

Written Problems: Do four of the following problems.

1. *The hat problem.* A team of 7 contestants enters a room. A red or blue hat is randomly put on each contestant; each contestant can see the hats of everyone else but *not* his or her own. Each contestant then (simultaneously) guesses the color of his or her hat, or passes. The team wins if at least one contestant guesses correctly, and no one guesses incorrectly.
Describe a good strategy for the team to use, if no communication can occur once the team enters the room. What is the best probability of success that a strategy can achieve?
2. A soccer betting form contains a list of 13 matches. Next to each listed match there are three fill-in boxes which correspond to the following three possible guesses: “first team wins”, “second team wins”, or “tied match”. The bettor checks one box for each match.
Describe a strategy for filling out the *smallest* number of forms so that at least one of the forms contains at least 12 correct guesses. How many forms need to be filled out under this strategy?
3. Let $F = \mathbb{F}_q$ and let n be a prime such that $\gcd(n, q) = 1$. Denote by e the multiplicative order of q in \mathbb{F}_n .
 - (a) Show that there exists a perfect linear $[n, k]$ code over \mathbb{F}_q only if e divides $n - k$.
 - (b) Find all the values of k that satisfy the necessary condition of part (a) in the following cases:
 $q = 2, n = 23$; and $q = 3, n = 11$.
4. *Doubly-extended GRS codes.* Let C be a linear $[n, k = n - r, d]$ code over \mathbb{F}_q defined by a parity-check matrix

$$H = \begin{bmatrix} 1 & 1 & \cdots & 1 & 0 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_{n-1} & 0 \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_{n-1}^2 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \alpha_1^{r-2} & \alpha_2^{r-2} & \cdots & \alpha_{n-1}^{r-2} & 0 \\ \alpha_1^{r-1} & \alpha_2^{r-1} & \cdots & \alpha_{n-1}^{r-1} & 1 \end{bmatrix} \begin{bmatrix} v_1 & & & & 0 \\ & v_2 & & & \\ & & \ddots & & \\ & & & \ddots & \\ 0 & & & & v_n \end{bmatrix},$$

where $\alpha_1, \alpha_2, \dots, \alpha_{n-1}$ are distinct elements of \mathbb{F}_q and v_1, \dots, v_n are nonzero elements of \mathbb{F}_q .

- (a) Show that C is MDS (maximum distance separable).
 - (b) Assuming that $k < n$, show that the dual code C^\perp is an $[n, n - k]$ doubly-extended GRS code that can be defined through the same code locators as C .
5. Let H be a canonical parity-check matrix of an $[n, k, d]$ GRS code over \mathbb{F}_q where $0 < k \leq n - 2$. Given a word $e \in \mathbb{F}_q^n$, denote by $(S_0, S_1, \dots, S_{d-2})^T$ its syndrome with respect to H .
 - (a) Let e be a nonzero word in \mathbb{F}_q^n of weight t . Show that the longest run of 0s in the sequence S_0, S_1, \dots, S_{d-2} has length less than t ; that is, for every i in the range $0 \leq i < d - t$ there is a j in the range $i \leq j < i + t$ such that $S_j \neq 0$.
 - (b) Show that the bound in part (a) is tight in the following sense: for every t in the range $0 < t \leq d$ and every i in the range $0 \leq i \leq d - t$, there is a word $e \in \mathbb{F}_q^n$ of weight t whose syndrome satisfies $S_j = 0$ for $i \leq j < i + t - 1$ (in fact, for every subset $J \subseteq [n]$ of size t , there is such a word whose support is J).
 - (c) Express the syndrome entries of a word of weight 1 in terms of S_0 and S_1 only.