CS-E4500 Advanced Course in Algorithms (5 cr)

Problem Set 5 *Spring 2019*

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.

   Hints: To reach a contradiction, assume that you have at least $d+1$ distinct roots. Recall what we know about Vandermonde matrices from our earlier problem sets.

2. Reed–Solomon codes.

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

   (b) Decoding in the presence of errors. Suppose that $\Xi = (1,2,3,4,5,6) \in \mathbb{F}_{13}^6$ and that $\Gamma = (3,8,6,0,7,1) \in \mathbb{F}_{13}^6$. Find the unique polynomial $f \in \mathbb{F}_{13}[x]$ of degree at most 1 such that $f(\Xi)$ agrees with Γ in all but at most 2 coordinates, or conclude that no such f exists.

   Hints: For part (a), we have $f = 7 + 6x + 5x^2 + 4x^3 + 3x^4 \in \mathbb{F}_{11}[x]$, $d = 4$, and $e = 7$. For part (b), we have $d = 1$ and $e = 6$. One possibility to decode is to try out all polynomials f of degree at most 1 over $\mathbb{F}_{13}$. How many such polynomials are there? Another is to use Gao's algorithm.

3. Coinciding pairs of polynomials and polynomial quotient. Let us study the two pairs of polynomials

$$f = 4 + 5x + 3x^2 + 2x^3 + 9x^4 + 8x^5 + x^6 + 3x^7 + 9x^8 + 5x^9 + 7x^{10} \in \mathbb{Z}_{11}[x]\,,$$
$$g = 5 + 7x + 5x^2 + 5x^3 + x^4 + 7x^5 + 4x^6 + 5x^7 + 8x^8 \in \mathbb{Z}_{11}[x]$$

   and

$$\tilde{f} = x^6 + 3x^7 + 9x^8 + 5x^9 + 7x^{10} \in \mathbb{Z}_{11}[x]\,,$$
$$\tilde{g} = 4x^6 + 5x^7 + 8x^8 \in \mathbb{Z}_{11}[x]\,.$$

   Observe that $(f,g) \equiv_4 (\tilde{f},\tilde{g})$. Using the classical algorithm for polynomial division (recall Lecture 1), divide f by g and divide $\tilde{f}$ by $\tilde{g}$. Observe that both divisions produce the same quotient. Using the structure of the classical algorithm, justify why the two divisions must produce the same quotient.

   Hints: Study carefully how the classical division algorithm obtains the coefficients of the quotient, one coefficient at a time. Which coefficients of the dividend and the divisor can have an effect on a particular coefficient of the quotient?

4. Coinciding pairs of polynomials, polynomial quotient, and further coincidence. Let F be a field and let $f,g,\tilde{f},\tilde{g} \in F[x]$ with $\deg f \geq \deg g \geq 0$ and $\deg \tilde{f} \geq \deg \tilde{g} \geq 0$. Suppose that $(f,g) \equiv_{2k} (\tilde{f},\tilde{g})$ for $k \in \mathbb{Z}$ with $k \geq \deg f - \deg g \geq 0$. Define $q,r,\tilde{q},\tilde{r} \in F[x]$ by division with quotients and remainders as follows

$$f = qg + r, \qquad \deg r < \deg g\,,$$
$$\tilde{f} = \tilde{q}\tilde{g} + \tilde{r}, \qquad \deg \tilde{r} < \deg \tilde{g}\,.$$

Prove that we have $q = \tilde{q}$ and at least one of the following holds: $(g, r) \equiv_{2(k-\deg q)} (\tilde{g}, \tilde{r})$ or $r = 0$ or $k - \deg q < \deg g - \deg r$.

Hints: Recall that $(f, g) \equiv_{2k} (\tilde{f}, \tilde{g})$ holds if and only if $f \restriction 2k = \tilde{f} \restriction 2k$ and $g \restriction (2k - (\deg f - \deg g)) = \tilde{g} \restriction (2k - (\deg \tilde{f} - \deg \tilde{g}))$. Show first that without loss generality (by multiplying each pair (f, g) and $(\tilde{f}, \tilde{g})$ with x^m for a nonnegative integer m as necessary), we can assume that $\deg f = \deg \tilde{f}$. Then conclude that $k \geq \deg f - \deg g \geq 0$ implies $\deg g = \deg \tilde{g}$. To show that $q = \tilde{q}$ holds, study the identity

$$f - \tilde{f} = q(g - \tilde{g}) + (q - \tilde{q})\tilde{g} + r - \tilde{r}$$

and seek to control the degrees of the differences $f - \tilde{f}$, $g - \tilde{g}$, and $r - \tilde{r}$ from above. For example, $f \restriction 2k = \tilde{f} \restriction 2k$ and $\deg f = \deg \tilde{f}$ imply that we have $\deg(f - \tilde{f}) < \deg f - 2k$. Finally, show that $r \neq 0$ and $k - \deg q \geq \deg g - \deg r$ together imply $(g, r) \equiv_{2(k-\deg q)} (\tilde{g}, \tilde{r})$.

Deadline and submission instructions. This problem set is due no later than Sunday 24 February 2019, 20:00 (8pm), Finnish time. Please submit your solutions as a single PDF file via e-mail to the lecturer (`petteri.kaski(atsymbol)aalto.fi`). Please use the precise title

```
CS-E4500 Problem Set 5: [your-student-number]
```

with "`[your-student-number]`" replaced by your student number. For example, assuming that my student number is 123456, I would carefully title my e-mail

```
CS-E4500 Problem Set 5: 123456
```

and attach to the e-mail a single PDF file containing my solutions. Please note that the submissions are automatically processed and archived, implying that failure to follow these precise instructions may result in your submission not being graded.