

Spring 2006

**Problem Set 3**

**Low Density Parity Check Codes, Reliable Information Storage, Reliable  
Dynamic Systems**

**Issued:** Tuesday, April 11th.

**Due:** Tuesday, April 18th.

---

**Reading:**

- (i) Class notes;
  - (ii) “Reliable Information Storage in Memories Designed from Unreliable Components” by M. G. Taylor;
  - (iii) Hadjicostis, Chapter 7 (“Unreliable Error Correction in Dynamic Systems”);
  - (iv) Papers:
    - (1) C. N. Hadjicostis and G. C. Verghese, “Fault-Tolerant Computation in Semigroups and Groups: Applications to Automata, Dynamic Systems and Petri Nets,” *Journal of the Franklin Institute*, vol. 339, no. 4-5, pp. 387–430, July-August 2002.
    - (2) C. N. Hadjicostis and G. C. Verghese, “Coding Approaches to Fault Tolerance in Linear Dynamic Systems,” *IEEE Transactions on Information Theory*, vol. 51, no. 1, pp. 210–228, January 2005.
- 

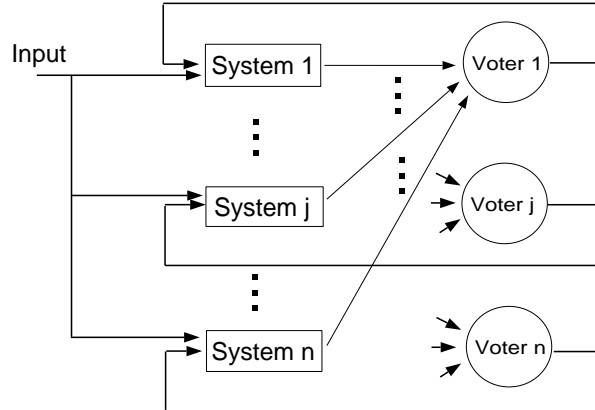
**Problem 3.1**

Characterize all systematic separate codes that are appropriate for protecting multiplication of positive integers (i.e., characterize all types of congruence classes for the semigroup  $(N, \times)$ ).

**Problem 3.2**

- (a) Construct  $GF(2^4)$  as an extension of  $GF(2)$  using the primitive polynomial  $x^4 + x + 1$ .
- (b) Construct  $GF(2^5)$  as an extension of  $GF(2)$  using a primitive polynomial of your choice.
- (c) Could addition and multiplication in  $GF(2^4)$  be protected by performing addition and multiplication in  $GF(2^5)$ ?

**Problem 3.3**



In class we discuss the set up in the paper “Coding Approaches to Fault Tolerance in Dynamic Systems” by C. Hadjicostis and G. Verghese. It has  $n$  replicas of the dynamic system and  $n$  voters, each of which is responsible for sending a correction term to only one of the systems as shown above.

Assuming that systems fail with probability  $p_s$  and voters fail with probability  $p_v$  (all failures are independent), we argued in class that the probability that the system suffers an overall failure during any time step in the interval  $[0, L]$  is given by

$$\Pr[\text{overall failure at or before time step } L] \leq L \sum_{i=\lfloor n/2 \rfloor}^n \binom{n}{i} p^i (1-p)^{n-i},$$

where  $p \equiv p_v + (1 - p_v)p_s$ .

In this problem we will show that the expression

$$\sum_{i=\lfloor n/2 \rfloor}^n \binom{n}{i} p^i (1-p)^{n-i} \tag{1}$$

goes down exponentially with the number of systems  $n$  if  $p < \frac{1}{2}$ . For simplicity we assume that  $n$  is even.

(a) Show that, if  $p < 1/2$  then

$$\binom{n}{n/2} [p(1-p)]^{n/2} \leq \sum_{i=n/2}^n \binom{n}{i} p^i (1-p)^{n-i} \leq \frac{1-p}{1-2p} \binom{n}{n/2} [p(1-p)]^{n/2}.$$

(b) Show that

$$\sqrt{\frac{1}{2n}} 2^n \leq \binom{n}{n/2} \leq \sqrt{\frac{2}{\pi n}} 2^n,$$

(c) Combine the results from parts (a) and (b) to show that the expression in (1) goes down exponentially with  $n$  if  $p < 1/2$ .