Hard problems: Complete decoding

Coding Theory Seminar

E. Martínez-Moro

Instituto de Investigación en Matemáticas (imUVa)

Universidad de Valladolid

References

Complexity issues in coding theory, in Handbook of Coding Theory (1998) by A. Barg.

Outline

Complete Decoding

Let $\mathcal{C}$ be a $[n, k, d]$ q-ary. We are interested in a mapping that given a vector $\mathbf{y} \in \mathbb{F}_q^n$ provides us one of the closest codeword(s) in $\mathcal{C}$.

Consider the partition of $\mathbb{F}_q^n$ in Voronoi regions. For each $\mathbf{c} \in \mathcal{C}$

$$D(\mathbf{c}) = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathrm{d}_H(\mathbf{x}, \mathbf{c}) \leq \mathrm{d}_H(\mathbf{x}, \mathbf{c}'), \mathbf{c} \neq \mathbf{c}' \in \mathcal{C}\}$$

Note that some points $\mathbf{y}$ can be contained in more than one region and the decoding problem is to find in which region(s) it lays.

A trivial way of solving it is to list all the q^k codewords, this has time complexity $\mathcal{O}(nq^k)$.

Complete Decoding

Let $\mathcal{C}$ be a $[n, k, d]$ q-ary. We are interested in a mapping that given a vector $\mathbf{y} \in \mathbb{F}_q^n$ provides us one of the closest codeword(s) in $\mathcal{C}$.

Consider the partition of $\mathbb{F}_q^n$ in Voronoi regions. For each $\mathbf{c} \in \mathcal{C}$

$$D(\mathbf{c}) = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathrm{d}_H(\mathbf{x}, \mathbf{c}) \leq \mathrm{d}_H(\mathbf{x}, \mathbf{c}'), \mathbf{c} \neq \mathbf{c}' \in \mathcal{C}\}$$

Note that some points $\mathbf{y}$ can be contained in more than one region and the decoding problem is to find in which region(s) it lays.

A trivial way of solving it is to list all the q^k codewords, this has time complexity $\mathcal{O}(nq^k)$.

Syndrome Decoding

Keep stored the table of q^{n-k} possible syndromes $\{H\mathbf{x}^t \mid \mathbf{x} \in \mathbb{F}_q^n\}$ and the coset leader $\mathbf{e}_{H\mathbf{x}^t}$ for each of them (i.e. the smallest vector $\mathbf{e}$ such that $H\mathbf{e}^t$ belongs to the coset $H\mathbf{x}^t$).

To decode one substracts to the received vector $\mathbf{y}$ the coset leader corresponding to its coset $\mathbf{e}_{\mathbf{H}\mathbf{y}^T}$.

Thus now the space complexity is $\mathcal{O}(nq^{n-k})$.

Syndrome Decoding

Keep stored the table of q^{n-k} possible syndromes $\{H\mathbf{x}^t \mid \mathbf{x} \in \mathbb{F}_q^n\}$ and the coset leader $\mathbf{e}_{H\mathbf{x}^t}$ for each of them (i.e. the smallest vector $\mathbf{e}$ such that $H\mathbf{e}^t$ belongs to the coset $H\mathbf{x}^t$).

To decode one substracts to the received vector $\mathbf{y}$ the coset leader corresponding to its coset $\mathbf{e}_{\mathbf{H}\mathbf{y}^T}$.

Thus now the space complexity is $\mathcal{O}(nq^{n-k})$.

Evseev Lemma - Bounded distance d.

Let $B \subset \{\mathbf{e} \in \mathbb{F}_q^n \mid \mathrm{w}_H(\mathbf{e}) \leq d_0\}$ the set of q^{n-k} most probable (may be not unique) error vectors.

Lemma.- Bounded distance decoding in the sphere of radious d_0 at most doubles the error probability p_c of complete decoding.

Proof: Let L be the set of coset leaders. An error pattern $\mathbf{e}$ outside L contributes to p_c, that is $p_c = \mathrm{Pr}(\{e \in \mathbb{F}_q^n \setminus L\})$.In the bounded case
$p_b = \mathrm{Pr}(\{e \in \mathbb{F}_q^n \setminus (L \cap B)\}) = \mathrm{Pr}(\{e \in \mathbb{F}_q^n \setminus L\}) + \mathrm{Pr}(\{e \in L \setminus (L \cap B)\})$
$\leq p_c + \mathrm{Pr}(\{e \in B \setminus (L \cap B)\})$ since $|B| = |L|$ and B are the most probable.Finally the last event is contained in $\{e \in \mathbb{F}_q^n \setminus L\}$. □

Evseev Lemma - Bounded distance d.

Let $B \subset \{\mathbf{e} \in \mathbb{F}_q^n \mid \mathrm{w}_H(\mathbf{e}) \leq d_0\}$ the set of q^{n-k} most probable (may be not unique) error vectors.

Lemma.- Bounded distance decoding in the sphere of radious d_0 at most doubles the error probability p_c of complete decoding.

Proof: Let L be the set of coset leaders. An error pattern $\mathbf{e}$ outside L contributes to p_c, that is $p_c = \Pr(\{e \in \mathbb{F}_q^n \setminus L\})$. In the bounded case

$p_b = \Pr(\{e \in \mathbb{F}_q^n \setminus (L \cap B)\}) = \Pr(\{e \in \mathbb{F}_q^n \setminus L\}) + \Pr(\{e \in L \setminus (L \cap B)\})$
$\leq p_c + \Pr(\{e \in B \setminus (L \cap B)\})$ since $|B| = |L|$ and B are the most probable. Finally the last event is contained in $\{e \in \mathbb{F}_q^n \setminus L\}$. □

Evseev Lemma - Bounded distance d.

Let $B \subset \{\mathbf{e} \in \mathbb{F}_q^n \mid \mathrm{w}_H(\mathbf{e}) \leq d_0\}$ the set of q^{n-k} most probable (may be not unique) error vectors.

Lemma.- Bounded distance decoding in the sphere of radious d_0 at most doubles the error probability p_c of complete decoding.

Proof: Let L be the set of coset leaders. An error pattern $\mathbf{e}$ outside L contributes to p_c, that is $p_c = \Pr(\{e \in \mathbb{F}_q^n \setminus L\})$.In the bounded case

$p_b = \Pr(\{e \in \mathbb{F}_q^n \setminus (L \cap B)\}) = \Pr(\{e \in \mathbb{F}_q^n \setminus L\}) + \Pr(\{e \in L \setminus (L \cap B)\})$
$\leq p_c + \Pr(\{e \in B \setminus (L \cap B)\})$ since $|B| = |L|$ and B are the most probable.Finally the last event is contained in $\{e \in \mathbb{F}_q^n \setminus L\}$. □

Evseev Lemma - Bounded distance d.

Let $B \subset \{\mathbf{e} \in \mathbb{F}_q^n \mid \mathrm{w}_H(\mathbf{e}) \leq d_0\}$ the set of q^{n-k} most probable (may be not unique) error vectors.

Lemma.- Bounded distance decoding in the sphere of radious d_0 at most doubles the error probability p_c of complete decoding.

Proof: Let L be the set of coset leaders. An error pattern $\mathbf{e}$ outside L contributes to p_c, that is $p_c = \Pr(\{e \in \mathbb{F}_q^n \setminus L\})$.In the bounded case
$p_b = \Pr(\{e \in \mathbb{F}_q^n \setminus (L \cap B)\}) = \Pr(\{e \in \mathbb{F}_q^n \setminus L\}) + \Pr(\{e \in L \setminus (L \cap B)\})$
$\leq p_c + \Pr(\{e \in B \setminus (L \cap B)\})$ since $|B| = |L|$ and B are the most probable.Finally the last event is contained in $\{e \in \mathbb{F}_q^n \setminus L\}$. $\square$

Bounded distance decoding

It can be proved (see page 41 of Barg's paper) that for almost all long $[n, k]$ linear codes it covering radius equals to $d_0(1 + o(1))$. By lemma before one can use the following adapted syndrome decoding:

- Inspect all the error patterns in a sphere of radius d_0 around the received word $\mathbf{y}$.

We can also now formulate complete decoding in the following combinatorial way

- Given a vector $\mathbf{y} \in \mathbb{F}_q^n$ with $\mathrm{d}_H(\mathbf{y}, \mathcal{C}) \leq d_0$ find the closest codeword $\mathbf{c}$ to $\mathbf{y}$.

Bounded distance decoding

It can be proved (see page 41 of Barg's paper) that for almost all long $[n, k]$ linear codes it covering radius equals to $d_0(1 + o(1))$. By lemma before one can use the following adapted syndrome decoding:

- Inspect all the error patterns in a sphere of radius d_0 around the received word $\mathbf{y}$.

We can also now formulate complete decoding in the following combinatorial way

- Given a vector $\mathbf{y} \in \mathbb{F}_q^n$ with $\mathrm{d}_H(\mathbf{y}, \mathcal{C}) \leq d_0$ find the closest codeword $\mathbf{c}$ to $\mathbf{y}$.

Bounded distance decoding

It can be proved (see page 41 of Barg's paper) that for almost all long $[n, k]$ linear codes it covering radius equals to $d_0(1 + o(1))$. By lemma before one can use the following adapted syndrome decoding:

- Inspect all the error patterns in a sphere of radius d_0 around the received word $\mathbf{y}$.

We can also now formulate complete decoding in the following combinatorial way

- Given a vector $\mathbf{y} \in \mathbb{F}_q^n$ with $\mathrm{d}_H(\mathbf{y}, \mathcal{C}) \leq d_0$ find the closest codeword $\mathbf{c}$ to $\mathbf{y}$.

Bounded distance decoding

If we have the parity check matrix of our code in systematic form

$$H = [\,\mathrm{Id}_{n-k} \mid A\,]$$

it is easy to check that if the syndrome has weight less that $\frac{d}{2}$ then the non-zero coordinates locate the errors in check part (the first $n-k$ coordinates).

Just take into account that every coset has at most one vector of weight $\frac{d}{2}$ and we can form them just with the check part.

Thus, syndromes of weight $\leq \frac{d}{2}$ do not need to be decoded.

Bounded distance decoding

If we have the parity check matrix of our code in systematic form

$$H = [\,\mathrm{Id}_{n-k} \mid A\,]$$

it is easy to check that if the syndrome has weight less that $\frac{d}{2}$ then the non-zero coordinates locate the errors in check part (the first $n-k$ coordinates).

Just take into account that every coset has at most one vector of weight $\frac{d}{2}$ and we can form them just with the check part.

Thus, syndromes of weight $\leq \frac{d}{2}$ do not need to be decoded.

Bounded distance decoding

If we have the parity check matrix of our code in systematic form

$$H = [\,\mathrm{Id}_{n-k} \mid A\,]$$

it is easy to check that if the syndrome has weight less that $\frac{d}{2}$ then the non-zero coordinates locate the errors in check part (the first $n-k$ coordinates).

Just take into account that every coset has at most one vector of weight $\frac{d}{2}$ and we can form them just with the check part.

Thus, syndromes of weight $\leq \frac{d}{2}$ do not need to be decoded.

Computing d

Unfortunately computing d for an arbitrary code is as hard as decoding, i.e. if one can compute a minimum weight codeword of a linear code one can decode. More formally

Lemma.- An algorithm that finds a minimum weight codeword of a linear code one can also decode up to $\lfloor \frac{d-1}{2} \rfloor$ errors.

Can you see why?

Computing d

Unfortunately computing d for an arbitrary code is as hard as decoding, i.e. if one can compute a minimum weight codeword of a linear code one can decode.More formally

Lemma.- An algorithm that finds a minimum weight codeword of a linear code one can also decode up to $\lfloor \frac{d-1}{2} \rfloor$ errors.

Can you see why?

Split syndrome decoding

We want to reduce the complexity of syndrome decoding by taking into account a better arrangement of the table spltting the syndrome in several parts.

As usual, let $\mathbf{y}$ be the received vector and $\mathbf{s} = H\mathbf{y}^T$, and suppose that t is the actual number of errors.

Consider $[n]$ partition in $L = \{1, \ldots, m\}$ and $R\{m+1, \ldots, n\}$ and H_l, H_r the corresponding partition of H.

Any error of type $\mathbf{e} = (\mathbf{e}_l|\mathbf{e}_r)$ where

$$H\mathbf{e}^T = H_l\mathbf{e}_l^T + H_r\mathbf{e}_r^T = \mathbf{s}$$

is a pausible candidate for decoding.

Split syndrome decoding

We want to reduce the complexity of syndrome decoding by taking into account a better arrangement of the table spltting the syndrome in several parts.

As usual, let $\mathbf{y}$ be the received vector and $\mathbf{s} = H\mathbf{y}^T$, and suppose that t is the actual number of errors.

Consider $[n]$ partition in $L = \{1, \ldots, m\}$ and $R\{m+1, \ldots, n\}$ and H_l, H_r the corresponding partition of H.

Any error of type $\mathbf{e} = (\mathbf{e}_l | \mathbf{e}_r)$ where

$$H\mathbf{e}^T = H_l\mathbf{e}_l^T + H_r\mathbf{e}_r^T = \mathbf{s}$$

is a pausible candidate for decoding.

Split syndrome decoding

Assume also that the number of errors in L is u where $u \leq m$ and $t - u \leq n - m$.

For every possible (m)-vector $\mathbf{e}_l$, compute $\mathbf{s}_l = H_l \mathbf{e}_l^T$ and store it in a table X_l together with $\mathbf{e}_l$. The size of X_l is

$$\mathcal{O}\left(n\binom{m}{u}(q-1)^u\right).$$

Likewise we have X_r of size

$$\mathcal{O}\left(n\binom{n-m}{t-u}(q-1)^{t-u}\right).$$

Split syndrome decoding

Assume also that the number of errors in L is u where $u \leq m$ and $t - u \leq n - m$.

For every possible (m)-vector $\mathbf{e}_l$, compute $\mathbf{s}_l = H_l \mathbf{e}_l^T$ and store it in a table X_l together with $\mathbf{e}_l$. The size of X_l is

$$\mathcal{O}\left(n\binom{m}{u}(q-1)^u\right).$$

Likewise we have X_r of size

$$\mathcal{O}\left(n\binom{n-m}{t-u}(q-1)^{t-u}\right).$$

Split syndrome decoding

Assume also that the number of errors in L is u where $u \leq m$ and $t - u \leq n - m$.

For every possible (m)-vector $\mathbf{e}_l$, compute $\mathbf{s}_l = H_l \mathbf{e}_l^T$ and store it in a table X_l together with $\mathbf{e}_l$. The size of X_l is

$$\mathcal{O}\left(n\binom{m}{u}(q-1)^u\right).$$

Likewise we have X_r of size

$$\mathcal{O}\left(n\binom{n-m}{t-u}(q-1)^{t-u}\right).$$

Split syndrome decoding

We will look in X_l, X_r for a pair of entries $\mathbf{s}_l$, $\mathbf{s}_r$ that add up the received syndrome $\mathbf{s}$ (for practical issues of how to order the tables see Barg's paper).

In practise we do not know neither the number of errors nor their distribution in L, R. Thus we must repeat the procedure for several choices of m and u, optimizing the choice of in order to reduce the size of memory needed to store X_l and X_r. Since their sizes are exponential we must choose a point where both tables are equally populated.

Finally the entire procedure need to be repeated for $t = 1, 2, \ldots, d_0$. An estimation of time and space complexity of this procedure can be found in page 47 of Barg's paper.

Split syndrome decoding

We will look in X_l, X_r for a pair of entries $\mathbf{s}_l$, $\mathbf{s}_r$ that add up the received syndrome $\mathbf{s}$ (for practical issues of how to order the tables see Barg's paper).

In practise we do not know neither the number of errors nor their distribution in L, R. Thus we must repeat the procedure for several choices of m and u, optimizing the choice of in order to reduce the size of memory needed to store X_l and X_r. Since their sizes are exponential we must choose a point where both tables are equally populated.

Finally the entire procedure need to be repeated for $t = 1, 2, \ldots, d_0$. An estimation of time and space complexity of this procedure can be found in page 47 of Barg's paper.

Split syndrome decoding

We will look in X_l, X_r for a pair of entries $\mathbf{s}_l$, $\mathbf{s}_r$ that add up the received syndrome $\mathbf{s}$ (for practical issues of how to order the tables see Barg's paper).

In practise we do not know neither the number of errors nor their distribution in L, R. Thus we must repeat the procedure for several choices of m and u, optimizing the choice of in order to reduce the size of memory needed to store X_l and X_r. Since their sizes are exponential we must choose a point where both tables are equally populated.

Finally the entire procedure need to be repeated for $t = 1, 2, \ldots, d_0$. An estimation of time and space complexity of this procedure can be found in page 47 of Barg's paper.

Gradient like decoding

In this section we want to define a steepest descent method for Hamming metric.

The general principle will be to construct a set $\mathcal{T}$ of codewords in such a way that given a vector $\mathbf{y} \in \mathbb{F}_q^n$ then

1. Either $\mathbf{y} \in D(\mathbf{0})$,
2. or there exist a $\mathbf{z} \in \mathcal{T}$ such that

$$\mathrm{w}_H(\mathbf{y} - \mathbf{z}) < \mathrm{w}_H(\mathbf{y}).$$

Any set $\mathcal{T} \subset \mathcal{C}$ satisfying this property will be called a test set.

Gradient like decoding

In this section we want to define a steepest descent method for Hamming metric.

The general principle will be to construct a set $\mathcal{T}$ of codewords in such a way that given a vector $\mathbf{y} \in \mathbb{F}_q^n$ then

1. Either $\mathbf{y} \in D(\mathbf{0})$,
2. or there exist a $\mathbf{z} \in \mathcal{T}$ such that

$$\mathrm{w}_H(\mathbf{y} - \mathbf{z}) < \mathrm{w}_H(\mathbf{y}).$$

Any set $\mathcal{T} \subset \mathcal{C}$ satisfying this property will be called a test set.

Gradient like decoding

In this section we want to define a steepest descent method for Hamming metric.

The general principle will be to construct a set $\mathcal{T}$ of codewords in such a way that given a vector $\mathbf{y} \in \mathbb{F}_q^n$ then

1. Either $\mathbf{y} \in D(\mathbf{0})$,
2. or there exist a $\mathbf{z} \in \mathcal{T}$ such that

$$\mathrm{w}_H(\mathbf{y} - \mathbf{z}) < \mathrm{w}_H(\mathbf{y}).$$

Any set $\mathcal{T} \subset \mathcal{C}$ satisfying this property will be called a test set.

Gradient like decoding algorithm

Suppose a test set $\mathcal{T} \subset \mathcal{C}$ has been precomputed.

- Set $\mathbf{c} = \mathbf{0}$.
- Find $\mathbf{z} \in \mathcal{T}$ such that

$$\mathrm{w}_H(\mathbf{y} - \mathbf{z}) < \mathrm{w}_H(\mathbf{y}).$$

  $\mathbf{c} \leftarrow \mathbf{c} + \mathbf{z}$, $\mathbf{y} \leftarrow \mathbf{y} - \mathbf{z}$.
- Repeat until no such a $\mathbf{z}$ is found.
- Output $\mathbf{c}$.

Gradient like decoding algorithm

Theorem .- For a test set $\mathcal{T}$ the gradient-like algorithm performs a complete-minimum distance decoding. The time complexity is $\mathcal{O}(n^2|\mathcal{T}|)$ and the space complexity is $\mathcal{O}(n|\mathcal{T}|)$.

Proof: Let $\mathbf{y} \notin D(\mathbf{0})$, then the algorithm expands $\mathbf{y}$ in a sum of test vectors. Suppose that after m step no further vector is added, this means that we brought $\mathbf{y}$ to $D(\mathbf{0})$, that is

$$\mathbf{e} = \mathbf{y} - \sum_{u=1}^{m} \mathbf{z}_u \in D(\mathbf{0}),$$

i.e. $\mathbf{y} \in D(\sum_{u=1}^{m} \mathbf{z}_u)$. □

Gradient like decoding algorithm

Theorem .- For a test set $\mathcal{T}$ the gradient-like algorithm performs a complete-minimum distance decoding. The time complexity is $\mathcal{O}(n^2|\mathcal{T}|)$ and the space complexity is $\mathcal{O}(n|\mathcal{T}|)$.

Proof: Let $\mathbf{y} \notin D(\mathbf{0})$, then the algorithm expands $\mathbf{y}$ in a sum of test vectors. Suppose that after m step no further vector is added, this means that we brought $\mathbf{y}$ to $D(\mathbf{0})$, that is

$$\mathbf{e} = \mathbf{y} - \sum_{u=1}^{m} \mathbf{z}_u \in D(\mathbf{0}),$$

i.e. $\mathbf{y} \in D(\sum_{u=1}^{m} \mathbf{z}_u)$. □

Gradient like decoding algorithm

Note that if we submit a codeword $\mathbf{0} \neq \mathbf{c} \in \mathcal{C}$ to the algorithm we get

$$\mathbf{0} = \mathbf{c} - \sum_{u=1}^{m} \mathbf{z}_u$$

with $\mathrm{w}_H(\mathbf{c}) > \mathrm{w}_H(\mathbf{c} - \sum_{u=1}^{1} \mathbf{z}_u) > \cdots > \mathrm{w}_H(\mathbf{c} - \sum_{u=1}^{m-1} \mathbf{z}_u) \geq 0$.

In particular $\mathcal{T}$ spands $\mathcal{C}$.

Minimal vectors

Let $\text{supp}(\mathbf{x}) = \{i \in [n] \mid \mathbf{x}_i \neq 0\}$ be the support of the vector $\mathbf{x}$. If $\text{supp}(\mathbf{x}) \subset \text{supp}(\mathbf{y})$ (resp. $\subseteq$) we say that $\mathbf{x} \prec \mathbf{y}$ (resp. $\preceq$).

A codeword $\mathbf{m} \in \mathcal{C}$ is said to be minimal if

$$\mathbf{0} \neq \mathbf{c} \preceq \mathbf{m}, \text{ and } \mathbf{c} \in \mathcal{C}$$

implies that $\mathbf{c} = \alpha \mathbf{m}$ for a non-zero constant $\alpha \in \mathbb{F}_q$.

We will denote by $\mathcal{M}$ the set of minimal codewords of a code $\mathcal{C}$. For binary codes it can be seen also as the set of minimal supports, in other case they define a set of projective points ("lines") in the code.

Minimal vectors

Let $\mathrm{supp}(\mathbf{x}) = \{i \in [n] \mid \mathbf{x}_i \neq 0\}$ be the support of the vector $\mathbf{x}$. If $\mathrm{supp}(\mathbf{x}) \subset \mathrm{supp}(\mathbf{y})$ (resp. $\subseteq$) we say that $\mathbf{x} \prec \mathbf{y}$ (resp. $\preceq$).

A codeword $\mathbf{m} \in \mathcal{C}$ is said to be minimal if

$$\mathbf{0} \neq \mathbf{c} \preceq \mathbf{m}, \text{ and } \mathbf{c} \in \mathcal{C}$$

implies that $\mathbf{c} = \alpha\mathbf{m}$ for a non-zero constant $\alpha \in \mathbb{F}_q$.

We will denote by $\mathcal{M}$ the set of minimal codewords of a code $\mathcal{C}$. For binary codes it can be seen also as the set of minimal supports, in other case they define a set of projective points ("lines") in the code.

Minimal vectors

Let $\mathrm{supp}(\mathbf{x}) = \{i \in [n] \mid \mathbf{x}_i \neq 0\}$ be the support of the vector $\mathbf{x}$. If $\mathrm{supp}(\mathbf{x}) \subset \mathrm{supp}(\mathbf{y})$ (resp. $\subseteq$) we say that $\mathbf{x} \prec \mathbf{y}$ (resp. $\preceq$).

A codeword $\mathbf{m} \in \mathcal{C}$ is said to be minimal if

$$\mathbf{0} \neq \mathbf{c} \preceq \mathbf{m}, \text{ and } \mathbf{c} \in \mathcal{C}$$

implies that $\mathbf{c} = \alpha\mathbf{m}$ for a non-zero constant $\alpha \in \mathbb{F}_q$.

We will denote by $\mathcal{M}$ the set of minimal codewords of a code $\mathcal{C}$. For binary codes it can be seen also as the set of minimal supports, in other case they define a set of projective points ("lines") in the code.

Minimal vectors g.d.d.

From now on $q = 2$.

Theorem .- For binary codes $\mathcal{M}$ is a test set, i.e. defines a gradient-like algorithm that performs a complete-minimum distance decoding.

Proof: One just need to check that for $\mathbf{y} \notin D(\mathbf{0})$ there is a codeword $\mathbf{c}$ such that

$$\mathrm{w}_H(\mathbf{y} + \mathbf{c}) < \mathrm{w}_H(\mathbf{y}).$$

Now spand $\mathbf{c}$ into a sum of minimal vectors whose support do not intersect and we have done. □

On average the time complexity of g.d.d. with $\mathcal{M}$ does not improve the sydrome decoding (see Bar's paper pages 50–51)

Minimal vectors g.d.d.

From now on $q = 2$.

Theorem .- For binary codes $\mathcal{M}$ is a test set, i.e. defines a gradient-like algorithm that performs a complete-minimum distance decoding.

Proof: One just need to check that for $\mathbf{y} \notin D(\mathbf{0})$ there is a codeword $\mathbf{c}$ such that

$$\mathrm{w}_H(\mathbf{y} + \mathbf{c}) < \mathrm{w}_H(\mathbf{y}).$$

Now spand $\mathbf{c}$ into a sum of minimal vectors whose support do not intersect and we have done. □

On average the time complexity of g.d.d. with $\mathcal{M}$ does not improve the sydrome decoding (see Bar's paper pages 50–51)

Minimal vectors g.d.d.

From now on $q = 2$.

Theorem .- For binary codes $\mathcal{M}$ is a test set, i.e. defines a gradient-like algorithm that performs a complete-minimum distance decoding.

Proof: One just need to check that for $\mathbf{y} \notin D(\mathbf{0})$ there is a codeword $\mathbf{c}$ such that

$$\mathrm{w}_H(\mathbf{y} + \mathbf{c}) < \mathrm{w}_H(\mathbf{y}).$$

Now spand $\mathbf{c}$ into a sum of minimal vectors whose support do not intersect and we have done. □

On average the time complexity of g.d.d. with $\mathcal{M}$ does not improve the sydrome decoding (see Bar's paper pages 50–51)

Minimal vectors

Some properties of minimal supports:

1. Let $E \subset [n]$ a support of a codeword $\mathbf{c}$. Then E is minimal iff
$$\mathrm{rk}(H(E)) = |E| - 1.$$
2. E is minimal $\Rightarrow |E| \leq n - k + 1$.
3. Every support of size $|E| \leq 2d - 1$ is minimal.

People with a combinatorial background can see here the definition of a representable matroid.

Zero neighbors

Let $A \subset \mathbb{F}_q^n$ and let $\mathcal{X}(A)$ be the set of all the points in $\mathbb{F}_q^n$ at distance 1 from A:

$$\mathcal{X}(A) = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathrm{d}_H(\mathbf{x}, A) = 1\}.$$

We define the boundary of A as

$$\delta(A) = \mathcal{X}(A) \cup \mathcal{X}(\mathbb{F}_q^n \setminus A).$$

A non-zero codeword $\mathbf{c} \in \mathcal{C}$ is called a zero neighbor if its Voronoi region shares a common boundary with $D(\mathbf{0})$, i.e.

$$\delta(D(\mathbf{c})) \cap \delta(D(\mathbf{0})) \neq \emptyset.$$

Zero neighbors

Let $A \subset \mathbb{F}_q^n$ and let $\mathcal{X}(A)$ be the set of all the points in $\mathbb{F}_q^n$ at distance 1 from A:

$$\mathcal{X}(A) = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathrm{d}_H(\mathbf{x}, A) = 1\}.$$

We define the boundary of A as

$$\delta(A) = \mathcal{X}(A) \cup \mathcal{X}(\mathbb{F}_q^n \setminus A).$$

A non-zero codeword $\mathbf{c} \in \mathcal{C}$ is called a zero neighbor if its Voronoi region shares a common boundary with $D(\mathbf{0})$, i.e.

$$\delta(D(\mathbf{c})) \cap \delta(D(\mathbf{0})) \neq \emptyset.$$

Zero neighbors

Let $A \subset \mathbb{F}_q^n$ and let $\mathcal{X}(A)$ be the set of all the points in $\mathbb{F}_q^n$ at distance 1 from A:

$$\mathcal{X}(A) = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathrm{d}_H(\mathbf{x}, A) = 1\}.$$

We define the boundary of A as

$$\delta(A) = \mathcal{X}(A) \cup \mathcal{X}(\mathbb{F}_q^n \setminus A).$$

A non-zero codeword $\mathbf{c} \in \mathcal{C}$ is called a zero neighbor if its Voronoi region shares a common boundary with $D(\mathbf{0})$, i.e.

$$\delta(D(\mathbf{c})) \cap \delta(D(\mathbf{0})) \neq \emptyset.$$

Zero neighbors

Note that if $\mathbf{c} \in \mathcal{C}$ is a zero neighbors so are all its scalar multiples. We will denote by $\mathcal{Z}$ the set of all the zero neighbors in $\mathcal{C}$. It is a direct consecuence of the definition that

$$\mathcal{X}(D(\mathbf{0})) \cap D(\mathbf{z}) \neq \emptyset \Rightarrow \mathbf{z} \in \mathcal{Z}.$$

Proof: $\mathbf{x} \in \mathcal{X}(D(\mathbf{0})) \cap D(\mathbf{z})$ implies that there exist a $\mathbf{y} \in D(\mathbf{0})$ at distance 1 from $\mathbf{x}$. Thus $\mathbf{y} \in \delta(D(\mathbf{0})) \cap \delta(D(\mathbf{z}))$. □

Zero neighbors

Note that if $\mathbf{c} \in \mathcal{C}$ is a zero neighbors so are all its scalar multiples. We will denote by $\mathcal{Z}$ the set of all the zero neighbors in $\mathcal{C}$. It is a direct consecuence of the definition that

$$\mathcal{X}(D(\mathbf{0})) \cap D(\mathbf{z}) \neq \emptyset \Rightarrow \mathbf{z} \in \mathcal{Z}.$$

Proof: $\mathbf{x} \in \mathcal{X}(D(\mathbf{0})) \cap D(\mathbf{z})$ implies that there exist a $\mathbf{y} \in D(\mathbf{0})$ at distance 1 from $\mathbf{x}$. Thus $\mathbf{y} \in \delta(D(\mathbf{0})) \cap \delta(D(\mathbf{z}))$. □

Zero neighbors g.d.d.

Theorem .- For binary codes $\mathscr{Z}$ is a test set, i.e. defines a gradient-like algorithm that performs a complete-minimum distance decoding.

Proof: Consider $\mathbf{y} \notin D(\mathbf{0})$ and a chain of inclusions

$$\mathbf{0} = \mathbf{y}_0 \prec \mathbf{y}_1 \prec \cdots \prec \mathbf{y}_{i-1} \prec \mathbf{y}_i \prec \cdots \prec \mathbf{y},$$

where $\mathrm{w}_H(\mathbf{y}_i) = i$. Then there exist a i such that $\mathbf{y}_{i-1} \in D(\mathbf{0})$ and $\mathbf{y}_i \in \delta(D(\mathbf{0})) \setminus D(\mathbf{0})$. Thus $\mathbf{y}_i \in D(\mathbf{z})$ for some $\mathbf{z} \in \mathscr{Z}$ and

$$\mathrm{w}_H(\mathbf{y} - \mathbf{z}) = \mathrm{d}_H(\mathbf{y}, \mathbf{z}) \leq \mathrm{d}_H(\mathbf{y}, \mathbf{y}_i) + \mathrm{d}_H(\mathbf{y}_i, \mathbf{z})$$

$$< \mathrm{d}_H(\mathbf{y}, \mathbf{y}_i) + \mathrm{d}_H(\mathbf{y}_i, \mathbf{0}) = \mathrm{w}_H(\mathbf{y})$$

therefore $\mathscr{Z}$ is a test set. □

Zero neighbors g.d.d.

Theorem .- For binary codes $\mathcal{Z}$ is a test set, i.e. defines a gradient-like algorithm that performs a complete-minimum distance decoding.

Proof: Consider $\mathbf{y} \notin D(\mathbf{0})$ and a chain of inclusions

$$\mathbf{0} = \mathbf{y}_0 \prec \mathbf{y}_1 \prec \cdots \prec \mathbf{y}_{i-1} \prec \mathbf{y}_i \prec \cdots \prec \mathbf{y},$$

where $\mathrm{w}_H(\mathbf{y}_i) = i$. Then there exist a i such that $\mathbf{y}_{i-1} \in D(\mathbf{0})$ and $\mathbf{y}_i \in \delta(D(\mathbf{0})) \setminus D(\mathbf{0})$. Thus $\mathbf{y}_i \in D(\mathbf{z})$ for some $\mathbf{z} \in \mathcal{Z}$ and

$$\mathrm{w}_H(\mathbf{y} - \mathbf{z}) = \mathrm{d}_H(\mathbf{y}, \mathbf{z}) \leq \mathrm{d}_H(\mathbf{y}, \mathbf{y}_i) + \mathrm{d}_H(\mathbf{y}_i, \mathbf{z})$$

$$< \mathrm{d}_H(\mathbf{y}, \mathbf{y}_i) + \mathrm{d}_H(\mathbf{y}_i, \mathbf{0}) = \mathrm{w}_H(\mathbf{y})$$

therefore $\mathcal{Z}$ is a test set. □

Size of $\mathcal{Z}$

Lemma .- For all $\mathbf{z} \in \mathcal{Z}$ the set of zero neighbors of the code $\mathcal{C}$,

$$\mathrm{w}_H(\mathbf{z}) \leq 2t + 2$$

where t is the covering radius of $\mathcal{C}$.

Proof: Let $\mathbf{x}$ be a point in $\delta(D(\mathbf{0})) \cap \delta(D(\mathbf{z}))$. Then

$$\mathrm{d}_H(\mathbf{0}, \mathbf{z}) \leq \mathrm{d}_H(\mathbf{z}, \mathbf{x}) + \mathrm{d}_H(\mathbf{x}, \mathbf{0}) \leq (t+1) + (t+1).$$

□

Size of $\mathcal{Z}$

Lemma .- For all $\mathbf{z} \in \mathcal{Z}$ the set of zero neighbors of the code $\mathcal{C}$,

$$\mathrm{w}_H(\mathbf{z}) \leq 2t + 2$$

where t is the covering radius of $\mathcal{C}$.

Proof: Let $\mathbf{x}$ be a point in $\delta(D(\mathbf{0})) \cap \delta(D(\mathbf{z}))$. Then

$$\mathrm{d}_H(\mathbf{0}, \mathbf{z}) \leq \mathrm{d}_H(\mathbf{z}, \mathbf{x}) + \mathrm{d}_H(\mathbf{x}, \mathbf{0}) \leq (t+1) + (t+1).$$

□

Size of $\mathcal{Z}$

Thus we have the following upper bound for the size of $\mathcal{Z}$.

Lemma .- For almost all codes $|\mathcal{Z}| \leq q^{n\alpha_q(R)}$ where

$$\alpha_q(R) = \begin{cases} R, & 0 \leq R \leq 1 - H_q\left(\frac{q-1}{2q}\right) \\ (H_q(2\delta_0) - (1-R))(1+o(1)), & 1 - H_q\left(\frac{q-1}{2q}\right) \leq R \leq 1 \end{cases}$$

Instituto de Matemáticas