An Algorithm for Constructing
Gröbner Bases from Characteristic Sets
and Its Application to Geometry

Shang-Ching Chou, William F. Schelter, and Jin-Gen Yang

Abstract. In Ritt's method, a prime ideal is given by a characteristic set. A characteristic set of a
prime ideal is generally not a set of generators of this ideal. In this paper we present a simple
algorithm for constructing Gröbner bases of a prime ideal from its characteristic set. We give a
method for finding new theorems in geometry as an application of this algorithm.

Key Words. Polynomial, (Prime) ideal, Generators, (Irreducible) ascending chain, (Irreducible)
algebraic set, Decomposition of an algebraic set, Geometric configuration, Nondegenerate component,
Geometry theorem proving.

1. Introduction. In Ritt's method [5], a prime ideal is given by a characteristic
set, which is not necessarily a set of generators of this ideal. There are algorithms
for constructing a set of generators of a prime ideal from its characteristic set
(see pp. 98-103 of [5] and pp. 76, 82-83 of [6]). Ritt's algorithm is complicated
and hard to implement. Rody's algorithm, which repeatedly uses Herman's
module basis algorithm (see [7]), also seems complicated. In this paper we present
a simple algorithm which uses only Buchberger's algorithm for constructing
Gröbner bases of a polynomial ideal [1]. The algorithm, which has been imple-
mented on a Symbolics 3600, is based on a key connection between a prime ideal
and its characteristic set (Theorem 2.2 below). Algorithms of this kind have many
applications, e.g., to decide whether an ideal is prime [6]. Our main interest in
such algorithms, however, is their application to geometry theorem proving and
discovering. In Section 3 we give such an application for finding new theorems
in geometry.

2. The Algorithm. Let $K$ be a computable field and $A = \mathbb{K}[y_1, \ldots, y_m]$ be a
polynomial ring. Let $u_1, \ldots, u_d$ and $x_1, \ldots, x_r$ be distinct variables among
$y_1, \ldots, y_m$. We use the abbreviations $u = u_1, \ldots, u_d$ and $x = x_1, \ldots, x_r$. Thus,
e.g., $K(u)$ is the field of rational functions in $u_1, \ldots, u_d$.

---

1 The first author was supported by NSF Grants Nos. DCR-8503498 and CCR-8702108. The computer
facility was supported by the NSF/CER Grant at the University of Texas.

2 Institute for Computing Science, University of Texas at Austin, Austin, TX 78712, USA.

3 Department of Mathematics, University of Texas at Austin, Austin, TX 78712, USA.

4 Current Address: Department of Mathematics, Fudan University, Shanghai, China.

Received September 1, 1987; revised March 2, 1988. Communicated by John E. Hopcroft.
DEFINITION 2.1. A sequence \( f_1(u, x_1), \ldots, f_r(u, x_1, \ldots, x_r) \) of polynomials in \( A \) such that \( f_i \in K[u, x_1, \ldots, x_i] \) but \( \not\in K[u, x_1, \ldots, x_{i-1}] \) is called an irreducible ascending chain if:

(i) \( \text{prem}(I_i; f_1, \ldots, f_{i-1}) \neq 0 \) for \( i = 2, \ldots, r \), where each \( I_i \) is the leading coefficient (the initial) of the polynomial \( f_i \) in the leading variable \( x_i \), and

(ii) each \( f_i \) is irreducible in the polynomial ring \( K(u)[x_1, \ldots, x_i]/(f_1, \ldots, f_{i-1}) \).

Thus the sequence \( F_0 = K(u), F_1 = F_0[x_1]/(f_1), \ldots, F_r = F_{r-1}[x_r]/(f_r) = F_0[x]/(f_1, \ldots, f_r) \) is a tower of field extensions.

THEOREM 2.2. Let \( f_1(u, x_1), \ldots, f_r(u, x_1, \ldots, x_r) \) be an irreducible ascending chain and \( g \in A \). Then the following conditions are equivalent:

(i) \( \text{prem}(g; f_1, \ldots, f_r) = 0 \).

(ii) Let \( E \) be an extension field of \( K \). If \( \mu = (\tilde{u}_1, \ldots, \tilde{u}_d, \tilde{x}_1, \ldots, \tilde{x}_r) \) in \( E^{d+r} \) is a common zero of \( f_1, \ldots, f_r \) with \( \tilde{u}_1, \ldots, \tilde{u}_d \) transcendental over \( K \), then \( \mu \) is also a zero of \( g \), i.e., \( g(\mu) = 0 \).

PROOF. See the proof of Lemma 3, p. 234 in [8].

The point \( \mu = (\tilde{u}_1, \ldots, \tilde{u}_d, \tilde{x}_1, \ldots, \tilde{x}_r) \) in (ii) is called a generic point of that irreducible ascending chain in the field \( E \). By elementary field theory, there are extension fields \( E \) of \( K \) in which generic points of \( f_1, \ldots, f_r \) exist.

THEOREM 2.3. Let \( f_1(u, x_1), \ldots, f_r(u, x_1, \ldots, x_r) \) be an irreducible ascending chain, then \( P = \{ g \in K[u, x] \mid \text{prem}(g; f_1, \ldots, f_r) = 0 \} \) is a prime ideal of \( A \).

PROOF. Let \( g \) and \( h \) be two polynomials such that \( g \cdot h \in P \). Let \( \mu \) be a generic point of \( f_1, \ldots, f_r \). Then by Theorem 2.2, \( g(\mu)h(\mu) = 0 \). Thus either \( g(\mu) = 0 \) or \( h(\mu) = 0 \). By Theorem 2.2 again, either \( g \in P \) or \( h \in P \). Therefore, \( P \) is prime.

The sequence \( f_1, \ldots, f_r \) is called a characteristic set of the prime ideal \( P \). Conversely, for every prime ideal \( P \) of \( A \), there is an irreducible ascending chain which is a characteristic set of \( P \) (see pp. 88–90 of [5], or more explicitly, Theorems 2.8 and 3.9, Chapter 2 of [2]). Note that \( f_i \in P \), but \( f_1, \ldots, f_r \) are generally not generators of \( P \). The following theorem gives an algorithm for constructing a Gröbner basis (hence a set of generators) of \( P \) from \( f_1, \ldots, f_r \). (For the definition of Gröbner bases see [1].) The theorem is based on the key theorem (Theorem 2.2).

---

5 Here we use \( \text{prem}(g, f_i, x_i) \) to denote the pseudoremainder of \( g \) by \( f_i \) in the variable \( x_i \) in the ring \( K[u, x_1, \ldots, x_i] \). We define \( \text{prem}(g; f_1, \ldots, f_k) \) inductively: \( \text{prem}(g; f_1) = \text{prem}(g, f_1, x_1); \text{prem}(g; f_1, \ldots, f_k) = \text{prem}(\text{prem}(g, f_k, x_k); f_1, \ldots, f_{k-1}) \).