On List Decoding of Alternant Codes in the Hamming and Lee metrics

Ido Tal       Ron M. Roth

Computer Science Department,
Technion, Haifa 32000, Israel.
Previous Work

Berlekamp, 1968: Negacyclic codes for the Lee metric.

Roth and Siegel, 1994: Classical decoding of RS and BCH codes in the Lee metric.

Sudan, 1997: List decoding for the Hamming metric.

Guruswami and Sudan, 1999: Improved list decoding for the Hamming metric.

Koetter and Vardy, 2000: Further improvement of list decoding for the Hamming metric.

Koetter and Vardy, 2002: List decoding for a general metric.
Our Results

• A refined analysis of the algorithm in [KV00] to finite list sizes.

• The decoding radius obtained for alternant codes in the Hamming metric is precisely the one guaranteed by an (improved) version of one of the Johnson bounds.

• A list decoder for alternant codes in the Lee metric.

• Unlike the Hamming metric counterpart, the decoding radius of our list decoder is generally strictly larger than what one gets from the Lee-metric Johnson bound.
List Decoding

Let $F$ be a finite field, and let $d$ be a metric over $F^n$. Let $C$ be an $(n, M, d)$ code over $F$.

- A list-$\ell$ decoder of decoding radius $\tau$ is a function $D : F^n \to 2^C$ such that
  - Each received word $y \in F^n$ is mapped to a set (list) of codewords.
  - The list is guaranteed to contain all codewords in the sphere of radius $\tau$ centered at $y$,
    \[ D(y) \supseteq \{ c \in C : d(c, y) \leq \tau \}. \]
  - The list is guaranteed to contain no more than $\ell$ codewords,
    \[ |D(y)| \leq \ell. \]

- For a fixed $\ell$, the bigger $\tau$ is, the better.
GRS and Alternant Codes

- Fix $F = \text{GF}(q)$ and $\Phi = \text{GF}(q^m)$.

- Denote by $\Phi_k[x]$ the set of all polynomials in the indeterminate $x$ with degree less than $k$ over $\Phi$.

- Hereafter, fix $C_{\text{GRS}}$ as an $[n, k]$ GRS code over $\Phi$ with distinct code locators $\alpha_1, \alpha_2, \ldots, \alpha_n \in \Phi$, and nonzero multipliers $v_1, v_2, \ldots, v_n \in \Phi$, that is

  $$C_{\text{GRS}} = \{ c = (v_1 u(\alpha_1) \ v_2 u(\alpha_2) \ldots \ v_n u(\alpha_n)) : u(x) \in \Phi_k[x] \} .$$

- Fix $C_{\text{alt}}$ as the respective alternant code over $F$,

  $$C_{\text{alt}} = C_{\text{GRS}} \cap F^n .$$
Score of a Codeword

• Define \([n] = \{1, 2, \ldots, n\}\).

• Let \(\mathcal{M} = (m_{\gamma,j})_{\gamma \in F, j \in [n]}\) be a \(q \times n\) matrix over the set \(\mathbb{N}\) of nonnegative integers. The score of a codeword \(c = (c_j)_{j=1}^n \in \mathcal{C}_{alt}\) with respect to \(\mathcal{M}\) is defined by

\[
S_{\mathcal{M}}(c) = \sum_{j=1}^{n} m_{c_j,j} .
\]

• Example:

\[
\begin{pmatrix}
2 & 0 & 1 & 0 & 0 \\
1 & 1 & 4 & 1 & 1 \\
0 & 4 & 1 & 4 & 4 \\
4 & 1 & 0 & 1 & 1 \\
3 & 0 & 0 & 0 & 0
\end{pmatrix}, \quad c = (0, 1, 2, 3), \quad S_{\mathcal{M}}(c) = 8.
\]
Lemma 1

The next lemma is the basis of the list decoder in [KV00],[KV02].

**Lemma 1** [KV00] Let \( \ell \) and \( \beta \) be positive integers and \( \mathcal{M} \) be a \( q \times n \) matrix over \( \mathbb{N} \). Suppose there exists a nonzero bivariate polynomial \( Q(x, z) = \sum_{h,i} Q_{h,i} x^h z^i \) over \( \Phi \) that satisfies

(i) \( \deg_{0,1} Q(x, z) \leq \ell \) and \( \deg_{1,k-1} Q(x, z) < \beta \),

(ii) for all \( \gamma \in F, \ j \in [n] \) and \( 0 \leq s + t < m_{\gamma,j} \),

\[
\sum_{h,i} \binom{h}{s} \binom{i}{t} Q_{h,i} \alpha_j^{h-s} (\gamma/v_j)^{i-t} = 0.
\]

Then for every \( c = (v_j u(\alpha_j))_{j=1}^n \in \mathcal{C}_{alt} \),

\[
\mathcal{S}_\mathcal{M}(c) \geq \beta \quad \Rightarrow \quad (z - u(x)) | Q(x, z).
\]
Design Process of a List Decoder for $\mathcal{C}_{\text{alt}}$

Fix some metric $d : F^n \times F^n \rightarrow \mathbb{R}$ and $\ell$. Find an integer $\beta$ and a mapping $\mathcal{M} : F^n \rightarrow \mathbb{N}^{q \times n}$ such that for the largest possible integer $\tau$, the following two conditions hold for the matrix $\mathcal{M}(y)$ that corresponds to any received word $y$, whenever a codeword $c \in \mathcal{C}_{\text{alt}}$ satisfies $d(c, y) \leq \tau$:

(C1) $S_{\mathcal{M}(y)}(c) \geq \beta$.

(C2) There exists a nonzero $Q(x, z) = \sum_{h, i} Q_{h, i} x^h z^i$ over $\Phi$ that satisfies

(i) $\deg_{0,1} Q(x, z) \leq \ell$ and $\deg_{1,k-1} Q(x, z) < \beta$,

(ii) for all $\gamma \in F$, $j \in [n]$ and $0 \leq s + t < m_{\gamma,j}$,

$$\sum_{h, i} \binom{h}{s} \binom{i}{t} Q_{h, i} \alpha_{j}^{h-s} (\gamma/v_j)^{i-t} = 0.$$
The Mapping $\mathcal{M}_H(y)$

- Let $r$ and $\bar{r}$ be positive integers such that $0 \leq \bar{r} < r \leq \ell$.

- Define the mapping $y = (y_j)_{j \in [n]} \mapsto \mathcal{M}_H(y) = (m_{\gamma,j})_{\gamma \in F, j \in [n]}$, as

$$m_{\gamma,j} = \begin{cases} r & \text{if } y_j = \gamma, \\ \bar{r} & \text{otherwise} \end{cases}, \quad \gamma \in F, \quad j \in [n].$$

- Example: $F = GF(5), \ n = 4, \ y = (0100), \ r = 7, \ \bar{r} = 4$.

$$\mathcal{M}_H = \begin{pmatrix} 2 & 4 & 4 & 4 & 4 \\ 1 & 4 & 7 & 4 & 4 \\ 0 & 7 & 4 & 7 & 7 \\ 4 & 4 & 4 & 4 & 4 \\ 3 & 4 & 4 & 4 & 4 \end{pmatrix}.$$
A Decoder for the Hamming Metric

Until further notice, assume that \( d(\cdot, \cdot) \) is the Hamming metric.

**Proposition 2** For integers \( 0 \leq \bar{r} < r \leq \ell \), let \( \theta \) be the unique real such that

\[
R_\mathcal{H} = \frac{k-1}{n} = 1 - \frac{1}{(\ell+1)} \left( (r-\bar{r})(\ell+1)\theta + \left(\frac{\ell+1-r}{2}\right) + \left(\bar{r}+1\right)(q-1) \right).
\]

Given any positive integer \( \tau < n\theta \), conditions (C1) and (C2) are satisfied for

\[
\beta = r(n-\tau) + \bar{r}\tau
\]

and

\[
\mathcal{M} = \mathcal{M}_\mathcal{H}.
\]
Maximizing over $r$ and $\bar{r}$

- Instead of maximizing $\theta = \theta(R_H, \ell, r, \bar{r})$ over $r$ and $\bar{r}$, we find it easier to maximize $R_H = R_H(\theta, \ell, r, \bar{r})$ for a given $\theta$ (and $\ell$).

- For $0 \leq \theta \leq 1 - \frac{1}{\ell+1} \left\lceil \frac{\ell+1}{q} \right\rceil$, the maximizing values are:
  
  $$r = \ell+1 - \left\lceil (\ell+1)\theta \right\rceil \quad \text{and} \quad \bar{r} = \left\lceil (\ell+1)\theta/(q-1) \right\rceil - 1.$$

- The decoding radius, $\tau$, obtained in this case is exactly the one implied by a Johnson-type bound for the Hamming metric.

- As $\ell \to \infty$, the value $R_H(\theta, \ell) = \max_{r,\bar{r}} R_H(\theta, \ell, r, \bar{r})$ converges to the expression $1 - 2\theta + \frac{q}{q-1}\theta^2$ obtained in [KV00].
The Lee Metric

• Denote by $\mathbb{Z}_q$ the integers modulo $q$.

• The Lee weight of an element $a \in \mathbb{Z}_q$, denoted $|a|$, is defined as the smallest nonnegative integer $s$ such that $s \cdot 1 \in \{a, -a\}$.

• The Lee distance between two elements $a, b \in \mathbb{Z}_q$ is $|a - b|$.

• Example: $\mathbb{Z}_8$

![Diagram of a cycle with points labeled 0 to 7, illustrating the Lee metric concept.]
The Lee Metric for $F = \text{GF}(q)$

Let $F = \text{GF}(q)$.

- How do we extend the Lee metric to $F^n$?
- Fix a bijection $\langle \cdot \rangle : F \rightarrow \mathbb{Z}_q$.
- Define the Lee distance $d_L : F^n \times F^n \rightarrow \mathbb{N}$ between two words $(x_i)_{i \in [n]}$ and $(y_i)_{i \in [n]}$ (over $F$) as

$$d_L \triangleq \sum_{i=1}^{n} |\langle x_i \rangle - \langle y_i \rangle|.$$
The Mapping $\mathcal{M}_L(y)$

- Let $r$ and $\Delta$ be positive integers such that $0 < \Delta \leq r$.
- Define the mapping $y = (y_j)_{j \in [n]} \mapsto \mathcal{M}_L(y) = (m_{\gamma,j})_{\gamma \in F, j \in [n]}$, as
  \[
  m_{\gamma,j} = \max\{0, r - |(\langle y_j \rangle - \langle \gamma \rangle)| \Delta\}, \quad \gamma \in F, \quad j \in [n].
  \]
- Example: $F = \text{GF}(5)$, $\langle \cdot \rangle = \text{Identity}$, $n = 4$, $y = (0100)$, $r = 7$, $\Delta = 4$.

\[
\mathcal{M}_L = \begin{pmatrix}
2 & 0 & 3 & 0 & 0 \\
1 & 3 & 7 & 3 & 3 \\
0 & 7 & 3 & 7 & 7 \\
4 & 3 & 0 & 3 & 3 \\
3 & 0 & 0 & 0 & 0
\end{pmatrix}.
\]
- If $d_L(c, y) = \tau$ then $S_M(c) \geq rn - \tau \Delta$. 

\( R_L(\theta, \ell) \) for the Lee Metric

Define \( R_L(\theta, \ell) = \max_{r, \Delta} R_L(\theta, \ell, r, \Delta) \), where

\[
R_L(\theta, \ell, r, \Delta) = \frac{1}{(\ell+1)} \left( (\ell+1)(r-\theta\Delta) - \binom{r+1}{2}(2\Lambda+1) + (\Lambda+1) \Delta(1+2r-\frac{(2\Lambda+1)}{3}\Delta) + T \right),
\]

\( \Lambda = \min \{ \lfloor r/\Delta \rfloor, \lfloor q/2 \rfloor \} \),

and

\[
T = \begin{cases} 
  \binom{r-\Lambda\Delta+1}{2} & \text{if } \Lambda = q/2 \\
  0 & \text{otherwise}
\end{cases}
\]
\( R_{\mathcal{L}}(\theta, \ell) \) for the Lee Metric (Continued)

- For any fixed \( 0 < \Delta \leq \ell \), the maximum of \( R_{\mathcal{L}}(\theta, \ell, r, \Delta) \) over \( r \) is attained for
  
  \[
  r_\Delta = \begin{cases} 
  \lfloor (\ell + \Delta \lambda^2)/(2\lambda) \rfloor & \text{if } \lambda = q/2 \\
  \lfloor (\ell + \Delta(\lambda^2+\lambda))/(2\lambda+1) \rfloor & \text{otherwise}
  \end{cases},
  \]

  where
  
  \[
  \lambda = \min \left\{ \left\lfloor \sqrt{\ell/\Delta} \right\rfloor, \lfloor q/2 \rfloor \right\} .
  \]

- \( R_{\mathcal{L}}(\theta, \ell) \) is piecewise linear in \( \theta \), where the intervals correspond to the integer values of \( \Delta \in \{1, 2, \ldots, \ell\} \).
Asymptotic Analysis

Proposition 3 Define \( \chi_L(q) = \lfloor \frac{1}{4} q^2 \rfloor / q \). For \( 0 < \theta \leq \chi_L(q) \), denote by \( L \) the unique integer such that \( \frac{L^2 - 1}{3L} \leq \theta < \frac{L^2 + 2L}{3(L+1)} \), and let \( \lambda = \min\{L, \lfloor q/2 \rfloor \} \). Then,

\[
R_L(\theta, \infty) = \lim_{\ell \to \infty} R_L(\theta, \ell) = \begin{cases} 
\frac{1+2\lambda^2-6\lambda\theta+6\theta^2}{2\lambda+\lambda^3} & \text{if } \lambda = q/2 \\
\frac{\lambda+3\lambda^2+2\lambda^3-6\lambda\theta-6\lambda^2\theta+3\theta^2+6\lambda\theta^2}{\lambda+2\lambda^2+2\lambda^3+\lambda^4} & \text{otherwise}
\end{cases}
\]

• The decoding radius obtained in the asymptotic case (\( \ell \to \infty \)) is generally strictly larger than the one implied by a Johnson-type bound for the Lee metric.
Figure 1: Curve $\theta \mapsto R_L(\theta, \ell)$ and the Johnson bound for $q = 5$ and $\ell = 7, \infty$. 
Comparison to Previous Work

our decoder
Roth & Siegel
non-algorithmic

\( \tau \)

5 10 15 20 25