Solutions 7

1. For each polynomial $Q(x,y) \in \mathbb{F}[x,y]$, let

$$\deg^*(Q(x,y)) := \max\{i + (k-1)j : x^i y^j \text{ has nonzero coefficient in } Q\}.$$

Clearly, if $p(x) \in \mathbb{F}[x]$ is a polynomial of degree $\deg(p(x)) < k$, then

$$\deg(Q(x,p(x))) \leq \deg^*(Q(x,y)).$$

We need to find a polynomial $Q(x,y)$ such that

1. $\deg^*(Q(x,y)) < t := \sqrt{2nk}$, and
2. $Q(x_i,y_i) = 0$ for all $i = 1,\ldots,n$ (the input of the algorithm).

If $p(x)$ is a polynomial such that $p(x_i) = y_i$ for at least t different values of i, then clearly $Q(x,y)$ is divisible by $y - p(x)$. This is true because if $r(x)$ and $q(x,y)$ denote the remainder and the quotient of the division of $Q(x,y)$ by the polynomial $y - p(x)$ with respect to the variable y, then

$$Q(x,y) = (y - p(x))q(x,y) + r(x),$$

hence $r(x) = Q(x,p(x))$, which implies that $\deg(r(x)) < t$. We then must have $r(x) \equiv 0$, since there are at least t different values of i for which $r(x_i) = 0$. Hence $Q(x,y)$ is divisible by $y - p(x)$.

Thus, in order to find the polynomials $p(x)$ satisfying $p(x_i) = y_i$ for at least t different values of i, it suffices to factorize the polynomial $Q(x,y)$ into factors of the form $y - p(x)$.

The linear space of all polynomials $Q(x,y)$ satisfying $\deg^*(Q(x,y)) < t$ has dimension

$$\sum_{j=0}^{\lfloor \frac{t-1}{k-1} \rfloor} t - (k-1)j \simeq \frac{t^2}{2k} = n,$$

hence clearly there is one such polynomial such that $Q(x_i,y_i) = 0$ for all $i = 1,\ldots,n$. Moreover, the size of the list will be bounded by the degree of y in $Q(x,y)$ which is at most $\sqrt{2n/k}$, finishing the proof.

Bitte wenden!

2. If we replace the RHS by $\frac{1}{\delta^5}$, the number of codewords in the ball of radius $\delta = \epsilon/m$ is bounded by $\frac{1}{\delta^5} = \left(\frac{m}{\epsilon}\right)^5$. If we redo the calculations in page TE4, we obtain

$$\begin{aligned}\mathbb{P}[x \in B] \leq \epsilon &\iff |G(S,T)| \cdot \left(\frac{m}{\epsilon}\right)^5 \cdot 2^{-k} \leq \epsilon \\ &\iff 2^{m \cdot 2^a + \log m + 2} \cdot 2^{5 \log \frac{m}{\epsilon}} \cdot 2^{-k} \leq \epsilon.\end{aligned}$$

If we choose $a = \log \frac{k}{2m}$, we obtain

$$2^{\frac{k}{2} + 6\log m + 2 - 5\log\epsilon - k} \leq 2^{\log \epsilon} \iff 2^{-\frac{k}{2} + 6\log m + 2 - 6\log\epsilon} \leq 1$$

Next, we choose $m < \frac{k}{2}$, so $\frac{k}{4} > \frac{m}{2} > 6\log m + 2$, for $m \geq 256$. Thus, we just need that

$$-\frac{k}{4} < 6\log\epsilon \iff \epsilon > 2^{-k/24},$$

and all the remaining calculations go through.

3. For each pair $m_1, m_2 \in \{1, \ldots, N\}$ of distinct elements, since Enc_1 has relative minimal distance δ_1, then there exists at least $\delta_1 n_1$ different values for $j \in \{1, \ldots, n_1\}$ such that

$$\text{Enc}_1(m_1)_j \neq \text{Enc}_1(m_2)_j.$$

For each such j, since Enc_2 has relative minimal distance δ_2, there exists at least $\delta_2 n_2$ different values for k such that

$$\text{Enc}_2(\text{Enc}_1(m_1)_j)_k \neq \text{Enc}_2(\text{Enc}_1(m_2)_j)_k. \tag{1}$$

In total, there are at least $(\delta_1 n_1) \cdot (\delta_2 n_2) = \delta_1\delta_2 n_1 n_2$ different pairs j, k such that (1) holds. Hence the Hamming distance between $\text{Enc}(m_1)$ and $\text{Enc}(m_2)$ is at least $\delta_1\delta_2 n_1 n_2$, thereby proving that Enc has relative minimal distance of at least $\delta_1\delta_2$.