d(x, y)$ denote the Hamming distance, i.e. the number of coordinates in which two vectors $x$ and $y$ differ, and let $wt(x)$ denote the (Hamming) weight, i.e. the number of nonzero coordinates of $x$. We say that the code $C$ has (minimum) distance $d$ if

$$d = \min_{\substack{c_i, c_j \in C \\ i \neq j}} \{d(c_i, c_j)\}. \tag{1}$$

The code $C$ is linear if its codewords form $k$ - dimensional linear subspace in $F_q^n$. We will write $[n, k, d]_q$ to emphasize that the code $C$ is linear. For linear codes there exist $k$ basis vectors that are kept as rows in a matrix $G$ called the generator matrix. Each linear code has a generator matrix of type $G = [I \quad A]$, known as the standard form of the generator matrix. It is well-known that for linear codes there exist additional matrix, known as the parity check matrix $H$, such that $\forall c_i \in C \quad Hc_i^T = 0$. Let $G = [I \quad A]$ is the generator matrix, then $H = [-A^T \quad I]$ is the parity check

M. Gusev and P. Mitrevski (Eds.): ICT Innovations 2010, CCIS 83, pp. 94–101, 2011.
© Springer-Verlag Berlin Heidelberg 2011

matrix of the code $C$. Two additional parameters that are frequently used to describe a code are the code rate $R = k/n$ and the relative distance $\delta = d/n$.

The *covering radius* $\rho$ of a code is the largest possible distance between the code $C$ and a vector from $F_q^n$, i.e.

$$\rho = \max_{x \in F_q^n} \min_{\forall c \in C} d(x,c). \tag{2}$$

In this paper, we are mainly interested in decoding of *maximal codes* [2], i.e. codes with $\rho \le d-1$. It is well known that these codes meet the asymptotical Gilbert-Varshamov bound

$$R \ge 1 - H(\delta). \tag{3}$$

where $H(\delta)$ is the entropy function.

A *Hamming ball* $Ball(x,d)$ with radius $d$ and center in $x$ is the set of points

$$Ball(x,d) = \{ y \in F_q^n \mid d(x,y) \le d \}. \tag{4}$$

The *volume* (cardinality) $V(n,d)$ of the Hamming ball is equal to

$$V(n,d) = \sum_{i=0}^{d} (q-1)^i \binom{n}{i}. \tag{5}$$

In estimating the complexity of an algorithm we will use the asymptotical relation between the entropy $H(\delta)$ the volume of a ball $V(n,\delta n)$

$$\lim_{n\to\infty} \left\{ \frac{\log\left(V(n,\delta n)\right)}{n} \right\} \to \begin{cases} H(\delta) & \text{for } \delta \le \dfrac{1}{2} \\ 1 & \text{for } \delta > \dfrac{1}{2} \end{cases}. \tag{6}$$

We adopt Random Access Machine (RAM) as a computational model and, hence, the time complexity is measured as the number of basic (sequential) steps needed for instance of the algorithm to end. It is considered that RAM has unlimited memory with instant access. Thus the space complexity is simply the number of registers used by an instance of the algorithm. We will use the standard Big-O asymptotic notation to describe the space and time complexity. Given $f, g : \mathrm{N} \to \mathrm{N}$ we will write $f = O(g)$ if there exist a constant $c > 0$ such that $f(n) \le c \cdot g(n)$ holds true for each $n \in \mathrm{N}$. If $f(n) = c \cdot g(n)$ then we will write $f = \Theta(g)$.

## 2 Combinatorial Decoding Strategies

Let $C$ be a linear code with parameters $[n,k,d]$ and parity check matrix $H$. Let assume that the sender has sent the codeword $c_x$ and the receiver has received the message $y$, such that $y \ne c_x$. The decoder's job is, in acceptable time, to make a

proper decision on which codeword has been sent, based on the observations of the received vector $y$. The decoding process is in general NP-hard problem [1,2].

The received message $y$ can be considered as an array of real numbers $y=(y_1,\ldots,y_n), y_i \in \mathrm{R}$. Let $p(y/c)$ denotes the conditional probability that the message $y$ is received, given that the codeword $c$ has been sent. Given $y$ the goal of the *Maximum Likelihood (ML) Decoding* is to find the codeword $c$ such that $p(y/c)$ is maximal, i.e.

$$\hat{c} = \arg\max_{c \in C} p(y/c). \tag{7}$$

If we assume $q-$ary symmetric channel, then ML decoding is simplified and known as *Nearest Neighbor Decoding* or *Minimum Distance (MD) Decoding*. In MD decoding, the received message $y$ is considered as array of field elements of $GF(q)$, $y=(y_1,\ldots,y_n), y_i \in GF(q)$. The decoder's job is to find the codeword $c$ such that $d(y,c)$ is minimal, i.e.

$$\hat{c} = \arg\min_{c \in C} d(y,c). \tag{8}$$

The time complexity of MD decoding is $O(nq^{Rn})$ [2]. Let assume that the $[n,k,d]$ code $C$ is maximal. Then as MD decoding is considered the following approach: subtract from the received vector $y=(y_1,\ldots,y_n), y_i \in GF(q)$, all possible error patterns $e$ of weight $\le d$ and output all vectors $y-e$ such that $y-e \in C$. The time complexity of this approach is $O(n^2 q^{H(\delta)n})$. Thus, combining these two MD decoding strategies, we obtain the time complexity of MD decoding

$$O\left(n^2 q^{\min(R,H(\delta))n}\right). \tag{9}$$

It is well known that Hamming balls $Ball(c,t)$ with radius $t=\lfloor (d-1)/2 \rfloor$ around the codewords $c \in C$ are disjoint. Let $y$ is the received message. Then the *Unique Decoding* strategy is to find the codeword $c_y \in C$, such that $y \in Ball(c_y,t)$, or return incomplete decoding, i.e. $y \notin Ball(c,t) \forall c \in C$. Trivial way to do this is to inspect all $q^k$ codewords and return the first $c_y$ such that $d(y,c_y) \le t$. The time complexity of this approach is $O(nq^{Rn})$. Another alternative, with time complexity $O(nq^{H(\delta/2)n})$, is to inspect all $V(n,t)$ error patterns $e$ and find the pattern such that $y-e \in C$. Combining these two decoding strategies, we obtain the time complexity of the unique decoding

$$O\left(n^2 q^{\min\left(R,H\left(\delta/2\right)\right)n}\right). \tag{10}$$

Each linear code $C$ defines partitioning of the space $F_q^n$ in $q^{n-k}$ disjoint sets known as *cosets*. Each coset has $q^k$ vectors. Two vectors $x$ and $y$ belong to same coset iff $x-y\in C$. Each coset $K$ can be spanned by a vector $x$ from the coset, namely

$$K\in\left\{x+c\mid c\in C\right\}. \tag{11}$$

Each coset has two special vectors: a unique *syndrome* $s\in F_q^{n-k}$ and *coset leader* $e(s)\in K$. Coset leader $e(s)$ is one of the minimum weight vectors in the coset $K$. The syndrome is obtained from the multiplication $s=H\cdot x^T$, where $H$ is the parity check matrix of the code and $x$ is arbitrary coset member. For the needs of *syndrome decoding* all pairs $(s,e(s))$ are stored in array known as *the standard array*. In syndrome decoding the error vector $e$ that corrupted the message is considered to be the coset leader $e(s)$ of the coset to which the received message $y$ belongs. Given the received message $y$, first the syndrome is computed $s_y=H\cdot y^T$, then using the array $(s,e(s))$ the leader $e(s_y)$ is found and the codeword $y-e(s_y)$ is outputted. Syndrome decoding has space complexity of exponential size $O\left(nq^{(1-R)n}\right)$.

In [3] it is given a variation of syndrome decoding with space complexity $O\left(\log(n)q^{(1-R)n}\right)$ and time complexity $O(n)$. In this approach, pairs $(s,w(s))$ are kept in memory, where $w(s)$ is the Hamming weight of the coset leader $e(s)$. In the decoding process all error vectors of weight 1 are subtracted from the received message $y$. Let $w(s_y)$ be the weight of the coset with syndrome $s_y=H\cdot y^T$. Then the error vector $e$ that corrupted the sent message is sum of all error vectors $e_1$ of weight 1 such that $w\left(H\cdot\left(y-e_1\right)^T\right)<w(s_y)$.

## 3 New Algorithms for Unique and Minimum Distance Decoding of Linear Codes

We will use $\langle a|b\rangle$ to denote concatenation of two vectors, such that $a$ belongs to the information set and $b$ belongs to the check set of a codeword. Let the message $x$ be encoded in the codeword $c_x=\langle x|r\rangle$ and sent over a noisy channel. Random error pattern is denoted with $e=\langle v|u\rangle$ and the received word is denoted with $y=\langle y_x|y_r\rangle$.

Let assume systematic $[n,k,d]$ code and let $t=\lfloor (d-1)/2 \rfloor$. The unique decoding algorithm, below, inspects all error patterns in the information set $e=\langle v|0\rangle$ with weight $wt(e)\le t$ and outputs the message $\langle x|u\rangle$ if $y$ belongs to some $Ball(c,t)$:

```
Unique_Decoding(y)
1. t ← ⌊(d−1)/2⌋
2.  s_y ← Hy^T
3. if  wt(s_y) ≤ t  return  y
4. foreach  v ∈ F_q^k
5.     if  wt(v) ≤ t
6.         e ← ⟨v|0⟩
7.         s_e ← He^T
8.         if  wt(e) + wt(s_y − s_e) ≤ t  return  y − e
9. return -1 // incomplete decoding
```

**Proposition 1.** The `Unique_Decoding(y)` algorithm removes any error pattern of weight $\le \left\lfloor \frac{d-1}{2} \right\rfloor$ from the received message $y$.

*Proof:* Let $e_v=\langle v|0\rangle$, $wt(e_v)\le t$, is the coset leader and $s_v=He_v^T$ is the syndrome of a coset. Let assume that the pairs $(s_v,e_v)$ are explicitly known; for example, they are stored in a look-up table.

We will consider the error pattern $e=\langle v|u\rangle$ as a linear combination of two vectors

$$e=\langle v|0\rangle+\langle 0|u\rangle=e_v+e_u. \tag{12}$$

Since $wt(e_u)\le t$ and $s_u=He_u^T=u$, we can say that $e_u$ is the leader and $u$ is the syndrome of the same coset. Hence, the syndrome $s$ of the received message $y$ is

$$s=Hy^T=H(c_x+e_v+e_u)^T=s_v+u. \tag{13}$$

From (13), we can formulate the decoding strategy: for each $e_v$ in the table $(s_v,e_v)$ denote with $x=y-e_v$ and compute the syndrome $s_x=Hx^T$. If $wt(e_v)+wt(s_x)\le t$ then the error pattern that corrupted the message is $e=\langle e_v|s_x\rangle$. ■

**Theorem 1.** The time complexity of the `Unique_Decoding` algorithm is upper-bounded by

$$\begin{cases} O\left(n^2 q^{R\cdot H\left(\frac{\delta}{2R}\right)n}\right) & \text{for } R \geq \dfrac{\delta}{2} \\ O\left(n^2 q^{R\cdot n}\right) & \text{for } R \leq \dfrac{\delta}{2} \end{cases}. \tag{14}$$

*Proof:* Given a systematic $[n,k,d]$ code, the `Unique_Decoding` algorithm checks all error patterns of weight $\leq \left\lfloor \frac{d-1}{2} \right\rfloor$ in the information set of $k$ bits. There are

$$V\left(k,\frac{d}{2}\right) = V\left(Rn,\frac{\delta}{2}n\right) \approx q^{n\frac{\log\left(V\left(Rn,\frac{\delta}{2}n\right)\right)}{n}}$$

possible error patterns that can occur in the information set. Thus using (6) we obtain (14). ■

If we use the fact that for long random linear codes the covering radius is equal to $d$, where $d$ is the largest integer solution of the Gilbert-Varshamov inequality [4]

$$V(n,d-1) \leq q^{n-k} \tag{15}$$

Then we can formulate Minimum Distance Decoding algorithm that inspects all error patterns of weight less than $d$ in the information set:

```
MD_Decoding(y)
 1. error ← 0
 2. error_wt ← n
 3. s_y ← Hy^T
 4. if wt(s_y) ≤ t return y
 5. foreach v ∈ F_q^k
 6.     if wt(v) ≤ d
 7.     e ← ⟨v|0⟩
 8.     s_e ← He^T
 9.     if wt(e) + wt(s_y − s_e) ≤ error_wt
10.         error ← e
11.         error_wt ← wt(e) + wt(s_y − s_e)
12. return y − error
```

The proof of correctness of the above algorithm is similar to the proof of Proposition 1. Using (6) we obtain the time complexity of MDD decoding

$$\begin{cases} O\left(n^2 q^{R\cdot H\left(\frac{\delta}{R}\right)n}\right) & \text{for } R \geq \dfrac{\delta}{2} \\ O\left(n^2 q^{R\cdot n}\right) & \text{for } R \leq \dfrac{\delta}{2} \end{cases}. \tag{16}$$

This result improves the previously known bounds on MD decoding found in [5]. Figure 1 plots the functions in the exponents of the complexity bounds (9) and (15), i.e. $\min\left(R, H\left(\delta\right)\right)$ and $RH\left(\frac{\delta}{R}\right)$ for maximal codes. These codes meet the asymptotical Gilbert-Varshamov bound

$$R \geq 1 - H\left(\delta\right). \tag{17}$$

Using (17) we can remove the dependency on the code rate $R$ in the functions $\min\left(R, H\left(\delta\right)\right)$ and $RH\left(\frac{\delta}{R}\right)$. From figure 1 we can observe the improvement of the new complexity expression (15) over the well-known complexity expression (9).

The space complexity of `Unique_Decoding(y)` and `MD_Decoding(y)` is proportional with the dimension of the generator matrix, i.e. $O\left(n^2\right)$.

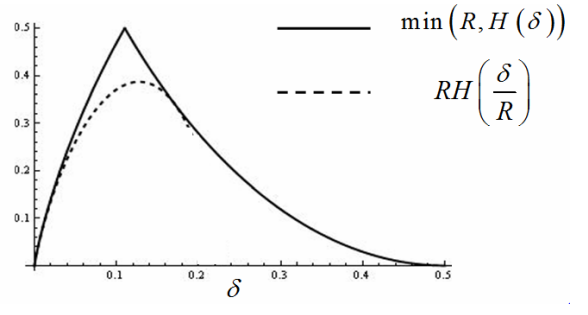


**Fig. 1.** Plot of the functions $\min\left(R, H\left(\delta\right)\right)$ and $RH\left(\frac{\delta}{R}\right)$

## 4 Conclusion

The main importance of *`Unique_Decoding(y)`* and *`MD_Decoding(y)`* algorithms is that they can be used to decode any linear code. Hence, they improve previously known complexity bounds on linear-code decoding. In [6] Evseev published a decoding algorithm with complexity $O\left(q^{R(1-R)n}\right)$ that pertains only to binary codes. Our decoding algorithms can decode linear codes over any alphabet.

Possible application of the `Unique_Decoding(y)` and `MD_Decoding(y)` may be found in *concatenated codes*. Concatenated codes were first introduced in [7] as a method for obtaining asymptotically good codes and they were used in deep space communications in the '70s and '80s [8]. Concatenated codes are obtained by combining two codes called *inner code* and *outer code*. The outer code is usually Reed-Solomon code, while the inner code can be a code meeting the Gilbert-Varshamov bound. Examples of such codes are the greedy codes. From figure 1 we can see that these codes can be decoded with reduced complexity with the new decoding algorithms.

## References

1. Berlekamp, E.R., McEliece, R.J., van Tilborg, H.C.A.: On the Inherent Intractability of Certain Codiig Problems. IEEE Transactions on Information Theory 24(3), 384–386 (1978)
2. Barg, A.: Complexity Issues in Coding Theory. In: Brualdi, R.A., Huffman, W.C., Pless, V. (eds.) Handbook of Coding Theory. Elsevier, Amsterdam (1998)
3. Peterson, W.W., Weldon Jr., E.J.: Error-Correcting Codes, 2nd edn. The Massachusetts Institute of Technology (1996)
4. Barg, A., Krouk, E., van Tilborg, H.: On the complexity of Minimum Distance Decoding of Long Linear Codes. IEEE Transactions on Information Theory 45(5), 1392–1405 (1999)
5. Dumer, I.: Suboptimal decoding of linear codes: Partition technique. IEEE Trans. Inform. Theory 42(6), 1971–1986 (1996)
6. Evseev, G.S.: Complexity of decoding for linear codes. Probl. Inform. Transm. 19(1), 3–8 (in Russian); 1–6 (English translation) (1983)
7. Forney, G.D.: Concatenated Codes. PhD Thesis, Massachusetts Institute of Technology, Cambridge, MA (1965)
8. Concatenated codes, `http://en.wikipedia.org/wiki/Concatenated_error_correction_code`