Manuel Kauers
RISC-Linz Hagenberg, December 17, 2002

# Computer Algebra Exercises
# Solution 2

**Ex. (6)** By the definition of polynomial multiplication,

$$\Big(\sum_{i=0}^{r} u_i x^i\Big) \cdot \Big(\sum_{i=0}^{s} v_i x^i\Big) = \sum_{i=0}^{r+s} c_i x_i \qquad \text{with} \qquad c_i = \sum_{k=0}^{i} u_k \cdot v_{i-k}$$

where $u_k, v_k = 0$ for $k < 0$ or $k$ greater than the polynomial's degree.

The sum in the definition of $c_i$ can have at most $\min\{r,s\}$ summands: If $k > \min\{r,s\}$, then $k - \min\{r,s\}$ coefficients of the shorter polynomial vanish. It follows, that

$$\begin{aligned} |c_{\max}| &= |\sum_{k=0}^{\min\{r,s\}} u_k \cdot v_{i-k}| \leq \sum_{k=0}^{\min\{r,s\}} |u_k \cdot v_{i-k}| \leq \sum_{k=0}^{\min\{r,s\}} m_1 m_2 \\ &= \min\{r,s\} \cdot m_1 \cdot m_2. \end{aligned}$$

It is obvious that this bound is sharp, just consider the special example $u_i = m_1$ $(i = 0, \ldots, r)$, $v_i = m_2$ $(i = 0, \ldots, s)$. ■.

**Ex. (7)** Let $F$ be a finite field, and $p, q \in F[x]$ of degree less than or equal to $n$. Write them as

$$p = p_1 X^{n/2} + p_0, \qquad q = q_1 X^{n/2} + q_0.$$

Then, according to KARATSUBA's trick, we compute $p_1 \cdot q_1$, $p_0 \cdot q_0$, and $(p_0 + p_1) \cdot (q_0 + q_1)$ recursively and return

$$p_1 \cdot q_1 X^n + ((p_0 + p_1) \cdot (q_0 + q_1) - p_0 \cdot q_0 - p_1 \cdot q_1) X^{n/2} + p_0 \cdot q_0$$

which is equal to $p \cdot q$.

Since $F$ is finite, arithmetic operations on coefficients are of constant cost, and so the complexity function is defined by the recurrence

$$T(1) = \mathrm{O}(1), \qquad T(n) = 3T(n/2) + \mathrm{O}(n)$$

which, by use of the Master Theorem, leads to $T(n) = \mathrm{O}(n^{\log_2 3})$ as desired.

**Ex. (8)** Given the following two polynomials over the integers:

$$u(x) = x^6 + x^5 - x^4 + 2x^3 + 3x^2 - x + 2, v(x) = 2x^3 + 2x^2 - x + 3 \in \mathbb{Z}[x].$$

We want to compute pseudo quotient and pseudo remainder of $u$ and $v$.

$$
\begin{array}{rl}
2^3\cdot(\ x^6 + x^5 - x^4 + 2x^3 + 3x^2 - x + 2) = v(x)\cdot(4x^3-2x+4) \\
-\underline{(8x^6+8x^5-4x^4+12x^3)} \qquad\qquad\qquad + (14x^2+2x+4). \\
-4x^4 + 4x^3 + 24x^2 - 8x + 16 \\
-\underline{(\ -4x^4 - 4x^3 + 2x^2 - 6x)} \\
8x^3 + 22x^2 - 2x + 16 \\
-\underline{(\ \ 8x^3 + 8x^2 - 4x + 12)} \\
14x^2 + 2x + 4
\end{array}
$$

It turns out that

$$
\begin{aligned}
\operatorname{pquot}(u,v) &= 4x^3 - 2x + 4,\\
\operatorname{prem}(u,v) &= 14x^2 + 2x + 4.
\end{aligned}
$$

**Ex. (9)** Evaluation of a polynomial at a certain point along the definition of the polynomial, i.e. evaluation of terms which are sumed up, takes $\mathrm{O}(n^2)$ multiplications: Evaluation of one term takes up to $\mathrm{O}(n)$ steps, and there are $n$ terms. To sum up $n$ terms, we need $\mathrm{O}(n)$ additions.

On the other hand, evaluation of a polynomial by HORNER's scheme takes only $\mathrm{O}(n)$ additions and multiplications: Both, the number of additions and multiplications satisfy the recurence relation

$$T(n) = T(n-1) + \mathrm{O}(1)$$

which clearly means $T(n) = \mathrm{O}(n)$.

HORNER's rule can be viewed as polynomial division by linear monic divisors. (However, it can also be generalized to non-linear divisors.) By direct evaluation, one sees that the parenteses evaluate to the coefficients of $p(x)/(x-\alpha)$. The remainder of this division is $p(\alpha)$.

$$(a_n x^n + a_{n-1}x^{n-1} + \dots) : (x-\alpha) = a_n x^{n-1} + (a_{n-1} + \alpha a_n)x^{n-1} + \dots$$

**Ex. (10)** First, we compute $p_1 = a\cdot b$ by the classical algorithm.

$$
\begin{array}{r}
(\alpha^3+\alpha+2)\cdot\ \ (3\alpha^4 \qquad + 2\alpha^2\ - \alpha) \\
\hline
3\alpha^7 + 3\alpha^5 + 6\alpha^4 \qquad\qquad\qquad\qquad \\
2\alpha^5 \qquad + 2\alpha^3 + 4\alpha^2 \qquad \\
- \alpha^4 \qquad\quad - \alpha^2 - 2\alpha \\
\hline
3\alpha^7 + 5\alpha^5 + 5\alpha^4 + 2\alpha^3 + 3\alpha^2 - 2\alpha
\end{array}
$$

Over $\mathbb{Q}[x]/(x^5-3)$, this result reduces to

$$a\cdot b = 5\alpha^4 + 2\alpha^3 + 12\alpha^2 - 2\alpha + 15.$$

Now, we use MAPLE to compute $c^{-1}$ using the extended Euclidian algorithm. This leads to

$$c^{-1} = \tfrac{1}{3691}(-128\alpha^4 + 281\alpha^3 - 69\alpha^2 + 411\alpha + 280).$$

Finally, using again MAPLE, we find

$$(a\cdot b)/c = \tfrac{1}{3691}(-1088\alpha^4 + 7925\alpha^3 + 4950\alpha^2 + 1648\alpha + 20835).$$