universität innsbruck

Program Verification	SS 2024	LVA 703083+703084
Sheet 12		Deadline: June 18, 2024, 3pm

- Prepare your solutions on paper.
- Mark the exercises in OLAT before the deadline.
- Marking an exercise means that a significant part of that exercise has been treated.

Exercise 1 *Recording Completion with Intermediate Equations* **5 p.**

Consider some initial (numbered) equations $\mathcal{E}$ with initial numbers N. The idea of recording completion is to generate new equations from existing ones in the following way: one somehow combines two steps with equations (i) and (j) to derive a new equation e. This new equation is added to the set of equations using some fresh number (k), and it is recorded that (k) was generated via (i) and (j), by adding the triple (k, i, j) to the history H, which is initially empty.

Full expansion of some generated equation is now repeatedly expanding each step $s \overset{k}{=} t$ by the two steps $s \overset{i}{=} u \overset{j}{=} t$ whenever $(k, i, j) \in H$ to get some equational steps $s =^*_{\mathcal{E}} t$.

Since full expansion might trigger an exponential increase in the number of steps, we want to support certification in the following way.

- The certificate contains all numbered equations $\mathcal{E}'$ that are generated during the recording completion run, and it also contains the full history H.
- For each equation $s = t \in \mathcal{E}'$ with number (k), such that $k \notin N$, it is checked that there are i, j, u such that (k, i, j) is in the history, and $s \overset{i}{=} u \overset{j}{=} t$

After successful certification, we would like to have ensured that each $s = t \in \mathcal{E}'$ is a consequence of $\mathcal{E}$, i.e., $s =^*_{\mathcal{E}} t$.

Is this property satisfied?

- If the answer is yes, then sketch a proof of the property.
- If the answer is no, then provide a counterexample, and modify the certification algorithm accordingly (without proof).

Note that a single equation might be applied from left to right, or from right to left.

Exercise 2 *Matrix Multiplication* **5 p.**

Given two matrices A and B, it is hard too see how to speed up a verified computation of $A \times B$ with the help of a certificate.

Now consider a list of matrices $A_1, A_2, \ldots, A_n$ of compatible dimensions, i.e., there is a list $d_1, \ldots, d_{n+1}$ such that A_i has dimensions $d_i \times d_{i+1}$ for each i.

Is there a possibility to speed up a verified computation of $A_1 \times \cdots \times A_n$ with the help of a certificate?

- If your answer is yes, then briefly explain the structure of the certificate and how it can help to speed up the computation.
- If your answer is no, then think about associativity of matrix multiplication and rethink your answer.

Exercise 3 *Factorization* **5 p.**

Consider a ring with 1-element. An element e is a unit, if there is some f such that $e \cdot f = 1$.
An element e is irreducible, if it is not a unit, it is not 0, and it cannot be decomposed into $e = f \cdot g$ for two non-units f and g.
A factorization of some non-unit and non-zero element e is of the form $e = f_1 \cdot \ldots \cdot f_n$ such that each f_i is not a unit, and each f_i is irreducible.
Examples

- In the ring of integers, the units are exactly 1 and -1, the irreducible elements are exactly the prime numbers and the negated prime numbers, and a factorization is a prime factorization, e.g., $1692197 = 13 \cdot 13 \cdot 17 \cdot 19 \cdot 31$.
- In the ring of univariate rational polynomials, the units are exactly non-zero polynomials of degree 0, every polynomial of degree 1 is irreducible, and a factorization of $x^{10} - 1$ is $(x-1)(x+1)(x^4 - x^3 + x^2 - x + 1)(x^4 + x^3 + x^2 + x + 1)$.

Design a potential certification algorithm for at least one of the given examples:

- factorization in the ring of integers
- factorization in the ring of univariate rational polynomials

Answer the following questions:
Which parts can easily be verified? Which parts are hard? Can you figure out the complexity class of the certification algorithm.

Exercise 4 *SCCs* **5 p.**

Recall: a set of nodes N in a directed graph $G = (V, E)$ is strongly connected iff from every node in N there is a path in G to every other node of N.
In the lecture a potential certificate to ensure strongly connectedness of N was proposed. It consists of a cyclic path in G such that the set of nodes on this path contains N.
The problem with this certificate is that the cyclic path might be of size $\Theta(|N|^2)$ even if $|E|$ is linear in $|V|$.
Figure out a graph where this problem occurs, and design an alternative certificate format to ensure connectedness of N that has size $\mathcal{O}(|N|)$. What must be checked?
For simplicity you can assume $N = V = \{1, \ldots, n\}$.