SS 2010 2010/04/29

Exercises to the Lecture Computer Algebra
Sheet 3

Prof. Dr. Klaus Madlener Delivery until 2010/05/07

Exercise 1: [Rings]

a) Let R, S be integral domains. Is the ring $R + S$ (the direct sum) also an integral domain?

b) Let $I = \{f \in \mathbb{R}[x] \mid f(5) = 0\}$ be the set of all real-valued polynomials that have 5 as a root. Prove that I is an Ideal in $\mathbb{R}[x]$ and find an isomorphism $\mathbb{R}[x]/I \to \mathbb{R}$.

Exercise 2:

a) Determine (in $\mathbb{Z}[[x]]$) the inverse of the formal power series

$$a(x) = \sum_{k=0}^{\infty} a_k x^k = 1 + x + 2x^2 + 3x^3 + 5x^4 + \cdots$$

with $a_k = a_{k-1} + a_{k-2}$ for $k \geq 2$.

Exercise 3: [Simplifikation]

a) Consider the following "'Definition"' of an *expanded canonical form* of multivariate polynomial terms over an integral domain D:

1. expand all products of polynomials
2. collect terms of the same degree
3. sort terms by degree in descending order

Is this a canonical simplifier according to the definition from the lecture? What Information do you need in order to answer the question. Is the above definition unique?

Apply the definition to the following term:

$$\begin{aligned} a(x,y) &= ((x^2 - xy + x) + (x^2 + 3) \cdot (x - y + 1)) \cdot \\ &\quad ((y^3 - 3y^2 - 9y - 5) + x^4 \cdot (y^2 + 2y + 1)) \end{aligned}$$

b) "'Simplify"' the following terms:

– $a(x,y) = \dfrac{1}{x^9 + x^8y + x^7y^2 + x^6y^3 + x^5y^4 + x^4y^5 + x^3y^6 + x^2y^7 + xy^8 + y^9}$

– $b(x,y) = \dfrac{x-4}{x^5+x^4y+x^3y^2+x^2y^3+xy^4+y^5} - \dfrac{x^2-xy+y^2}{x^6-y^6}$

c) We consider a free monoid $M = (\Sigma, \circ)$, where the Elements are the strings over the alphabet Σ, the netral element ϵ is the empty string and $\circ$ is an associative mapping from tuples of strings to a string with $a \circ b = ab, a, b \in \Sigma^*$. For a $w \in M$ let $(w)^n, n \in \mathbb{N}_+$ be defined by $(w)^1 = w$ and $(w)^n = w(w)^{n-1}$. What do normal forms (of minimal length) of strings in M look like? I.e. given an arbitrary string, how can you find another string with a minimal number of symbols that represents the same string? Can you find an efficient algorithm that computes such normal forms?

Exercise 4: [Potenzen]

Let $n \in \mathbb{N}^+$. An addition chain for n is a finite sequence of positive integers $a_0, \ldots, a_r$ with $a_0 = 1$, $a_r = n$, and for all $i = 1, \ldots, r$ there are j and k with $k \leq j < i$, such that $a_i = a_j + a_k$. r denotes the length of the addition chain and $l(n)$ is the minimal length of an addition chain for n.

a) How are $l(n)$ and the computation of x^n related? Does the binary method to compute x^n always use a minimal number of multiplications?

b) Let $s(n)$ be the sum of the bits in the binary representation of n (i.e. the number of 1). Prove $l(n) \leq \lfloor \log_2 n \rfloor + s(n) - 1$ and $l(mn) \leq l(m) + l(n)$.

c) Let $a > b \geq 0$ be integers. Show that $l(2^a) = a$ and $l(2^a + 2^b) = a + 1$.

Exercise 5: [Fibonacci]

a) We want to compute the Fibonacci numbers F_k modulo $n \in \mathbb{N}$. Find an asymptotic upper bound for the number of bit operations of a simple method to compute F_k modulo n.

A different method makes use of the fact that F_{k+1} can be computed in the following way gewinnen lässt:

$$\begin{pmatrix} F_{k+1} & F_k \\ F_k & F_{k-1} \end{pmatrix} = \begin{pmatrix} F_k & F_{k-1} \\ F_{k-1} & F_{k-2} \end{pmatrix} \cdot X,$$

where you have to specify X. Refine this method to compute F_k modulo n and find an asymptotic upper bound for the number of bit operations.

b) Show how to compute $1+x+\cdots+x^{n-1} \bmod m$ for $x, n, m \in \mathbb{N}^+$ with $O(\lambda(n)\lambda(m)^2)$ bit operations in the worst case. Mind the case that m is not a prime.