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 $\mathcal{C}$ be an (n, M, d) code over F.

- A list-ℓ decoder of decoding radius τ is a function $\mathcal{D} : F^n \to 2^{\mathcal{C}}$ such that
  - Each received word $\mathbf{y} \in F^n$ is mapped to a set (list) of codewords.
  - The list is guaranteed to contain all codewords in the sphere of radius τ centered at $\mathbf{y}$,

$$\mathcal{D}(\mathbf{y}) \supseteq \{\mathbf{c} \in \mathcal{C} : \mathsf{d}(\mathbf{c}, \mathbf{y}) \leq \tau\} .$$

  - The list is guaranteed to contain no more than ℓ codewords,

$$|\mathcal{D}(\mathbf{y})| \leq \ell .$$

- For a fixed ℓ, the bigger τ is, the better.

GRS and Alternant Codes

- Fix $F = \mathrm{GF}(q)$ and $\Phi = \mathrm{GF}(q^m)$.
- Denote by $\Phi_k[x]$ the set of all polynomials in the indeterminate x with degree less than k over Φ.
- Hereafter, fix $\mathcal{C}_{\mathrm{GRS}}$ as an $[n, k]$ GRS code over Φ 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

$$\mathcal{C}_{\mathrm{GRS}} = \{\mathbf{c} = (v_1 u(\alpha_1) \;\; v_2 u(\alpha_2) \;\; \ldots \;\; v_n u(\alpha_n)) \, : \, u(x) \in \Phi_k[x]\} \; .$$

- Fix $\mathcal{C}_{\mathrm{alt}}$ as the respective alternant code over F,

$$\mathcal{C}_{\mathrm{alt}} = \mathcal{C}_{\mathrm{GRS}} \cap F^n \; .$$

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 $\mathbf{c} = (c_j)_{j=1}^n \in \mathcal{C}_{\mathrm{alt}}$ with respect to $\mathcal{M}$ is defined by

$$\mathcal{S}_{\mathcal{M}}(\mathbf{c}) = \sum_{j=1}^{n} m_{c_j,j} \ .$$

- Example:

$$\mathcal{M} = \begin{matrix} 2 \\ 1 \\ 0 \\ 4 \\ 3 \end{matrix} \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 4 & 1 & 1 \\ 4 & 1 & 4 & 4 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \ , \quad \mathbf{c} = (0, 1, 2, 3) \ , \quad \mathcal{S}_{\mathcal{M}}(\mathbf{c}) = 8 \ .$$

Lemma 1

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

Lemma 1 [KV00] *Let* ℓ *and* β *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* Φ *that satisfies*

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

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

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

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

$$\mathcal{S}_{\mathcal{M}}(\mathbf{c}) \ge \beta \quad \Longrightarrow \quad (z - u(x)) \,|\, Q(x,z) \ .$$

Design Process of a List Decoder for $\mathcal{C}_{\text{alt}}$

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

(C1) $\mathcal{S}_{\mathcal{M}(\mathbf{y})}(\mathbf{c}) \ge \beta$.

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

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

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

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

The Mapping $\mathcal{M}_{\mathcal{H}}(\mathbf{y})$

- Let r and $\bar{r}$ be positive integers such that $0 \leq \bar{r} < r \leq \ell$.
- Define the mapping $\mathbf{y} = (y_j)_{j\in[n]} \mapsto \mathcal{M}_{\mathcal{H}}(\mathbf{y}) = (m_{\gamma,j})_{\gamma\in F, j\in[n]}$, 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: $F = \mathrm{GF}(5)$, $n = 4$, $\mathbf{y} = (0100)$, $r = 7$, $\bar{r} = 4$.

$$\mathcal{M}_{\mathcal{H}} = \begin{matrix} 2 \\ 1 \\ 0 \\ 4 \\ 3 \end{matrix} \begin{pmatrix} 4 & 4 & 4 & 4 \\ 4 & 7 & 4 & 4 \\ 7 & 4 & 7 & 7 \\ 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 \end{pmatrix} .$$

A Decoder for the Hamming Metric

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

Proposition 2 *For integers* $0 \le \bar{r} < r \le \ell$*, let* θ *be the unique real such that*

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

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 $\bar{r}$

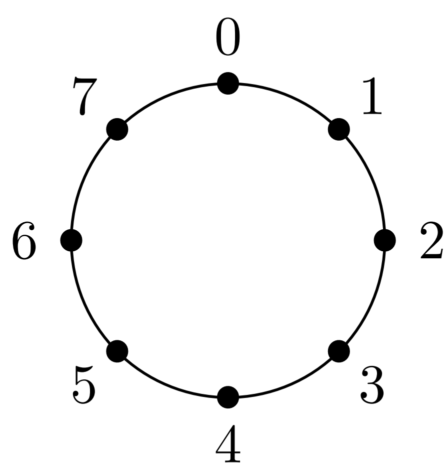
- Instead of maximizing $\theta = \theta(R_{\mathcal{H}}, \ell, r, \bar{r})$ over r and $\bar{r}$, we find it easier to maximize $R_{\mathcal{H}} = R_{\mathcal{H}}(\theta, \ell, r, \bar{r})$ for a given θ (and ℓ).
- For $0 \le \theta \le 1 - \frac{1}{\ell+1}\lceil \frac{\ell+1}{q} \rceil$, the maximizing values are:

$$r = \ell+1 - \lceil (\ell+1)\theta \rceil \qquad \text{and} \qquad \bar{r} = \lceil (\ell+1)\theta/(q-1) \rceil - 1 \ .$$

- The decoding radius, τ, obtained in this case is exactly the one implied by a Johnson-type bound for the Hamming metric.
- As $\ell \to \infty$, the value $R_{\mathcal{H}}(\theta, \ell) = \max_{r,\bar{r}} R_{\mathcal{H}}(\theta, \ell, r, \bar{r})$ 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: $\mathbb{Z}_8$



The Lee Metric for $F = \mathrm{GF}(q)$

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

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

$$\mathsf{d}_{\mathcal{L}} \triangleq \sum_{i=1}^{n} \left| \langle x_i \rangle - \langle y_i \rangle \right| \ .$$

The Mapping $\mathcal{M}_{\mathcal{L}}(\mathbf{y})$

- Let r and Δ be positive integers such that $0 < \Delta \le r$.
- Define the mapping $\mathbf{y} = (y_j)_{j \in [n]} \mapsto \mathcal{M}_{\mathcal{L}}(\mathbf{y}) = (m_{\gamma,j})_{\gamma \in F, j \in [n]}$, as

$$m_{\gamma,j} = \max\{0, r - |(\langle y_j \rangle - \langle \gamma \rangle)| \, \Delta\} \; , \quad \gamma \in F \; , \quad j \in [n] \; .$$

- Example: $F = \mathrm{GF}(5)$, $\langle \cdot \rangle = \text{Identity}$, $n = 4$, $\mathbf{y} = (0100)$, $r = 7$, $\Delta = 4$.

$$\mathcal{M}_{\mathcal{L}} = \begin{matrix} 2 \\ 1 \\ 0 \\ 4 \\ 3 \end{matrix} \begin{pmatrix} 0 & 3 & 0 & 0 \\ 3 & 7 & 3 & 3 \\ 7 & 3 & 7 & 7 \\ 3 & 0 & 3 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix} .$$

- If $\mathsf{d}_{\mathcal{L}}(\mathbf{c}, \mathbf{y}) = \tau$ then $\mathcal{S}_{\mathcal{M}}(\mathbf{c}) \ge rn - \tau\Delta$.

$R_{\mathcal{L}}(\theta, \ell)$ for the Lee Metric

Define $R_{\mathcal{L}}(\theta, \ell) = \max_{r,\Delta} R_{\mathcal{L}}(\theta, \ell, r, \Delta)$, where

$$R_{\mathcal{L}}(\theta, \ell, r, \Delta) =$$
$$\frac{1}{\binom{\ell+1}{2}} \left((\ell+1)(r-\theta\Delta) - \binom{r+1}{2}(2\Lambda+1) + \binom{\Lambda+1}{2}\Delta(1+2r-\frac{(2\Lambda+1)}{3}\Delta) + T \right),$$

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

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 $0 < \Delta \le \ell$, the maximum of $R_{\mathcal{L}}(\theta, \ell, r, \Delta)$ over r is attained for

$$r_\Delta = \begin{cases} \left\lfloor (\ell + \Delta\lambda^2)/(2\lambda) \right\rfloor & \text{if } \lambda = q/2 \\ \left\lfloor (\ell + \Delta(\lambda^2 + \lambda))/(2\lambda + 1) \right\rfloor & \text{otherwise} \end{cases} ,$$

  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 θ, where the intervals correspond to the integer values of $\Delta \in \{1, 2, \ldots, \ell\}$.

Asymptotic Analysis

Proposition 3 *Define* $\chi_{\mathcal{L}}(q) = \lfloor \frac{1}{4} q^2 \rfloor / q$. *For* $0 < \theta \leq \chi_{\mathcal{L}}(q)$, *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,*

$$R_{\mathcal{L}}(\theta, \infty) = \lim_{\ell \to \infty} R_{\mathcal{L}}(\theta, \ell) =$$

$$\begin{cases} \frac{1+2\lambda^2-6\lambda\theta+6\theta^2}{2\lambda+\lambda^3} & \textit{if } \lambda = q/2 \\ \frac{\lambda+3\lambda^2+2\lambda^3-6\lambda\theta-6\lambda^2\theta+3\theta^2+6\lambda\theta^2}{\lambda+2\lambda^2+2\lambda^3+\lambda^4} & \textit{otherwise} \end{cases}.$$

- 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.

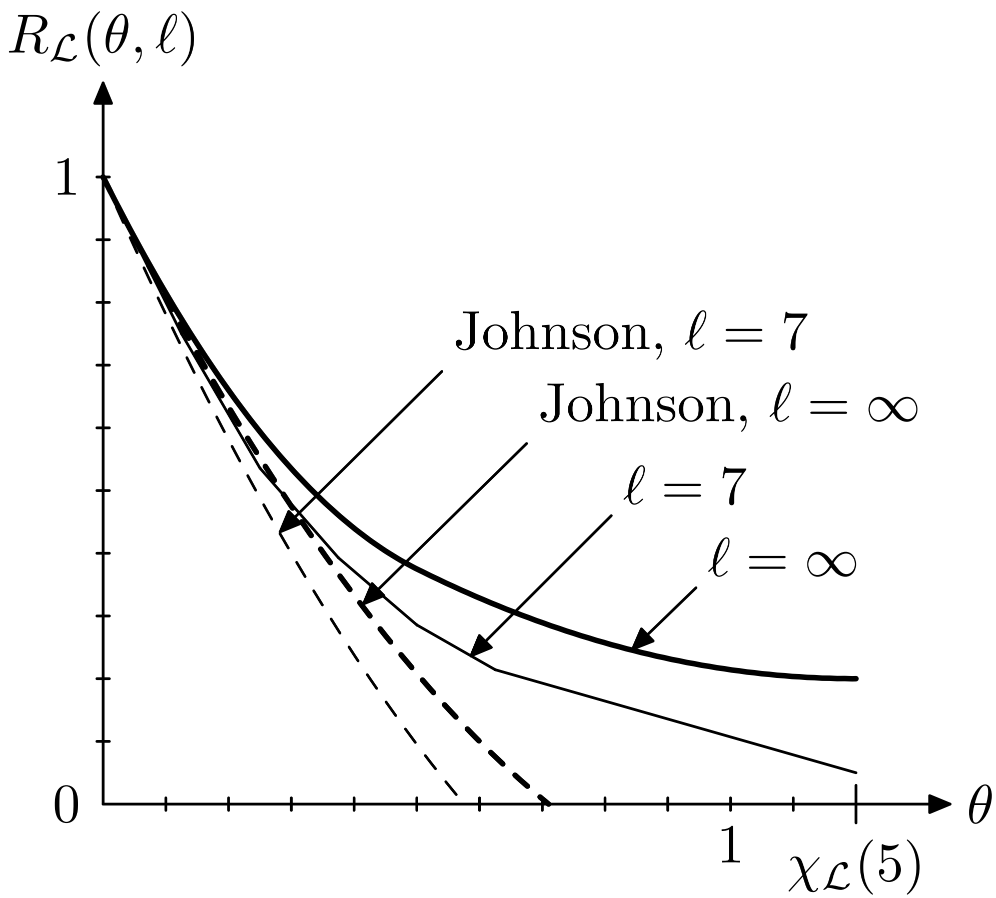


Figure 1: Curve $\theta \mapsto R_{\mathcal{L}}(\theta, \ell)$ and the Johnson bound for $q = 5$ and $\ell = 7, \infty$.

Comparison to Previous Work