Lean Characteristic Set

YuXuan Xiao

February 2, 2026

Chapter 1

Definitions

Definition 1. The class of a multivariate polynomial p is the largest variable index appearing in p.

Definition 2. The degree of p with respect to its class.

Definition 3. The rank of a polynomial p is the pair $(mainVar(p), deg(p))$ ordered lexicographically.

Definition 4. q is reduced with respect to p if the degree of q in the main variable of p is strictly less than the main degree of p.

Definition 5. q is reduced with respect to a polynomial set PS if it is reduced with respect to all elements of PS.

Definition 6. The initial of a polynomial p with respect to a variable i. It is the coefficient of the highest power of x_i appearing in p.

Definition 7. The initial of a polynomial p is the initial with respect to its class.

Definition 8. The product of initials of a set of polynomials.

Definition 9. A Triangulated Set is a finite ordered sequence of non-zero polynomials with strictly increasing classes.

Definition 10. The rank of a Triangulated Set is a lexicographic sequence of ranks of its polynomials. More intuitively, $S < T$ if one of the following two occurs:

- There exists some $k < S.length$ such that $S_0 \sim T_0, S_1 \sim T_1, ..., S_{k-1} \sim T_{k-1}$, while $S_k < T_k$.
- $S.length > T.length$ and $\forall i < T.length, S_i \sim T_i$.

Definition 11. "S.takeConcat p" tries to construct a new Triangulated Set by taking a prefix of S and appending p.

- If p fits naturally at the end of S, it behaves like "S.concat p".
- If p conflicts with some element in S (in terms of class order), "takeConcat" finds the first element in S that has a higher or equal class than p, truncates S before that element, and appends p.

Definition 12. A remainder r of g by f is a polynomial which is reduced with respect to f and satisfies $init(f)^s \cdot g = q \cdot f + r$ for some $s \in \mathbb{N}$ and $q \in R[X_\sigma]$.

Definition 13. A remainder r of g by a set S is a polynomial which is reduced with respect to S and satisfies $(\prod S_i^{e_i}) \cdot g = \sum q_i \cdot S_i + r$ for some $\{e_i\}$ and $\{q_i\}$.

Definition 14. Pseudo-division of g by f with respect to i.
Returns a triple containing the exponent, the quotient and the remainder.

Definition 15. Pseudo-division of g by f with respect to $mainVar(f)$.
Returns a triple containing the exponent, the quotient and the remainder.

Definition 16. Pseudo-divides g successively by elements of S. Typically, this involves dividing by S_{l-1}, then S_{l-2}, ..., down to S_0.
Returns a triple containing the exponents, the quotients and the remainder.

Definition 17. A Triangulated Set is an Ascending Set if every element is reduced with respect to its predecessors. Here "reduced" is an abstract predicate.

Definition 18. A Triangulated Set is a Standard Ascending Set if every element is reduced with respect to its predecessors.

Definition 19. A Triangulated Set is a Weak Ascending Set if the initial of every element is reduced with respect to its predecessors.

Definition 20. The interface for algorithms computing Basic Sets. Any instance of this class provides a "basicSet" function that computes a minimal ascending set contained in a given list of polynomials.

Definition 21. Computes the Standard Basic Set of a list of polynomials.
The algorithm works by:

1. Sort the list and let $BS = \emptyset$.
2. Pick the first (minimal) element B in the list.
3. Append B to the tail of the current basic set BS.
4. Filter the remaining list to keep only elements reduced w.r.t. the new BS and go to step 2.

Definition 22. Computes the Weak Basic Set of a list of polynomials.
Difference from Standard: The filter condition includes $mainVar(p) > mainVar(B)$.

Definition 23. CS is a characteristic set of PS if every polynomial in PS, 0 is its remainder by CS, and $Zero(PS) \subseteq Zero(CS)$.

Definition 24. Computes the Characteristic Set of a polynomial list l.
Algorithm:

1. Set $l_0 = l$.
2. Compute $BS = BasicSet(l)$.
3. Compute remainders RS of $l \setminus BS$ with respect to BS.
4. If $RS = \emptyset$, BS is the characteristic set.

5. If not, let $l = l_0 ++ RS ++ BS$ and go to step 2.

Termination is guaranteed by the well-ordering of ranks.

Definition 25. Decomposes the zero set of a polynomial list into a union of zero sets of triangular sets. The algorithm recursively computes the characteristic set CS and adds branches for the initials of CS.

Chapter 2

Theorems

Lemma 26. *q is reduced w.r.t. p if $mainVar(q) < mainVar(p)$.*

Proof. □

Lemma 27. *If $mainVar(p) = mainVar(q)$, then q is reduced with respect to p if and only if $q < p$.*

Proof. □

Lemma 28. *$mainVar(p) < mainVar(q)$ if $p \leq q$ and q is reduced with respect to p.*

Proof. □

Lemma 29. *$init_i(p) = p$ if $deg_i(p) = 0$ (i.e. x_i does not appear in p).*

Proof. □

Lemma 30. *$deg_i(init_i(p)) = 0$.*

Proof. □

Lemma 31. *$init_i(init_i(p)) = init_i(p)$.*

Proof. □

Lemma 32. *$\forall ij, deg_j(init_i(p)) \leq deg_j(p)$*

Proof. □

Theorem 33. *$init_i(p)$ is the leading coefficient when viewing p as a univariate polynomial in x_i.*

Proof. □

Theorem 34. *$p = init_i(p)x_i^d + q$, where $deg_i(q) < d = deg_i(p)$.*

Proof. □

Lemma 35. *$deg_i(p + q) < deg_i(p)$ if $deg_i(p) = deg_i(q)$ and $init_i(p) + init_i(q) = 0$.*

Proof. □

Theorem 36. $init_i(p \cdot q) = init_i(p) \cdot init_i(q)$ *if there is no zero divisors in the coefficient ring.*

Proof. □

Lemma 37. $mainVar(init(p)) < mainVar(p)$ *for non-constant* p*.*

Proof. □

Lemma 38. $init_i(p)$ *is reduced w.r.t.* q *if* p *is reduced w.r.t. to* q*.*

Proof. □

Lemma 39. $init_i(p)$ *is reduced w.r.t.* p *for non-constant* p*.*

Proof. □

Theorem 40. *The set of Triangulated Sets is well-founded under the lexicographic rank ordering. This guarantees the termination of the Characteristic Set Algorithm.*

Proof. □

Theorem 41. *If* $p \neq 0$ *and is reduced with respect to* S*, then modifying* S *by appending* p *(using "takeConcat") strictly decreases the rank of* S*.*

Proof. □

Lemma 42. $deg_i(r) < deg_i(g)$ *where* r *is the remainder of* g *by* f *w.r.t.* i *if* $deg_i(f) \neq 0$*.*

Proof. □

Theorem 43. *The remainder* r *of* g *by* f *is reduced with respect to* f *and satisfies* $init(f)^s \cdot g = q \cdot f + r$ *for some* $s \in \mathbb{N}$ *and* $q \in R[X_\sigma]$*.*

Proof. □

Lemma 44. *The remainder* r *of* g *by* f *satisfies* $deg_i(r) \leq deg_i(g)$ *if* $deg_i(f) = 0$

Proof. □

Theorem 45. *The remainder* r *of* g *by a set* S *is reduced with respect to* S *and satisfies* $(\prod S_i^{e_i}) \cdot g = \sum q_i \cdot S_i + r$ *for some* $\{e_i\}$ *and* $\{q_i\}$*.*

Proof. □

Theorem 46. *The remainder of* g *by* f *is* 0 *if* f *is a divisor of* g*.*

Proof. □

Theorem 47. *The remainder of* g *by* f *is* g *if* $deg_c(g) = 0$ *where* $c = mainVar(f)$*.*

Proof. □

Theorem 48. *The remainder of* p *by a set* S *is* 0 *if* p *is in* S*.*

Proof. □

Theorem 49. *If* p *is in* S *and* $mainVar(p) \neq \bot$*, then* $init(p)$ *is in* S*.*

Proof. □

Theorem 50. *The algorithm computes a minimal standard ascending set contained in the input list.*

Proof. □

Theorem 51. *The algorithm computes a minimal weak ascending set contained in the input list.*

Proof. □

Theorem 52. *Appending an element which is reduced w.r.t. the basic set of list strictly decreases the rank. Crucial for proving termination of characteristic set and zero decomposition algorithms.*

Proof. □

Theorem 53. *Well-ordering principle (1):* $Zero(CS/IP) \subseteq Zero(PS)$*, where* IP *is the initial-product of* CS*.*

Proof. □

Theorem 54. *Well-ordering principle (2):* $Zero(CS/IP) = Zero(PS/IP)$*, where* IP *is the initial-product of* CS*.*

Proof. □

Theorem 55. *Well-ordering principle (3):*

$$Zero(PS) = Zero(CS/IP) \cup \left(\bigcup_{p \in CS} Zero(PS \cup init(p)) \right)$$

.

Proof. □

Theorem 56. *The algorithm computes a valid characteristic set for the input list.*

Proof. □

Theorem 57. *The computed characteristic set is an ascending set.*

Proof. □

Theorem 58. *The rank of computed characteristic set* $\leq$ *the rank of the input list.*

Proof. □

Theorem 59. $\forall CS \in \mathcal{ZD}(PS), g \in PS,$ 0 *is the remainder of* g *by* CS*.*

Proof. □

Theorem 60. ***Zero Decomposition Theorem****: The zero set of a polynomial system* PS *is the union of the zero sets of the triangular systems computed by the algorithm:*

$$Zero(PS) = \bigcup_{CS \in \mathcal{ZD}(PS)} Zero(CS/IP(CS))$$

.

Proof. □