Murray Bremner

Page 328  line -2, proof of Theorem 12.2: Lemma 8.2 is not general enough to imply the first claim; see the correction for page 222. (MURRAY BREMNER, 29. 10. 2003)

Winfried Bruns

Page 156  line –5, Lemma 6.25: replace \(\mathrm{lc}(f)/B^4\) by \(\mathrm{lc}(f)/B^4\) is not a zero divisor (WINFRIED BRUNS, 10. 6. 2003)

Olav Geil

Page 38  line 17: 260, not 26 (OLAV GEIL, 12. 10. 2003)

Page 104  line 13: the reference should be to Section 3.1 instead of 2.4 (OLAV GEIL, 12. 10. 2003)

Page 226  line 6, Lemma 8.7: replace \(1/B_0/B_0^m\) by \(1/B_0/B_0^m\) (OLAV GEIL, 27. 10. 2003)

Page 228  line –7: \(R[x]\), not \(F[x]\) (OLAV GEIL, 27. 10. 2003)

Page 247  line –22, Exercise 8.10 (iv): replace \(V_1/B_0/B_0/V_1\) by \(V_1/f/B_1/V_1\) (identifying the polynomials \(f, g\) with their coefficient vectors) (OLAV GEIL, 12. 10. 2003)

Stefan Gerhold

Page 485  line 2, Notes 16.2 and 16.3: insert is after “it” (STEFAN GEROHLD, 16. 7. 2003)

Tom Koornwinder

Page 256  line –8, proof of Theorem 9.4: replace \(f, g\) by \(f, g, -1\) (TOM KOORNWINDER, 6. 3. 2003)

Page 404  line 4, proof of Theorem 14.49: replace the formula by

\[
 f_r(x^{m/i}) = \Phi_m(x^{m/i}) = \Phi_n,
\]

(TOM KOORNWINDER, 6. 3. 2003)

Page 592  line –11, proof of Theorem 21.18: \((\alpha_1, \ldots, \alpha_n) \in B, not \in A\) (TOM KOORNWINDER, 24. 4. 2003)

Heiko Körner

Page 51  line –8: \(\ell > 2\) instead of \(\ell \geq 2\) (HEIKO KÖRNER, 17. 12. 2002)

Page 52  line 9: add \(if n \geq 1\)

line 10, equation (8): \(\ell = n - 1\), not \(\ell = n\) (HEIKO KÖRNER, 17. 12. 2002)
Addenda and corrigenda, 2003 edition

Page 72  line 14, Lemma 4.5: $K$ is an extension field of $F$ (HEIKO KÖRNER, 19. 2. 2003)

Page 100 line –5, Theorem 5.1: $7n^2 - 7n$ instead of $7n^2 - 8n + 1$ (HEIKO KÖRNER, 19. 2. 2003)
line –1, proof of Theorem 5.1: this formula should read
\[ \sum_{1 \leq i < n} 2i = n^2 - n \]
(HEIKO KÖRNER, 19. 2. 2003)

Page 101 lines 1–5, proof of Theorem 5.1: replace this paragraph by:

\[ \text{arithmetic operations. Then for each } i, \text{ we divide } m \text{ by } m_i, \text{ taking } 2n - 2 \text{ operations (Exercise 5.3), evaluate } m/m_i \text{ at } u_i, \text{ taking at most } 2n - 3 \text{ operations since } m/m_i \text{ is monic, and divide } v_i \text{ by that value. This amounts to } 4n^2 - 4n \text{ operations for all } i. \text{ Finally, computing the linear combination (3) takes another } 2n^2 - 2n \text{ operations, and the estimate follows by adding up.} \]
(HEIKO KÖRNER, 19. 2. 2003)

Page 119 line 1: $t = x/2$, not $t = -x/2$ (HEIKO KÖRNER, 19. 2. 2003)
Page 124 line 6: $t = \alpha t_j^*$ instead of $t = \alpha t_j$ (HEIKO KÖRNER, 19. 2. 2003)
Page 125 line –9: $q = 2$ instead of $q = 1$ (HEIKO KÖRNER, 19. 2. 2003)
Page 127 line 4, proof of Lemma 5.29: replace (33) by (34) (HEIKO KÖRNER, 19. 2. 2003)
Page 155 line 1: replace Gauß’ lemma 6.6 by Corollary 6.10 (HEIKO KÖRNER, 25. 4. 2003)

Volker Krummel

Page 590 line 13, Example 21.10 (continued): this should read $-(x^2y - x)$, not $-(xy^2 - x)$ (VOLKER KRAMMEL, 19. 2. 2003)

Eugene Luks

Page 476 line 12: replace $q^* = q^{**} + r^{**}$ by $r^* = q^{**}u + r^{**}$ (EUGENE LUKS, 1. 12. 2002)

Olga Mendoza

Page 212 line –5, Example 7.4 (continued): the Padé approximant is $v/u$ and not $u/v$ (OLGA MENDOZA, 18. 4. 2003)

Helmut Meyn

Page 456 line –20, Exercise 15.10 (v): $a_{n,r} = 0$ instead of $a_{nr} = 0$ (HELMUT MEYN, 9. 9. 2003)
line –18, Exercise 15.10 (v): replace $1 \leq k \leq n \leq 8$ by $1 \leq r \leq n \leq 8$ (HELMUT MEYN, 9. 9. 2003)
Olaf Müller


Page 661 line –4, Exercise 23.4 (iii): This line should read

\[ f = \sum_{0 \leq i < n} \frac{(\Delta_i f)(0)}{h^i} x(x-h) \cdots (x-ih+h), \]

(OLAF MÜLLER, 12. 8. 2003)

Kathy Sharrow

Page 92 line –16, Exercise 4.30 (i): replace max\{\nu(f), \nu(g)\} by min\{\nu(f), \nu(g)\} (KATHY SHARROW, 21. 2. 2002)

Huang Yong

Page 108 line 10: see page 140 for a justification of this formula (HUANG YONG, 9. 4. 2002)

The authors
The following figure is missing: (8. 8. 2003)

**Fast multiplication**

<table>
<thead>
<tr>
<th>multiplication algorithm</th>
<th>time $\mathcal{M}(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>classical</td>
<td>$2n^2$</td>
</tr>
<tr>
<td>Karatsuba</td>
<td>$O(n^{1.59})$</td>
</tr>
<tr>
<td>Schönhage &amp; Strassen</td>
<td>$O(n \log n \log \log n)$</td>
</tr>
</tbody>
</table>

**Fast integer and polynomial arithmetic**

<table>
<thead>
<tr>
<th>task</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>multiplication (§8.1)</td>
<td>$O(\mathcal{M}(n))$</td>
</tr>
<tr>
<td>division with remainder (§9.1)</td>
<td></td>
</tr>
<tr>
<td>modular multiplication (§9.1)</td>
<td></td>
</tr>
<tr>
<td>radix conversion (§9.2)</td>
<td>$O(\mathcal{M}(n) \log n)$</td>
</tr>
<tr>
<td>multipoint evaluation (§10.1)</td>
<td></td>
</tr>
<tr>
<td>interpolation (§10.2)</td>
<td></td>
</tr>
<tr>
<td>reduction modulo several moduli (§10.3)</td>
<td>$O(\mathcal{M}(n) \log n)$</td>
</tr>
<tr>
<td>Chinese Remainder Algorithm (§10.3)</td>
<td></td>
</tr>
<tr>
<td>Extended Euclidean Algorithm (§11.1)</td>
<td></td>
</tr>
<tr>
<td>modular inversion (§11.1)</td>
<td></td>
</tr>
</tbody>
</table>

Classical arithmetic: time $O(n^2)$ for all tasks (Chapters 2–5)
Lemma 8.2 is correct but not general enough to cover its application in Theorem 12.2. If you are interested in that Theorem, you may replace Lemma 8.2 and its proof by:

**Lemma 8.2.** Let \( b, c \in \mathbb{R}_{>0}, d \in \mathbb{R}_{\geq 0}, S, T : \mathbb{N} \rightarrow \mathbb{N} \) be functions with \( S(2n) \geq cS(n) \) for all \( n \in \mathbb{N} \), and

\[
T(1) = d, \quad T(n) \leq bT(n/2) + S(n) \quad \text{for } n = 2^i \text{ and } i \in \mathbb{N}_{\geq 1}.
\]

Then for \( i \in \mathbb{N} \) and \( n = 2^i \) we have

\[
T(n) \leq \begin{cases} 
dn \log b + S(n) \log n & \text{if } b = c, \\
dn \log b + \frac{c}{n^c} S(n) (n^{\log (b/c)} - 1) & \text{if } b \neq c.
\end{cases}
\]

In particular, if \( n^{\log c} \in O(S(n)) \), then \( T(n) \in O(S(n) \log n) \) if \( b = c \), and \( T(n) \in O(S(n) n^{\log (b/c)}) \) if \( b > c \).

**Proof.** Unraveling the recursion, we obtain inductively

\[
T(2^i) \leq bT(2^{i-1}) + S(2^i) \leq b(bT(2^{i-2}) + S(2^{i-1})) + S(2^i) \leq b^2 T(2^{i-2}) + bS(2^{i-1}) + S(2^i) \leq \cdots
\]

\[
\leq b^i T(1) + \sum_{0 \leq j < i} b^j S(2^{i-j}) \leq \sum_{0 \leq j \leq i} b^j \left( \frac{b}{c} \right)^j \sum_{0 \leq j < i} b^j S(2^{i-j}) \leq d^{i+1} b^{\log b} + S(2^i) \sum_{0 \leq j < i} \left( \frac{b}{c} \right)^j,
\]

where we have used that \( S(2^{i-j}) \leq c^{-j} S(2^i) \) in the last inequality. If \( b = c \), then the last sum simplifies to \( S(2^i) \cdot i \). If \( b \neq c \), then we have a geometric sum

\[
\sum_{0 \leq j < i} \left( \frac{b}{c} \right)^j = \left( \frac{b}{c} \right)^i - 1 = \frac{c}{b-c} (2^i (\log (b/c)) - 1),
\]

and the first claim follows. □

(29.11.2003)
Figure 14.5: The labels in this figure are left-shifted too far. The figure with correct labels is:

\[
\begin{array}{cccccccccccccccc}
0 & 1 & 2 & x & x^2 & x^3 & x^4 & x^5 & x^6 & x^7 & x^8 & x^9 & x^{10} & x^{11} & x^{12} \\
2x^2 & 2x^3 & x^3 \pm 2x^2 & x^3 + x^2 & x^2 & x^3 & 2x^3 + x^2 & 2x^3 + 2x^2 & 2x + 2 & 2x & x + 1 & x + 2 & 2 & 1 & 0
\end{array}
\]

Figure 14.5: The lucky and unlucky choices for factoring \(x^4 + x^3 + x - 1 \in F_5[x]\). (8. 8. 2003)

Page 376

Page 619

Page 623

Page 624

Page 625

Page 636

Page 753

Modern Computer Algebra, JOACHIM VON ZUR GATHEN and JÜRGEN GERHARD, version 30 November 2003