Solutions 4

Exercise 4.1.

1. We first show that any pair of columns of H is linearly independent. Note that a linear dependency $ac_1 + bc_2 = 0$ for any two columns c_1 and c_2 would imply $a = b$, since the columns are all of the form $(1, *, *)^\top$. It is thus enough to check that the sum of any two columns cannot be zero. This is clearly the case if one of the two columns is either the first column of the second column. If the two columns are of the form $(1, \alpha, *)^\top$ and $(1, \alpha^2, *)^\top$, then their independence is clear too, since projection onto the first two coordinates gives two independent vectors. Otherwise, projection onto the last two coordinates gives two independent vectors.

   On the other hand,
   $$\alpha \begin{pmatrix} 1 \\ \alpha \\ 1 \end{pmatrix} + \alpha^2 \begin{pmatrix} 1 \\ \alpha \\ \alpha \end{pmatrix} + 1 \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$
   is a linear dependency among three columns. In other words, the weight-3 word $(00\alpha\alpha^2 1000)$ belongs to the code.

2. The weight distribution of this code involves only the nonnegative parameters A_0, A_3, A_4, A_5, A_6, A_7 and A_8. The objective function we want to maximize is
   $$A_0 + A_3 + A_4 + A_5 + A_6 + A_7 + A_8.$$
   Recall the definition of the Krawtchouk polynomials
   $$K_k(x) := \sum_{j=0}^{k} (-1)^j \binom{x}{j} \binom{n-x}{k-j} (q-1)^{k-j}.$$
   Thus
   $$\begin{aligned} K_0(x) &= 1 \\ K_1(x) &= 3(8-x) - x = -4x + 24 \\ K_2(x) &= 9\binom{8-x}{2} - 3x(8-x) + \binom{x}{2} = 8x^2 - 92x + 252, \end{aligned}$$
   and the corresponding linear constraints are
   $$\begin{aligned} A_0 + A_3 + A_4 + A_5 + A_6 + A_7 + A_8 &\geq 0 \\ 24\,A_0 + 12\,A_3 + 8\,A_4 + 4\,A_5 - 4\,A_7 - 8\,A_8 &\geq 0 \\ 252\,A_0 + 48\,A_3 + 12\,A_4 - 8\,A_5 - 12\,A_6 + 28\,A_8 &\geq 0. \end{aligned}$$
   The full linear program is
   $$\max A_0 + A_3 + A_4 + A_5 + A_6 + A_7 + A_8 \text{ subject to}$$

$$\begin{aligned}
A_0 + A_3 + A_4 + A_5 + A_6 + A_7 + A_8 &\geq 0\\
24\,A_0 + 12\,A_3 + 8\,A_4 + 4\,A_5 - 4\,A_7 - 8\,A_8 &\geq 0\\
252\,A_0 + 48\,A_3 + 12\,A_4 - 8\,A_5 - 12\,A_6 + 28\,A_8 &\geq 0\\
1512\,A_0 + 44\,A_3 - 40\,A_4 - 28\,A_5 + 16\,A_6 + 28\,A_7 - 56\,A_8 &\geq 0\\
5670\,A_0 - 150\,A_3 - 74\,A_4 + 50\,A_5 + 30\,A_6 - 70\,A_7 + 70\,A_8 &\geq 0\\
13608\,A_0 - 252\,A_3 + 120\,A_4 + 44\,A_5 - 96\,A_6 + 84\,A_7 - 56\,A_8 &\geq 0\\
20412\,A_0 + 216\,A_3 + 108\,A_4 - 144\,A_5 + 100\,A_6 - 56\,A_7 + 28\,A_8 &\geq 0\\
17496\,A_0 + 324\,A_3 - 216\,A_4 + 108\,A_5 - 48\,A_6 + 20\,A_7 - 8\,A_8 &\geq 0\\
6561A_0 - 243A_3 + 81A_4 - 27A_5 + 9A_6 - 3A_7 + A_8 &\geq 0\\
A_0, A_3, A_4, A_5, A_6, A_7, A_8 &\geq 0
\end{aligned}$$

The linear program gives a solution

$$A_0 = 1, A_3 = 72, A_4 = 210, A_5 = 432, A_6 = 792, A_7 = \frac{4152}{7}, A_8 = \frac{1683}{7}.$$

The sum of these values is $16384/7$, so that $A_4(8,3) \leq \lfloor \log_4(16384/7) \rfloor = 5$, which shows the optimality of the code.

The following code works under Magma and is the implementation of the previous program. It shows that a quaternary linear code of length 8 and minimal distance 3 has dimension $k \leq 5.597$, i.e. $k \leq 5$.

```
clear;

n:=8;
q:=4;
F4<omega>:=FiniteField(q);
RR:=RealField();
Liste_Pol:=[KrawchoukPolynomial(F4,n,k) : k in [0..n]];
LP:=LPProcess(RR, n+1);

Obj:=Matrix(RR,[[1: i in [0..n]]]);
SetObjectiveFunction(LP, Obj);
SetMaximiseFunction(LP, true);

Contrleft:=Matrix(RR,[[Evaluate(p,i) : i in [0..n]] : p in Liste_Pol]);
Contrright:=Matrix(RR,[[0] : i in [0..n]]);
AddConstraints(LP, Contrleft, Contrright : Rel := "ge");

Zeros:=Matrix(RR,[[0 : i in [0..n] ] ]);
V0:=Zeros; V0[1,1]:=1;
AddConstraints(LP, V0, Matrix(RR,[[1]]));
V1:=Zeros; V1[1,2]:=1;
AddConstraints(LP, V1, Matrix(RR,[[0]]));
V2:=Zeros; V2[1,3]:=1;
```

```
AddConstraints(LP, V2, Matrix(RR,[[0]]));
for i in [3..n] do
   Vi:=Zeros; Vi[1,i+1]:=1;
   AddConstraints(LP, Vi, Matrix(RR,[[0]]): Rel := "ge");
end for;

S:=Solution(LP);
M:=&+ElementToSequence(S);
Log(M)/Log(4);
```

Exercise 4.2. The solution is similar to the proof of Gilbert-Varshamov bound for linear codes.

1. If the first k entries in $y = (y_1, \ldots, y_n)$ are zero, then the linear constraint $\langle H_i \mid y \rangle = 0$, where H_i is the ith row of H, simplifies to $y_{k+i} = 0$. As y is nonzero, this cannot happen for all i's, and thus, the probability of y being in the right kernel of H is zero.

   Now suppose $y_1, \ldots, y_k$ are not all zero and note that the linear map
   $$\begin{aligned} \phi_y : \mathbb{F}_q^k &\rightarrow \mathbb{F}_q \\ (a_1, \ldots, a_k) &\mapsto \sum a_i y_i \end{aligned}$$
   being nontrivial, the preimage set of each $\alpha \in \mathbb{F}_q$ has the same size. Thus as the ith row A_i of A is picked uniformly in $\mathbb{F}_q^k$, $\langle A_i \mid (y_1, \ldots, y_k) \rangle$ will be uniformly distributed over $\mathbb{F}_q$, so that $\langle A_i \mid (y_1, \ldots, y_k) \rangle = y_{k+i}$ with probability $1/q$. But $Hy^\top = 0$ means that $\langle A_i \mid (y_1, \ldots, y_k) \rangle = y_{k+i}$ for each i. This happens with probability $(1/q)^{n-k} = q^{k-n}$.

2. We want to upper bound the probability that the code defined by the parity check matrix H contains a word of weight $d-1$ or less. For each fixed word y of weight $d-1$ or less, the probability that y is in the code (i.e., *bad event*) is given by the previous part. Now we use a union bound on all choices of y that have 1 as their first nonzero entry (this prevents overcounting since y belongs to the code if and only if αy belongs to the code for any nonzero scalar α); the number of such y is the volume of Hamming ball of radius $d-1$, that we denote by $V_q(n, d-1) = \sum_{i=1}^{d-1} \binom{n}{i}$, divided by $q-1$. Among these, $V_q(n-k, d-1)/(q-1)$ have zeros as their first k entries, and for these the bad event probability is zero. Thus, the probability that we wish to compute is upper bounded by
   $$q^{k-n} \cdot \frac{V_q(n, d-1) - V_q(n-k, d-1)}{q-1},$$
   which is exactly ρ.

3. This is immediate from the previous part by observing that, for each i, H contains i dependent columns iff the linear code $\mathcal{C}_H$ for which it is a parity check matrix contains a codeword of weight i. Therefore
   $$\Pr[\mathcal{C}_H \text{ has minimum distance } \leq d-1] \leq \Pr[H \text{ has } d-1 \text{ dependent columns}] \leq \rho.$$

Exercise 4.3. For the first part, write

$$\begin{aligned}(1+(q-1)z)^{n-x}(1-z)^x &= (1+(q-1)z)^n\left(1+\frac{-qz}{1+(q-1)z}\right)^x \\ &= (1+(q-1)z)^n\sum_{r=0}^{x}\binom{x}{r}\left(\frac{-qz}{1+(q-1)z}\right)^r \\ &= \sum_{r=0}^{x}\binom{x}{r}(1+(q-1)z)^{n-r}(-qz)^r.\end{aligned}$$

The coefficient of z^ℓ on the left hand side is exactly $K_\ell(x)$ as defined in the exercise. The same coefficient, on the right hand side, is

$$\sum_{r=0}^{\ell}\binom{x}{r}\binom{n-r}{\ell-r}(-q)^r(q-1)^{\ell-r}$$

which gives the alternative form of Krawtchouk polynomials.

Exercise 4.4.

1. Consider the subcode $\mathcal{C}'$ of $\mathcal{C}$ consisting of all nonzero words of weight at most d. All codewords of this code must have weight exactly d (because $\mathcal{C}$ cannot have a nonzero word of weight less than d because of its distance), and the minimum distance of this code is still d. Thus $|\mathcal{C}'| \leq A(n,d,d)$.

2. This is because the Hamming distance of two words of the same weight must be even, and thus, the minimum distance of any constant weight code is even.

3. As the hint suggests, suppose that $\mathcal{C}$ is a binary code of length n, minumum distance at least $2k$ for which all codewords have weight w. Moreover, suppose that $\mathcal{C}$ is optimal in that it has $A(n,2k,w)$ words. Let $M := |\mathcal{C}| = A(n,2k,w)$. Arrange the words of $\mathcal{C}$ as rows of an $M \times n$ matrix T. Consider the set of rows of T for which the ith column of T has a one. These rows, with the ith column removed, list the codewords of a code of length $n-1$, distance at least $2k$, and constant weight $w-1$, which must have at most $A(n-1,2k,w-1)$ codewords. Thus, every column of T can have at most $A(n-1,2k,w-1)$ ones, which gives an upper bound of $nA(n-1,2k,w-1)$ on the number of ones in T. On the other hand this number is exactly Mw. Therefore, $Mw \leq nA(n-1,2k,w-1)$.

4. Follows by induction on n from the previous part, and the trivial fact that $A(n,2k,k-1) = 1$.