CS-E4500 Problem Set 1

Jaan Tollander de Balsch - 452056

January 19, 2019

Problem 1

a)

Multiply $a = x + x^2 \in \mathbb{Z}_2[x]$ and $b = 1 + x + x^3 \in \mathbb{Z}_2[x]$.

$$a \cdot b = x + x^3 + x^4 + x^5 \in \mathbb{Z}_2[x]$$

b)

Divide $a = 1 + x^2 + x^3 + x^4 + x^6 \in \mathbb{Z}_2[x]$ and $b = 1 + x^3 + x^4 \in \mathbb{Z}_2[x]$. Present a quotient $q \in \mathbb{Z}_2[x]$ and a remainder $r \in \mathbb{Z}_2[x]$ such that $a = q \cdot b + r$ and $\deg r < \deg b$.

First division gives us

$$a = q_1 b + r_1,$$

where the quotient $q_1 = x^2$ and the remainder $r_1 = 1 + x^3 + x^4 + x^5$. Since $\deg r_1 > \deg b$ we'll divide again. Second division given us

$$r_1 = q_2 b + r_2,$$

where the quotient $q_2 = x$ and the remainder $r_2 = 1 + x + x^3$. The division terminates because $\deg r_2 < \deg b$. Lets collect the terms

$$\begin{aligned} a &= q_1 b + r_1 \\ &= q_1 b + (q_2 b + r_2) \\ &= (q_1 + q_2) b + r_2 \\ &= qb + r. \end{aligned}$$

We see that the quotient and the remainder takes the form

$$q = q_1 + q_2 = x + x^2$$
$$r = r_2 = 1 + x + x^3.$$

Problem 2

a)

Find the greatest common divisor of $f = 1234567$ and $g = 123$ in $\mathbb{Z}$. Using the output of the algorithm, find $g^{-1} \in \mathbb{Z}_f$.

Using the Traditional Euclidian algorithm on f and g gives us

$$\begin{aligned} 1234567 &= 10037 \cdot 123 + 16 \\ 123 &= 7 \cdot 16 + 11 \\ 16 &= 1 \cdot 11 + 5 \\ 11 &= 2 \cdot 5 + 1. \end{aligned}$$

Written in another form

$$\begin{aligned} 1 &= 11 - 2 \cdot 5 \\ 5 &= 16 - 1 \cdot 11 \\ 11 &= 123 - 7 \cdot 16 \\ 16 &= 1234567 - 10037 \cdot 123 \end{aligned}$$

Now using back substitution on the equation we can obtain coefficients for the Diophantine equation

$$a \cdot f + b \cdot g = 1.$$

where $a = -23$ and $b = 230854$.

Written in another form

$$b \cdot g = -a \cdot f + 1$$

we see that the coefficient b is answer for $g^{-1} \in \mathbb{Z}_f$ because

$$\begin{aligned} g \cdot g^{-1} \mod f &= 1 \\ g \cdot g^{-1} &= k \cdot f + 1, \quad k \in \mathbb{Z}_f \end{aligned}$$

where $k = -a = 23$ and $g^{-1} = b = 230854$.

b)

Find a greatest common divisor of $f = 1 + x + x^3 + x^4$ and $g = 1 + x^4$ in $\mathbb{Z}_2[x]$.

Using Traditional Euclidian algorithm on f and g gives us

$$\begin{aligned} 1 + x + x^3 + x^4 &= 1 \cdot (1 + x^4) + (x + x^3) \\ 1 + x^4 &= x \cdot (x + x^3) + (1 + x^2) \\ x + x^3 &= x \cdot (1 + x^2) + 0. \end{aligned}$$

From the output we can see that

$$\gcd(f, g) = 1 + x^2 \in \mathbb{Z}_2[x].$$

Problem 3

Let $\xi_0, \xi_1, ..., \xi_d \in F$ be distinct elements in a field F. Show that Vandermonde matrix

$$\Xi = \begin{bmatrix} \xi_0^0 & \xi_0^1 & \cdots & \xi_0^d \\ \xi_1^0 & \xi_1^1 & \cdots & \xi_1^d \\ \vdots & \vdots & & \vdots \\ \xi_d^0 & \xi_d^1 & \cdots & \xi_d^d \end{bmatrix} \in F^{(d+1)\times(d+1)}$$

is invertible.

The Lagrange polynomial $L(x) \in F[x]$ for $i = 0, 1, ..., d$ is defined by

$$L_i(x) = \prod_{j=0, j\neq i}^{d} \frac{x - \xi_j}{\xi_i - \xi_j} = \sum_{k=0}^{d} \lambda_{ik} x^k.$$

Then evaluating it at the point $x = \xi_m$ where $m \in \{0, 1, ..., d\}$ gives us

$$\begin{aligned} L_i(\xi_m) &= \prod_{j=0, j\neq i}^{d} \frac{\xi_m - \xi_j}{\xi_i - \xi_j} \\ &= \begin{cases} 0, & m \neq i \\ 1, & m = i \end{cases} \\ &= \delta_{m,i} \end{aligned}$$

and

$$\begin{aligned} L_i(\xi_m) &= \sum_{k=0}^{d} \lambda_{k,i} \xi_m^k \\ &= \sum_{k=0}^{d} \xi_m^k \lambda_{k,i} \\ &= \begin{bmatrix} \xi_m^0 & \xi_m^1 & ... & \xi_m^d \end{bmatrix} \cdot \begin{bmatrix} \lambda_{0,i} \\ \lambda_{1,i} \\ \vdots \\ \lambda_{d,i} \end{bmatrix}. \end{aligned}$$

Written in matrix form over $i, m \in \{0, 1, ..., d\}$ gives us

$$\begin{bmatrix} \xi_0^0 & \xi_0^1 & ... & \xi_0^d \\ \xi_1^0 & \xi_1^1 & ... & \xi_1^d \\ \vdots & \vdots & & \vdots \\ \xi_d^0 & \xi_d^1 & ... & \xi_d^d \end{bmatrix} \cdot \begin{bmatrix} \lambda_{0,0} & \lambda_{0,1} & ... & \lambda_{0,d} \\ \lambda_{1,0} & \lambda_{1,1} & ... & \lambda_{1,d} \\ \vdots & \vdots & & \vdots \\ \lambda_{d,0} & \lambda_{d,1} & ... & \lambda_{d,d} \end{bmatrix} = \begin{bmatrix} \delta_{0,0} & \delta_{0,1} & ... & \delta_{0,d} \\ \delta_{1,0} & \delta_{1,1} & ... & \delta_{1,d} \\ \vdots & \vdots & & \vdots \\ \delta_{d,0} & \delta_{d,1} & ... & \delta_{d,d} \end{bmatrix}$$

$$\Xi \cdot \mathbf{\Lambda} = \mathbf{I}$$

$$\mathbf{\Lambda} = \Xi^{-1}.$$

Because the Kronecker delta generates the indentity matrix $\mathbf{I}$, the matrix $\mathbf{\Lambda}$ generated by the coefficients $\lambda_{i,j}$ is the inverse of Ξ.

Problem 4

The initial values in the traditional Euclidian algorithm are

$$\begin{aligned} r_0 = f, \quad s_0 = 1, \quad t_0 = 0, \\ r_1 = g, \quad s_1 = 0, \quad t_1 = 1. \end{aligned}$$

The subsequent values when $i \geq 1$ are given by recursive relationship as

$$\begin{aligned} q_i &= quo(r_{i-1}, r_i), \\ r_{i+1} &= r_{i-1} - q_i r_i, \\ s_{i+1} &= s_{i-1} - q_i s_i, \\ t_{i+1} &= t_{i-1} - q_i t_i. \end{aligned}$$

The matrices R and Q are defined

$$R_0 = \begin{bmatrix} s_0 & t_0 \\ s_1 & t_1 \end{bmatrix}, \; Q_i = \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix}, \quad i = 1, 2, ..., l.$$

and

$$R_i = Q_i Q_{i-1} \cdots Q_1 R_0, \quad i = 0, 1, ..., l.$$

Note that Q is also invertible

$$Q_i^{-1} = \begin{bmatrix} q_i & 1 \\ 1 & 0 \end{bmatrix}.$$

Another useful relation is

$$\begin{aligned} R_{i+1} &= Q_{i+1}Q_iQ_{i-1}\cdots Q_1R_0, \quad i = 0, 1, ..., l \\ &= Q_{i+1}R_i. \end{aligned}$$

a)

Show that invariant holds for all $i = 0, 1, ..., l$:

$$R_i \begin{bmatrix} f \\ g \end{bmatrix} = \begin{bmatrix} r_i \\ r_{i+1} \end{bmatrix}.$$

Lets show that the **base case** $i = 0$ is true.

$$\begin{aligned} R_0 \begin{bmatrix} f \\ g \end{bmatrix} &= \begin{bmatrix} r_0 \\ r_1 \end{bmatrix} \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} f \\ g \end{bmatrix} &= \begin{bmatrix} r_0 \\ r_1 \end{bmatrix} \\ \begin{bmatrix} f \\ g \end{bmatrix} &= \begin{bmatrix} r_0 \\ r_1 \end{bmatrix}. \end{aligned}$$

We will assume that the **case** $i = n \geq 1$ is true and show that then also **case** $i = n + 1$ is true.

$$\begin{aligned} R_{n+1} \begin{bmatrix} f \\ g \end{bmatrix} &= \begin{bmatrix} r_{n+1} \\ r_{(n+1)+1} \end{bmatrix} \\ Q_{n+1}R_n \begin{bmatrix} f \\ g \end{bmatrix} &= \begin{bmatrix} r_{n+1} \\ r_{(n+1)+1} \end{bmatrix} \\ R_n \begin{bmatrix} f \\ g \end{bmatrix} &= Q_{n+1}^{-1} \begin{bmatrix} r_{n+1} \\ r_{(n+1)+1} \end{bmatrix} \\ &= \begin{bmatrix} q_{n+1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} r_{n+1} \\ r_{(n+1)+1} \end{bmatrix} \\ &= \begin{bmatrix} q_{n+1}r_{n+1} + r_{n+2} \\ r_{n+1} \end{bmatrix} \\ &= \begin{bmatrix} r_n \\ r_{n+1} \end{bmatrix}. \end{aligned}$$

b)

Show that invariant holds for all $i = 0, 1, ..., l$:

$$R_i = \begin{bmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{bmatrix}$$

Base case $i = 0$ is true by definition. We'll assume case $i = n \geq 1$ to be true and then show that $i = n + 1$ is also true.

$$\begin{aligned} R_{n+1} &= \begin{bmatrix} s_{n+1} & t_{n+1} \\ s_{(n+1)+1} & t_{(n+1)+1} \end{bmatrix} \\ R_n &= Q_{n+1}^{-1} \begin{bmatrix} s_{n+1} & t_{n+1} \\ s_{(n+1)+1} & t_{(n+1)+1} \end{bmatrix} \\ &= \begin{bmatrix} q_{n+1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} s_{n+1} & t_{n+1} \\ s_{(n+1)+1} & t_{(n+1)+1} \end{bmatrix} \\ &= \begin{bmatrix} q_{n+1}s_{n+1} + s_{n+2} & q_{n+1}t_{n+2} + t_{n+1} \\ s_{n+1} & t_{n+1} \end{bmatrix} \\ &= \begin{bmatrix} s_n & t_n \\ s_{n+1} & t_{n+1} \end{bmatrix}. \end{aligned}$$

c)

The output of Euclidian algorithm is as follows.

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ r_2 &= q_3 r_3 + r_4 \\ &\vdots \\ r_{l-2} &= q_{l-1} r_{l-1} + r_l \\ r_{l-1} &= q_l r_l + r_{l+1} \end{aligned}$$

Then the algorithm terminates when $r_{l+1} = 0$. This means that r_{l-1} is divisible by r_l which implies that r_{l-2} is divisible by r_l and by this logic all $r_{l-1}, ..., r_0$ are divisible by r_l. Divisor r_l must be the greatest common divisor, otherwise there would exists $i \in [0, l]$ such that $r_i = 0$.

d)

By using the statements proven in sections (a) and (b) we have

$$R_i \begin{bmatrix} f \\ g \end{bmatrix} = \begin{bmatrix} r_i \\ r_{i+1} \end{bmatrix}$$
$$\begin{bmatrix} s_i & t_i \\ s_{i+1} & t_{i+1} \end{bmatrix} \begin{bmatrix} f \\ g \end{bmatrix} = \begin{bmatrix} r_i \\ r_{i+1} \end{bmatrix}$$
$$s_i f + t_i g = r_i.$$