

1. [5 points] An  $(n, k)$  binary block code is used to transmit  $k$ -bit messages over a binary symmetric channel with crossover probability  $p < \frac{1}{2}$ . All the  $k$ -bit messages are equally likely. Show that the minimum distance decoder maximizes the probability of correct decision.
2. [5 points] Prove that for a binary block code with minimum distance  $d_{min}$ , the minimum distance decoder can correct upto  $\lfloor \frac{d_{min}-1}{2} \rfloor$  errors.
3. [5 points] Let  $p$  be a prime number. Prove that the set  $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$  is a field under integer addition and multiplication modulo  $p$ . Give an example to show that  $\mathbb{F}_p$  is not a field if  $p$  is composite.
4. [5 points] Let  $S$  be a nonempty subset of a vector space  $V$  over a field  $F$ . Prove that  $S$  is a subspace of  $V$  if
  - For any  $\mathbf{u}, \mathbf{v} \in S$ ,  $\mathbf{u} + \mathbf{v}$  also belongs to  $S$ .
  - For any  $a \in F$  and  $\mathbf{u} \in S$ ,  $a \cdot \mathbf{u}$  is also in  $S$ .