Math-Net.Ru

Общероссийский математический портал

О. Н. Герман, Доказательство критерия Фожера для алгоритма F5, *Матем. заметки*, 2010, том 88, выпуск 4, 502–510

DOI: <https://doi.org/10.4213/mzm8849>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.162.85.209

26 апреля 2023 г., 18:00:23

Доказательство критерия Фожера для алгоритма F5

О. Н. Герман

Доказан критерий Фожера для алгоритма F5.

Библиография: 7 названий.

1. Введение

Пусть R – кольцо многочленов от m переменных над полем $\mathbb{F}$ и $I = (f_1, \dots, f_n)$ – идеал, порожденный многочленами $f_1, \dots, f_n \in R$. Пусть G – конечное подмножество идеала I , содержащее многочлены $f_1, \dots, f_n$. Данная заметка посвящена доказательству критерия того, что множество G является базисом Грёбнера идеала I .

Напомним, что G называется *базисом Грёбнера* в том случае, если старший моном каждого многочлена из I делится на старший моном какого-то многочлена из G .

Для того чтобы говорить о старших мономах многочленов, нужно ввести порядок на множестве *термов*, т.е. мономов со старшим коэффициентом 1. Термы образуют полугруппу относительно умножения, которую мы будем обозначать буквой $\mathcal{T}$. Пусть “ $\preceq$ ” – некоторый порядок на полугруппе $\mathcal{T}$, относительно которого $\mathcal{T}$ является вполне упорядоченным множеством. Пусть порядок “ $\preceq$ ” согласован с умножением в полугруппе $\mathcal{T}$, т.е. для любых $t, s, r \in \mathcal{T}$ из неравенства $t \preceq s$ следует неравенство $tr \preceq sr$, и пусть он удовлетворяет аксиоме обрыва убывающих цепочек.

Относительно порядка “ $\preceq$ ” у любого многочлена f однозначно определяется *старший терм*, который мы будем обозначать символом $\text{HT}(f)$. Ему соответствует старший моном, о котором и говорится в определении базиса Грёбнера.

Существует ряд алгоритмов, позволяющих по заданным многочленам $f_1, \dots, f_n$ построить базис Грёбнера идеала I . Самым быстрым на данный момент алгоритмом является алгоритм F5, предложенный Фожером в 2002-м г. [1]. С алгебраической точки зрения ключевым моментом этого алгоритма является критерий того, что набор многочленов образует базис Грёбнера. Соответствующая теорема была сформулирована самим Фожером, однако корректного доказательства до сих пор нигде опубликовано не было. В текстах Фожера, включая его докторскую диссертацию [2], предлагается лишь идея доказательства, основной же упор делается на обсуждение конкретных примеров. Реализовать идею попытался в своей дипломной работе Штегерс [3], но попытка эта оказалась неудачной, поскольку, как признает сам Штегерс, полностью доказать основную теорему он не смог. Его рассуждения,

Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 09-01-00371) и грантов Президента РФ (гранты №№ МК-4466.2008.1, МК-1226.2010.1).

но в терминах работы [1], воспроизвел Гаш [4]. В работах Перри и Эдера [5], [6] изучается случай однородных многочленов и предлагается более общая формулировка критерия F5. В оригинальной версии алгоритма F5 требовалось, чтобы исходные многочлены были однородными и образовывали регулярную последовательность. Это требование было устранено в работе [7], в которой было показано, что на вход можно подавать произвольный набор многочленов.

В данной работе предлагается подробное доказательство критерия Фожера. Мы не касаемся алгоритма в целом, не доказываем его корректность и не приводим псевдокод. Целью данного исследования было только доказательство самого критерия. Используемая в доказательстве конструкция существенно отличается от предлагавшейся Фожером. В частности, мы не используем рассуждения в модуле векторных многочленов, а ограничиваемся стандартной алгеброй многочленов.

2. Формулировка критерия

2.1. Индекс, сигнатура и метка многочлена. Для каждого $i = 1, \dots, n$ положим $I_i = (f_i, \dots, f_n)$. Рассмотрим произвольный многочлен $f \in I$.

Индексом $i(f)$ многочлена f будем называть максимальное i такое, что $f \in I_i$.

Очевидно, что существуют такие многочлены $\lambda \in R$, что

$$f \equiv \lambda f_{i(f)} \pmod{I_{i(f)+1}}.$$

Среди старших термов всех таких многочленов есть минимальный. Будем его называть *сигнатурой* $s(f)$ многочлена f .

Пару $\mathfrak{S}(f) = (i(f), s(f))$ будем называть *меткой* многочлена f . На множестве меток введем порядок “ $\leq$ ” следующим образом:

$$\mathfrak{S}(f) \leq \mathfrak{S}(g) \iff \begin{cases} i(f) > i(g); \\ i(f) = i(g), \quad s(f) \leq s(g). \end{cases}$$

Отметим, что множество $\mathbb{Z} \times \mathcal{T}$ относительно подобного порядка является вполне упорядоченным. Соответственно, строгое неравенство “ $\triangleleft$ ” определяем так:

$$\mathfrak{S}(f) \triangleleft \mathfrak{S}(g) \iff \begin{cases} i(f) > i(g); \\ i(f) = i(g), \quad s(f) \prec s(g). \end{cases}$$

Здесь и далее символ “ $\prec$ ” используется как строгий вариант неравенства “ $\leq$ ”.

Определим также умножение меток на термы: для любого $t \in \mathcal{T}$ положим

$$t\mathfrak{S}(f) = (i(f), ts(f)).$$

2.2. s-Полиномы. Напомним, что *s-полиномом* двух многочленов f, g со старшими коэффициентами c_f и c_g соответственно называется многочлен

$$\text{spol}(f, g) = c_g u_{f,g} f - c_f u_{g,f} g,$$

где

$$u_{f,g} = \frac{\text{НОК}(\text{HT}(f), \text{HT}(g))}{\text{HT}(f)}, \quad u_{g,f} = \frac{\text{НОК}(\text{HT}(f), \text{HT}(g))}{\text{HT}(g)}.$$

Тем самым, по многочленам f, g , помимо их *s-полинома*, мы определили терм $u_{f,g}$, которым будем активно пользоваться в дальнейшем.

2.3. Символ $\mathfrak{o}_G$. Пусть $f, h \in I$. Тогда будем говорить, что

$$f = \mathfrak{o}_G(h),$$

если существует такое представление

$$f = \sum_{g \in G} \lambda_g g,$$

что для каждого $g \in G$ справедливы неравенства

$$\text{HT}(\lambda_g g) \prec \text{HT}(h) \quad \text{и} \quad \mathfrak{S}(\lambda_g g) \leq \mathfrak{S}(h).$$

2.4. Формулировка теоремы. Для того чтобы сформулировать критерий Фожера, остается ввести следующее обозначение: для произвольного подмножества M кольца R через $\text{HT}(M)$ мы будем обозначать множество всех старших термов многочленов из M .

Следующая теорема и представляет собой критерий Фожера.

ТЕОРЕМА 1. Пусть G – конечное подмножество идеала $I = (f_1, \dots, f_n)$, содержащее многочлены $f_1, \dots, f_n$. Пусть для любых $f, g \in G$ таких, что

$$u_{f,g} \mathfrak{s}(f) \notin \text{HT}(I_{i(f)+1}), \quad u_{g,f} \mathfrak{s}(g) \notin \text{HT}(I_{i(g)+1}), \quad u_{f,g} \mathfrak{S}(f) \neq u_{g,f} \mathfrak{S}(g),$$

выполняется соотношение

$$\text{spol}(f, g) = \mathfrak{o}_G(u_{f,g} f).$$

Тогда G – базис Грёбнера идеала I .

3. Доказательство критерия

3.1. Определение символов $\mathfrak{n}(f)$, $\mathfrak{m}(f)$ и множеств $\mathcal{B}_i$, $\mathcal{N}_i$, $\mathcal{M}_i$. Положим $G_i = G \cap I_i$. Тогда $(G_i \setminus G_{i+1}) \cap I_{i+1} = \emptyset$.

Зафиксируем произвольный индекс $i \in \{1, \dots, n\}$.

Для каждого $f \in I$, $i(f) = i$, введем обозначение

$$\mathfrak{n}(f) = \min \max_{g \in G_i \setminus G_{i+1}} \text{HT}(\lambda_g \mathfrak{s}(g)),$$

где $\min$ берется по всем представлениям

$$f \equiv \sum_{g \in G_i \setminus G_{i+1}} \lambda_g g \pmod{I_{i+1}}, \quad (1)$$

а также обозначение

$$\mathfrak{m}(f) = \min \max_{g \in G_i \setminus G_{i+1}} \text{HT}(\lambda_g g),$$

где $\min$ берется по всем представлениям (1), на которых достигается $\mathfrak{n}(f)$.

Определим множества $\mathcal{B}_i$, $\mathcal{N}_i$ и $\mathcal{M}_i$ следующим образом:

$$\mathcal{B}_i = \{f \in I \mid i(f) = i, \text{HT}(f) \prec \mathfrak{m}(f)\},$$

$$\mathcal{N}_i = \left\{f \in \mathcal{B}_i \mid \mathfrak{n}(f) = \min_{g \in \mathcal{B}_i} \mathfrak{n}(g)\right\}, \quad \mathcal{M}_i = \left\{f \in \mathcal{N}_i \mid \mathfrak{m}(f) = \min_{g \in \mathcal{N}_i} \mathfrak{m}(g)\right\}.$$

Сразу отметим, что $\mathcal{B}_n = \emptyset$. Если же при каком-то i множество $\mathcal{B}_i$ непусто, то непусто и множество $\mathcal{M}_i$.

3.2. Нередуцируемость $\mathfrak{n}(f)$.

ЛЕММА 1. Для любого $f \in I$ справедливо соотношение

$$\mathfrak{n}(f) \notin \text{HT}(I_{i(f)+1}).$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим произвольное представление

$$f \equiv \sum_{g \in G_{i(f)} \setminus G_{i(f)+1}} \lambda_g g \pmod{I_{i(f)+1}},$$

на котором достигается $\mathfrak{n}(f)$, и положим для этого представления

$$J = \{g \in G_{i(f)} \setminus G_{i(f)+1} \mid \text{HT}(\lambda_g \mathfrak{s}(g)) = \mathfrak{n}(f)\}.$$

Если $\mathfrak{n}(f) \in \text{HT}(I_{i(f)+1})$, то найдется такой многочлен $h \in I_{i(f)+1}$, что

$$\text{HT}\left(\sum_{g \in J} \lambda_g \mathfrak{s}(g) - h\right) \prec \mathfrak{n}(f).$$

Следовательно, представление

$$f \equiv \sum_{g \in (G_{i(f)} \setminus G_{i(f)+1}) \setminus J} \lambda_g g + \left(\sum_{g \in J} \lambda_g \mathfrak{s}(g) - h\right) f_{i(f)} \pmod{I_{i(f)+1}}$$

противоречит минимальности $\mathfrak{n}(f)$.

Из леммы 1 очевидным образом следует

ЛЕММА 2. Пусть $g \in G$ и

$$\text{HT}(\lambda \mathfrak{s}(g)) \in \text{HT}(I_{i(g)+1}).$$

Тогда либо

$$\lambda g \in I_{i(g)+1},$$

либо

$$\mathfrak{n}(\lambda g) \prec \text{HT}(\lambda \mathfrak{s}(g)).$$

3.3. Представление многочленов из $\mathcal{M}_1$.

ЛЕММА 3. Пусть $f \in \mathcal{M}_1$, и пусть задано произвольное представление

$$f \equiv \sum_{g \in G \setminus G_2} \lambda_g g \pmod{I_2},$$

на котором достигаются $\mathfrak{n}(f)$ и $\mathfrak{m}(f)$. Тогда найдется такой многочлен $g \in G \setminus G_2$, что

$$\text{HT}(\lambda_g \mathfrak{s}(g)) = \mathfrak{n}(f) \quad \text{и} \quad \text{HT}(\lambda_g g) = \mathfrak{m}(f).$$

ДОКАЗАТЕЛЬСТВО. Положим, как и прежде,

$$J = \{g \in G \setminus G_2 \mid \text{HT}(\lambda_g \mathfrak{s}(g)) = \mathfrak{n}(f)\}.$$

Предположим, что

$$\max_{g \in J} \text{HT}(\lambda_g g) \prec \mathfrak{m}(f). \quad (2)$$

Положим

$$h = f - \sum_{g \in J} \lambda_g g. \quad (3)$$

Тогда $\mathfrak{n}(h) \prec \mathfrak{n}(f)$, т.е. $h \notin \mathcal{B}_1$, так как $f \in \mathcal{M}_1$. При этом из (2) следует, что $h \notin I_2$. Стало быть, существует представление

$$h \equiv \sum_{g \in G \setminus G_2} \nu_g g \pmod{I_2} \quad (4)$$

такое, что

$$\max_{g \in G \setminus G_2} \text{HT}(\nu_g \mathfrak{s}(g)) = \mathfrak{n}(h) \quad \text{и} \quad \max_{g \in G \setminus G_2} \text{HT}(\nu_g g) \preceq \text{HT}(h).$$

Но $\text{HT}(h) \prec \mathfrak{m}(f)$ в силу (2), (3) и неравенства $\text{HT}(f) \prec \mathfrak{m}(f)$ (которое, в свою очередь, следует из того, что $f \in \mathcal{B}_1$). Стало быть,

$$\max_{g \in G \setminus G_2} \text{HT}(\nu_g g) \prec \mathfrak{m}(f). \quad (5)$$

Из (3) и (4) получаем представление

$$f \equiv \sum_{g \in J} (\lambda_g + \nu_g)g + \sum_{g \in (G \setminus G_2) \setminus J} \nu_g g \pmod{I_2},$$

которое в силу (2) и (5) противоречит минимальности $\mathfrak{m}(f)$.

ЛЕММА 4. Пусть $f \in \mathcal{M}_1$. Тогда найдется представление

$$f \equiv \sum_{g \in G \setminus G_2} \lambda_g g \pmod{I_2}, \quad (6)$$

на котором достигаются $\mathfrak{n}(f)$ и $\mathfrak{m}(f)$ такие, что существует ровно один многочлен $g \in G \setminus G_2$, удовлетворяющий соотношениям

$$\text{HT}(\lambda_g \mathfrak{s}(g)) = \mathfrak{n}(f) \quad \text{и} \quad \text{HT}(\lambda_g g) = \mathfrak{m}(f). \quad (7)$$

ДОКАЗАТЕЛЬСТВО. Рассмотрим произвольное представление (6), на котором достигаются $\mathfrak{n}(f)$ и $\mathfrak{m}(f)$. По лемме 3 множество $G \setminus G_2$ содержит хотя бы один многочлен, удовлетворяющий соотношениям (7). Предположим, что такой многочлен не один: пусть $g_1, g_2 \in G \setminus G_2$, $g_1 \neq g_2$,

$$\text{HT}(\lambda_{g_j} \mathfrak{s}(g_j)) = \mathfrak{n}(f) \quad \text{и} \quad \text{HT}(\lambda_{g_j} g_j) = \mathfrak{m}(f) \quad \text{для} \quad j = 1, 2. \quad (8)$$

Пусть c – такой элемент поля $\mathbb{F}$, что старшие коэффициенты многочленов $c\lambda_{g_1} \mathfrak{s}(g_1)$ и $\lambda_{g_2} \mathfrak{s}(g_2)$ совпадают.

Рассмотрим представление

$$f \equiv (1+c)\lambda_{g_1}g_1 + (\lambda_{g_2}g_2 - c\lambda_{g_1}g_1) + \sum_{g \in (G \setminus G_2) \setminus \{g_1, g_2\}} \lambda_g g \pmod{I_2}.$$

Положим

$$h = \lambda_{g_2}g_2 - c\lambda_{g_1}g_1.$$

Как легко видеть, $\mathbf{n}(h) \prec \mathbf{n}(f)$. Стало быть, $h \notin \mathcal{B}_1$, т.е. либо $h \in I_2$, либо существует представление

$$h \equiv \sum_{g \in G \setminus G_2} \nu_g g \pmod{I_2} \quad (9)$$

такое, что

$$\max_{g \in G \setminus G_2} \text{HT}(\nu_g \mathfrak{s}(g)) = \mathbf{n}(h) \quad \text{и} \quad \max_{g \in G \setminus G_2} \text{HT}(\nu_g g) \preceq \text{HT}(h).$$

Учитывая, что при $h \in I_2$ можно также записать представление (9) со всеми ν_g равными нулю, будем считать, что вне зависимости от того, лежит h в I_2 или нет, имеет место представление (9), для которого справедливы неравенства

$$\max_{g \in G \setminus G_2} \text{HT}(\nu_g \mathfrak{s}(g)) \prec \mathbf{n}(f) \quad \text{и} \quad \max_{g \in G \setminus G_2} \text{HT}(\nu_g g) \preceq \text{HT}(f). \quad (10)$$

При этом, если $\text{HT}(\lambda_g \mathfrak{s}(g)) = \mathbf{n}(f)$ для некоторого $g \in G \setminus G_2$, то, как видно из первого неравенства (10), $\text{HT}(\nu_g) \prec \text{HT}(\lambda_g)$ для этого g и, стало быть, $\text{HT}(\nu_g g) \prec \text{HT}(\lambda_g g) \preceq \mathbf{m}(f)$. Следовательно, в представлении

$$f \equiv ((1+c)\lambda_{g_1} + \nu_{g_1})g_1 + \nu_{g_2}g_2 + \sum_{g \in (G \setminus G_2) \setminus \{g_1, g_2\}} (\lambda_g + \nu_g)g \pmod{I_2}$$

количество тех $g \in G \setminus G_2$, на которых одновременно достигаются $\mathbf{n}(f)$ и $\mathbf{m}(f)$, меньше, чем в исходном представлении либо на 1, либо на 2 (в зависимости от того, равно $1+c$ нулю или нет).

Повторив описанную процедуру должное количество раз, получим в итоге требуемое представление.

3.4. Представление многочленов, которые “ниже” $\mathcal{B}_1$. По аналогии с символами $\mathfrak{s}(f)$ и $\mathfrak{S}(f)$ для $\mathbf{n}(f)$ определим $\mathfrak{N}(f) = (\mathbf{i}(f), \mathbf{n}(f))$. На множестве символов $\mathfrak{N}(f)$ введем точно такой же порядок “ $\leq$ ”, как и на множестве символов $\mathfrak{S}(f)$.

ЗАМЕЧАНИЕ. Будем считать для удобства, что если t – пустой терм, то пара (i, t) меньше любой другой, каким бы ни был индекс i .

ЛЕММА 5. Пусть $\mathcal{B}_i = \emptyset$ для любого $i = 2, \dots, n$. Пусть $f \in I \setminus \mathcal{B}_1$,

$$\mathfrak{N}(f) \leq \min_{g \in \mathcal{B}_1} \mathfrak{N}(g).$$

Тогда существует представление

$$f = \sum_{g \in G} \lambda_g g \quad (11)$$

такое, что

$$\max_{g \in G} (\text{HT}(\lambda_g) \mathfrak{S}(g)) = \mathfrak{N}(f) \quad \text{и} \quad \max_{g \in G} \text{HT}(\lambda_g g) \preceq \text{HT}(f),$$

и такое, что для любого $g \in G$, удовлетворяющего равенству $\text{HT}(\lambda_g g) = \text{HT}(f)$, выполняется соотношение

$$\text{HT}(\lambda_g \mathfrak{s}(g)) \notin \text{HT}(I_{i(g)+1}). \quad (12)$$

ДОКАЗАТЕЛЬСТВО. Существование представления (11), удовлетворяющего всем требованиям леммы, кроме соотношения (12), следует непосредственно из определения множеств $\mathcal{B}_i$ и условия леммы. Рассмотрим такое представление.

Положим для него

$$J = \{g \in G \mid \text{HT}(\lambda_g g) = \text{HT}(f), \text{HT}(\lambda_g \mathfrak{s}(g)) \in \text{HT}(I_{i(g)+1})\}.$$

Для каждого $g \in J$ существует представление

$$\lambda_g g = \sum_{h \in G} \nu_h h \quad (13)$$

такое, что

$$\max_{h \in G} (\text{HT}(\nu_h) \mathfrak{S}(h)) = \mathfrak{N}(\lambda_g g) \quad \text{и} \quad \max_{h \in G} \text{HT}(\nu_h h) \preceq \text{HT}(\lambda_g g),$$

поскольку $\lambda_g g \notin \mathcal{B}_1$, а все $\mathcal{B}_i$, кроме $\mathcal{B}_1$, суть пустые множества.

Но по лемме 2 для каждого $g \in J$ справедливо неравенство

$$\mathfrak{N}(\lambda_g g) \triangleleft \text{HT}(\lambda_g) \mathfrak{S}(g).$$

Следовательно, переписывая представление (11) при помощи представлений (13) должное количество раз, получим в итоге требуемое представление.

3.5. Доказательство теоремы 1. Докажем, что $\mathcal{B}_1 = \emptyset$. Отсюда будет следовать, что G – базис Грёбнера идеала I .

Из индуктивных соображений будем считать, что $\mathcal{B}_i = \emptyset$ для любого $i = 2, \dots, n$, ибо при $i = n$ это верно.

Предположим, что множество $\mathcal{B}_1$ непусто. Тогда $\mathcal{M}_1$ также непусто. Рассмотрим произвольный многочлен $f \in \mathcal{M}_1$ и представление

$$f \equiv \sum_{g \in G \setminus G_2} \lambda_g g \pmod{I_2}, \quad (14)$$

о котором идет речь в лемме 4. Для этого представления существует ровно один многочлен в $G \setminus G_2$, на котором одновременно достигаются $\mathfrak{n}(f)$ и $\mathfrak{m}(f)$. Обозначим его g_1 . Многочлен $f - \lambda_{g_1} g_1$ в силу единственности g_1 удовлетворяет условию леммы 5, поэтому можно считать, что представление (14) является ограничением на $G \setminus G_2$ представления

$$f = \sum_{g \in G} \lambda_g g \quad (15)$$

такого, что для порождаемого им представления многочлена $f - \lambda_{g_1} g_1$ выполняется утверждение леммы 5.

Поскольку $\text{HT}(f - \lambda_{g_1}g_1) = \mathfrak{m}(f)$, найдется многочлен $g_2 \in G$, отличный от g_1 такой, что

$$\text{HT}(\lambda_{g_2}g_2) = \mathfrak{m}(f) \quad \text{и} \quad \text{HT}(\lambda_{g_2})\mathfrak{S}(g_2) \triangleleft \mathfrak{N}(f).$$

Таким образом,

$$\text{HT}(\lambda_{g_2})\mathfrak{S}(g_2) \triangleleft \text{HT}(\lambda_{g_1})\mathfrak{S}(g_1), \quad (16)$$

причем в силу лемм 1 и 5

$$\text{HT}(\lambda_{g_j}\mathfrak{s}(g_j)) \notin \text{HT}(I_{i(g_j)+1}), \quad j = 1, 2. \quad (17)$$

Из (16) и (17) следует, что

$$u_{g_2, g_1}\mathfrak{S}(g_2) \triangleleft u_{g_1, g_2}\mathfrak{S}(g_1), \quad u_{g_j, g_{3-j}}\mathfrak{s}(g_j) \notin \text{HT}(I_{i(g_j)+1}), \quad j = 1, 2,$$

соответственно.

Стало быть, по условию теоремы

$$\text{spol}(g_1, g_2) = \mathfrak{o}_G(u_{g_1, g_2}g_1),$$

т.е. имеет место представление

$$\text{spol}(g_1, g_2) = \sum_{g \in G} \nu_g g \quad (18)$$

такое, что для каждого $g \in G$ справедливы неравенства

$$\text{HT}(\nu_g g) \prec \text{HT}(u_{g_1, g_2}g_1) \quad \text{и} \quad \mathfrak{S}(\nu_g g) \trianglelefteq \mathfrak{S}(u_{g_1, g_2}g_1).$$

Но

$$\mathfrak{S}(u_{g_1, g_2}g_1) \trianglelefteq u_{g_1, g_2}\mathfrak{S}(g_1);$$

следовательно, для каждого $g \in G$

$$\text{HT}(\nu_g g) \prec \text{HT}(u_{g_1, g_2}g_1) \quad \text{и} \quad \mathfrak{S}(\nu_g g) \trianglelefteq u_{g_1, g_2}\mathfrak{S}(g_1). \quad (19)$$

Найдется такой моном μ , что старший моном многочлена λ_{g_1} равен $\mu u_{g_1, g_2}$, т.е.

$$\text{HT}(\lambda_{g_1} - \mu u_{g_1, g_2}) \prec \text{HT}(\lambda_{g_1}). \quad (20)$$

Тогда

$$\text{HT}(\lambda_{g_2}) = \text{HT}(\mu u_{g_2, g_1}) \quad (21)$$

и, как следует из (19),

$$\text{HT}(\mu \nu_g g) \prec \text{HT}(\lambda_{g_1}g_1) = \mathfrak{m}(f) \quad \text{и} \quad \mathfrak{S}(\mu \nu_g g) \trianglelefteq \text{HT}(\lambda_{g_1})\mathfrak{S}(g_1) = \mathfrak{N}(f) \quad (22)$$

для всех $g \in G$.

Прибавим к правой части равенства (15) и тут же вычтем из нее многочлен $\mu \text{spol}(g_1, g_2)$. Ввиду (18) получим представление

$$f = (\lambda_{g_1} - \mu u_{g_1, g_2} + \mu \nu_{g_1})g_1 + (\lambda_{g_2} + \mu u_{g_2, g_1} + \mu \nu_{g_2})g_2 + \sum_{g \in G \setminus \{g_1, g_2\}} (\lambda_g + \mu \nu_g)g. \quad (23)$$

На этом представлении в силу (20), (21) и (22) достигаются $\mathfrak{N}(f)$ и $\mathfrak{m}(f)$.

При этом, если $\text{HT}(\lambda_g g) = \mathfrak{m}(f)$ для некоторого $g \in G \setminus G_2$, то, как видно из первого неравенства (22), $\text{HT}(\mu \nu_g) \prec \text{HT}(\lambda_g)$ и, стало быть,

$$\text{HT}(\mu \nu_g \mathfrak{s}(g)) \prec \text{HT}(\lambda_g \mathfrak{s}(g)) \preceq \mathfrak{n}(f).$$

т.е. для такого g

$$\mathfrak{S}(\mu \nu_g g) \triangleleft \mathfrak{N}(f) \quad \text{и} \quad \text{HT}(\mu \nu_g g) \prec \mathfrak{m}(f).$$

Стало быть, в этом случае многочлен $\mu \nu_g g$ представим в виде

$$\mu \nu_g g \equiv \sum_{g \in G \setminus G_2} \mu_g g \pmod{I_2}, \quad (24)$$

где

$$\max_{g \in G \setminus G_2} (\text{HT}(\mu_g) \mathfrak{S}(g)) \triangleleft \mathfrak{N}(f) \quad \text{и} \quad \max_{g \in G \setminus G_2} \text{HT}(\mu_g g) \prec \mathfrak{m}(f).$$

Следовательно, из представлений (23) и (24) можно составить представление многочлена f , на котором будут достигаться $\mathfrak{N}(f)$ и $\mathfrak{m}(f)$, но таких $g \in G \setminus G_2$, на которых достигаются одновременно и $\mathfrak{n}(f)$, и $\mathfrak{m}(f)$, существовать не будет (см. (20)), что противоречит лемме 3.

Стало быть, множество $\mathcal{B}_1$ действительно пусто.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] J.-Ch. Faugère, “A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)”, *Proceedings of the 2002 International Symposium on Symbolic and Algebraic Computation*, ACM, New York, 2002, 75–83.
- [2] J.-Ch. Faugère, *Calcul efficace des bases de Gröbner et applications*, Habilitation à diriger des recherches, Université Paris VI, 2007.
- [3] T. Stegers, *Faugère’s F5 algorithm revisited*, Thesis for the degree of Diplom-Mathematiker, Technische Universität Darmstadt, 2005, <http://wwwcsif.cs.ucdavis.edu/~stegers/>.
- [4] J. M. Gash, *On efficient computation of Gröbner bases*, PhD Thesis, Indiana University, Bloomington, 2008.
- [5] C. Eder, *On the criteria of the F5 algorithm*, arXiv: [math.AC/0804.2033](https://arxiv.org/abs/math.AC/0804.2033).
- [6] C. Eder, J. Perry, *F5C: a variant of Faugère’s F5 algorithm with reduced Gröbner bases*, arXiv: [math.AC/0906.2967](https://arxiv.org/abs/math.AC/0906.2967).
- [7] А. И. Зобнин, “Обобщение алгоритма F5 вычисления базиса Грёбнера полиномиальных идеалов”, *Программирование*, **36**:2 (2010), 75–82.

О. Н. Герман

Московский государственный университет

им. М. В. Ломоносова

E-mail: german.oleg@gmail.com

Поступило

01.12.2009