Solutions 5

1. Given a fixed codeword $w \in \mathrm{Im}(C) \subseteq \mathbb{F}_q^n$, let $B_t(w) \subseteq \mathbb{F}_q^n$ be the set of messages having Hamming distance at most t from w (the *Hamming ball* of radius t centered at w). We have

$$|B_t(w)| = \sum_{k=0}^{t} \binom{n}{k} (q-1)^k.$$

Note that the size of the Hamming ball does not depend on the center w, We claim that $|B_t(w)| \geq q^t$. To see this, look at the set $S_t(w)$ of all codewords $w' \in \mathcal{F}_q^n$ which agree with w on the last $n-t$ coordinates. More formally, let $S_t(w) = \{w' \in \mathbb{F}_q : w'_i = w_i \text{ for all } i > t\}$. Clearly $|S_t(w)| = q^t$ and $S_t(w) \subseteq B_t(w)$, hence $|B_t(w)| \geq q^t$. If the minimal distance of $\mathrm{Im}(C)$ is d, then the balls $B_t(w)$ for $w \in \mathrm{Im}(C)$ must be pairwise disjoint, where $t = \lfloor \frac{d}{2} \rfloor$. In particular

$$q^{t+k} = q^t \cdot |\mathbb{F}_q^k| \leq \sum_{w \in \mathrm{Im}(C)} |B_t(w)| \leq |\mathbb{F}_q^n| = q^n.$$

This implies that $t \leq n-k$, hence the minimal distance d is at most $2t+1 \leq 2(n-k)+1$.

There is another argument that yields a better bound of $d \leq n-k+1$. We begin with $|\mathrm{Im}(C)| = q^k$ codewords. By the pigeonhole principle, there exists a subset $X_1 \subseteq \mathrm{Im}(C)$ of size at least $|X_1| \geq q^{k-1}$ for which all the codewords from X_1 agree on the first coordinate. Using the same principle again, we can find a subset $X_2 \subseteq X_1$ of size at least q^{k-2} such that all the codewords in X_2 agree on the first two coordinates. Repeating this process $k-1$ times, we obtain a set X_{k-1} of size at least q, such that all the codewords in X_{k-1} agree on the first $k-1$ coordinates. Hence the minimal distance of C is at most $n-k+1$.

2. (i) Let $e \in \mathbb{R}^n$ be any vector. We claim that all coordinates of $H \cdot e$ are less than $||e||_1$ in absolute value. More formally,

$$||H \cdot e||_\infty \leq ||e||_1. \tag{1}$$

The claims is true, because for every $w \in \{-1, 1\}^n$, we have

$$|e \cdot w| = \left| \sum_{i=1}^{n} e_i w_i \right| = \left| \sum_{i=1}^{n} e_i w_i \right| \leq \sum_{i=1}^{n} |e_i w_i| = \sum_{i=1}^{n} |e_i| = ||e||_1.$$

Bitte wenden!

Let $\widetilde{h}$ be the vector obtained from the original codeword h by replacing 0's with -1's. This vector $\widetilde{h}$ is the actual row from which h was obtained. We know that exactly one coordinate of $H \cdot \widetilde{h}$ is n, and all the remaining others are zero. The index of the nonzero coordinate in x is the same as the index of the row $\widetilde{h}$ in H, and we denote it by j. Since the code h was transmitted, with less than $\frac{n}{4}$ errors, we have

$$||\widetilde{y} - \widetilde{h}||_1 < 2 \cdot \frac{n}{4} = \frac{n}{2}. \tag{2}$$

Let $x = H \cdot \widetilde{y}$, and let $e = \widetilde{y} - \widetilde{h}$. We have

$$x = H \cdot \widetilde{y} = H \cdot (\widetilde{h} + e) = H \cdot \widetilde{h} + H \cdot e,$$

and by (1) and (2), we have

$$||x - H \cdot \widetilde{h}||_\infty = ||H \cdot e||_\infty \leq ||e||_1 < \frac{n}{2}.$$

This implies that $|x_j - n| < \frac{n}{2}$, hence $x_j > \frac{n}{2}$. On the other hand, for every $i \neq j$, we have $|x_i - 0| < \frac{n}{2}$, hence $x_i < \frac{n}{2}$. Thus the largest coordinate of x indicates what was the original codeword h.

(ii) We remark that the matrix in the statement of the exercise can also be described as

$$M = \begin{pmatrix} H \\ -H \end{pmatrix} = \Big((-1)^{\langle x,y \rangle}\Big)_{x \in \{0,1\}^{m+1}, y \in \{1\} \times \{0,1\}^m},$$

where $\langle x, y \rangle$ denotes the inner product of x and y, while the $2n \times 2n$-Hadamard matrix can be written as

$$M' = \begin{pmatrix} H & H \\ H & -H \end{pmatrix} = \Big((-1)^{\langle x,y \rangle}\Big)_{x,y \in \{0,1\}^{m+1}}.$$

The process of decoding for this punctuated Hadamard code, is slightly different. For each received message y, let $\widetilde{y}$ be vector obtained from y by replacing 0's with -1's. To find the original codeword h from the faulty message y, we look at the coordinate of $H \cdot \widetilde{y}$ having highest absolute value, say, coordinate j. If that particular coordinate is positive, the codeword h corresponds to the j^{th} row of H. But if the coordinate is negative, then the codeword h corresponds to the j^{th} row of $-H$.

3. If $S_1, \ldots, S_m \subseteq [d]$ is a (m, d, l, a)-design, then for every $1 \leq i \leq m$, we have

$$\sum_{j=1}^{i-1} 2^{|S_i \cap S_j|} \leq \sum_{j<i} 2^a = 2^a(i-1) \leq 2^a(m-1).$$

The above inequality proves that $S_1, \ldots, S_m$ is also a weak (m, d, l, a)-design.

Siehe nächstes Blatt!

4. Let $\alpha = \mathbb{P}_y[A(y, P(y_{|S_1}) \cdots P(y_{|S_{i-1}}) = P(y_{|S_i})]$. By an averaging argument, there is a choice $\widetilde{y}$ for the bits of y outside the set S_i such that

$$\mathbb{P}_{y'}[A(y', P(y'_{|S_1}) \cdots P(y'_{|S_{i-1}}) = P(y'_{|S_i})] \geq \alpha,$$

where in the above probability, $y' \in \{0,1\}^d$ is taken uniformly among all vectors agreeing with $\widetilde{y}$ on the coordinates outside of S_i.

Renaming $y'_{|S_i}$ as x, we observe that x varies uniformly over $\{0,1\}^l$, while $P(y_{|S_j})$ for $j \neq i$ is now a function P_j of x, that depends only on $|S_i \cap S_j|$ bits of x. So, we have

$$\mathbb{P}_x[A(y(x), P_1(x) \cdots P_{i-1}(x)) = P(x)] \geq \alpha.$$

Therefore, it suffices to let $\mathcal{F}_i$ to be the set of all functions f of the form $x \mapsto (y(x), P_1(x) \cdots P_{i-1}(x))$, where $P_j(x)$ depends only on a set T_{ij} of input bits of x, where $|T_{ij}| = |S_i \cap S_j|$. The number of such functions P_j is $2^|T_ij| = 2^{|S_i \cap S_j|}$. Also, $y(x)$ is a function that places x in the positions indexed by S_i and fixes all the other $d - l$ positions according to $\widetilde{y}$. The total number of choices for $y(x)$ is exactly 2^{d-l}. Hence the size of $\mathcal{F}_i$ can be bounded by

$$\log |\mathcal{F}_i| \leq d - l + \sum_{j=1}^{i=1} 2^{|S_i \cap S_j|},$$

finishing the proof.