Summary of the Work

Main Result

- A lower bound on \( \#(\text{uncorrectable errors of weight } \left\lfloor d/2 \right\rfloor) \) for binary linear codes.
  - \( d \): the minimum distance of the code
- A generalization to weight \( > \left\lfloor d/2 \right\rfloor \).

Main Techniques

- Monotone error structure (Larger half)
  - Monotone error structure appears in [Peterson, Weldon, 1972].
  - Larger half was introduced in [Helleseth, Kløve, Levenshtein, 2005].
Outline

- Correctable/Uncorrectable Errors
- Our Results
- Monotone Error Structure
- Proof Sketch of Our Results
Outline

- Correctable/Uncorrectable Errors
- Our Results
- Monotone Error Structure
- Proof Sketch of Our Results
Problem Setting

- Binary linear code \( C \subseteq \{0,1\}^n \)

- Error vector \( e \in \{0,1\}^n \)

- If \( w(e) < d/2 \) \( \Rightarrow \) \( e \) is always correctable.
  - If \( w(e) \geq d/2 \) \( \Rightarrow \) ?
    - \( w(x) \) : the Hamming weight of \( x \)

In this work,
we investigate \#( correctable errors of weight \( i \) ) for \( i \geq d/2 \).
Correctable/Uncorrectable Errors

- **Correctable errors** $E_0^0(C)$
  - $E_0^0(C) = \{0,1\}^n \setminus E_0^0(C)$
  - $E_i^0(C)$: Correctable errors of weight $i$

- **Uncorrectable errors** $E_1^1(C)$
  - $E_i^1(C)$: Uncorrectable errors of weight $i$
  - $|E_i^0(C)| + |E_i^1(C)| = \binom{n}{i}$
  - The error probability over BSC $P_{error}$ is $P_{error} = \sum_{i=0}^{n} p^i (1-p)^{n-i} |E_i^1(C)|$.

- **Minimum distance decoding**
  - Outputs a nearest (w.r.t. Hamming dist.) codeword to the input.
  - Performs ML decoding for BSC.
  - **Syndrome decoding** is a minimum distance decoding.
Syndrome Decoding

- Coset partitioning
  \[
  \{0, 1\}^n = \bigcup_{i=1}^{2^{n-k}} C_i, \quad C_i \cap C_j = \emptyset \quad \text{for } i \neq j
  \]
  
  \[C_i = \{v_i + c : c \in C\} \quad : \text{Coset of } C\]
  
  \[v_i = \arg \min_{v \in C_i} w(v) \quad : \text{Coset leader of } C_i\]

- Syndrome decoding
  - Output \( y + v_i \) if \( y \in C_i \) (\( y \) is the input).
  - Coset leaders = Correctable errors.
Outline

- Correctable/Uncorrectable Errors
- Our Results
- Monotone Error Structure
- Proof Sketch of Our Results
Previous Results for $|E_i^{1}(C)|$

- For the first-order Reed-Muller code $RM_m$
  - $|E_{d/2}^{1}(RM_m)|$ [Wu, 1998]
  - $|E_{d/2+1}^{1}(RM_m)|$ [Yasunaga, Fujiwara, 2007]

- For binary linear codes
  - Upper bounds on $|E_i^{1}(C)|$ for every $0 \leq i \leq n$ [Poltyrev 1994], [Helleseth, Kløve 1997], [Helleseth, Kløve, Levenshtein 2005]
Our Results

- A lower bound on $|E^1_{[d/2]}(C)|$ for codes satisfying some condition.
  - The condition is not too restrictive.
    - Long Reed-Muller codes and random linear codes satisfy
  - Given by #$($codewords of weight $d$ (and $d+1)$).
  - Asymptotically coincides with the corresponding upper bound for Reed-Muller codes and random linear codes.

- A generalization to $|E^1_i(C)|$ for $i > \left\lceil d/2 \right\rceil$.
  - The bound is weak.
Outline

- Correctable/Uncorrectable Errors
- Our Results
- Monotone Error Structure
- Proof Sketch of Our Results
Monotone Error Structure

- Recall that a coset leader is a minimum weight vector in a coset.

- There may be more than one minimum weight vector in the same coset. \( \Rightarrow \) Any of them will do.

- If we take the lexicographically smallest one for all cosets, \( \Rightarrow \) Correctable/uncorrectable errors have a monotone structure.
Monotone Error Structure

■ Notation
  - Support of \( \mathbf{v} \): \( S(\mathbf{v}) = \{ i : v_i \neq 0 \} \)
  - \( \mathbf{v} \) is covered by \( \mathbf{u} \): \( S(\mathbf{v}) \subseteq S(\mathbf{u}) \)

■ Monotone error structure
  - \( \mathbf{v} \) is correctable.
    \( \Rightarrow \) All vectors that are covered by \( \mathbf{v} \) are correctable.
  - \( \mathbf{v} \) is uncorrectable.
    \( \Rightarrow \) All vectors that cover \( \mathbf{v} \) are uncorrectable.

■ Example
  - 1100 is correctable. \( \Rightarrow \) 0000, 1000, 0100 are correctable.
  - 0011 is uncorrectable. \( \Rightarrow \) 1011, 0111, 1111 are uncorrectable.
Minimal Uncorrectable Errors

- Errors have the monotone structure (w.r.t $\subseteq$).
  $\Rightarrow E^1(C)$ is characterized by minimal vectors (w.r.t. $\subseteq$).

- Minimal uncorrectable errors $M^1(C)$
  - = Uncorrectable errs. that are not covered by other uncorrectable errs.
  - $M^1(C)$ uniquely determines $E^1(C)$.

- Larger half $LH(c)$ of $c \in C$
  - Introduced for characterizing $M^1(C)$ in [Helleseth et al., 2005].
  - Combinatorial construction is given in [Helleseth et al., 2005].

  $M^1(C) \subseteq LH(C \setminus \{0\}) \subseteq E^1(C)$, where $LH(S) = \bigcup_{c \in S} LH(c)$. 
Outline

- Correctable/Uncorrectable Errors
- Previous Results
- Our Results
- Monotone Error Structure
- Proof Sketch of Our Results
Proof Sketch of Our Results

- **Objective**: To derive a lower bound on $|E_{d/2}^1(C)|$.

- The following equalities hold:
  \[
  M_{d/2}^1(C) = LH_{d/2}(C \setminus \{0\}) = E_{d/2}^1(C)
  \]
  
  **[Proof]**
  
  - $M^1(C) \subseteq LH(C \setminus \{0\}) \subseteq E^1(C)$
  
  - Since $d/2$ is the smallest weight in $E^1(C)$, uncorrectable errors of weight $d/2$ do not cover any other uncorrectable errors.

  \[\Rightarrow M_{d/2}^1(C) = E_{d/2}^1(C)\]

- Derive a lower bound on $|LH_{d/2}(C \setminus \{0\})|$. 
Proof Sketch of Our Results ( \(d \) is even)

- \( LH_{d/2}(C \setminus \{0\}) = LH(A_d(C)) \), where \( A_i(C) = \{ \text{codewords of weight } i \text{ in } C \} \).

- Larger halves of two codewords in \( A_d(C) \) are almost disjoint.

\[
|LH(c_1) \cap LH(c_2)| \leq 1 \quad \text{for every } c_1, c_2 \in A_d(C)
\]

\[
LH_{d/2}(C \setminus \{0\})
\]

For every \( c_i \in A_d(C) \),

\[
\#(\text{common LH}) \text{ is less than } |A_d(C)|.
\]

\[
\left| \left| LH(c_i) \right| - |A_d(C)| + 1 \right| A_d(C) \leq \left| LH_{d/2}(C \setminus \{0\}) \right|
\]

\[
\frac{1}{2} \binom{d}{d/2}
\]

\[
\left| E_{d/2}^1(C) \right|
\]
The Results ( $d$ is even )

When $d$ is even, if $\frac{1}{2}\left(\begin{array}{c} d \\ d/2 \end{array}\right) > |A_d(C)| - 1$ holds, then

$$\frac{1}{2}\left(\begin{array}{c} d \\ d/2 \end{array}\right)|A_d(C)| - (|A_d(C)| - 1)|A_d(C)| \leq |E^{1}_{d/2}(C)| \leq \frac{1}{2}\left(\begin{array}{c} d \\ d/2 \end{array}\right)|A_d(C)|.$$ 

Upper bound is from [Helleseth et al. 2005]

- If $|A_d(C)|/\left(\begin{array}{c} d \\ d/2 \end{array}\right) \to 0$ as $n \to \infty$ then upper and lower bounds asymptotically coincide.
  - For Reed-Muller codes and random linear codes, the upper and lower bounds asymptotically coincide.
The Results (d is odd)

When $d$ is odd, if \( \left(\frac{d}{(d+1)/2}\right) > |A_d(C)| + |A_{d+1}(C)| - 1 \) holds, then

\[
\left(\frac{d}{(d+1)/2}\right) \left(\|A_d(C)| + |A_{d+1}(C)|\right) - (2|A_d(C)| + |A_{d+1}(C)| - 1) |A_{d+1}(C)| 
\leq |E_{(d+1)/2}^1(C)| \leq \left(\frac{d}{(d+1)/2}\right) \left(\|A_d(C)| + |A_{d+1}(C)|\right).
\]

Upper bound is from [Helleseth et al. 2005]

- If \( |A_{d+1}(C)| \left(\frac{d}{(d+1)/2}\right) \to 0 \) as \( n \to \infty \) then upper and lower bounds asymptotically coincide.
A Generalization to Larger Weights

- A similar argument can be applied to weight $i > \left\lceil \frac{d}{2} \right\rceil$.

For an integer $i$ with $\lceil d/2 \rceil \leq i \leq \lfloor n/2 \rfloor$, if

$$\binom{2i-3}{i} > 3\binom{2i-\left\lceil d/2 \right\rceil}{i} B_i$$

holds, then

$$B_i \leq |LH_i(C)| \leq |E_i^1(C)|$$

$$\leq \binom{2i-3}{i} |A_{2i-2}(C)| + 2\binom{2i-1}{i} (|A_{2i-1}(C)| + |A_{2i}(C)|)$$

where $B_i = |A_{2i-2}(C)| + |A_{2i-1}(C)| + |A_{2i}(C)|$.

For large $i$

- The condition for the bound is more restrictive.
- The bound is weak.
  - The bound is a lower bound on $LH_i(C)$.
  - The difference between $LH_i(C)$ and $E_i^1(C)$ is large.
Conclusion

Main results

- A lower bound on \( #(\text{correctable errors of weight } \left\lceil d/2 \right\rceil) \) for binary linear codes satisfying some condition.
  
  - The bound asymptotically coincides with the upper bound for Reed-Muller codes and random linear codes.
  - Monotone error structure & larger half are main tools.
  - A generalization to weight \( i > \left\lceil d/2 \right\rceil \) is also obtained.
    - The generalized bound is weak for large \( i \).

Future work

- A good lower bound for weight \( > d/2 \).
Codes Satisfying the Condition

The condition

\[
\frac{1}{2} \binom{d}{d/2} > |A_d(T)| - 1 \quad \text{for even } d
\]

\[
\binom{d}{(d+1)/2} > |A_d(T)| + |A_{d+1}(T)| - 1 \quad \text{for odd } d
\]

Codes satisfying the condition

- \((n, k)\) primitive BCH codes for \(n = 127\) and \(k \leq 64\), \(n = 63\) and \(k \leq 24\)
- \((n, k)\) extended primitive BCH codes for \(n = 127\) and \(k \leq 64\), \(n = 63\) and \(k \leq 24\)
- \(r\)-th order Reed-Muller codes of length \(2^m\)
  - fixed \(r\) and \(m \to \infty\)
- Random linear codes for \(n \to \infty\)

<table>
<thead>
<tr>
<th>(r)</th>
<th>(m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(\geq 4)</td>
</tr>
<tr>
<td>2</td>
<td>(\geq 6)</td>
</tr>
<tr>
<td>3</td>
<td>(\geq 8)</td>
</tr>
<tr>
<td>4</td>
<td>(\geq 10)</td>
</tr>
<tr>
<td>5</td>
<td>(\geq 11)</td>
</tr>
<tr>
<td>6</td>
<td>(\geq 13)</td>
</tr>
</tbody>
</table>
Proof Sketch of Our Results ( $d$ is even )

$LH_{d/2}(C)$

\[
\begin{array}{c}
\vdots \\
\vdots \\
\end{array}
\]

\[
\begin{array}{c}
x_1 \\
x_2 \\
\vdots \\
\end{array}
\]
Proof Sketch of Our Results (\(d\) is even)

\[ \mathcal{LH}_{d/2}(\mathcal{C}) \]

\[ A_d(\mathcal{C}) \]

\[ A_i(\mathcal{C}) : \text{the set of codewords with weight } i \]
Proof Sketch of Our Results ( $d$ is even )

$A_d(C)$ : the set of codewords with weight $i$
Proof Sketch of Our Results ( $d$ is even )

$A_d(C) \subseteq LH_{d/2}(C)$

$A_i(C) :$ the set of codewords with weight $i$
Proof Sketch of Our Results (\(d\) is even)

\(A_d(C)\) : the set of codewords with weight \(i\)
Proof Sketch of Our Results ( \( d \) is even)

\[
LH_{d/2}(C)
\]

\[
A_d(C) \quad \text{and} \quad A_i(C) : \text{the set of codewords with weight } i
\]
Proof Sketch of Our Results ( \( d \) is even )

\[ LH_{d/2}(C) \]

\[ |LH(c_i)| = \frac{1}{2} \binom{d}{d/2} \]

\( A_d(C) \) : the set of codewords with weight \( i \)
Proof Sketch of Our Results ( $d$ is even )

\[ LH_{d/2}(C) \]

\[ \{ |LH(c_i)| = \frac{1}{2} \binom{d}{d/2} \} \leq |A_d(T)| - 1 \]

\[ A_d(C) \]

\[ A_i(C) : \text{the set of codewords with weight } i \]
Proof Sketch of Our Results ( \( d \) is even)

\[
LH_{d/2}(C)
\]

\[
LH(\cdot)
\]

\[
A_d(C) \quad \{ \text{the set of codewords with weight } i \}
\]

For every \( c_i \in A_d(T) \),
\(#(\text{common LH}) \) is less than \( |A_d(T)| - 1 \)

Thus,
if \( |LH(c_i)| > |A_d(T)| - 1 \), then
\[
(|LH(c_i)| - |A_d(T)| + 1) |A_d(T)| \leq |LH_{d/2}(T)|
\]
A Generalization to Larger Weight

- The lower bound for weight $\lceil d/2 \rceil$ is obtained by considering the vectors of weight $\lceil d/2 \rceil$ in
  $$M^1(C) \subseteq LH(C) \subseteq E^1(C)$$

- A similar argument can be applied to weight $i \geq \lceil d/2 \rceil + 1$
  However, for large $i$,
    - The condition for the bound is more restrictive
    - The bound is weak
      - The bound is a lower bound on $LH_i(C)$
      - The difference between $LH_i(C)$ and $E_{i}^{1}(C)$ is large