CS-E4500 Advanced Course in Algorithms (5 cr)

Problem Set 1 *Spring 2019*

1. Warmup with univariate polynomials over $\mathbb{Z}_2 = \{0, 1\}$.

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

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

   Hints: Recall that arithmetic in $\mathbb{Z}_2$ is super-easy. We have $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$, $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$, and $1^{-1} = 1$. If you want, you can rely on a computer algebra system, or perhaps implement the algorithms from the lecture slides yourself. Make sure that your solutions are correct and the coefficients are reduced to $\{0, 1\}$.

2. The traditional extended Euclidean algorithm. Present the complete output of the algorithm (as defined in the lecture slides) in the following two cases.

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

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

   Hints: You may want to use a computer algebra system to avoid error-prone manual calculations. Make sure to present the complete output of the algorithm. Refer to Problem 4(d) for the second part of 2(a).

3. Let $\xi_0, \xi_1, \ldots, \xi_d \in F$ be distinct elements in a field F. Show that the 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.

   Hints: For $i = 0, 1, \ldots, d$, define the *Lagrange polynomial* $\ell_i \in F[x]$ by

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

   Observe that the polynomial ℓ_i has degree d and is well defined because the values $\xi_0, \xi_1, \ldots, \xi_d$ are distinct. What happens if you evaluate ℓ_i at $x = \xi_j$? Arrange the coefficients λ_{ik} into a matrix. Show that this matrix is the inverse of Ξ.

4. Analysis of the traditional extended Euclidean algorithm. Suppose we run the algorithm on input $f, g \in E$ in an Euclidean domain E, and obtain the output ℓ, r_i, s_i, t_i for $i = 0, 1, \ldots, \ell + 1$, and q_i for $i = 1, 2, \ldots, \ell$. Introduce the matrices

$$R_0 = \begin{bmatrix} s_0 & t_0 \\ s_1 & t_1 \end{bmatrix} \in E^{2\times 2}\,, \qquad Q_i = \begin{bmatrix} 0 & 1 \\ 1 & -q_i \end{bmatrix} \in E^{2\times 2} \quad \text{for } i = 1, 2, \ldots, \ell,$$

   and $R_i = Q_i Q_{i-1} \cdots Q_1 R_0 \in E^{2\times 2}$ for $i = 0, 1, \ldots, \ell$.

   Show that each of the following invariants holds for all $i = 0, 1, \ldots, \ell$:

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

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

(c) r_ℓ is a greatest common divisor of r_i and r_{i+1}.

(d) $s_i f + t_i g = r_i$.

Hints: Study the steps of the algorithm as presented in the lecture slides. For (a) and (b), use induction on i. Do not forget to verify the base case. For (c), use (a), $r_{\ell+1} = 0$, and the fact that Q_i is invertible with $Q_i^{-1} = \begin{bmatrix} q_i & 1 \\ 1 & 0 \end{bmatrix}$. For (d), study (a) and (b). It is a good idea to solve Problem 2 first and review that the invariants hold in practice.

Deadline and submission instructions. This problem set is due no later than Sunday 20 January 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 1: [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 1: 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.