

Cryptography Assignment 7

1. Create a secret sharing scheme for the following situation: There are two groups of six people each.
 - If three members of each group get together (for a total of six) they can determine the secret.
 - If four members of any one group gets together they can learn the secret.
 - No smaller groups can gain any information about the secret.
2. Show that the Hamming distance $d(u, v)$ on strings, where $d(u, v)$ is the number of characters where u and v differ is a metric, i.e.
 - (a) $d(u, v) = 0$ if and only if $u = v$,
 - (b) $d(u, v) = d(v, u)$ and
 - (c) $d(u, v) \leq d(u, w) + d(w, v)$
3. Let u and v be vectors over F_q (finite field on q elements with q prime). Show that, for vectors u and v , the weight of $u + v$ is at most the sum of the weight of u and the weight of v . Recall the weight of u is the number of non-zero coordinates of u .
4. Consider the hats problem we talked about in class.

Three players enter a room and a red or blue hat is placed on each person's head. The color of each hat is determined by a coin toss, with the outcome of one coin toss having no effect on the others. Each person can see the other players' hats but not his own.

No communication of any sort is allowed, except for an initial strategy session before the game begins. Once they have had a chance to look at the other hats, the players must simultaneously guess the color of their own hats or pass. The group shares a hypothetical \$3 million prize if at least one player guesses correctly and no players guess incorrectly. What is their best strategy?

- (a) Consider the strategy we discussed in class. Show that the set of hats where the strategy fails forms a perfect code with $n = 3$, $t = 1$, $d = 3$ and $q = 2$.
- (b) Suppose we had a perfect code for larger n with $t = 1$, $d = 3$ and $q = 2$. Show how to use the code to create a scheme that does well for the hats problem with n players. What is the probability of success?
- (c) Find a perfect code to use for $n = 7$.
- (d) Show that you can't do better for a specific n than to use the perfect code if there is one.