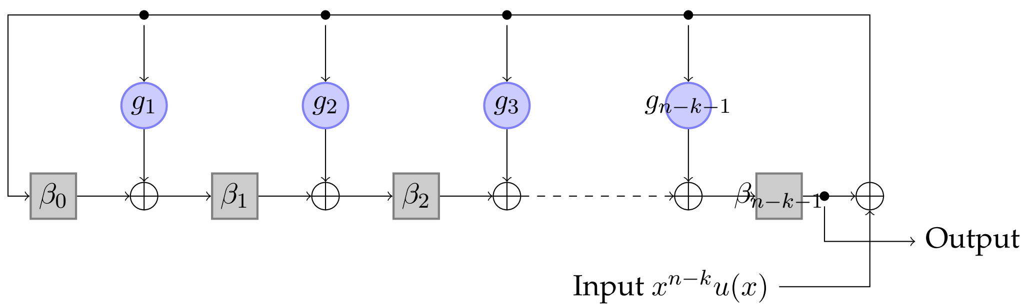
Exercise Sheet 6

Exercise 6.1. Let $\mathcal{C}$ be a$[n,k]_2$-cyclic code with generator polynomial $g(x) = 1 + g_1x + \cdots + g_{n-k-1}x^{n-k-1} + x^{n-k} \in \mathbb{F}_2[x]/(x^n - 1)$.

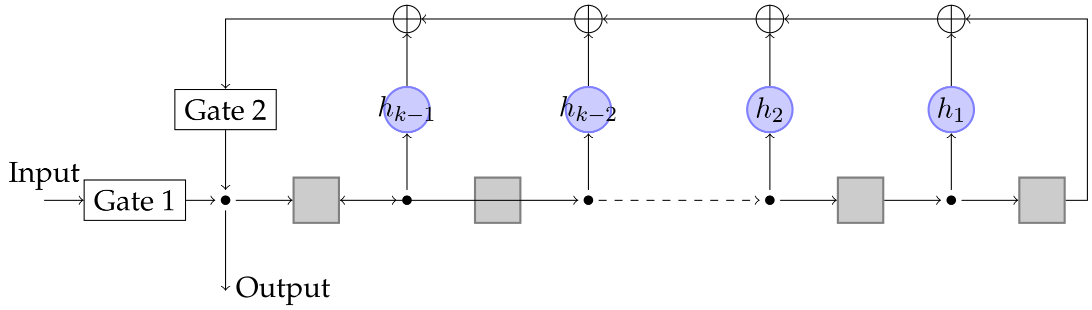
1. Suppose you want to send $u(x) = u_0 + u_1 + \cdots + u_{k-1}x^{k-1}$. Let $b(x)$ be the remainder of $x^{n-k}u(x)$ by $g(x)$. Show that sending $m(x) = x^{n-k}u(x) + b(x)$ is an encoding in the systematic form.

2. Show that the following linear $(n-k)$-stage shift register with feedback with initial seed $\beta = 0$ computes $b(x)$ after k steps.



(Hint : represent the current contents of the registers by $\beta(x) = \beta_0 + \beta x + \cdots + \beta_{n-k-1}x^{n-k-1}$)
NB : A shift register is a chain of boxes that contain each one bit and that are updated simultaneously, according to what they receive. In the graph, rectangles stand for the registers, circles for multiplication by g_i and crosses for XOR operation.

3. Let $h(x) = h_0 + \cdots + h_kx^k$ be the polynomial such that $x^n - 1 = g(x)h(x)$. Show that the following circuit, where gate 1 is open during the emission of the k first symbols and gate 2 during the last $n-k$ symbols, performs a systematic encoding of $\mathcal{C}$.



4. Compare how many Xor and registers you need with each scheme for the Hamming $[7,4]_2$-code ($g(x) = x^3 + x + 1$).

5. For cyclic code, the syndrom of a received word $r(x) = r_0 + \cdots + r_{n-1}x^{n-1}$ is the remainder of r divided by g. Propose a circuit that computes s.

Exercise 6.2. In this exercise, we design a 2-error-correcting BCH code of length 13, and dimension 6 over $\mathbb{F}_3$.

1. If ω denotes a primitive 13th root of unity over $\mathbb{F}_3$, show that the smallest extension field of $\mathbb{F}_3$ in which ω lives has degree 3.
2. Let $g_i(x)$ denote the minimal polynomial of ω^i over $\mathbb{F}_3$. What is a generator polynomial of a 2-error correcting BCH code of length 13 and dimension 6 in terms of the $g_i(x)$?
3. Now we want to calculate the polynomials $g_i(x)$. First, find an irreducible polynomial of degree 3 over $\mathbb{F}_3$.
4. Use the irreducible polynomial obtained in the previous part to find a primitive element α in a degree 3 extension of $\mathbb{F}_3$, and show that we can choose $\omega := \alpha^2$. Calculate the minimal polynomials $g_0(x), g_1(x), g_2(x), g_4(x), g_7(x)$, and show that this is the complete list of $g_i(x)$.
5. Now compute the generator polynomial for the code.
6. Suppose that we have received the word $y := (0, -1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0)$. Apply the decoding algorithm that we saw in the lecture to decode this string to its nearest codeword.