On List Decoding of Alternant Codes in the Hamming and Lee Metrics[1]

Ido Tal Ron M. Roth
Computer Science Department,
Technion, Haifa 32000, Israel.
{idotal, ronny}@cs.technion.ac.il

I. Preliminaries

Let $F = \mathrm{GF}(q)$ and $\Phi = \mathrm{GF}(q^m)$ and consider the alternant code over F,

$$\mathcal{C}_{\mathrm{alt}} = \left\{ (v_j u(\alpha_j))_{j=1}^n \in F^n \,:\, u(x) \in \Phi[x],\ \deg u(x) < k \right\} ,$$

where α_j are distinct elements of Φ and $v_j \in \Phi \setminus \{0\}$ for every j in $[n] = \{1, 2, \ldots, n\}$.

The next lemma is the basis of the list decoder in [1],[2]. Let $\mathcal{M} = (\mathcal{M}_{\gamma,j})_{\gamma \in F, j \in [n]}$ 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 $\mathcal{S}_{\mathcal{M}}(\mathbf{c}) = \sum_{j=1}^n \mathcal{M}_{c_j,j}$.

Lemma 1 [1] *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 $Q(x,z) = \sum_{i=0}^{\ell} \sum_h Q_{h,i} x^h z^i$ over Φ that satisfies*

(i) $(k-1)i + h \geq \beta \quad \Longrightarrow \quad Q_{h,i} = 0$, *and—*

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

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

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

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

Fix some metric $\mathsf{d} : F^n \times F^n \to \mathbb{R}$. A list-$\ell$ decoder for $\mathcal{C}_{\mathrm{alt}}$ (with respect to $\mathsf{d}(\cdot,\cdot)$) can now be designed as follows. 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 $\mathbf{c} \in \mathcal{C}_{\mathrm{alt}}$ satisfies $\mathsf{d}(\mathbf{c}, \mathbf{y}) \leq \tau$:

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

(C2) (i) and (ii) are satisfied by some $Q(x,z) \neq 0$.

II. List decoder in the Hamming metric

Assume in this section that $\mathsf{d}(\cdot,\cdot)$ is the Hamming metric.

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

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

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

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

and

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

Instead of maximizing $\theta = \theta(R, \ell, r, \bar{r})$ over r and $\bar{r}$, we find it easier to maximize $R = R(\theta, \ell, r, \bar{r})$ for a given θ (and ℓ). For $0 \leq \theta \leq 1 - \frac{1}{\ell+1}\lceil \frac{\ell+1}{q} \rceil$, 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. Also, as $\ell \to \infty$, the value $R(\theta, \ell) = \max_{r,\bar{r}} R(\theta, \ell, r, \bar{r})$ converges to the expression $1 - 2\theta + \frac{q}{q-1}\theta^2$ obtained in [1].

III. List decoder in the Lee metric

For an element a in $\mathbb{Z}_q$ (the ring of integers modulo q), let $|a|$ be the Lee weight of a. We fix a bijection $\langle \cdot \rangle : F \to \mathbb{Z}_q$ and assume in this section that $\mathsf{d}((x_j),(y_j)) = \sum_{j=1}^n |\langle x_j \rangle - \langle y_j \rangle|$.

Proposition 3 *For integers $0 < \Delta \leq r \leq \ell$, let θ be the unique real such that*

$$\begin{aligned} R = \tfrac{k-1}{n} = \tfrac{1}{\binom{\ell+1}{2}} \Big(& (\ell+1)(r - \theta\Delta) - \tbinom{r+1}{2}(2\lambda+1) \\ & + \tbinom{\lambda+1}{2}\Delta(1 + 2r - \tfrac{(2\lambda+1)}{3}\Delta) + \tbinom{r-\lambda\Delta+1}{2}\delta \Big) , \end{aligned} \tag{1}$$

where $\lambda = \min\{\lfloor r/\Delta \rfloor, \lfloor q/2 \rfloor\}$, and $\delta=1$ if $\lambda=q/2$ and $\delta=0$ otherwise. Given any positive integer $\tau < n\theta$, conditions (C1) and (C2) are satisfied for

$$\beta = rn - \tau\Delta$$

and

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

For fixed $\Delta \in [\ell]$, the expression in (1) is maximized when $\lambda = \min\{\lfloor \sqrt{\ell/\Delta} \rfloor, \lfloor q/2 \rfloor\}$ and

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

We then maximize (1) over Δ to get the best $R = R(\theta, \ell)$.

Proposition 4 *For $0 < \theta \leq \lfloor \frac{1}{4}q^2 \rfloor / q$, let L be the largest integer such that $L \leq q/2$ and $L^2 \leq 3L\theta+1$. Then,*

$$\lim_{\ell \to \infty} R(\theta, \ell) = \begin{cases} \frac{1+2L^2-6L\theta+6\theta^2}{2L+L^3} & \text{if } L = \frac{q}{2} \\ \frac{L+3L^2+2L^3-6L\theta(1+L-\theta)+3\theta^2}{L+2L^2+2L^3+L^4} & \text{if } L < \frac{q}{2} \end{cases} .$$

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.

References

[1] R. Koetter, A. Vardy, *Algebraic soft-decision decoding of Reed-Solomon codes*, preprint, 2000.

[2] R. Koetter, A. Vardy, *Decoding of Reed-Solomon codes for additive cost functions, Proc. Int'l Symp. Inform. Theory (ISIT'2002)*, Lausanne, Switzerland (July 2002), p. 313.

[1] This work was supported by Grant No. 94/99 from the Israel Science Foundation.