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

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

I. Preliminaries

Let $F = GF(q)$ and $\Phi = GF(q^m)$ and consider the alternant code over $F$, $C_{alt} = \{(v_j u(\alpha_j))_{j=1}^n \in F^n : u(x) \in \Phi[x], \deg u(x) < k\}$, where $\alpha_j$ are distinct elements of $\Phi$ 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 $M = (M_{i,j})_{j \in F, j \in \mathbb{N}}$ be a $q \times n$ matrix over the set $\mathbb{N}$ of nonnegative integers. The score of a codeword $c = (c_j)_{j=1}^n \in C_{alt}$ with respect to $M$ is defined by $S_M(c) = \sum_{j=1}^n M_{i,j}c_j$.

Lemma 1 [1] Let $\ell$ and $\beta$ be positive integers and $M$ be a $q \times n$ matrix over $\mathbb{N}$. Suppose there exists a nonzero bivariate polynomial $Q(x,z) = \sum_{i=0}^\ell \sum_{b} Q_{b,i} x^b z^i$ over $\Phi$ that satisfies

(i) $(k-1)i + h \geq \beta \implies Q_{h,i} = 0$, and—
(ii) for all $\gamma \in F$, $j \in [n], 0 \leq s + t < M_{i,j}$,

$$\sum_{h,i} (\gamma) (Q_{h,i} a_{\gamma,i})^{s+t} = 0.$$ Then for every $c = (v_j u(\alpha_j))_{j=1}^n \in C_{alt}$,

$$S_M(c) \geq \beta \implies (z - u(x)) | Q(x,z).$$

Fix some metric $d : F^n \times F^n \rightarrow R$. A list-$\ell$ decoder for $C_{alt}$ (with respect to $d(\cdot, \cdot)$) can now be designed as follows. Find an integer $\beta$ and a mapping $M : F^n \rightarrow \mathbb{N}^{\times n}$ such that for the largest possible integer $\tau$, the following two conditions hold for the matrix $M(y)$ that corresponds to any received word $y$; whenever a codeword $c \in C_{alt}$ satisfies $d(c, y) \leq \tau$:

(C1) $S_M(y) \geq \beta$.

(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 $d(\cdot, \cdot)$ is the Hamming metric.

Proposition 2 For integers $0 \leq r < \ell \leq \ell$, let $\theta$ be the unique real such that

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

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

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

and

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

Instead of maximizing $\theta = \theta(R, \ell, r, \hat{r})$ over $r$ and $\hat{r}$, we find it easier to maximize $R = R(\theta, \ell, r, \hat{r})$ for a given $\theta$ and $\ell$. For $0 \leq \theta \leq 1 - \frac{1}{n\binom{n}{2}^{[\frac{\ell+1}{2}]}}$, the maximizing values are:

$$r = \ell+1 - [(\ell+1)\theta] \quad \text{and} \quad \hat{r} = [(\ell+1)(\theta(q-1))-1].$$ The decoding radius, $\tau$, obtained in this section is exactly the one implied by a Johnson-type bound for the Hamming metric. Also, as $\ell \rightarrow \infty$, the value $R(\theta, \ell, r, \hat{r})$ converges to the expression $1 - 2\delta + \frac{1}{q-1}\delta^2$ obtained in [1].

III. List decoder in the Lee metric

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

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

$$R = \frac{k-1}{n} = \frac{1}{\binom{n}{2}} \left( ((r-\ell)(\ell+1)\theta - (\ell+1)\delta (2\lambda+1) + (\lambda^2+1)\Delta (1+2\delta - 2(\lambda^2+1)\Delta) - (\ell+1)(\theta(q-1)-1) \right),$$

where $\lambda = \min \{|r|/\Delta, |q/2|\}$, 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

$$\beta = rn - r\Delta$$

and

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

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

$$r = \frac{\left( (\ell+1)(\theta(2\lambda+1)) - (\ell+1)(\theta(2\lambda+1)-1) \right)}{\lambda^2+1}$$

if $\lambda = q/2$.

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

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

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

The decoding radius obtained in the asymptotic case ($\ell \rightarrow \infty$) is generally strictly larger than the one implied by a Johnson-type bound for the Lee metric.

References
