Algorithmic Algebra

Bhubaneswar Mishra

Courant Institute of Mathematical Sciences

Errata

Following corrections need to be made to the book "Algorithmic Algebra" (Author: Bhubaneswar Mishra, Publisher: Springer-Verlag, ISBN 0-387-**94090**-1, ISBN 3-540-**94090**-1).

Last updated August 16, 1995.

pp. viii The e-mail address at the bottom of the page should be corrected from "mishra@nyu.edu.arpa" to "mishra@cs.nyu.edu." [3].

pp. 8 The word "Staring" (¶4, line 1) should be corrected to "Starting." [2]. The spelling of the name "Engleman" (¶4, line 3) should be corrected to "Engelman." [3].

pp. 40 In the statement of Proposition 2.2.4 (item 1), the line

$$pq \underset{\mathrm{L}}{\leq} p'q', \quad \text{where } p, p \in \mathrm{PP}(X) \text{ and } q, q' \in \mathrm{PP}(Y),$$

should be corrected to

$$pq \underset{\mathrm{L}}{\leq} p'q', \quad \text{where } p, p' \in \mathrm{PP}(X) \text{ and } q, q' \in \mathrm{PP}(Y).[6]$$

pp. 83 The statement "$\mathsf{return}\ f - \sum_{g_i \in G} a_i \cdot \frac{\mathrm{Hterm}(f)}{\mathrm{Hterm}(g_i)} \cdot g_i;$" in the else part of the if -statement in the routine OneHeadReduction should be modified to "$\mathsf{return}\ f - \sum_{g_i \in G_f} a_i \cdot \frac{\mathrm{Hterm}(f)}{\mathrm{Hterm}(g_i)} \cdot g_i;$" [4]

pp. 108 In the "Hint" for Problem 3.2, add the additional assumption that $x \underset{\mathrm{TLEX}}{<} y$. [6]

pp. 150 In the algorithm FindZeros, the line

$$X_{n-1} := \{\langle \xi_n \rangle \ : \ p(\xi_n) = 0\};$$

should be as follows:[6]

$$X_{n-1} := \{\langle \xi_n \rangle \ : \ p_{n-1}(\xi_n) = 0\};$$

pp. 202 In the line starting with "More explicitly, the second condition ...", (¶4) the statement "If $a = p_1 \cdots p_m = q_1 \cdots q_m$," should read "If $a = p_1 \cdots p_m = q_1 \cdots q_n$,' instead. [5]

pp. 226 The word "resultant" (¶4, line 2) should read "resultants."[2]

pp. 230 At the end of the first half of the proof of lemma 7.2.2 (¶4), the following lines should be added: [2]

Thus at least one of $T(x)$ and $U(x)$ must be nonzero. But the equation

$$A(x) \cdot T(x) + B(x) \cdot U(x) = 0$$

can only hold when either both $T(x)$ and $U(x)$ are zero or both are nonzero.

pp. 231 Delete the inequation "$t_{n-1} \neq 0$," at the end of line 4 (¶1) and similarly, the inequation "$u_{m-1} \neq 0$." at the end of the next line.[2]

pp. 236 On line 4 (¶2), the last subscript in $L[x_1, \ldots, x_{r-1}]$ should be r instead of $r - 1$. [2]

pp. 254 In the CASE 2 ($i = \lambda$) of Proposition 7.7.1, the formula should read as follows:[2]

$\mathrm{SubRes}_\lambda(A, B)$

$$= \begin{cases} \mathrm{DetPol}\left(x^{n-m-1}A, \ldots, xA, A\right) \\ = \mathrm{Hcoef}(A)^{n-m-1} \cdot A, & \text{if } \deg(B) > \deg(A) + 1; \\ \\ \mathrm{DetPol}\left(x^{m-n-1}B, \ldots, xB, B\right) \\ = \mathrm{Hcoef}(B)^{m-n-1} \cdot B, & \text{if } \deg(A) > \deg(B) + 1. \end{cases}$$

pp. 267 In the sentence beginning with "Note that ...," the expression "$S_{i-1} \neq 0$" (¶1, line 3) should be corrected to "$S_{i+1} \neq 0$."[2]

pp. 268 In the statement of Theorem 7.9.1, after the first paragraph, the following sentence should be added: "*Let R_j $(0 \leq j \leq n+1)$ be the j^{th} principal subresultant coefficient of S_{n+1} and S_n.*" [2]

pp. 284 The exponent of the term a_m (¶1, line 3) should be $n - k$ instead of $n - m$, where $k = \deg(R)$.[2]. That is the item 3 should read:

If $m \leq n$ and $R(x)$ is the remainder of $B(x)$ with respect to $A(x)$ [i.e., $B(x) = Q(x) \cdot A(x) + R(X)$, $\deg(R) = k$ is minimal], then

$$\text{Resultant}(A, B) = a_m^{n-k} \text{Resultant}(A, R).$$

pp. 309 In Definition 8.4.1, (¶4, line 1) the phrase "In general, If ..." should read "In general, if ...'

pp. 324 The line "$f(x) \in \mathbb{Z}[x]\}$; $\deg(f) = n$" in the **Input** specification of the routine RootIsolation should read "$f(x) \in \mathbb{Z}[x]$; $\deg(f) = n$." [5]

pp. 327 The line "...we may require $f(x)$ to be a minimal polynomial α..." (¶2, line 1) should read "...we may require $f(x)$ to be a minimal polynomial of α..."

pp. 334–335 The terms "sentence(s)" should be replaced by "formula(s)" in lines 26 and 28 on page 334 and 8, 9, 10, 14, 17, 18, 19, 22, 24 and 29 on page 335. [7]

pp. 335 In the paragraph after Proposition 8.6.1, (¶7, line 2), the phrase "...a more detailed discussion of Tarski sentences..." should read "...a more detailed discussion of Tarski formulas and sentences..." [7]

pp. 338 The second paragraph should now read: "While real algebraic sets are quite interesting as they would be natural objects of study in this context, *they are not closed under projection onto a subspace*. Hence, they tend to be unwieldy."[7]

pp. 339–341 The initial portion of the subsection **Delineability** (§§8.6.2) starting on page 339 and up to the ¶2 on page 341 should be replaced by the following text. [1]

8.6.2 Delineability

Let $f_i(x_1, \ldots, x_{n-1}, x_n) \in \mathbb{R}[x_1, \ldots, x_{n-1}, x_n]$ be a polynomial in n variables:

$$\begin{aligned} f_i(x_1, \ldots, x_{n-1}, x_n) &= f_i^{d_i}(x_1, \ldots, x_{n-1})\, x_n^{d_i} \\ &\quad + \cdots + f_i^0(x_1, \ldots, x_{n-1}), \end{aligned}$$

where f_i^j's are in $\mathbb{R}[x_1, \ldots, x_{n-1}]$. Let $p' = \langle \xi_1, \ldots, \xi_{n-1} \rangle \in \mathbb{R}^{n-1}$. Then we write

$$f_{i,p'}(x_n) = f_i^{d_i}(p')\, x_n^{d_i} + \cdots + f_i^0(p'),$$

for the univariate polynomial obtained by substituting p' for the first $(n-1)$ variables.

Let $0 \leq k_i \leq d_i$ then we write $\widehat{f}_i^{k_i}(x_1, \ldots, x_{n-1}, x_n)$ to denote

$$\begin{aligned}\widehat{f}_i^{k_i}(x_1, \ldots, x_{n-1}, x_n) &= f_i^{k_i}(x_1, \ldots, x_{n-1})\, x_n^{k_i} \\ &\quad + \cdots + f_i^0(x_1, \ldots, x_{n-1}).\end{aligned}$$

Thus, if $f_i^{d_i}(p') = \cdots = f_i^{k_i+1}(p') = 0$ and $f_i^{k_i}(p') \neq 0$, then

$$f_{i,p'}(x_n) = \widehat{f}_i^{k_i}(p') = f_i^{k_i}(p')\, x_n^{k_i} + \cdots + f_i^0(p').$$

Definition 8.6.4 (Delineable Sets) Let

$$\mathcal{F} = \left\{ \begin{array}{l} f_1(x_1, \ldots, x_n), \\ f_2(x_1, \ldots, x_n), \\ \vdots \\ f_s(x_1, \ldots, x_n) \end{array} \right\} \subseteq \mathbb{R}[x_1, \ldots, x_n]$$

be a set of s n-variate real polynomials. Let $C \subseteq \mathbb{R}^{n-1}$ be a nonempty set homeomorphic to $\mathbb{R}^\delta$ $(0 \leq \delta \leq n-1)$.

We say $\mathcal{F}$ is *delineable* on C (or, C is $\mathcal{F}$-*delineable*), if it satisfies the following invariant properties:

1. For every $1 \leq i \leq s$, the *total number of complex roots* of $f_{i,p'}$ (counting multiplicity) remains invariant as p' varies over C.
2. For every $1 \leq i \leq s$, the *number of distinct complex roots* of $f_{i,p'}$ (not counting multiplicity) remains invariant as p' varies over C.
3. For every $1 \leq i < j \leq s$, the *total number of common complex roots* of $f_{i,p'}$ and $f_{j,p'}$ (counting multiplicity) remains invariant as p' varies over C. $\square$

Theorem 8.6.2 *Let $\mathcal{F} \subseteq \mathbb{R}[x_1, \ldots, x_n]$ be a set of polynomials as in the preceding definition, and let $C \subseteq \mathbb{R}^{n-1}$ be a connected maximal $\mathcal{F}$-delineable set. Then C is semialgebraic.*

PROOF.
We show that all the three invariant properties of the definition for delineability have semialgebraic characterizations.

(1) The first condition states that

$$\Big(\forall\, i\Big)\ \Big(\forall\, p' \in C\Big)\ \Big[|\mathcal{Z}(f_{i,p'})| = \text{invariant}\Big],$$

where $\mathcal{Z}(f)$ denotes the complex roots of f. This condition is simply equivalent to saying that "$\deg(f_{i,p'})$ is invariant (say, k_i)." A straightforward semialgebraic characterization is as follows:

$$\begin{aligned}&\Big(\forall\, 1 \leq i \leq s\Big)\ \Big(\exists\, 0 \leq k_i \leq d_i\Big) \\ &\qquad \Big[(\forall\, k > k_i)\ [f_i^k(x_1, \ldots, x_{n-1}) = 0] \ \wedge\ f_i^{k_i}(x_1, \ldots, x_{n-1}) \neq 0\Big]\end{aligned}$$

holds for all $p' \in C$.

(2) The second condition, in view of the first condition, can be restated as follows:

$$\Big(\forall\, i\Big)\ \Big(\forall\, p' \in C\Big)\ \Big[|\mathcal{CZ}(f_{i,p'}, D_{x_n}(f_{i,p'}))| = \text{invariant}\Big],$$

where D_{x_n} denotes the formal derivative operator with respect to the variable x_n and $\mathcal{CZ}(f,g)$ denotes the common complex roots of f and g. Using principal subresultant coefficients, we can provide the following semialgebraic characterization:

$$\begin{aligned}
&\Big(\forall\, 1 \le i \le s\Big)\ \Big(\exists\, 0 < k_i \le d_i\Big)\ \Big(\exists\, 0 \le l_i \le k_i - 1\Big)\\
&\quad\Big[(\forall\, k > k_i)\ [f_i^k(x_1, \ldots, x_{n-1}) = 0]\ \wedge\ f_i^{k_i}(x_1, \ldots, x_{n-1}) \ne 0\\
&\quad\wedge (\forall\, l < l_i)\ [\mathrm{PSC}_l^{x_n}(\widehat{f}_i^{k_i}(x_1, \ldots, x_n), D_{x_n}(\widehat{f}_i^{k_i}(x_1, \ldots, x_n))) = 0]\\
&\quad\wedge \mathrm{PSC}_{l_i}^{x_n}(\widehat{f}_i^{k_i}(x_1, \ldots, x_n), D_{x_n}(\widehat{f}_i^{k_i}(x_1, \ldots, x_n))) \ne 0\Big]
\end{aligned}$$

holds for all $p' \in C$; here $\mathrm{PSC}_l^{x_n}$ denotes the l^{th} principal subresultant coefficient with respect to x_n.

(3) Finally, the last condition can be restated as follows:

$$\Big(\forall\, i \ne j\Big)\ \Big(\forall\, p' \in C\Big)\ \Big[|\mathcal{CZ}(f_{i,p'}, f_{j,p'})| = \text{invariant}\Big].$$

Using principal subresultant coefficients, we can provide the following semialgebraic characterization:

$$\begin{aligned}
&\Big(\forall\, 1 \le i < j \le s\Big)\ \Big(\exists\, 0 < k_i \le d_i\Big)\ \Big(\exists\, 0 < k_j \le d_j\Big)\\
&\quad\Big(\exists\, 0 \le m_{i,j} \le \min(k_i, k_j)\Big)\\
&\quad\Big[(\forall\, k > k_i)\ [f_i^k(x_1, \ldots, x_{n-1}) = 0]\ \wedge\ f_i^{k_i}(x_1, \ldots, x_{n-1}) \ne 0\\
&\quad\ \wedge (\forall\, k > k_j)\ [f_j^k(x_1, \ldots, x_{n-1}) = 0]\ \wedge\ f_j^{k_j}(x_1, \ldots, x_{n-1}) \ne 0\\
&\quad\ \wedge (\forall\, m < m_{i,j})\ [\mathrm{PSC}_m^{x_n}(\widehat{f}_i^{k_i}(x_1, \ldots, x_n), \widehat{f}_j^{k_j}(x_1, \ldots, x_n)) = 0]\\
&\quad\ \wedge \mathrm{PSC}_{m_{i,j}}^{x_n}(\widehat{f}_i^{k_i}(x_1, \ldots, x_n), \widehat{f}_j^{k_j}(x_1, \ldots, x_n)) \ne 0\Big],
\end{aligned}$$

holds for all $p' \in C$; here $\mathrm{PSC}_m^{x_n}$ denotes the m^{th} principal subresultant coefficient with respect to x_n. $\square$

In summary, given a set of polynomials, $\mathcal{F} \in \mathbb{R}[x_1, \ldots, x_n]$, as shown below, we can compute another set of $(n-1)$-variate polynomials, $\Phi(\mathcal{F}) \in \mathbb{R}[x_1, \ldots, x_{n-1}]$, which precisely characterizes the connected maximal $\mathcal{F}$-delineable subsets of $\mathbb{R}^{n-1}$. Let

$$\mathcal{F} = \Big\{f_1,\ f_2,\ \ldots,\ f_s\Big\};$$

then

$$\begin{aligned}\Phi(\mathcal{F}) &= \Big\{ f_i^k(x_1,\ldots,x_{n-1}) \;:\; 1 \le i \le s,\;\; 0 \le k \le d_i \Big\} \\ &\cup \Big\{ \mathrm{PSC}_l^{x_n}(\widehat{f}_i^k(x_1,\ldots,x_n), D_{x_n}(\widehat{f}_i^k(x_1,\ldots,x_n)) \;: \\ &\qquad\qquad 1 \le i \le s,\;\; 0 \le l < k \le d_i - 1 \Big\} \\ &\cup \Big\{ \mathrm{PSC}_m^{x_n}(\widehat{f}_i^{k_i}(x_1,\ldots,x_n), \widehat{f}_j^{k_j}(x_1,\ldots,x_n)) \;: \\ &\qquad\qquad 1 \le i < j \le s,\;\; 0 \le m \le k_i \le d_i,\;\; 0 \le m \le k_j \le d_j \Big\}.\end{aligned}$$

pp. 350 The statement "$|\Phi(\mathcal{F})| = O(d\ |\mathcal{F}|^2)$" (¶1, under item **Project**) should now read "$|\Phi(\mathcal{F})| = O(d^2\ |\mathcal{F}|^2)$." [1]

pp. 354–357 The terms "sentence(s)" should be replaced by "formula(s)" in the following lines: 17, 19, 24, 25, 26, 27, 28, 29, 32 and 34 on page 354; 10 and 22 on page 355; 9, 12, 13 and 14 on page 356; and 1, 12 and 16 on 357.[7]

pp. 354 At the end of paragraph ¶4, add the following sentence: "A Tarski formula without free variables is called a Tarski sentence."

pp. 361 The Theorem 8.6.10 should read as shown below:[7]

Theorem 8.6.10

- *Let Φ be a Tarski sentence with rational coefficients. There is an effective decision procedure for Φ.*
- *Let Φ be a Tarski formula. There is a quantifier-free propositional sentence ϕ logically equivalent to Φ. If Φ involves only polynomials with rational coefficients, then so does the sentence ϕ.*

The Corollary 8.6.11 should read as shown below:

Corollary 8.6.11 *Tarski sets (subsets of $\mathbb{R}^n$ defined by a Tarski formula) are exactly the semialgebraic sets.*

pp. 381 The word "field" (§Bibliographic Notes ¶4 line 1) should be corrected to "fields." In the same paragraph (line 3), the phrase "the numbers in an algebraic number field" should read "the elements in an algebraic number field," instead. [2]

pp. 382 The name "Vorbjov" (¶4 line 5) should be corrected to "Vorobjov." [2]

pp. 399 The reference items [112] and [113] (D. Kapur, Geometry Theorem Proving Using Hilbert's Nullstellensatz, etc.) in the Bibliography are duplicates. Please delete the reference item [112].

Bibliography

[1] Saugata Basu. Personal Communication, Dept. of Computer Science, Courant Institute, New York University, April 1994.

[2] Bob Caviness. Electronic Communication, Computer and Information Sciences, University of Delaware, Newark, DE, June 1994.

[3] Lars W. Ericson. Personal Communication, New York University, March 1994.

[4] David P. Jacobs. Electronic Communication, Dept. of Computer Science, Clemson University, February 1994.

[5] Seongbin Park, Electronic Communication, Dept. of Computer Science, University of California, February & April 1994.

[6] Lidia Ricca, Private Communication, Courant Institute, New York University, September 1994.

[7] Marie-Francoise Roy, Private Communication, University of Rennes, France, August 1995.