UNIVERSITY OF DUBLIN

TRINITY COLLEGE

Faculty of Science

school of mathematics

JS Mathematics
SS Mathematics

Trinity Term 1992

Course 373

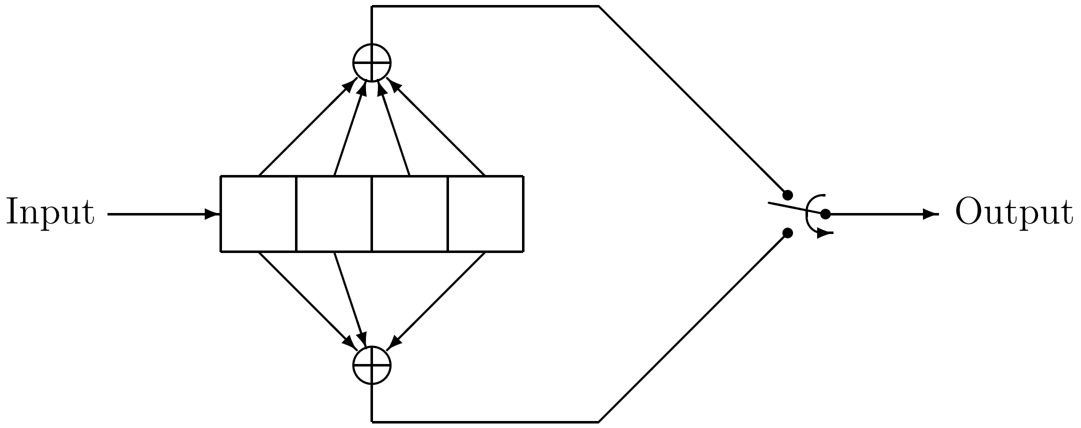
Friday, June 5 Exam Hall 09.30 - 12.30

Dr. M. Purser and Dr. T.G. Murphy

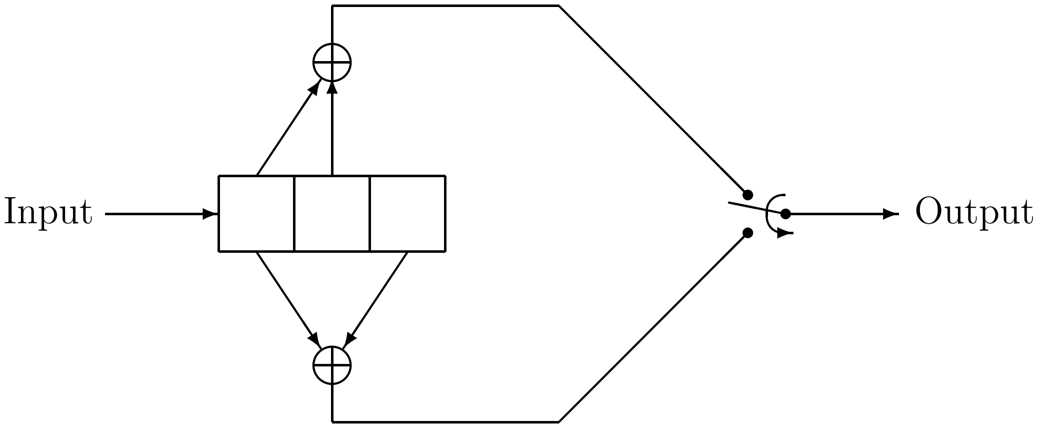
Answer Section A and B in separate answer books. Section A - Answer 3 out of the 6 questions. Section B - Answer 2 out of the 4 questions.

SECTION A

1. What is a convolutional code? Explain. What is the free distance of the non-systematic half-rate code with constraint length = 4, whose encoder is illustrated?



Comment on the code with constraint length = 3 whose encoder is illustrated below.



2. Generate the null-matrix of a non-binary extended Hamming code over $\mathbf{GF}(4)$ with 3 parity-check digits.

3. Prove that the number of check digits $(n-k)$ in a binary linear code exceeds the Plotkin Bound:
$$n-k \geq 2d-2-\log_2 d,$$
where d is the distance, provided that $n \geq 2d-1$, where n is the length.

4. A $(15,7)$ binary cyclic code with distance $=5$ has as generating polynomial
$$g(x)=x^8+x^7+x^6+x^4+1.$$
The vector 001100100011111 is received.

   Use the Kasami algorithm to evaluate the transmitted code vector.

5. Describe the procedure for decoding BCH codes based on the use of error locators. Can this procedure be applied to non-binary as well as binary codes? Illustrate your discussion by finding the 3 errors in the vector 000010001011110 received, which should be a codevector of the $(15,5)$ code with generating polynomial
$$x^{10}+x^8+x^5+x^4+x^2+x+1=(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1).$$

6. What are the Reed-Solomon codes? Why, for these codes, does the distance $d = n-k+1$ and $n=q-1$? (Here n is the length, k the number of information symbols, and the code is over $\mathbf{GF}(q)$).

   Show that the set of values taken by *any* k symbol-positions in an R–S code are distinct over all q^k codewords. How many codewords are there of weight $=d$?

   Present a $(7,3)$ R–S code.

SECTION B

7. Define the *characteristic* of a field. Prove that the characteristic of a finite field is a prime number.

   Show that a finite field of characteristic p contains p^n elements, for some positive integer n. Show also that if $K \subset F$ is a subfield, then K contains p^m elements, where $m \mid n$.

   Describe explicitly the field $\mathbf{GF}(2^3)$ containing 8 elements, verifying that it *is* a field.

8. Show that the multiplicative group $F^\times = F - \{0\}$ of a finite field F is cyclic.

   Determine all the primitive elements (multiplicative generators) in $\mathbf{GF}(19)$.

   How many primitive elements does $\mathbf{GF}(2^6)$ possess?

   Prove that 2 finite fields containing the same number of elements are necessarily isomorphic.

9. Suppose F is a finite field of characteristic p. Show that the map

   $$\Phi : x \mapsto x^p$$

   is an automorphism of F; and show that every automorphism of F is of the form Φ^i.

   Suppose $p(x)$ is a prime polynomial over the prime subfield $P = \mathbf{GF}(p)$ of F. Show that if $p(x)$ has a root in F then it splits completely in F.

   Sketch the proof that there exists a field $\mathbf{GF}(p^n)$ with p^n elements for every prime-power p^n.

10. Let $\Pi(n) = \Pi_p(n)$ denote the number of prime polynomials of degree n over $\mathbf{GF}(p)$. Show that

    $$\sum_{d \mid n} d\Pi(d) = p^n$$

    for each positive integer n.

    Determine all the prime polynomials of degree ≤ 7 over $\mathbf{GF}(2)$.

    Explain what is meant by saying that a prime polynomial of $\mathbf{GF}(p)$ is *primitive*. Show that there are

    $$\frac{1}{n}\phi\left(p^n - 1\right)$$

    primitive polynomials of degree n over $\mathbf{GF}(p)$.

    Determine which of the polynomials of degree ≤ 7 over $\mathbf{GF}(2)$ are primitive.