Key Polynomials

As we have seen, the Round Two integral basis algorithm involves repeatedly solving $n^2 \times n$ systems of linear equations and so (with the use of up-to-date matrix algorithms) would be expected to take no fewer than $O(n^{1+\log_2 7})$ operations (with $1 + \log_2 7 \approx 3.81$). The Round Four algorithm does considerably better, terminating after

$$O\big(m^{1+\epsilon} n^3 + m^{2+\epsilon} n^2\big)$$

operations, where $m = v_p(\operatorname{disc} f)$. The behavior of Round Four is dominated by the cost of computing polynomial resultants, which are required in determining the p-adic values of the various elements that arise.

Another approach is to construct sequences of *valuations*, avoiding the explicit construction of individual elements but working instead with their minimal or characteristic polynomials. Determination of p-adic (and other) values is via Newton polygons, of both elementary and "higher order" types; computation of polynomial resultants is thus avoided.

1. Discrete Valuations of $\mathbb{Q}[x]$

Suppose W is a (non-trivial) discrete valuation of $\mathbb{Q}[x]$. We can approximate W by a sequence $V_0, V_1, V_2, \ldots,$ of *inductive valuations* of $\mathbb{Q}[x]$.

We define the valuation V_0 as

$$V_0(a_n x^n + \cdots + a_0) \;=\; \min\big\{W(a_n), \ldots, W(a_0)\big\}.$$

Next we let $\phi_1(x) = x$ and $\mu_1 = W(x)$ and define

$$V_1(a_n x^n + \cdots + a_0) \;=\; \min\big\{\, V_0(a_i) + i\mu_1 \;\big|\; i = 0, \ldots, n \,\big\}.$$

For $k > 1$ we assume $W \neq V_{k-1}$. We choose a monic polynomial ϕ_k of minimal degree such that $W(\phi_k) > V_{k-1}(\phi_k)$ and let $\mu_k = W(\phi_k)$.

We define V_k to be the (ϕ_k, μ_k)*-augmentation of* V_{k-1}, denoted

$$V_k \;=\; \big[\, V_{k-1},\, \phi_k \to \mu_k \,\big] \tag{1}$$

and given by

$$V_k(f) \;=\; \min\big\{\, V_{k-1}(f_i) + i\mu_k \;\big|\; i = 0, \ldots, n \,\big\} \tag{2}$$

for $f(x)$ with ϕ_k-adic expansion

$$f(x) \;=\; f_n(x)\,\phi_k^n + f_{n-1}(x)\,\phi_k^{n-1} + \cdots + f_0(x). \tag{3}$$

Each valuation in the chain $V_0, V_1, \ldots, V_k$ is called an *inductive valuation*. If the construction of the successive inductive valuations does not terminate with $W = V_k$ then we define the valuation V_∞ by

$$V_\infty(f) \;=\; \lim_{k\to\infty} V_k(f)$$

for each $f(x)$ in $\mathbb{Q}[x]$.

If $W(f) > V_k(f)$ for all k then $V_{k+1}(f) > V_k(f)$ for all k and, since W is discrete, this implies the limit is ∞. But this limit is bounded by $W(f)$, hence $W(f) = \infty$ and $f = 0$. Otherwise $W(f) = V_k(f)$ for all $k \geq t$ for some t. Thus $W = V_\infty$.

Theorem (M_1)**.** *Every non-trivial discrete valuation of* $\mathbb{Q}[x]$ *can be represented either as an inductive valuation or as the limit of an infinite sequence of inductive valuations.*

2. Homogeneous Form

Definitions. A valuation V of $\mathbb{Q}[x]$ induces certain relations on $\mathbb{Q}[x]$.

$$\textit{equivalence in } V: a \approx_V b \iff V(b-a) > V(b).$$
$$\textit{equivalence-divisibility in } V: \ a \parallel_V b \iff b \approx_V ca \ \text{ for some } c(x) \in \mathbb{Q}[x].$$

Theorem (M_1)**.** *In the inductive valuation V_k any nonzero polynomial $f(x)$ in $\mathbb{Q}[x]$ has a unique $(\phi_1, \ldots, \phi_k)$-adic expansion*

$$f(x) \ = \ \sum_j c_j \, p^{m_{0j}} \phi_1^{m_{1j}} \phi_2^{m_{2j}} \cdots \phi_k^{m_{kj}} \tag{4}$$

with $c_j \in \mathbb{Q}$, $v_p(c_j) = 0$, and $0 \le m_{ij} < \deg \phi_{i+1} / \deg \phi_i$ for $i = 1, \ldots, k-1$.

The polynomial $f(x)$ is *homogeneous in* V_k if all terms in the expansion (4) have the same value in V_k and each coefficient c_j belongs to $\{1, \ldots, p-1\}$.

Each class of polynomials equivalent in V_k contains a unique representative in homogeneous form. The representative of the class of a polynomial $f(x)$ is its k*-homogeneous part*, formed by omitting from the expansion (4) all terms with value greater than $V_k(f)$ and in each remaining term replacing the coefficient c_j by c_j **mod** p.

We denote the k-homogeneous part of $f(x)$ by $f^{(V_k)}$. In general,

$$f \approx_{V_k} f^{(V_k)}, \quad V_k(f) = V_k(f^{(V_k)}), \quad f \approx_{V_k} g \ \text{ if and only if } f^{(V_k)} = g^{(V_k)}.$$

Exercises. *Let V_k defined as in section 1. Prove the following.*

1. *V_k is a (discrete) non-archimedean valuation of $\mathbb{Q}[x]$, i.e.,*
   - $V_k(f) = \infty$ *if and only if* $f = 0$,
   - $V_k(fg) = V_k(f) + V_k(g)$,
   - $V_k(f+g) \ge \min\{V_k(f), V_k(g)\}$.
2. *$W(f) \ge V_k(f)$ for all $f(x)$ in $\mathbb{Q}[x]$.*
3. *If $\deg f < \deg \phi_k$ then $W(f) = V_k(f)$.*
4. *$W(\phi_i) = V_k(\phi_i)$ for $i = 1, \ldots, k$.*
5. *$W(f) > V_{k-1}(f)$ if and only if $\phi_k \parallel_{V_{k-1}} f$.*
6. *$V_k(f) > V_{k-1}(f)$ if and only if $\phi_k \parallel_{V_{k-1}} f$.*
7. *$\phi_k(x) \not\approx_{V_{k-1}} \phi_{k-1}(x)$.*
8. *If $\phi_k \parallel_{V_{k-1}} f$ and $f \neq 0$ then $\deg f \ge \deg \phi_k$.*
9. *If $\phi_k \parallel_{V_{k-1}} fg$ then $\phi_k \parallel_{V_{k-1}} f$ or $\phi_k \parallel_{V_{k-1}} g$.*

Note: *The exercises appear as lemmas and theorems in MacLane's 1936 papers.*

Bibliography

[M$_1$] S. MacLane, *A construction for absolute values in polynomial rings*, Transactions of the American Mathematical Society **40**(3) (1936) 363–395.

[M$_2$] S. MacLane, *A construction for prime ideals as absolute values of an algebraic field*, Duke Mathematical Journal **2** (1936) 492–510.

3. Key Polynomials and Augmented Valuations

The construction of inductive valuations outlined in the previous section relies on the properties of *key polynomials*.

Definition. A *key polynomial* over a valuation V of $\mathbb{Q}[x]$ is a non-constant monic polynomial $\phi(x)$ in $\mathbb{Z}[x]$ that is *minimal in* V, *i.e.*,

$$\phi \parallel_V f \text{ and } f \neq 0 \implies \deg f \geq \deg \phi,$$

and *equivalence-irreducible in* V, *i.e.*,

$$\phi \parallel_V fg \implies \phi \parallel_V f \text{ or } \phi \parallel_V g.$$

Definition. For V a valuation of $\mathbb{Q}[x]$, $\phi(x)$ a non-constant polynomial in $\mathbb{Q}[x]$, and $\mu \in \mathbb{Q}$, the (ϕ, μ)*-augmentation of* V is the map

$$W \;=\; \big[\,V, \phi \to \mu\,\big]$$

given by

$$W(f) \;=\; \min\{\, V(f_i) + i\mu \mid i = 0, \ldots, n\,\}$$

for $f(x)$ with ϕ-adic expansion

$$f(x) \;=\; f_n(x)\,\phi^n + f_{n-1}(x)\,\phi^{n-1} + \cdots + f_0(x).$$

Exercises. *Let $\phi(x)$ be a key polynomial over V, let $\mu > V(\phi)$, and let W be the (ϕ, μ)-augmentation of V. Prove the following.*

1. *If $f(x) \neq 0$ then*
   - (i) $V(f \bmod \phi) \geq V(f)$, *and*
   - (ii) $V(f \bmod \phi) > V(f)$ *if and only if* $\phi \parallel_V f$.
2. *Let $a(x)$ and $b(x)$ be polynomials with $\deg a < \deg \phi$ and $\deg b < \deg \phi$, and let $a(x)b(x) = q(x)\phi + r(x)$ with $r(x) = a(x)b(x) \bmod \phi$. Then*
$$V(q\phi) \geq V(ab) = V(r).$$
3. *If $a(x)$ and $b(x)$ are polynomials with $\deg a < \deg \phi$ and $\deg b < \deg \phi$ then*
$$W(a\phi^s \cdot b\phi^t) = W(a\phi^s) + W(b\phi^t).$$
4. *If the polynomials $f(x)$, $g(x)$, and $f(x)g(x)$ have ϕ-adic expansions*
$$f(x) = \textstyle\sum_j f_j(x)\phi^j,\;\; g(x) = \sum_k g_k(x)\phi^k,\;\; f(x)g(x) = \sum_m h_m(x)\phi^m$$
   respectively, and if s and t are the largest integers such that
$$W(f_s\phi^s) = W(f), \quad W(g_t\phi^t) = W(g)$$
   respectively, then
$$W(h_{s+t}\phi^{s+t}) = W(f) + W(g).$$
5. *W is a valuation of $\mathbb{Q}[x]$.*

Exercise. *Let V and W be valuations of $\mathbb{Q}[x]$ such that $W(f) \geq V(f)$ for all $f(x)$ and let $\phi(x)$ be a monic polynomial of minimum degree such that $W(\phi) > V(\phi)$. Show that $\phi(x)$ is a key polynomial over V, as follows.*

1. *Show that $W(f) > V(f)$ if and only if $\phi \parallel_V f$.*
2. *Show that $\phi(x)$ is equivalence-irreducible in V.*
3. *Show that $\phi(x)$ is minimal in V.*

4. Non-finite Valuations

Definition. A *non-finite valuation of* $\mathbb{Q}[x]$ is a map $W : \mathbb{Q}[x] \to \mathbb{Q} \cup \{\infty\}$ such that

- $W(0) = \infty$,
- $W(fg) = W(f) + W(g)$,
- $W(f+g) \geq \min\{W(f),\, W(g)\}$

for all $f(x)$, $g(x)$ in $\mathbb{Q}[x]$.

Suppose $G(x)$ is the defining polynomial for an algebraic extension $\mathcal{K}$ of $\mathbb{Q}$, given by $\mathcal{K} = \mathbb{Q}(\xi)$ for some root ξ of $G(x)$. We are interested in extending the p-adic valuation v_p to $\mathcal{K}$. Any such extension gives rise to a non-finite valuation W of $\mathbb{Q}[x]$, defined by

$$W(f) = v_p(f(\xi))$$

for $f(x) \in \mathbb{Q}[x]$. The non-finite valuation W can be approximated by a sequence of inductive valuations, in just the same way a discrete valuation of $\mathbb{Q}[x]$ can.

Note that W depends on the choice of ξ, and if $\mu(x)$ is the minimal polynomial of ξ over $\mathbb{Q}_p$ then $W(f) = \infty$ if and only if $\mu(x)$ divides $f(x)$ in $\mathbb{Q}_p[x]$.

Exercise. *Assume $1 \leq k \leq n-1$. Show that*

1. $V_n(\phi_k) = V_k(\phi_k)$, *and*
2. *if* $\deg f < \deg \phi_{k+1}$ *then* $V_n(f) = V_k(f)$.

The G-projection of V_k

Suppose $G(x)$ has ϕ_k-adic expansion

$$G(x) \;=\; g_m(x)\,\phi_k^m + g_{m-1}(x)\,\phi_k^{m-1} + \cdots + g_0(x) \tag{5}$$

and that the expression $V_k(g_i\phi_k^i)$ is minimal for the single value $i = e$. By the exercise and the triangle law, if $n > k$ then

$$V_n(G) \;=\; V_n(g_e\phi_k^e) \;=\; V_k(g_e\phi_k^e) \;=\; V_k(G)$$

and W cannot be the limit of the sequence $V_0,\, V_1,\, V_2,\, \ldots$.

Definition. The difference

$$\max\{\, i \mid V_k(G) = V_k(g_i\phi_k^i)\,\} \;-\; \min\{\, i \mid V_k(G) = V_k(g_i\phi_k^i)\,\}$$

from the expansion (5) is called the *G-projection* of V_k.

To approximate W we are constrained to choose only key polynomials ϕ_k and key values μ_k so that each valuation V_k will have positive G-projection.

Definition. V_k is called a k^{th} *approximant to* G if the G-projection of V_k is positive.

Key Values

The key polynomial ϕ_k having been determined the expansion (5) can be computed and its *level k Newton polygon*, the lower convex hull of the set

$$\{\, \big(i, V_{k-1}(g_i)\big) \mid i = 0,\, \ldots,\, m\,\},$$

can be drawn.

The G-projection constraint obliges us to choose μ_k so that the lower convex hull of the set

$$\{\, \big(i, V_{k-1}(g_i) + i\mu_k\big) \mid i = 0,\, \ldots,\, m\,\}$$

has a horizontal edge, and this is the case if and only if $-\mu_k$ is the slope of an edge of the level k Newton polygon.

It is also necessary to have $\mu_k > V_{k-1}(\phi_k)$.

Finding ϕ_k

Definition. A polynomial $e(x)$ with ϕ_k-adic expansion

$$e(x) \;=\; e_m(x)\,\phi_k^m + e_{m-1}(x)\,\phi_k^{m-1} + \cdots + e_0(x)$$

is an *equivalence-unit in V_k* if $V_k\big(e_0(x)\big) < V_k\big(e_j(x)\,\phi_k^j\big)$ for $j = 1,\, \ldots,\, m$.

Lemma (M_2). *The polynomial ϕ_k is a key polynomial over V_k.*

Theorem (M_2). *In the inductive valuation V_k every polynomial $f(x)$ has a decomposition*

$$f(x) \;\approx_{V_k}\; e(x)\,\psi_1(x)\,\psi_2(x)\cdots\,\psi_t(x)$$

as a product of homogeneous polynomials, with $e(x)$ an equivalence-unit and each $\psi_i(x)$ a key polynomial, and this decomposition is unique except for the order of the factors.

Lemma (M_2). *If V_k is a k^{th} approximant to G then $\phi_k \parallel_{V_{k-1}} G$.*

Lemma (M_2). *If $G(x)$ is not itself a key polynomial over V_{k-1} then*

$$G(x) \;\approx_{V_{k-1}}\; e(x)\,\psi_1(x)\cdots\,\psi_t(x)$$

with $e(x)$ a homogeneous equivalence-unit and $\psi_1(x),\, \ldots,\, \psi_t(x)$ homogeneous key polynomials over V_{k-1}.

Lemma (M_2). *If ϕ_k is chosen to be one of $\psi_1,\, \ldots,\, \psi_t$, but with $\phi_k \neq \phi_{k-1}$, and if the key value μ_k is chosen as described above, then*

$$V_k \;=\; \big[\, V_{k-1},\, \phi_k \to \mu_k \,\big]$$

is a k^{th} approximant to G.

5. Residue-classes

Definitions. A valuation V of $\mathbb{Q}[x]$ induces certain relations on $\mathbb{Q}[x]$.

$$\textit{congruence in } V: a \equiv_V b \iff V(b-a) > 0.$$

$$\textit{congruence-divisibility in } V: \ a \parallel\!|_V\, b \iff b \equiv_V ca \ \text{ for some } c(x) \in \mathbb{Q}[x].$$

Definitions. For a valuation V of $\mathbb{Q}[x]$, the *valuation ring* O_V of V, the prime ideal P_V of O_V, the *residue-class* $[\![a]\!]_V$ of a polynomial $a(x)$ in O_V, and the *residue-class ring* Δ_V are given by

$$O_V = \{\, a(x) \in \mathbb{Q}[x] \mid V(a) \geq 0 \,\},$$

$$P_V = \{\, a(x) \in \mathbb{Q}[x] \mid V(a) > 0 \,\},$$

$$[\![a]\!]_V = \{\, b(x) \in O_V \mid V(b-a) > 0 \,\},$$

$$\Delta_V = O_V / P_V = \{\, [\![a]\!]_V \mid a(x) \in O_V \,\}.$$

Definition. We let Γ_V denote the *value-group* of V, *i.e.*,

$$\Gamma_V = V(\mathbb{Q}[x]).$$

Definition. For $W = [V, \phi \to \mu]$ and $f(x)$ a polynomial with $W(f) \in \Gamma_V$, a *W-flattener of f* is a polynomial $f^\flat_W(x)$ such that

$$V(f^\flat_W) = W(f^\flat_W) = -W(f).$$

Proposition (M_1). *Let $W = [V, \phi \to \mu]$, let $f(x)$ be a polynomial with $\phi \nparallel_W f$, and let $f^\flat_W(x)$ be an arbitrary W-flattener of f.*

(i) *If $g(x) \in \mathbb{Q}[x]$ with $W(g) = 0$ then*

$$f \parallel_W g \iff f^\flat_W f \parallel\!|_W\, g.$$

(ii) *The polynomial $f(x)$ is equivalence-irreducible in W if and only if*

$$f^\flat_W f \parallel\!|_W\, gh \implies f^\flat_W f \parallel\!|_W\, g \ \text{ or } \ f^\flat_W f \parallel\!|_W\, h$$

for all polynomials $g(x)$ and $h(x)$ with $W(g) = W(h) = 0$.

Definitions. For $W = [V, \phi_W \to \mu_W]$ we define F_W, τ_W, $\phi^{\tau_W \flat}_{WW}$, y_W as follows.

- F_W is the subring of Δ_W given by

$$F_W = \{\, [\![f]\!]_W \mid V(f) \geq 0 \,\} = \{\, [\![f]\!]_W \mid f \in O_V \,\}.$$

- τ_W denotes the smallest positive integer such that $\tau_W \mu_W \in \Gamma_V$.
- $\phi^{\tau_W \flat}_{WW}(x)$ denotes an arbitrary W-flattener of $\phi^{\tau_W}_W$.
- y_W denotes the residue-class $[\![\phi^{\tau_W \flat}_{WW} \phi^{\tau_W}_W]\!]_W$.

Lemma (M_1). *y_W is transcendental over F_W and $\Delta_W = F_W[y_W]$.*

Lemma (M_1). *If V is the (ϕ, μ)-augmentation of the valuation U and $\psi(x)$ is a key polynomial over V not equivalent in V to $\phi(x)$ then $V(\psi) \in \Gamma_U$.*

Theorem (M_1). *Let V be the (ϕ_V, μ_V)-augmentation of the valuation U, let W be the (ϕ_W, μ_W)-augmentation of V, with $\phi_W \not\approx_V \phi_V$, and let $\phi^\flat_{WV}(x)$ be an arbitrary V-flattener of ϕ_W. Then the following hold.*

(i) *The polynomial $\psi_W(y_V) = [\![\phi^\flat_{WV}\, \phi_W]\!]_V$ is irreducible in $F_V[y_V]$.*

(ii) *If θ_W is a root of ψ_W then $F_W = F_V(\theta_W)$.*

(iii) *If $m = \deg \psi_W$ then $\deg \phi_W = m\, \tau_V \deg \phi_V$.*