Ефремов Роман Дмитриевич,
магистрант, МГТУ им. Н.Э. Баумана, Москва
Efremov Roman Dmitrievich,
BMSTU

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ПОСТРОЕНИЯ БАЗИСОВ ГРЕБНЕРА
COMPARATIVE ANALYSIS OF METHODS FOR CONSTRUCTING GROEBNER BASES

Аннотация: В статье рассматриваются основные понятия теории базисов Гребнера. Проводится подробный сравнительный анализ ключевых методов построения базисов Гребнера: классического алгоритма Бухбергера, продвинутого подхода Gebauer and Moller Installation (GMI), а также современных техник F4 и F5, разработанных Ж.-Ш. Фожером.

Abstract: The article discusses the fundamental concepts of Groebner bases theory. A detailed comparative analysis is conducted on key methods for constructing Groebner bases: the classical Buchberger's algorithm, the advanced approach of Gebauer and Moller Installation (GMI), as well as modern techniques F4 and F5 developed by J.-C. Faugere.

Ключевые слова: базис Гребнера, метод построения базиса Гребнера, алгоритм Бухбергера, GMI, F4, F5.

Keywords: Groebner basis, method for constructing Groebner basis, Buchberger’s algorithm, GMI, F4, F5.

Введение.

Актуальность исследования, посвященного сравнению методов построения базиса Гребнера, обусловлена широким спектром задач, возникающих в алгебраической геометрии, теории идеалов и компьютерной алгебре. Базисы Гребнера занимают важное место в данных областях, так как они позволяют решать системы многочленов, проводить анализ свойств идеалов и осуществлять упрощение выражений [1].

Базис Гребнера представляет собой особую конечную систему генераторов идеала, которая сохраняет важные свойства исходного идеала и позволяет эффективно решать алгебраические задачи [2]. Существуют различные алгоритмы и методы для построения базисов Гребнера, каждый из которых обладает своими преимуществами и недостатками в зависимости от характеристик рассматриваемых многочленов и структуры идеала.

Целью исследования является определение лучшего метода построения базиса Гребнера. Для достижения цели необходимо решить следующие задачи:

- рассмотреть основные понятия теории базисов Гребнера;
- провести обзор методов построения базиса Гребнера;
- сформулировать критерии сравнения рассмотренных методов;
- провести сравнительный анализ методов по этим критериям.

Таким образом, работа по сравнению методов построения базиса Гребнера является важным вкладом в развитие алгебраической теории и ее приложений в информатике и смежных областях.

Обзор предметной области.

Пусть натуральное число n и некоторое поле $\mathbb{K}$ (можно считать, что $\mathbb{K}$ есть поле рациональных чисел $\mathbb{Q}$, поле действительных чисел $\mathbb{R}$ или поле комплексных чисел $\mathbb{C}$). Пусть $x_1, \dots, x_n$ — переменные, а

$$P_1(x_1, \dots, x_n), P_2(x_1, \dots, x_n), \dots \quad (1)$$

– набор (возможно, бесконечный) многочленов от переменных $x_1, \dots, x_n$ с коэффициентами в поле $\mathbb{K}$.

Определение 1. Тогда *САУ* называется система вида

$$\begin{cases} P_1(x_1, \dots, x_n) = 0, \\ P_2(x_1, \dots, x_n) = 0, \\ \dots\dots\dots\dots\dots\dots. \end{cases} \quad (2)$$

Определение 2. САУ называется *конечной*, если в нее входит лишь конечное число уравнений.

Определение 3. Набор чисел $(a_1, a_2, \dots, a_n)$ из поля $\mathbb{K}$ называется *решением* системы 1, если

$$P_1(a_1, a_2, \dots, a_n) = 0, P_2(a_1, a_2, \dots, a_n) = 0, \dots \quad (3)$$

Определение 4. Две САУ называются *эквивалентными*, если множества их решений совпадают.

Задача о решении произвольной САУ вряд ли может быть решена в общей постановке. Исторически алгебра формировалась как наука о решении САУ (одно алгебраическое уравнение можно рассматривать как частный случай системы уравнений). Было накоплено огромное количество результатов, в том числе и негативного характера, например, теорема Абеля о неразрешимости в радикалах общего алгебраического уравнения степени ≥ 5 [3].

Интересно также качественное исследование множества решений САУ.

Например:

- имеет ли система хотя бы одно решение;
- эквивалентны ли две данные системы;
- конечно или бесконечно множество решений системы.

Простейший пример САУ – система линейных уравнений, о решении которой существует вполне завершенная теория. Наиболее распространенный метод решения – использование теоремы Кронекера-Капелли о совместимости системы [4] (имеет хотя бы одно решение) и деления «в столбик».

Сложнее же получить решение системы нелинейных алгебраических уравнений от конечного числа переменных с конечными степенями.

Пусть $\mathbb{K}[x_1, \dots, x_n]$ – это множество всех многочленов от переменных $x_1, \dots, x_n$ с коэффициентами в поле $\mathbb{K}$ (или над полем $\mathbb{K}$). На этом множестве определены операции сложения и умножения. Множества с такими операциями в алгебре называют *кольцами*.

Пусть R – коммутативное ассоциативное кольцо с единицей 1.

Определение 5. Тогда непустое подмножество I кольца R называется *идеалом* в R ($I \lhd R$), если:

- для любых элементов $a, b \in I$ элемент $a - b \in I$;
- для любых $a \in I$, $c \in R$ элемент $ac \in I$.

Определение 6. Идеал I кольца R называется *главным*, если существует такой элемент $a \in I$, что $I = (a)$. Элемент a называется *порождающим* (или *образующим*) для идеала I.

Определение 7. Элементы $a_1, \dots, a_k$ составляют *базис* идеала $I = (a_1, a_2, \dots, a_k)$. Говорят, что идеал $I \lhd R$ допускает *конечный базис*, если в нем найдутся такие элементы $a_1, a_2, \dots, a_k$, что $I = (a_1, a_2, \dots, a_k)$.

При этом в определении базиса идеала (в отличие от определения базиса векторного пространства) нет требования минимальности на число элементов базиса. Например, добавляя к базису произвольный элемент идеала, получается базис того же идеала.

Дэвид Гильберт сформулировал **теорему о базисе** [5], которая гласит: каждый идеал $I \lhd \mathbb{K}[x_1, \dots, x_n]$ допускает конечный базис, т. е. найдутся такие $f_1(x_1, \dots, x_n), \dots, f_k(x_1, \dots, x_n) \in I$, что

$$I = \{f_1 r_1 + \dots + f_k r_k; r_1, \dots r_k \in \mathbb{K}[x_1, \dots, x_n]\}. \quad (4)$$

Со всякой САУ

$$\begin{cases} P_1(x_1, \dots, x_n) = 0, \\ P_2(x_1, \dots, x_n) = 0, \\ \dots\dots\dots\dots\dots\dots \end{cases} \quad (5)$$

можно связать идеал I, порожденный многочленами, отвечающими уравнениям системы:

$$I = (P_1(x_1, \dots, x_n), P_2(x_1, \dots, x_n), \dots). \quad (6)$$

Если систему 5 обозначить S, то соответствующий идеал будет обозначен через $I(S)$.

Лемма 1. Если $F \in \mathrm{I(S)}$, то $F(x_1^0, \dots, x_n^0) = 0$ для всякого решения $(x_1^0, \dots, x_n^0)$ системы S.

Лемма 2. Если $\{P_1, \dots, P_m\}$ и $\{\bar{P}_1, \dots, \bar{P}_m\}$ – два базиса одного идеала I, то соответствующие им системы 7 и 8 эквивалентны.

Соответствующая базису $\{P_1, \dots, P_m\}$:

$$\begin{cases} P_1(x_1, \dots, x_n) = 0, \\ \dots\dots\dots\dots\dots \\ P_m(x_1, \dots, x_n) = 0. \end{cases} \quad (7)$$

Соответствующая базису $\{\bar{P}_1, \dots, \bar{P}_m\}$:

$$\begin{cases} \bar{P}_1(x_1, \dots, x_n) = 0, \\ \dots\dots\dots\dots\dots \\ \bar{P}_m(x_1, \dots, x_n) = 0. \end{cases} \quad (8)$$

Так, множество решений системы однозначно определяется идеалом системы. Различные базисы одного идеала отвечают эквивалентным системам. При этом каждая система алгебраических уравнений эквивалентна конечной системе.

Ответ на вопрос, можно ли, зная идеалы двух систем $I(S_1)$ и $I(S_2)$ определить эквивалентны ли системы S_1 и S_2, сформулировал Дэвид Гильберт в теореме о нулях [5]. Согласно этой теореме для системы

$$\begin{cases} f_1(x_1, \dots, x_n) = 0, \\ \dots\dots\dots\dots\dots \\ f_m(x_1, \dots, x_n) = 0. \end{cases} \quad (9)$$

алгебраических уравнений многочлен $F(x_1, \dots, x_n)$ обращается в нуль на всех решениях данной системы тогда и только тогда, когда найдутся многочлены $r_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)$ и $s \in \mathbb{N}$ такие, что $F^s = r_1 f_1 + \dots + r_m f_m$.

Для нахождения базиса Гребнера идеала $\mathrm{I} \lhd \mathbb{K}[x_1, \dots, x_n]$ необходимо определить для многочлена $P[x_1, \dots, x_n]$ понятие старшего члена.

Определение 8. Многочлен, состоящий из одного члена

$$P = a x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}, \quad (10)$$

$a \in \mathbb{K}$, называют *одночленом* или *мономом*.

Старшим членом многочлена $P = \sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$ называется один из его одночленов $a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$. Каждому такому одночлену можно сопоставить набор $(i_1, \dots, i_n)$ целых неотрицательных чисел, который называют *набором степеней*.

Например, при $n = 4$ одночлену $2x_1 x_3^3$ соответствует набор (1,0,3,0).

Первым рассматриваемым способом упорядочивания одночленов называется **лексикографический** [6].

Определение 9. Набор $(i_1, \dots, i_n)$ больше набора $(j_1, \dots, j_n)$, если существует такое $k \leq n, i_1 = j_1, i_2 = j_2, \dots, i_{k-1} = j_{k-1}, i_k > j_k$,

Другим примером сравнения одночленов в многочлене является **градуированный лексикографический** [6].

Определение 10. Набор $(i_1, \dots, i_n)$ больше набора $(j_1, \dots, j_n)$, если степени мономов $\sum_{k=1}^n i_k > \sum_{k=1}^n j_k$, или $\sum_{k=1}^n i_k = \sum_{k=1}^n j_k$ и $(i_1, \dots, i_n) > (j_1, \dots, j_n)$.

Третьим рассматриваемым способом упорядочивания мономов в полиноме является **обратный градуированный лексикографический** порядок [6]. Допустим, даны два одночлена α и β с наборами степеней $(i_1, \dots, i_n)$ и $(j_1, \dots, j_n)$ соответственно. Тогда набор степеней $\alpha - \beta \in \mathbb{Z}$ это следующий набор степеней $(i_1 - j_1, \dots, i_n - j_n)$.

Определение 11. Набор $(i_1, \dots, i_n)$ больше набора $(j_1, \dots, j_n)$, если степени мономов $\sum_{k=1}^n i_k > \sum_{k=1}^n j_k$, или $\sum_{k=1}^n i_k = \sum_{k=1}^n j_k$ и самый правый ненулевой элемент набор $\alpha - \beta \in \mathbb{Z}$ отрицателен.

Указанными способами можно сравнить два набора одинаковой длины. Значит, можно однозначно задать порядок мономов в полиноме.

Определение 12. Старшим членом многочлена

$$P(x_1, \dots, x_n) = \sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} \quad (11)$$

называется ненулевой одночлен $a_{i_1^0 \dots i_n^0} x_1^{i_1^0} \dots x_n^{i_n^0}$, такой, что набор степеней этого одночлена $(i_1^0 \dots i_n^0)$ больше всякого другого набора степеней, встречающегося в $P(x_1, \dots, x_n)$, на определенном мономиальном порядке.

Как выяснить, принадлежит ли на самом деле многочлен $h(x)$ главному идеалу $I(f(x))$? Необходимо делить многочлен $h(x)$ на $f(x)$ «в столбик», и, если разделится без остатка, ответ будет положительным, в ином случае –отрицательным.

Задача вхождения [7] формулируется так: пусть идеал $I \lhd \mathbb{K}[x_1, \dots, x_n]$ задан своим базисом $I = (f_1, \dots, f_m)$. Необходимо выяснить, принадлежит ли данный многочлен $h(x_1, \dots, x_n)$ идеалу I, т. е. существуют ли такие многочлены $r_1(x_1, \dots, x_n), \dots, r_m(x_1, \dots, x_n)$, что $h = f_1 r_1 + \dots + f_m r_m$.

Пусть для всякого многочлена P есть $P = P_c + P_m$, где P_c – старший член P, а P_m – сумма остальных членов. Например, для $P = 2x^3 - 4xz^2 + 2y^3$ есть $P_c = 2x^3, P_m = -4xz^2 + 2y^3$.

Тогда **операция редукции** определена следующими образом: предположим, что старший член многочлена h делится на старший член некоторого из многочленов f_i, т.е. $h_c = f_{ic} Q$, где Q – одночлен. Тогда пусть $h_1 = h - Q f_i = Q(-f_{iM}) + h_m$. При этом старший член многочлена h_1 меньше старшего члена многочлена h.

Итак, задачу вхождения теперь можно решать не для h, а для h_1 и вновь можно применять редукцию (возможно, с другим f_i). Если за конечное число редукций многочлен h сведется (редуцируется) к нулю, то $h \in (f_1, \dots, f_m)$, так как нуль принадлежит любому идеалу.

Определение 13. Таким образом, базис $f_1, \dots, f_m$ идеала исходного $I = (f_1, \dots, f_m)$ называется *базисом Гребнера* этого идеала, если всякий многочлен $h \in I$ редуцируется к нулю при помощи $f_1, \dots, f_m$.

Из теоремы Гильберта о базисе вытекает существование базиса Гребнера в любом идеале. Однако доказательство существования не дает алгоритма построения базиса Гребнера идеала по некоторому его исходному базису.

Математическую постановку задачи можно определить так: пусть задан идеал $I = (f_1, \dots, f_m) \lhd \mathbb{K}[x_1, \dots, x_n]$ и фиксирован некоторый мономиальный порядок ($\preccurlyeq$). Необходимо найти базис Гребнера $\mathcal{G} = \{g_1, g_2, \dots, g_t\} \subseteq I$ (систему полиномов) таким образом, чтобы любое приведение произвольного многочлена $p \in I$ относительно элементов $\mathcal{G}$ заканчивалось нулевым результатом. Иначе говоря, искомый базис $\mathcal{G}$ удовлетворяет условию, что всякий многочлен $p \in I$ сводится к нулю после ряда операций редукции.

Обзор методов построения базиса Гребнера.

Алгоритм Бухбергера: пусть $I \lhd \mathbb{K}[x_1, \dots, x_n]$ – идеал, $f_1, \dots, f_m$ – его базис.

Определение 14. Многочлены f_i и f_j имеют *зацепление*, если их старшие члены f_i и f_j делятся одновременно на некоторый одночлен w, отличный от константы.

Если f_i и f_j имеют зацепление, т. е. $f_i = wq_1$, $f_j = wq_2$, где w – наибольший общий делитель f_i и f_j, то рассматривается многочлен $F_{i,j} = f_i q_2 - f_j q_1 \in I$ (S-многочлен пары $f_i, f_j, S(f_i, f_j)$ или $S(i,j)$). Редуцируется многочлен $F_{i,j}$ с помощью базиса $f_1, \dots, f_m$ до тех пор, пока это возможно. В результате получается нередуцируемый многочлен $\tilde{F}_{i,j}$. Если $\tilde{F}_{i,j} \equiv 0$, то зацепление называется разрешимым [8]. Иначе можно добавить к базису идеала I: $f_{m+1} = \tilde{F}_{i,j}$.

В новом базисе $f_1, \dots, f_m, f_{m+1}$ можно вновь искать возможные зацепления и редуцировать соответствующие многочлены $F_{i,j}$.

Теорема 1. Для каждого набора многочленов $f_1, \dots, f_m \in \mathbb{K}[x_1, \dots, x_n]$ после редуцирования конечного числа зацеплений получается набор многочленов $f_1, \dots, f_m, f_{m+1}, \dots, f_M$, в котором каждое зацепление разрешимо.

Теорема 2. Базис $f_1, \dots, f_m$ идеала I является базисом Гребнера тогда и только тогда, когда в нем нет зацеплений или каждое зацепление разрешимо.

Теоремы 1 и 2 обосновывают существование эффективного алгоритма для построения базиса Гребнера идеала [9].

Алгоритм [7] использует понятие S-пар и многократно выполняет полиномиальную операцию редукции. Пусть $f_1, \ldots, f_m$ – набор многочленов, являющийся базисом идеала I.

1. Проверка, есть ли в наборе зацепления. Если зацеплений нет, то набор является базисом Гребнера идеала I, иначе переход к пункту 2.
2. По найденному зацеплению (i, j) многочленов f_i и f_j положить $f_{iC} = wq_1$, $f_{jC} = wq_2$, и составить многочлен $F_{i,j} = f_i q_2 - f_j q_1$. Редуцировать многочлен $F_{i,j}$ с помощью набора f_i до тех пор, пока это возможно. Если многочлен $F_{i,j}$ редуцировался к ненулевому многочлену f, то переход к пункту 3, иначе к пункту 4. (Редуцируемость многочлена $F_{i,j}$ к нулю и вид многочлена f зависят от выбранной последовательности применяемых редукций. В алгоритме используется любая применимая последовательность редукций и, после получения нередуцируемого многочлена f, переход к пункту 3, более никогда зацепление (i, j) не рассматривается.)
3. Добавление многочлена f к набору $f_1, f_2, \ldots, f_k$ в качестве f_{k+1} и переход к пункту 4.
4. В построенном к настоящему моменту множестве многочленов f_i рассматривается зацепление, которое не было рассмотрено ранее, и переход к пункту 2. Если все имеющиеся зацепления ранее рассматривались, алгоритм завершен.

За конечное число шагов получается такой набор $f_1, \ldots, f_m, f_{m+1}, \ldots, f_M$, где каждое зацепление разрешимо. Это и есть базис Гребнера идеала $I = (f_1, \ldots, f_m)$.

Классический алгоритм Бухбергера представляет собой метод «грубой силы» (или полного перебора), поскольку по ходу решения рассматривает всевозможные S-полиномы и выполняет над ними операции редукции.

Улучшенный алгоритм Бухбергера (GMI): большинство операций редукции, выполняемых над S-парами в алгоритме Бухбергера, приведут к нулю. Это значит, что новый полином не будет добавлен в базис. Необновление базиса после большинства операций наталкивает на мысли о том, что, распознавание редукции к нулю и, как следствие, отбрасывание такого вычисления приведут к значительному уменьшению времени построения базиса Гребнера.

Первой попыткой распознать нулевые редукции стало предложение метода GMI [10, 11]. Он основан на классическом алгоритме Бухбергера с тем лишь изменением, что добавляет отбор пар, которые имеет смысл рассматривать для дальнейшей редукции.

Существуют два основных критерия, по которым можно понять, что вычисления для определенного S-полинома избыточны, так как он будет редуцирован к нулю.

Теорема 3. НОД критерий. Если p_1 и p_2 полиномы в F, у которых наибольший общий делитель $gcd\big(lt(p_1), lt(p_2)\big) = 1, S(p_1, p_2) \xrightarrow{F} 0$.

Теорема 4. НОК критерий. Если p_1, p_2 и p_3 полиномы в F, $S(p_1, p_2) \xrightarrow{F} 0$, и $S(p_2, p_3) \xrightarrow{F} 0$ и $lt(p_2) | lcm\big(lt(p_1), lt(p_3)\big)$, то $S(p_1, p_3) \xrightarrow{F} 0$.

Так, перед запуском основного цикла прохода по всем S-парам, все S- пары необходимо проверить этими двумя критериями, и если пара подходит под какой-либо критерий, то ее рассматривать не имеет смысла, ибо редукция приведет к нулю, а базис останется неизменным.

Улучшенный алгоритм Бухбергера подразумевает, что такую же проверку необходимо запускать перед добавлением очередной пары в список для дальнейшего рассмотрения.

Так, алгоритм GMI позволяет избежать часть избыточных вычислений, что приводит к уменьшению времени построения базиса Гребнера.

F4 Фожера: алгоритм Бухбергера и его улучшенная версия – старейшие алгоритмы вычисления базисов Гребнера. Они просты в реализации, но не лишены из-за этого недостатков. Одной из ключевых проблем этих алгоритмов является выбор S-пар.

Выбор S-полиномов для редукции и полиномов, используемых для их редукции, является эвристическим. Как и во многих вычислительных задачах, эвристика не может обнаружить большинство скрытых упрощений, и если избегать эвристического выбора, можно получить резкое улучшение эффективности алгоритма.

Метод F4 [12, 13, 14, 15] строит базис Гребнера идеала в кольце многочленов с помощью серии стандартных процедур линейной алгебры: приведений матриц к ступенчатому виду. Суть его схожа с алгоритмом Бухбергера, но имеет ряд ключевых отличий:

- в отличие от алгоритма Бухбергера можно выбрать несколько S-пар из набора пар P одновременно, например, все одинаковой минимальной степени, и хранить эти S-пары в подмножестве $L \subset P$;
- затем для всех членов всех генераторов S-пар в L ищется в текущем промежуточном базисе Гребнера G возможные редукторы, они добавляются к L и снова осуществляется поиск всех их членов для редукторов в G;
- после того, как все доступные данные о редукции собраны с последнего шага, генерируется матрица со столбцами, соответствующими членам, появляющимся в L, и строками, соответствующими коэффициентам каждого полинома в L;
- чтобы теперь сократить все выбранные S-пары одновременно, применяется метод последовательного исключения переменных (метод Гаусса) к матрице и затем перепроверяется, какие строки обновленной матрицы дают новый старший член, которого еще нет в L(G).

Этот метод имеет следующие преимущества в сравнении с алгоритмом Бухбергера и GMI:

- уменьшается количество редукций S-пар, которые в конечном итоге приведут к нулю;
- уменьшается время решения задачи за счет выбора сразу нескольких S-пар;
- уменьшается время решения задачи за счет использования матричных преобразований вместо обычных операций над полиномами.

F5 Фожера: Появление алгоритма F5 [16, 17, 18, 19, 20] ввело новую концепцию построения базиса Гребнера. Одной из главных особенностей метода является работа с дополнительной информацией о каждом полиноме. Такая информация получила название сигнатуры полинома. А сам полином вместе с сигнатурой называется дополненным полиномом.

Помимо новых терминов F5 предлагает два новых критерия, которые позволяют полностью исключить избыточные вычисления.

Данный алгоритм предполагает следующие шаги:

- инициализация дополненных полиномов от исходной САУ;
- инициализация S-пар от образованных на прошлом шаге дополненных полиномов;
- выбор S-пары для рассмотрения на текущем шаге;
- если S-пара удовлетворяет хотя бы одному из критериев, она отбрасывается, поскольку редукция такой пары приведет к нулю;
- проводится редукция выбранной пары.
- результат редукции добавляется в список дополненных полиномов, и в список S-пар добавляются новые, образованные результатом редукции и всеми дополненными полиномами;
- шаги повторяются, пока список S-пар не окажется пустым.

Основная идея условия F5 заключается в том, что определенный набор полиномов должен быть «конструктивно независимым» при добавлении новых полиномов в базис. Это означает, что для каждого нового полинома, который потенциально может быть добавлен в базис, необходимо проверить, что он не может быть представлен как линейная комбинация полиномов, уже находящихся в базисе, с использованием стандартного представления.

Алгоритм позволяет удалять полиномы, которые можно выразить через остальное множество, сохраняя при этом необходимую «независимость» идеала. Это делает алгоритм эффективным и позволяет контролировать размер базиса.

Все это позволяет полностью исключить избыточные вычисления, что максимально уменьшает время решения задачи построения базиса Гребнера. Выбор S-пары на каждом шаге является ключевым аспектом, который влияет на скорость сходимости алгоритма. Вместе с F5 большое множество методов, отличающихся стратегией выбора очередной S-пары: Incremental F5, NonIncremental F5, F5B, F5M. Несмотря на разные стратегии выбора суть этих методов схожа и все вместе они образуют семейство сигнатурных методов построения базиса Гребнера. В данной работе подробно стратегии разобраны не будут.

Сравнение методов построения базиса Гребнера.

Описанные выше алгоритмы позволяют построить базис Гребнера, который может быть использован для решения широкого спектра задач.

Сравнение направлено на отражение сходств и различий между рассматриваемыми объектами в структурной форме. Такой подход позволяет выделить важнейшие свойства и изучить сущности предметов анализа.

Наилучшим образом сравнить объекты можно по критериям. Критерий представляет собой некоторую выделенную особенность, с помощью которой можно охарактеризовать объект. Несмотря на то, что рассмотренные выше методы построения базиса Гребнера, возможно сформулировать критерии для их сравнения. С помощью критериев могут быть обеспечены надежность и независимость оценки.

Для сравнения рассмотренных методов выделены 5 критериев.

1. К1 – сложность. В разрезе рассмотренных алгоритмов она может быть описана количеством избыточных вычислений. То есть, наименьшую сложность будут иметь те методы, которые производят минимально возможное количество редукций к 0.
2. К2 – устойчивость к росту размера задачи. Другими словами, эффективность обработки больших входных данных.
3. К3 – устойчивость к росту сложности задачи. Важно, поскольку, например, симметричные семейства систем уравнений представляют особенную сложность для рассмотренных алгоритмов из-за своих свойств. Даже на размерах исходной САУ до 10 полиномов, время решения задачи может превышать часы.
4. К4 – отсутствие избыточного увеличения размера промежуточных объектов. Другими словами, это нетребовательность к памяти.
5. К5 – надежность. Алгоритм должен точно находить базис Гребнера для исходного набора полиномов.

Сравнение рассмотренных методов построения базиса Гребнера по сформулированным выше критериям представлено в таблице 1.

Таблица 1

Сравнение методов построения базиса Гребнера

Метод	**Критерий**				
	К1	**К2**	**К3**	**К4**	**К5**
Алгоритм Бухбергера	–	–	–	–	+
GMI	+	–	–	–	+
F4	+	–	+	–	+
F5	+	+	+	+	+

Все рассмотренные методы кроме классического алгоритма Бухбергера определяют критерии для того, чтобы избежать избыточных вычислений и, как следствие, уменьшить сложность.

Поскольку только метод F5 избегает всех нулевых редукций, только его можно назвать устойчивым к росту размера задачи.

Особые критерии и матричные преобразования методов F5 и F4 соответственно позволяют этим методам быть устойчивыми к росту сложности задачи. С другой стороны, классический алгоритм Бухбергера и его улучшенная версия такой устойчивостью не обладают.

Классический алгоритм Бухбергера решает задачу методом полного перебора. Из-за этого медленно уменьшается размер очереди S-пар, что требует памяти для их хранения. Похожая ситуация с GMI: не все избыточные вычисления могут быть определены, а значит очередь все так же будет расти. F4 производит куда меньше редукций к нулю, но по своей природе требует создания матриц для каждой операции редукции, что влечет требовательность к памяти. Несмотря на то, что F5 оперирует дополненными полиномами вместо обычных, большой памяти для хранения дополнительной информации не требует: необходимо хранить лишь одночлен с индексом для каждого полинома.

Все алгоритмы считаются надежными, доказательства этого приведены в оригинальных статьях, впервые опубликованных для описанных методов.

По результатам сравнения можно заметить, что метод F5 является лучшим для решения задачи построения базиса Гребнера, поскольку удовлетворяет выдвинутым критериям.

Заключение.

В ходе исследования были выявлены преимущества и недостатки методов построения базиса Гребнера путем их критического анализа. Выявлен лучший алгоритм, среди известных на данный момент. Достигнута поставленная цель и решены задачи исследования.

Метод построения базиса Гребнера F5 Фожера имеет следующие преимущества над алгоритмом Бухбергера, GMI и F4: производит минимально возможное количество редукций к 0, устойчив к росту и размеру задачи, нетребователен к памяти. При этом он является таким же надежным, как и остальные методы. Все это делает метод F5 лучшим методом построения базиса Гребнера.

Список литературы:

1. Sturmfels B. Algorithms in Invariant Theory, Texts & Monographs in Symbolic Computation // Vienna: Springer-Verlag. – 1993.

2. Buchberger B. An Algorithmical Criterion for the Solvability of Algebraic Systems of Equations // Aequationes Mathematicae. – 1970. – Vol. 4, Issue 3. – pp. 374-383.

3. Алексеев В. Б. Теорема Н. Абеля в задачах и решениях // М. – 2001.

4. Федоров Ф. М. О рангах и декрементах миноров, определителей и матриц бесконечной системы // Вестник СВФУ. – 2015. – № 2. – С. 11-18.

5. Кокс Д., Литтл Дж., О ’Ши Д. Идеалы, многообразия и алгоритмы // М.:Мир. – 2000.

6. Eisenbud D. Commutative Algebra with a View Toward Algebraic Geometry // New York: Springer-Verlag. – 1995.

7. Аржанцев И. В. Базисы Гребнера и системы алгебраических уравнений // М.:МЦНМО. – 2003. – 68 с.

8. Buchberger B. An Algorithm for Finding the Basis Elements in the Residue Class Ring Modulo a Zero Dimensional Polynomial Ideal // PhD thesis: Universität Innsbruck. – 1965.

9. Бокуть Л. А. Базисы Гребнера и Гребнера-Ширшова в алгебре и конформные алгебры / Бокуть Л. А., Фонг Ю., Ке В.-Ф., Колесников П. С. // Фундамент. и прикл. матем. – 2000. Том 6, Выпуск 3. – С. 669-706.

10. Gebauer R., Moller H. M. On an Installation of Buchberger’s Algorithm // Journal of Symbolic Computation. – 1988. – Vol. 6, Issue 2-3. – pp. 275-286.

11. Becker T., Weispfenning V. Gröbner Bases: A Computational Approach to Commutative Algebra // Berlin: Springer-Verlag. – 1993.

12. Faugere J.-C. A new efficient algorithm for computing Groebner bases (F4) // Journal of Pure and Applied Algebra. – 1999. – Vol. 139. – pp. 61-88.

13. Storjohann A. Algorithms for Matrix Canonical Forms // Zürich: Ph.D. thesis. – 2000.

14. Stein W., Joyner D. SAGE: System for Algebra and Geometry Experimentation // Communications in Computer Algebra. –2005. –Vol. 39, No. 2.

15. Greuel G.-M., Pfister G. A Singular Introduction to Commutative Algebra // Berlin: Springer-Verlag. – 2008.

16. Faugere J.-C. A new efficient algorithm for computing Groebner bases without reduction to zero (F5) // Proceedings of the 2002 international symposium on Symbolic and algebraic computation. – 2002. – pp. 75-83.

17. Stegers T. Faugere's F5 Algorithm Revisited // Thesis For The Degree Of Diplom-Mathematiker. – 2005.

18. Eder C. A New Attempt On The F5 Criterion // Computer Science Journal of Moldova. – 2008. – Vol.16, No.1. – pp. 4-14.

19. Sun Y., Wang D. The F5 Algorithm in Buchberger's Style // Computing Research Repository. – 2010. – Vol. abs/1006.5299.

20. Kim Y.-J. An algorithm for computing Groebner basis and the complexity evaluation / Kim Y.-J., Paek H.-S., Kim N.-C., Byon C.-I. // Computing Research Repository. – 2015. – Vol. abs/1507.03217.