An Introduction to Gröbner Bases for Algebras and Modules

James A. Shepherd

Summerschool on Conjectures in Homological Algebra

for Finite Dimensional Algebras, Nordforjdeid, Norway.

August 12th-19th 2001.

Introduction

We use Edward Green's paper:

Multiplicative Bases, Gröbner Bases, and Right Gröbner Bases
J. Symbolic Computation (2000)

For the Linear Gröbner basis stuff see a book such as *Ideals, varieties and algorithms*, Cox, Little, O'Shea, Springer-Verlag.

- Why?
  - Always useful to have a basis,
  - Can do 'concrete' calculations,
  - Explicit construction of projective resolutions,
  - Solving systems of equations over algebras,
  - Elimination theory.

- How?
  - Constructive techniques,
  - Can do using symbolic computation,
  - Description of algebras with a Gröbner Basis theory.

Linear Gröbner Bases

k a field.
V vector space over k with a *well-ordered* k-basis $\mathcal{B} = \{b_i\}_{i \in I}$.

Def$^{\mathbf{n}}$ If $v = \sum_i \alpha_i b_i$ we say b_i *occurs* in v if $\alpha_i \neq 0$.

Def$^{\mathbf{n}}$

$\mathrm{Tip}(v) = b_i$ iff
- b_i occurs in v,
- b_j occurs in v implies $b_j \leq b_i$.

Def$^{\mathbf{n}}$
$\mathrm{CTip}(v)$ is the coefficient of $\mathrm{Tip}(v)$ in v.

Def$^{\mathbf{n}}$ Let $X \subset V$.

$$\begin{aligned} \mathrm{Tip}(X) &= \{b \in \mathcal{B} : b = \mathrm{Tip}(x) \text{ some } x \in X\}, \\ \mathrm{NonTip}(X) &= \mathcal{B} \setminus \mathrm{Tip}(X). \end{aligned}$$

Theorem 1 *Let W be a subspace of V,*

$$V = W \oplus \text{Span}(\text{NonTip}(W)).$$

Proof

- $W \cap \text{Span}(\text{NonTip}(W)) = 0$:
  Let $x \in \text{Span}(\text{NonTip}(W)) \setminus \{0\}$.
  If $x \in W$ then $\text{Tip}(x) \in \text{Tip}(W)$.#

- $W + \text{Span}(\text{NonTip}(W)) = V$:
  Let $v \in V$ s.t. $\text{Tip}(v) = b$ is minimal w.r.t. $v \notin W + \text{Span}(\text{NonTip}(W))$.
  Let $\alpha = \text{CTip}(v)$.

  – Assume $b \in \text{NonTip}(W)$.
    Then, $\text{Tip}(v - \alpha b) < \text{Tip}(v)$, so $v - \alpha b = w + z \in W + \text{Span}(\text{NonTip}(W))$.
    $v = w + [z + \alpha b] \in W + \text{Span}(\text{NonTip}(W))$.#

– Assume $b \in \text{Tip}(W)$.
Let $w \in W$ s.t. $\text{Tip}(w) = b$.
Let $\beta = \text{CTip}(w)$. Then,
$\text{Tip}(v - (\alpha/\beta)w) < \text{Tip}(v)$, so
$v - (\alpha/\beta)w = w' + z \in W + \text{Span}(\text{NonTip}(W))$.
$v = [w' + (\alpha/\beta)w] + z \in W + \text{Span}(\text{NonTip}(W))$.#

If $v \in V$ then there exists unique $w_v \in W$ $N(v) \in \text{Span}(\text{NonTip}(W))$ s.t. $v = w_v + N(v)$.

Def^n We call $N(v)$ the *normal form* of v.

Def^{n} Let W be a subspace of V, $\mathcal{G} \subset W$. Then $\mathcal{G}$ is a *linear Gröbner Basis (L.G.b.) for W w.r.t. $<$* if:

$$\text{Span}(\text{Tip}(\mathcal{G})) = \text{Span}(\text{Tip}(W)).$$

Lemma 2 *If $\mathcal{G}$ is a L.G.b. of W then,*

$$\text{Span}(\mathcal{G}) = W.$$

Proof $(\subset)$ $\mathcal{G} \subset W$.

$(\supset)$ Let $w = w_1 \in W$,
$\text{Tip}(w_1) = \sum \alpha_{1i}\text{Tip}(g_{1i})$ by def. of $\mathcal{G}$.
and $\beta_1 = \text{CTip}(w_1)$, $\gamma_{1i} = \text{CTip}(g_{1i})$.
Let $w_2 = w_1 - \beta_1 \sum(\alpha_{1i}/\gamma_{1i})g_{1i}$, then if $w_2 \neq 0$: $\text{Tip}(w_2) < \text{Tip}(w_1)$. Repeat to obtain $0 = w - \beta_1 \sum(\alpha_{1i}/\gamma_{1i})g_{1i} - \cdots - \beta_l \sum(\alpha_{li}/\gamma_{li})g_{li}$.

∎

Reduced Linear Gröbner Bases

Def^{n}
$\mathcal{G} \subset W$ is a *reduced L.G.b.* for W w.r.t. $<$ if:

1. $\mathcal{G}$ is a L.G.b. of W
2. $g \in \mathcal{G} \;\Rightarrow\;$ CTip$(g) = 1$
3. $g \neq g' \in \mathcal{G} \;\Rightarrow\;$ Tip$(g) \neq$ Tip(g')
4. $g \in \mathcal{G} \;\Rightarrow$
   $g -$ Tip$(g) \in$ Span(NonTip(W)).

Lemma 3 *There is a unique r.L.G.b.*

Proof Let $\mathcal{T} =$ Tip(W) and let $\mathcal{G} = \{t - N(t) : t \in \mathcal{T}\}$. By Theorem (1) $t - N(t) \in W$. Also, Tip$(t - N(t)) = t$. Thus $\mathcal{G}$ is a L.G.b. of W. Rest of properties easy.

∎

Example

Let $k^4 \supset W = \text{Span}(a, b, c)$.

Write as matrix:

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \end{pmatrix}$$

Row reduce:

$$\begin{pmatrix} 1 & * & 0 & * \\ 0 & 0 & 1 & * \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Rows are a reduced L.G.b.

Algebra Gröbner Bases

R a k-algebra.

Def$^{\mathbf{n}}$ $\mathcal{B}$ is a *multiplicative basis* for R if $\mathcal{B}$ is a k-basis and $\forall b_1, b_2 \in \mathcal{B}$, $b_1 b_2 \in \mathcal{B} \cup \{0\}$.

Def$^{\mathbf{n}}$ A well-order $>$ is an *admissable order* on $\mathcal{B}$ if $\forall b_1, b_2, c, d \in \mathcal{B}$:

A1. $b_1 > b_2 \;\Rightarrow\; b_1 c > b_2 c$ if $b_1 c \neq 0 \neq b_2 c$

A2. $b_1 > b_2 \;\Rightarrow\; c b_1 > c b_2$ if $c b_1 \neq 0 \neq c b_2$

A3. $c = b_1 d b_2 \;\Rightarrow\; c \geq d$.

Def$^{\mathbf{n}}$ We call $(\mathcal{B}, >)$ an *ordered multiplicative basis* in case $>$ is an admissable order.

Let I be an ideal in R.

Def$^{\mathbf{n}}$ A set $\mathcal{G} \subset I$ is a *Gröbner basis* w.r.t. $>$ if:

$$\langle \mathsf{Tip}(\mathcal{G}) \rangle = \langle \mathsf{Tip}(I) \rangle.$$

i.e. the same two-sided ideal is generated.

Note: Theorem (1) still applies in vector space sense.

2-nomial Ideals

Def$^{\mathbf{n}}$ An ideal I of R is a *2-nomial ideal* if it can be generated by elements of the form $b_1 - b_2$ and b, where $b_1, b_2, b \in \mathcal{B}$.

Proposition 4 *There is a 1-1 correspondence between the set of equivalence relations on $\mathcal{B} \cup \{0\}$ and 2-nomial ideals.*

Notation: Greek letters in k, $b_i \in \mathcal{B}$.

Lemma 5 *Let I be a 2-nomial ideal with associated relation $\sim_I$. Then $\sum_{i=1}^{r} \alpha_i b_i \in I$ iff $\forall [b]$ of $\sim_I$, $\sum_{b_i \in [b]} \alpha_i b_i \in I$.*

Theorem 6 *Suppose S is a k-algebra with mult. basis $\mathcal{C}$. Let I be an ideal in S, $\pi\colon S \longrightarrow S/I$, and $\mathcal{B} = \pi(\mathcal{C})$. Then,*

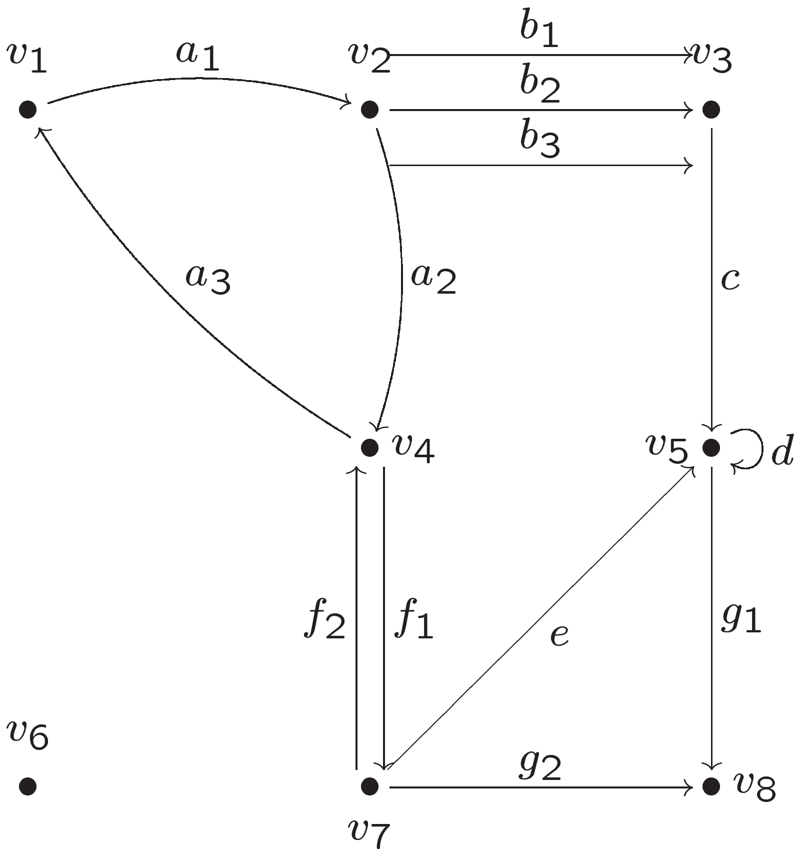
$\mathcal{B}$ is a mult. basis for S/I
iff
I is a 2-nomial ideal.

Proof *Linear independence:*
Suppose $\sum_{i=1}^{n} \alpha_i \pi(c_i) = 0$, $\pi(c_i) \neq 0$.
Therefore, $\sum_{i=1}^{n} \alpha_i c_i \in I$.
So, $\forall [c] \sum_{c_i \in [c]} \alpha_i c_i \in I$ by Lemma (5). If $c_i \in [c]$ then $\pi(c_i) = \pi(c)$. Therefore, different c_i's in different $[c]$'s as $\pi(c_i)$ distinct. So, $\alpha_i c_i \in I$. Since $\pi(c_i) \neq 0$, $\alpha_i = 0$.

∎

Quivers

A *quiver* $\Gamma(\Gamma_0, \Gamma_1)$ is
- a set Γ_0 of *vertices*
- a set Γ_1 of *arrows*



Initial and terminal vertex of an arrow:

$$ia_1 = v_1, \quad ta_1 = v_2$$

similarly for a vertex:

$$iv = v, \quad tv = v.$$

Path Algebras

Let $a, b \in \Gamma_0 \cup \Gamma_1$:

$$ab = \begin{cases} 0 & ta \neq ib \\ a & b = ta \\ b & a = ia \\ ab & \text{otherwise.} \end{cases}$$

Def$^{\mathbf{n}}$ A *path* p in Γ is a product of arrows, or a single vertex.

Note: We define ip, tp, and length of a path.

Def$^{\mathbf{n}}$ The *path algebra* $k\Gamma$ of Γ has k-basis the paths and multiplication as above.

Theorem 7 *Let R be a k-algebra with ordered multiplicative basis $(\mathcal{B}, >)$. Let Γ be the graph associated to $\mathcal{B}$. Then there is a surjective k-algebra homomorphism $\phi\colon k\Gamma \longrightarrow R$ s.t.:*

1. *If p is a directed path in Γ then $\phi(p) \in \mathcal{B} \cup \{0\}$*

2. *If $b \in \mathcal{B}$ then $\exists p \in \Gamma$ s.t. $\phi(p) = b$*

3. *$\ker\phi$ is a 2-nomial ideal.*

Proof Let $1 = \sum_{i=1}^{n} \alpha_i v_i$ with $\alpha_i \in k^*$, distinct $v_i \in \mathcal{B}$.

- $v_1, \ldots, v_n$ *orthogonal idempotents,* $\alpha_i = 1$.

$$v_i = v_i.1 = \sum_{j=1}^{n} \alpha_j v_i v_j$$

But $v_i v_j = b \in \mathcal{B}$ if non-zero. Assume $b \neq v_i$ then must be another $v_i v_l = b$ to cancel. Now, $v_j > v_l$ or $v_l > v_j$ so $v_i v_l \neq v_i v_j$.#

- *Cancellation:* $b_1 \neq b_2 \in \mathcal{B}, b \in \mathcal{B}$:

$$b_1 b = b_2 b \;\Rightarrow\; b_1 b = 0 = b_2 b$$

$$b b_1 = b b_2 \;\Rightarrow\; b b_1 = 0 = b b_2.$$

  As $b_1 > b_2 \;\Rightarrow\; b_1 b > b_2 b.$

- $b \in \mathcal{B}$. *Unique* i, j *s.t.* $v_i b = b$, $b v_j = b$ *and* $l \neq i$ *means* $v_l b = 0$.

$$b = b.1 = \sum_{i=1}^{n} b v_i.$$

- v_i*'s minimal w.r.t* $>$ as $b = b v_i v_i$ and A3.

- $b \in \mathcal{B} \setminus \{v_1, \ldots, v_n\} \;\Rightarrow\; b^2 \neq b.$

$$b > v_i, b v_i = b \;\Rightarrow\; b^2 > b \quad \text{by A2.}$$

- $\Gamma_0 := \{v_1, \ldots, v_n\}$ *full set of primitive orthogonal idempotents.*
  - $1 = \sum_{i=1}^n v_i$ therefore full.
  - Suppose $v_i = x + y$, x, y orth. idem. $x = \sum_i \alpha_i v_i + \sum_l \beta_l b_l$. But $v_i = v_i x v_i + v_i y v_i$. So, $v_i b_l = b_l$ and,

    $$x = \alpha_i v_i + \sum_l \beta_l b_l, \quad y = (1 - \alpha_i) v_i - \sum_l \beta_l b_l$$

  - Now $xy = 0$, $b_l b_j \neq v_i$, so $\alpha_i(1 - \alpha_i) = 0$. Say $\alpha_i = 1$.
  - Let b denote smallest b_l. Now, $v_i b = b$ and $b < b_l b_j$ where non-zero. So can't cancel $v_i b$ in $xy = 0$ and all $\beta_l = 0$.

Def$^{\mathbf{n}}$ $b \in \mathcal{B}$ is *product indecomposible* if $b \notin \Gamma_0$ and $b \neq b_1 b_2$ with $b_1, b_2 \in \mathcal{B} \setminus \Gamma_0$.

Def$^{\mathbf{n}}$ Let Γ_1 be the set of product indecomposibles.

- $\forall b \in \mathcal{B} \setminus \Gamma_0 \;\; \exists b_1 \ldots b_r \in \Gamma_1$ *s.t.* $b = b_1 \cdots b_r$.
  If $b \notin \Gamma_0 \cup \Gamma_1$, $b = b_1 b_2$ for some $b_1 b_2 \in \mathcal{B} \setminus \Gamma_0$.
  $b = i b_1 b_1 b_2 = b_1 b_2 t b_2 \;\Rightarrow\; b \geq b_1,\ b \geq b_2$ by A3.
  $b = b_1 \;\Rightarrow\; b.tb = b_1 b_2 = b b_2$. Cancelling, $tb = b_2$.
  So, $b > b_1$, $b > b_2$, done by induction.

Open Question 8 *Given a quiver* Γ*, what are necessary and sufficient conditions on a 2-nomial ideal* I *s.t.* $k\Gamma/I$ *has a Gröbner Basis theory in the sense that the image of the paths admits an admissible order?*

Admissible orders

length-lexicographic order:
Order vertices and arrows arbitrarily and set vertices smaller than arrows:

$$a_1 > \cdots > a_m > v_1 > \cdots > v_n.$$

If p, q are paths of length at least 1, $p > q$ if $\ell(p) > \ell(q)$, or if $p = b_1 \cdots b_m$ and $q = c_1 \cdots c_m$ then $b_i > c_i$ where i is the smallest integer s.t. $b_j \neq c_j$.

weight-lexicographic order:
Let $W : \Gamma_1 \longrightarrow \mathbb{N}$. Extend W additively to $\mathcal{B}$, so $W(a_1 \cdots a_r) = \sum_i W(a_i)$. Order the vertices and set them smaller than arrows. Order arrows s.t. $W(a) < W(b) \Rightarrow a < b$. Define $p < q$ if $W(p) < W(q)$. Or if $W(p) = W(q)$ use lexicographic order.

Theory of Right Gröbner bases

Let R be a k-algebra with $(\mathcal{B}, >)$. Let M be a right (unital) R-module. Let $\mathcal{M}$ be a k-basis of M.

Def$^{\mathbf{n}}$ $\mathcal{M}$ is a *coherent* basis if:

$$\forall m \in \mathcal{M} \quad \forall b \in \mathcal{B} \quad mb \in \mathcal{M} \cup \{0\}.$$

Lemma 9 *If $\mathcal{M}$ is coherent then $\forall m \in \mathcal{M} \quad \exists v \in \Gamma_0$ s.t. $mv = m$.*

Proof $m = m.1 = \sum_{v \in \Gamma_0} mv.$

∎

Def^n A well-order $\succ$ on $\mathcal{M}$ is *right admissible* if $\forall m, m_1, m_2 \in \mathcal{M} \quad \forall b, b_1, b_2 \in \mathcal{B}$:

M1. $m_1 \succ m_2 \;\Rightarrow\; m_1 b \succ m_2 b$ if $m_1 b \neq 0 \neq m_2 b$

M2. $b_1 > b_2 \;\Rightarrow\; m b_1 \succ m b_2$ if $m b_1 \neq 0 \neq m b_2$.

Def^n $(\mathcal{M}, \succ)$ is an *ordered basis* if $\mathcal{M}$ is coherent and $\succ$ is right admissible.

Note: If $m \in \mathcal{M} \quad b \in \mathcal{B} \setminus \Gamma_0$ then
$mb \succ m$ if $mb \neq 0 \neq m$.

Def^n Define Tip, CTip, NonTip, and $N(m)$ as before.

Def^{n} Let N be a right submodule of M. Then $\mathcal{G} \subset N$ is a *Right Gröbner basis* for N w.r.t. $\succ$ if:

$$\langle \text{Tip}(\mathcal{G}) \rangle = \langle \text{Tip}(N) \rangle.$$

Proposition 10 *N submodule of M. Then:*

1. *There is a Right G.b. for N w.r.t. $\succ$*

2. *If $\mathcal{G}$ is a R.G.b. for N then $\mathcal{G}$ generates N as a submodule*

3. *As vector spaces* $M = N \oplus \text{Span}(\text{NonTip}(N))$.

WARNING 11 *Most modules* DON'T *have a right Gröbner basis theory.*

Def$^{\mathbf{n}}$ $m, m' \in \mathcal{M}$. m *left divides* m' if:

$$\exists b \in \mathcal{B} \text{ s.t. } m' = mb.$$

Def$^{\mathbf{n}}$ A R.G.b. $\mathcal{G}$ of N is *reduced* if for $g = \sum_{i=1}^{r} \alpha_i m_i \in \mathcal{G}$ and $g' \in \mathcal{G} \setminus \{g\}$:

- Tip(g') doesn't left divide m_i

- CTip(g) $= 1$

Equivalently: If $g \in \mathcal{G}$ then $g -$ Tip(g) $\in$ Span(NonTip(N)).

Def$^{\mathbf{n}}$ $\mathcal{G}$ is *tip-reduced* if $g, g' \in \mathcal{G}$ and Tip(g) left divides Tip(g') then $g = g'$.

Note: reduced $\Rightarrow$ tip-reduced.

Def$^{\mathbf{n}}$ $x \in M$ is *(left) uniform* if $\exists v \in \Gamma_0$ s.t. $xv = x$.

Proposition 12 *Tip-reduced uniform right Gröbner bases exist.*

Projective Modules

Let R be a k-algebra with $(\mathcal{B}, >)$.

$$\bigoplus_{v \in \Gamma_0} vR = R$$

So vR is a projective, which we denote by P_v.

If X is an index set and $V : X \longrightarrow \Gamma_0$ then

$$P = \bigoplus_{i \in X} P_{V(i)}$$

is a projective module.

Gröbner Bases for Projectives

Let $\mathcal{P}_v = \{x \in P_v : x = vx, x \in \mathcal{B}\}$.
Let $(\mathcal{P}_v, \succ)$ be the restriction of $(\mathcal{B}, >)$. If $P = \bigoplus_{i \in X} P_{V(i)}$ let:

$$\mathcal{P}_i = \{x \in P : x_i \in \mathcal{P}_{V(i)}, x_j = 0 \text{ if } j \neq i\}.$$

Let $\mathcal{P} = \bigcup_{i \in X} \mathcal{P}_i$.
If we have an ordering on X and then we can extend to an ordering $(\mathcal{P}, \succ)$.

Construction of Uniform Tip-reduced Right Gröbner Bases

Let $P = \bigoplus_{i \in X} P_{V(i)}$ as above, with $(\mathcal{P}, \succ)$.

If Q is a submodule of P with generating set $\mathcal{F}'$, let,

$$\mathcal{F} = \{fv : f \in \mathcal{F}', v \in \Gamma_0\}.$$

Thus, $\mathcal{F}$ is a set of uniform elements that generates Q.

Theorem 13 *Every uniform tip-reduced generating set of Q is a R.G.b.*

Algorithm 14

1. *$\mathcal{H}$ finite uniform generating set for Q without* 0.

2. *$\mathcal{T} = \{\text{Tip}(h) : \text{Tip}(h')$ doesn't left divide $\text{Tip}(h), h' \in \mathcal{H} \setminus \{h\}\ \}$.*

3. *For each $t \in \mathcal{T}$ choose some $h \in \mathcal{H}$ s.t. $\text{Tip}(h) = t$, and renumber so these are $h_1, \ldots, h_s$.*

4. *If $s = r$* STOP.

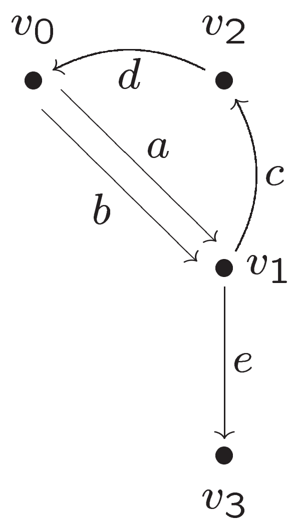
5. *Let $Q^* = \langle h_1, \ldots, h_s \rangle$.*

6. *For $i = s + 1, \ldots, r$ write $h_i = h_i^* + N(h_i)$ using $P = Q^* \oplus \text{Span}(\text{NonTip}(Q^*))$.*

7. *$\mathcal{H} = \{h_1, \ldots, h_s, N(h_{s+1}), \ldots, N(h_r)\}$.*

Repeat.

Example



$$
\mathcal{B} = \begin{array}{ll} \{ & v_0 < v_1 < v_2 < v_3, \\ & < a < b < c < d < e, \\ & < ac < ae < bc < be < cd < da < db, \\ & < acd < bcd < cda < cdb < dac < dbc, \\ & < acda < acdb < acde < bcda < bcdb, \\ & < bcde < cdac < cdbc < cdbe < dacd, \\ & < dbcd < \cdots \} \end{array}
$$

$$P = P_0 \oplus P_1 \oplus P_1$$

$$
\begin{aligned}
\mathcal{P}_0 &= \begin{aligned}[t] \{\ & v_0, \\ & < a < b, \\ & < ac < ae < bc < be, \\ & < acd < bcd, \\ & < acda < acdb < bcda < bcdb < \cdots \} \end{aligned}
\end{aligned}
$$

$$
\mathcal{P}_1 = \{v_1 < e\}
$$

$$
Q = \langle \mathcal{F}' \rangle = \langle abc + ac + cd - acd, e_1 - a, a - b \rangle
$$

$$
\begin{aligned}
\mathcal{F} &= \{fv : f \in \mathcal{F}', v \in \Gamma_0\} \\
&= \{0, cd - acd, -a, a, -b, abc + ac, e_1\}
\end{aligned}
$$

1. $\mathcal{H} = \{cd - acd, -a, a, -b, abc + ac, e_1\}$

2. $\text{Tip}(\mathcal{H}) = \{cd, a, b, ac, e_1\}$
   $\mathcal{T} = \{cd, a, b, e_1\}$

3. $\mathcal{H} = \{cd - acd, a, -b, e_1, abc + ac, -a\}$

4. $4 = s \neq r = 6$

5. $Q^* = \langle cd - acd, a, -b, e_1 \rangle$

6. $N(abc + ac) = 0$
   $N(-a) = 0$

7. $\mathcal{H} = \{cd - acd, a, -b, e_1, 0\}$

So, required Gröbner Basis is:

$$\mathcal{Q} = \{cd - acd, a, -b, e_1\}$$