CS-E4500 Advanced Course in Algorithms (5 cr)

Problem Set 4 *Spring 2019*

1. Secret sharing in action. Select a secret that is an integer between 0 and 99 (inclusive) that you want to share as follows. Split the secret into $s = 10$ shares such that knowledge of any $k = 5$ shares enables one to recover the secret, and knowledge of any $k - 1 = 4$ or fewer shares reveals no information about the secret. Demonstrate the successful recovery of the secret for a concrete choice of k of the shares.

   Hint: Select a large enough prime p and follow Shamir's construction in $\mathbb{Z}_p[x]$.

2. Evaluation via recursive remaindering. Let R be a ring.

   (a) Show that for all $\xi \in R$ and $f \in R[x]$ we have $f(\xi) = f \operatorname{rem} (x - \xi)$.

   (b) Let $a, b, c \in R[x]$, with b and c monic, and suppose that c divides b. Show that $a \operatorname{rem} c = (a \operatorname{rem} b) \operatorname{rem} c$.

   Hints: Recall that the quotient and remainder are unique for $a, b \in R[x]$ with b monic. Use the defining equality $a = qb + r$ with $\deg r < \deg b$ for both parts. For part (a), investigate what happens when you evaluate the defining equality at ξ.

3. Preliminaries for fast interpolation. Let R be a ring, let $\xi_0, \xi_1, \ldots, \xi_{e-1} \in R$, and $\lambda_0, \lambda_1, \ldots, \lambda_{e-1} \in R$ be given as input. The form of the Lagrange interpolation polynomial (4) suggests that one should first seek to construct the coefficients of the polynomial

   $$\ell = \sum_{i=0}^{e-1} \lambda_i \prod_{\substack{j=0 \\ j \neq i}}^{e-1} (x - \xi_j) \in R[x] \,. \tag{1}$$

   Show that we can compute the coefficients of ℓ in $O(M(e) \log e)$ operations in R. You may assume that $e = 2^k$ for a nonnegative integer k. Here $M(e) = e \log e \log \log e$.

   Hints: Work with binary strings and the representation of the perfect binary tree using binary strings in $\{0,1\}^{\underline{k}}$. To construct the coefficients of the polynomial (1), first construct a subproduct tree with polynomials s_u for all $u \in \{0,1\}^{\underline{k}}$ from $\xi_0, \xi_1, \ldots, \xi_{e-1}$ as during fast evaluation. Next, annotate the tree with another family of polynomials such that the polynomial at the root will be equal to (1). You may want to try associating with each leaf $v \in \{0,1\}^k$ the polynomial

   $$\ell_v = \lambda_v \tag{2}$$

   and with each internal node $u \in \{0,1\}^{\underline{k-1}}$ the polynomial

   $$\ell_u = \ell_{u0} s_{u1} + s_{u0} \ell_{u1} \,. \tag{3}$$

   Why is this a good choice? Prepare a small example, say with $k = 2$ or $k = 3$ as necessary. Show that $\ell_\epsilon = \ell$, where ϵ is the empty binary string.

4. Fast interpolation via subproducts and fast evaluation. Let R be a ring and let $\xi_0, \xi_1, \ldots, \xi_{e-1} \in R$ and $\eta_0, \eta_1, \ldots, \eta_{e-1} \in R$ such that $\xi_i - \xi_j$ is a unit in R for all

$0 \le i < j \le e-1$. Show that we can compute the coefficients of the Lagrange interpolation polynomial

$$\ell = \sum_{i=0}^{e-1} \left(\eta_i \prod_{\substack{j=0\\ j\neq i}}^{e-1} (\xi_i - \xi_j)^{-1} \right) \prod_{\substack{j=0\\ j\neq i}}^{e-1} (x - \xi_j) \in R[x] \tag{4}$$

that satisfies $\ell(\xi_i) = \eta_i$ for all $i = 0, 1, \ldots, e-1$ in $O(M(e)\log e)$ operations in R. You may assume that $e = 2^k$ for a nonnegative integer k.

Hints: Apply your solution to Problem 3 in two passes. In the first pass, set $\lambda_v = 1$ for all $v \in \{0,1\}^k$ and compute the coefficients of the polynomial $f = \ell_\epsilon$ using (2) and (3). Evaluate f at $\xi_0, \xi_1, \ldots, \xi_{e-1}$ using fast evaluation. Then do a second pass (with a different choice for the values λ_v) so that at the root you recover the Lagrange interpolation polynomial (4).

Deadline and submission instructions. This problem set is, exceptionally, due no later than Monday 11 February 2019, 13:00 (1pm), 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 4: [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 4: 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.