CS-E4500 Problem Set 5

Jaan Tollander de Balsch - 452056

February 24, 2019

Problem 1

Let F be a field, Show that a nonzero polynomial $f \in F[x]$ of degree at most d has at most d distinct roots.

Let $\xi_1, \xi_2, ..., \xi_n \in F$ be $n \geq d+1$ distinct roots of polynomial f. Then the polynomial can be represented using the roots as

$$f(x) = a(x-\xi_1)^{k_1}(x-\xi_2)^{k_2} \cdots (x-\xi_n)^{k_n}$$

where $a \in F$ is a scaling coefficient and $k_1, k_2, ..., k_n \in \mathbb{N}$ are the multiples of the roots. The degree of the polynomial is

$$\begin{aligned}
\deg f(x) &= k_1 + k_2 + ... + k_n \\
&\geq \min_{k_1, k_2, ..., k_n \in \mathbb{N}} (k_1 + k_2 + ... + k_n) \\
&= n \\
&\geq d+1.
\end{aligned}$$

This implies that a polynomial that has $d+1$ distinct roots has degree of atleast $d+1$. Equivalently a polynomial that has degree d has at most d distinct roots.

Problem 2

Reed-Solomon codes.

(a)

Encoding: Suppose we want ot encode data vector $\Phi = (7,6,5,4,3) \in \mathbb{F}_{11}^5$ using the evaluation points $\Xi = (0,1,2,3,4,5,6) \in \mathbb{F}_{11}^5$. Find the encoding $\Psi = f(\Xi) \in \mathbb{F}_{11}^7$.

Create a polynomial f by using Φ as the coefficients

$$f(x) = 3x^4 + 4x^3 + 5x^2 + 6x + 7 \in \mathbb{F}_{11}[x].$$

Then evaluate the polynomial at points Ξ to obtain the encoding

$$f(\Xi) = (7, 3, 9, 3, 2, 7, 3) \in \mathbb{F}_{11}^7.$$

(b)

Decoding in the presence of errors. Suppose that $\Xi = (1, 2, 3, 4, 5, 6) \in \mathbb{F}_{13}^6$ and that $\Gamma = (3, 8, 6, 7, 1) \in \mathbb{F}_{13}^6$. Find the unique polynomial $f \in \mathbb{F}_{13}[x]$ of degree at most 1 such that $f(\Xi)$ agrees iwth Γ in all but at most 2 coordinates, or conclude that no such f exists.

The decoding can be done using Gao's algorithm (Gao 2002). I used Python with the Sympy library to calculate the polynomial operations on finite fields.

We have

$$\begin{aligned} e &= 6 \\ d &= 1 \end{aligned}$$

The polynomial g_0 is constructed as

$$g_0 = \prod_{i=0}^{e}(x - \xi_i) = x^6 + 5x^5 + 6x^4 + 6x^3 + 12x^2 + 4x + 5.$$

The polynomial g_1 is obtained using Lagrange interpolation in points (ξ_i, φ_i) for all $i = 1, 2, ..., e$

$$g_1 = 7x^5 + 5x^4 + 9x^3 + x + 7$$

The initial values of the Bezout coefficient

$$\begin{aligned} t_0 &= 0 \\ t_1 &= 1 \end{aligned}$$

Then we apply extended Euclidian algorithm to g_0 and g_1 to produce the concecutive remainders g_h, g_{h+1} with $\deg g_h \geq D$, and $\deg g_{h+1} < D$ for $D = (e + d + 1)/2 = 4$

First iteration: $g_0 = q_1 g_1 + g_2$

$$\begin{aligned} q_1 &= 2x + 3 \\ g_2 &= 12x^4 + 5x^3 + 10x^2 + 10 \\ t_2 &= t_0 - q_1 t_1 = 11x + 10 \\ \deg g_2 &= 4 \geq D \end{aligned}$$

Second iteration: $g_1 = q_2 g_2 + g_3$

$$\begin{aligned} q_2 &= 6x + 12 \\ g_3 &= 6x^3 + 10x^2 + 6x + 4 \\ t_3 &= t_1 - q_2 t_2 = 12x^2 + 3x + 11 \\ \deg g_3 &= 3 < D \end{aligned}$$

By dividing g_3 with t_3 we obtain quotient

$$f = g_3 / t_3 = 7x + 11$$

with remainder $r = 0$. The decoding is succesful and the reconstructed data vector is

$$(11, 7).$$

We can see that Γ has two errors

$$\begin{aligned} f(\Xi) = [5, 12, 6, 0, 7, 1] \neq \\ \Gamma = [3, 8, 6, 0, 7, 1]. \end{aligned}$$

Problem 3

The solution to this problem are based on (Gathen and Gerhard 2013, chap. 11.1). Let a polynomial f be defined

$$f = f_n x^n + f_{n-1} x^{n-1} + ... + f_0 \in \mathbb{F}[x]$$

where the leading coefficient $f_n \neq 0$ and $n = \deg f$ is the degree. A **truncated polynomial** is defined

$$f \upharpoonright k = f \operatorname{quo} x^{n-k} = f_n x^k + f_{n-1} x^{k-1} + ... + f_{n-k},$$

where $k \in \mathbb{Z}$. Then the polynomial f can be written in form

$$f = (f \upharpoonright k) x^{n-k} + r,$$

where $r \in \mathbb{F}[x]$ and $\deg r < n - k$ and $k \leq n$.

Let f, g, f', g' be polynomials in field $\mathbb{F}[x]$ such that $\deg f \geq \deg g \geq 0$ and $\deg f' \geq \deg g' \geq 0$ and which **coincide up to** $k \in \mathbb{N}_0$

$$(f, g) \equiv_k (f', g').$$

Equivalently written

$$\begin{aligned} f \upharpoonright k = f' \upharpoonright k, \\ g \upharpoonright (k - (\deg f - \deg g)) = g' \upharpoonright (k - (\deg f' - \deg g')). \end{aligned}$$

Then written in the division form with quotients and remainders

$$\begin{aligned} f &= qg + r, \quad \deg r < \deg g \\ f' &= q'g' + r', \quad \deg r' < \deg g' \end{aligned}$$

the remainders $q = q'$ are equal.

Proof: (This might not be the cleanest way to prove this.)

For simplicity lets denote the degrees with

$$\begin{aligned} \deg f &= n \\ \deg g &= m \\ \deg f' &= n' \\ \deg g' &= m'. \end{aligned}$$

We have

$$k \geq n - m = n' - m' = \delta \geq 0$$

then

$$\begin{aligned} f \upharpoonright k &= f' \upharpoonright k, \\ g \upharpoonright k' &= g' \upharpoonright k', \end{aligned}$$

where

$$k' = k - (n - m) = k - (n' - m') = k - \delta.$$

We also have the following indentities

$$\begin{aligned} n &= n' + \delta \\ m &= m' + \delta \\ m - k' &= n - k \end{aligned}$$

Now by writing the polynoamials in terms of their *truncations* we obtain

$$f' = (f' \upharpoonright k)x^{n'-k} + r_{f'}, \quad \deg r_{f'} < n' - k$$

$$\begin{aligned} f &= (f \upharpoonright k)x^{n-k} + r_f, \quad \deg r_f < n - k \\ &= (f' \upharpoonright k)x^{n'-k}x^{\delta} + r_f \\ &= (f' - r_{f'})x^{\delta} + r_f \end{aligned}$$

and

$$g' = (g' \upharpoonright k')x^{m'-k'} + r_{g'}, \quad \deg r_{g'} < m' - k'$$

$$
\begin{aligned}
g &= (g \restriction k')x^{m-k'} + r_g, \quad \deg r_g < m - k' \\
&= (g' \restriction k')x^{m'-k'}x^{\delta} + r_g \\
&= (g' - r_{g'})x^{\delta} + r_g
\end{aligned}
$$

Then substituting them into the division formula

$$
\begin{aligned}
f &= qg + r \\
(f' - r_{f'})x^{\delta} + r_f &= q((g' - r_{g'})x^{\delta} + r_g) + r \\
f'x^{\delta} &= qg'x^{\delta} + (r - r_f + qr_g + (r_{f'} - qr_{g'})x^{\delta}) \\
f' &= qg' + ((r - r_f + qr_g)x^{-\delta} + r_{f'} - qr_{g'}) \\
f' &= q'g' + r'.
\end{aligned}
$$

In order to prove that $q = q'$ we need to prove that $\deg r' < \deg g' = \deg g$. The degree of the quotient q is $\deg q = \deg f - \deg g = \delta$. Then the degree of the remainder r'

$$
\begin{aligned}
\deg r' &= \deg((r - r_f + qr_g)x^{-\delta} + r_{f'} - qr_{g'}) \\
&= \max\{\deg rx^{-\delta}, \deg -r_f x^{-\delta}, \deg qr_g x^{-\delta}, \deg r_{f'}, \deg -qr_{g'}\} \\
&= \max\{\deg r - \delta, \deg r_f - \delta, \deg r_g, \deg r_{f'}, \delta + \deg r_{g'}\} \\
&< \deg g = \deg g'
\end{aligned}
$$

1) $\deg r - \delta < \deg r < \deg g$
2) $\deg r_f - \delta < n - k - \delta \leq m - k < \deg g$
3) $\deg r_g < m - k' = m - k - \delta = m - (k + \delta) < \deg g$
4) $\deg r_{f'} < n' - k = (n - \delta) - k = m - k < \deg g$
5) $\deg r_{g'} + \delta < m' - k' + \delta = m' - (k - \delta) + \delta$
   $= m' - k = (m - \delta) - k < \deg g$

Therefore $\deg r' < \deg g = \deg g'$. $\square$

This answers to the question why the division $f, g \equiv_4 (\tilde{f}, \tilde{g})$ produce the same quotient for the polynomials in question.

Problem 4

The proof made in the problem 3 should atleast partially answer this question.

References

Gao, Shuhong. 2002. "A New Algorithm for Decoding Reed-Solomon Codes." *Communications, Information and Network Security*, 1–11.

Gathen, Joachim von zur, and Jurgen Gerhard. 2013. *Modern Computer Algebra*. 3rd ed. New York, NY, USA: Cambridge University Press.