Christian Schindelhauer
Stefan Rührup

Freiburg, 2008-11-21

Solution for Exercise No. 4

Algorithms and Methods for Distributed Storage

Winter 2008/09

Exercise 7 *Compute the inverse matrix over $GF[2]$ of*

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

using the Gaussian elimination method.

$$(A|I) := \left(\begin{array}{ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right) \Rightarrow \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right) = (I|A^{-1})$$

(Gauss-Jordan-Algorithm using element-wise XOR as elementary row operation)

Exercise 8 *Consider the Liberation Code for a RAID-6 system with 5 hard disks (three data words and two check words). The word length is three bits.*

1. *Give the full $GF[2]$ matrix to compute P and Q.*

   The coding distribution matrix (CDM) consists of one row of 3×3-identity matrices (for the parity word P) and another row of coding matrics X_i (for the code word Q).

$$X_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad X_1 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \quad X_2 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix} \quad I^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\text{CDM} = \begin{bmatrix} I^3 & I^3 & I^3 \\ X_0 & X_1 & X_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

The full binary distribution matrix is as follows:

$$\text{BDM} = \begin{bmatrix} I^3 & 0 & 0 \\ 0 & I^3 & 0 \\ 0 & 0 & I^3 \\ I^3 & I^3 & I^3 \\ X_0 & X_1 & X_2 \end{bmatrix}$$

2. *Compute P and Q for the inputs $D_0 = 010, D_1 = 011, D_2 = 100$.*

$$\text{DATA} = \begin{bmatrix} D_0 \\ D_1 \\ D_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \qquad \text{PQ} := \begin{bmatrix} P \\ Q \end{bmatrix} = \text{CDM} \cdot \text{DATA} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

3. *Now the hard disks with D_1 and D_2 are not available. Compute their contents based on the knowledge $D_0 = 000, P = 110, Q = 111$.*

We consider the last 9 rows of the BDM and calculate the inverse:

$$B := \begin{bmatrix} 0&0&0&0&0&0&1&0&0 \\ 0&0&0&0&0&0&0&1&0 \\ 0&0&0&0&0&0&0&0&1 \\ 1&0&0&1&0&0&1&0&0 \\ 0&1&0&0&1&0&0&1&0 \\ 0&0&1&0&0&1&0&0&1 \\ 1&0&0&0&1&0&0&0&1 \\ 0&1&0&0&1&1&1&0&0 \\ 0&0&1&1&0&0&1&1&0 \end{bmatrix} \qquad B^{-1} := \begin{bmatrix} 1&0&1&1&1&1&0&1&1 \\ 1&1&0&1&0&1&1&1&1 \\ 1&1&1&0&1&1&0&1&0 \\ 0&0&1&0&1&1&0&1&1 \\ 1&0&0&1&1&1&1&1&1 \\ 1&1&0&0&1&0&0&1&0 \\ 1&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&0 \end{bmatrix}$$

The last 6 rows of B^{-1} give the inverse coding matrix:

$$\text{CDM}' := \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Recovering D_0 and D_1 from the original (D_2, P, Q):

$$V := \begin{bmatrix} D_2 \\ P \\ Q \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \qquad \begin{bmatrix} D_0 \\ D_1 \end{bmatrix} = V \cdot \text{CDM}' = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

Recovering D_1 and D_2 from $D_0 = 000, P = 110, Q = 111$:

$$V' := \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} \qquad \begin{bmatrix} D_0 \\ D_1 \end{bmatrix} = V' \cdot \text{CDM}' = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$