Exercise Sheet 4

(Solutions)

Exercise 4.1. 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 4.2. 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. Otherwise, $\langle A_i \mid (y_1,\ldots,y_k)\rangle$ (where A_i denotes the ith row of A) will be uniformly distributed over $\mathbb{F}_q$ (because the set of vectors x satisfying $\langle x \mid (y_1,\ldots,y_k)\rangle = \alpha$ for a fixed $\alpha\in\mathbb{F}_q$ defines a hyperplane and the probability of a random x falling into this hyperplane is $1/q$). Thus the distribution of $A(y_1,\ldots,y_k)$ will be uniform on $\mathbb{F}_q^{n-k}$. On the other hand, $Hy^\top = 0$ means that $A(y_1,\ldots,y_k)=(y_{k+1},\ldots,y_n)$, where the left hand side is uniformly distributed and the right hand side is fixed. So the probability that this particular event happens is q^{k-n}.

2. We want to upper bound the probability that the code defined by the partity 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; the number of such y is the volume of Hamming ball of radius $d-1$, that we denote by $V_q(n,d-1)=\sum_P i = 1^{d-1}\binom{n}{i}$, 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 for which it is a parity check matrix contains a codeword of weight i.

Exercise 4.3.

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 $A(n, 2k, k-1) = 1$.