NTIN100 Intro to Info Transmission and Processing summer 2020/2021

4th homework assignment - Error correcting codes II

turn in by June 7, 2021.

Problem 1. Consider a code over the alphabet {-1,1}. For two vectors $u, v \in \{-1,1\}^n$, what is the relationship between the Hamming distance of u and v and the inner product $\langle u, v \rangle = \Sigma_{i=1}^n u_i \cdot v_i$? Show, that if $v_1, v_2, \ldots, v_k \in \mathbb{R}^n$ and $0 < \alpha$ are such that $\langle v_i, v_i \rangle = 1$ a $\langle v_i, v_j \rangle \leq -\alpha$ for all $i \neq j$, then $k \leq 1 + \frac{1}{\alpha}$. Conclude that a binary code with the relative minimum distance $\delta = \frac{1}{2} + \epsilon$ has at most $\frac{1}{2\epsilon} + 1$ codewords. (*Hint:* Take a look at $\langle z, z \rangle$, where $z = \sum_{i=1}^k v_i$.)

Problem 2. Consider a $(n, k, d)_q$ code.

a) What type of code do we get if we remove a given position from all the codewords.

b) What type of code do we get if we pick a position in the codewords, choose a symbol which appears most often in that position, remove all codewords which have a different symbol in that position, and remove the position from all the remaining codewords.

Problem 3. Consider an undirected graph $G = (V, E)$ with m vertices and n edges. Each subset of the edges of G can be represented by a vector $\{0,1\}^n$, where each coordinate corresponds to an edge of G and indicates whether the edge is present in the subset. Define a code $C_{\text{cut}} \subseteq \{0,1\}^n$ of vectors that represent cuts in G, that is subsets of edges $F \subseteq E$ such that for some subset $S \subseteq V$, $F = \{\{u, v\} \in E,\ u \in S\ \&\ v \notin S\}$.

a) Show that C_{cut} is a linear code.

b) Show that if we can efficiently find for each $x \in \{0,1\}^n$ the closest codeword from C_{cut}, then we can efficiently find the largest cut in G. Finding the largest cut in G is so called MAX-CUT problem that is known to be NP-complete.

Problem 4. *How to share a secret.* Consider n clerks in a bank. We want to divide a secret code (number) among them so that any group of k of them can recover the secret but no group of $k-1$ or less of them has any information about the code (that is based on their information the code could still be arbitrary). Construct such a scheme. (You can think of the scheme as a function $f : \{1, \ldots, N\} \times \{1, \ldots, R\} \to \{1, \ldots, N\}^n$ where each subset of k coordinates in $f(x, r)$ determines x, but for any setting of $k-1$ coordinates of $f(x, r)$, x can be arbitrary. Here x represents the secret code and r is a parameter that will be chosen at random and kept secret.) What is the connection of such a scheme to error correcting codes?