Nowadays a number of researchers have conducted work on accelerating the process of calculating a Gröbner basis by analyzing the existing essential algorithms. A series of improvements has been made toward this end. At the same time, the fact that each of them maintains its own terminology makes the task of comparing each of the algorithms exceedingly troublesome. Hence there arises the need to compare and systematize these solutions.

Buchberger’s algorithm provides the basic algorithm to construct a Gröbner basis. Further on, we will fashioned it in its traditional appearance, in which it appears in [1]. For optimization they use two criteria of Buchberger that allow one to exclude a series of $S$-polynomials from examination. In the algorithm the polynomials in $G$ are indexed, and pairs of distinct polynomials $f_i, f_j$ are denoted $(i, j)$, $i < j$. The algorithms maintain a list $B$ of the pairs corresponding to those $S$-polynomials that need to be calculated and reduced during the course of the algorithm.

**Definition 1.** We denote by $\prec$ an admissible ordering on the monoid $\mathbb{M}$. The monomial $u \in \mathbb{M}$ in the polynomial $f$ that is ordered highest relative to $\prec$ is called the leading monomial of $f$ and is written $\text{lm} (f)$. The coefficient of $\text{lm} (f)$ is called the leading coefficient of $f$ and is written as $\text{lc} (f)$. The leading term $\text{lc} (f) \text{lm} (f)$ is written as $\text{lt} (f)$. In the same way, we can fix the second highest term in $f$, denoted as $\text{sc} (f) \text{sm} (f)$.

The monomial $\text{lcm} (\text{lm} (f), \text{lm} (g))$ is written as $\text{lcm} (f, g)$, where the lcm is the least common multiple. The largest common divisor of $\text{lm} (f), \text{lm} (g)$ is written as $\text{gcd} (f, g)$.

The first of Buchberger’s Criteria consists in the following. If $\text{lcm} (f, g) = \text{lm} (f) \text{lm} (g)$, then that pair can be excluded from the examination during the course of the algorithm.

The second of Buchberger’s Criteria we denote by the function $\text{Criterion} (f_i, f_j, B)$. To define this, we introduce for the pair

$$[i, j] = \begin{cases} (i, j), & i < j, \\ (j, i), & j < i. \end{cases}$$

Then $\text{Criterion} (f_i, f_j, B)$ is satisfied if $\exists \ell \not\in \{i, j\}$ such that $[i, \ell]$ and $[j, \ell]$ do not belong to $B$ and $\text{lm} (f_\ell) \mid \text{lcm} (f_i, f_j)$.

**Algorithm 1. Buchberger’s Algorithm**

**Input:** A finite set of polynomials $F$

**Output:** A Gröbner basis $F$ of the ideal $I = \text{Id} (F)$

$$(f_1, \ldots, f_s) = \text{Interreduce} (F)$$

$G := (f_1, \ldots, f_s)$

$B := \{(i, j) : 1 \leq i < j \leq s\}$

---

This work was partly sponsored by the Russian Foundation for Fundamental Investigation, Project No. 05-01-00671.
The algorithm does not specify how to choose the current pair \((i, j) \in B\). One rule, called the **normal strategy**, chooses the pair such that \(\text{lcm}(f_i, f_j)\) has the smallest rank relative to some admissible ordering \(\sqsubseteq\), which need not be the same as the monomial ordering \(<\).

In the process of executing the given algorithm, one encounters the problem of discarding as many \(S\)-pairs as possible for which it can be known beforehand that they reduce to zero.

There exist two approaches to exclusion of reduction to zero: using representation and using syzygies.

**Definition 2.** If the polynomial \(f\) can be represented in the form of a sum \(h_1g_1 + \cdots + h_sg_s\), where the \(h_i\) are polynomials, the \(g_i\) are elements of \(G\), and they satisfy \(\text{lm}(f) \geq \text{lm}(h_ig_i)\), then we write

\[
   f \equiv 0 \pmod{G}.
\]

If \(f - g \equiv 0 \pmod{G}\), then \(f \equiv g \pmod{G}\). The relation \(\equiv\) satisfies the reflexive, symmetric, and transitive properties, and thus it is an equivalence relation.

Note that if a polynomial reduces to 0 mod \(G\), then it is equivalent to 0 mod \(G\), but a representation of a polynomial in the appearance of a sum \(h_1g_1 + \cdots + h_sg_s\) (with \(\text{lm}(f) \geq \text{lm}(h_ig_i)\)) does not automatically induce by itself reduction of \(f\) to 0 mod \(G\). However, if \(G\) is a Gröbner basis of the ideal of \(G\), then the fact that \(f \equiv 0 \pmod{G}\) induces by itself the correlation \(\text{NF}(f, G) = 0\). The validity of Buchberger’s criteria derives from this property.

In the works cited [2, 3], the number of useless pairs generated by Buchberger’s algorithm can exceed the number of those that generate new \(S\)-polynomials. This prompts the authors use a special terminology, **polynomial syzygies**.

**Definition 3.** Let \(g_i\) be polynomials of the set \(G\) \((i = 1, 2, \ldots, n)\). Then the list of \(n\) polynomials \((h_1, \ldots, h_n)\) is called a syzygy if it satisfies \(h_1g_1 + \cdots + h_ng_n = 0\).

Obviously, if the \(S\)-polynomial \(S(f, g)\) was reduced to 0 mod \(G\), then the process of creating the \(S\)-polynomial, along with its subsequent reduction to 0, gives us a sequence of additions and subtractions of polynomials that correspond to some syzygy.

In [2, 3] it is shown that a series of two criteria cannot consider as expense using “trivial” syzygies \(g_jg_i - g_ig_j\), where \(g_i, g_j\) are distinct polynomials of \(G\). Consequently, there
arises the task of enlarging and reinforcing the criteria of Buchberger, bringing in to them “information” contained in the previously seen “trivial” equalities, and understood as far as important effect given new information. The given problem can be solution of help of polynomial representation only partly.

**Lemma 1.** Let $G$ be a set of polynomials, and $g_1, g_2$ two distinct polynomials that satisfy the property $\text{sm}(g_1)\text{lm}(g_2) \neq \text{sm}(g_2)\text{lm}(g_1)$. Then $\gcd(g_1, g_2)S(g_1, g_2) \equiv 0 \pmod{G}$.

**Proof.** Consider the identity $g_1g_2 - g_2g_1 = 0$. Write $g_1 - \text{lc}(g_1)\text{lm}(g_1) + p$ and $g_2 = \text{lc}(g_2)\text{lm}(g_2) + q$. An obvious consequence of this equality is the expression

$$\text{lc}(g_1)\text{lm}(g_1)g_2 - \text{lc}(g_2)\text{lm}(g_2)g_1 = -p \cdot g_2 + q \cdot g_1.$$ 

It is evident that $\text{lm}(\text{lc}(g_1)\text{lm}(g_1)g_2 - \text{lc}(g_2)\text{lm}(g_2)g_1) = \max\{\text{lm}(p \cdot g_2), \text{lm}(q \cdot g_1)\}$. It follows from this, from $\text{sm}(g_1) = \text{lm}(p)$, $\text{sm}(g_2) = \text{lm}(q)$, and from $\text{sm}(g_1)\text{lm}(g_2) \neq \text{sm}(g_2)\text{lm}(g_1)$ that the leading terms $\text{lm}(p \cdot g_2)$ and $\text{lm}(q \cdot g_1)$ do not cancel. Thus, the expression $-pg_2 + qg_1$ gives a representation modulo $G$ for the left hand side of the equation. We concluded by remarking that $\text{lc}(g_1)\text{lm}(g_1)g_2 - \text{lc}(g_2)\text{lm}(g_2)g_1 = \gcd(g_1, g_2)S(g_1, g_2)$.

**Lemma 2.** If $\gcd(g_1, g_2) = 1$, then the previous lemma ensures that the first Buchberger criterion is satisfied. That is, $S(g_1, g_2) \equiv 0 \pmod{G}$.

**Proof.** We need only show that the hypothesis $\text{sm}(g_1)\text{lm}(g_2) \neq \text{sm}(g_2)\text{lm}(g_1)$ is satisfied. Indeed, if $\gcd(g_1, g_2) = 1$, the contrary expression would imply that $\text{lm}(g_1) \mid \text{sm}(g_1)$, an impossibility since $\text{lm}(g_1) \succ \text{sm}(g_1)$.

In this way, we see that Buchberger’s first criterion is not that different from trivial syzygies, insofar as useful information. Nevertheless, the transition from syzygies to a deeper understanding of representation in the general case requires analysis of additional information, namely, the second leading terms of the polynomials.

**Remark 1.** Lemma 1 also applies in the more case where $\text{sm}(g_1)\text{lm}(g_2) = \text{sm}(g_2)\text{lm}(g_1)$ and $\text{sc}(g_1)\text{lc}(g_2) \neq \text{sc}(g_2)\text{lc}(g_1)$. Nevertheless, operations with coefficients often occupy much time and checking the conditions of representation is expensive.

Lemma 1 allows some insight into Buchberger’s second criterion and discarded pairs.

**Theorem 1.** Let $G$ be a set of polynomials and $g_1, g_2, g_3$ three distinct elements of $G$, such that $\text{lm}(g_3) \mid \text{lcm}(g_1, g_2)$. Suppose that for each pair $(g_i, g_j)$ (where $i \in \{1, 2\}$ and $j$ is an integer not equal to $i$ in $\{1, 2\}$) the following holds:

- either $S(g_i, g_3) \equiv 0 \pmod{G}$
- or $\text{lm}(g_j) \mid \frac{\text{lcm}(g_i, g_j)}{\text{gcd}(g_1, g_2)}$ and $\text{sm}(g_j)\text{lm}(g_3) \neq \text{sm}(g_3)\text{lm}(g_j)$.

Then $S(g_1, g_2) \equiv 0 \pmod{G}$.

**Proof.** The proof is based on the identity

$$S(g_1, g_2) = \alpha \frac{\text{lcm}(g_1, g_2)}{\text{lcm}(g_1, g_3)}S(g_1, g_3) - \beta \frac{\text{lcm}(g_2, g_3)}{\text{lcm}(g_1, g_3)}S(g_2, g_3),$$

where $\alpha, \beta$ are coefficients.

If both $S$-polynomials $S(g_1, g_3)$ and $S(g_2, g_3)$ have representations, then the proof is obvious. That leaves us to examine the two conditions of the theorem.
Let $i = 2$, $j = 1$. We have the equality
\[
\frac{\text{lcm} (g_1, g_2)}{\text{lcm} (g_1, g_3)} S (g_1, g_3) = \frac{\text{lm} (g_1) \text{lm} (g_2)}{\text{lm} (g_1) \text{lm} (g_3)} \frac{\text{gcd} (g_1, g_2)}{\text{gcd} (g_1, g_3)} S (g_1, g_3) = \frac{\text{lm} (g_2)}{\text{lm} (g_3) \text{gcd} (g_1, g_2)} \frac{\text{gcd} (g_1, g_3)}{\text{lm} (g_1) \text{lm} (g_3)} S (g_1, g_3) .
\]

If the second condition is satisfied, we have
\[
\frac{\text{lcm} (g_1, g_2)}{\text{lcm} (g_1, g_3)} S (g_1, g_3) \equiv 0 \pmod{G} .
\]

Thus, Buchberger’s second criterion can be generalized in the following manner.

The logical function $\text{Criterion} (f_i, f_j, B)$ is satisfied if $\exists \ell \notin \{i, j\}$ such that $\text{lm} (f_\ell) \mid \text{lcm} (f_i, f_j)$, where the element $[i, \ell]$ does not belong to $B$, or belongs to $B$ and the condition $\text{lm} (g_\ell) \mid \frac{\text{lm} (g_\ell)}{\text{gcd} (g_1, g_2)}$ and $\text{sm} (g_j) \text{lm} (g_\ell) \neq \text{sm} (g_\ell) \text{lm} (g_j)$, and similarly for $[j, \ell]$ by swapping the places of indices $i, j$ between themselves.

Thanks to the property $\text{lm} (f_\ell) \mid \text{lcm} (f_i, f_j)$ in the case of the \textbf{normal strategy} and subsequent executions of Buchberger’s algorithm, this generalization of the second criterion will not provide any additional benefit. Nevertheless, when parallelizing of Buchberger’s algorithm, or when adopting a strategy different from the normal strategy, one can expect that the given criteria will discover a number of new “useless” $S$-pairs. In connection with this we note that the strategy of the algorithm F5 ([2]) is not the normal strategy, inasmuch as it is based on consecutive calculation of Gröbner bases of the ideals $\langle f_n \rangle, \langle f_{n-1}, f_n \rangle, ...$, $\langle f_1, \ldots, f_n \rangle$.

\textbf{REFERENCES}


Translated by JOHN PERRY

\textit{Current address}: Moscow State University, College of Mechanics and Mathematics
\textit{E-mail address}: semyonov1980@mail.ru