ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 **МАТЕМАТИКИ** **Выпуск 2,3**
2012

К. Д. Жуков (Москва, ТВП). **О возможности применения методов базисов Гребнера в фактор-кольцах.**

В общем случае не существует эффективных способов решения полиномиальных систем уравнений. Часто для решения таких систем применяется метод базисов Гребнера. С помощью этого метода можно строить более простые следствия системы. Когда система уравнений от переменных задана над конечным полем $\mathrm{GF}(q)$, естественно перенести задачу из кольца многочленов в фактор-кольцо по идеалу, порожденному многочленами $x_i^q - x_i$, $i = 1, 2, \ldots, n$. Такой переход позволяет использовать более эффективные в реализации операции в фактор-кольце вместо классических операций над многочленами.

Основным понятием в теории базисов Гребнера является мономиальный порядок на множестве мономов из $P[x_1, x_2, \ldots, x_n]$. *Мономиальным* называется такой порядок $\leqslant$, что: 1) $\leqslant$ – линеен; 2) $\forall \vec{x}^{\vec{a}}, \vec{x}^{\vec{b}}, \vec{x}^{\vec{c}}\colon\ \vec{x}^{\vec{a}} \leqslant \vec{x}^{\vec{b}} \ \Rightarrow\ \vec{x}^{\vec{a}}\vec{x}^{\vec{c}} \leqslant \vec{x}^{\vec{b}}\vec{x}^{\vec{c}}$; 3) $\forall \vec{x}^{\vec{a}}\colon\ 1 \leqslant \vec{x}^{\vec{a}}$. Лексикографический порядок является мономиальным. В фактор-кольце не существует мономиального порядка, поэтому возникает вопрос о возможности применения методов базисов Гребнера в фактор-кольце. Порядок в фактор-кольце можно задать следующим образом. Пусть $J = (x_i^q - x_i\colon\ i = 1, 2, \ldots, n)$ – идеал в $P[x_1, x_2, \ldots, x_n]$. В этом случае минимальные относительно набора $\{x_i^q - x_i\colon\ i = 1, 2, \ldots, n\}$ представители элементов из фактор-кольца $P[\vec{x}]/J$ определены однозначно. Зададим на множестве мономов из $P[\vec{x}]/J$ следующее отношение порядка:

$$\left[\vec{x}^{\vec{a}}\right] \leqslant \left[\vec{x}^{\vec{b}}\right] \ \Leftrightarrow\ \vec{x}^{\vec{a}} \leqslant \vec{x}^{\vec{b}}, \tag{1}$$

где $\vec{x}^{\vec{a}}$ и $\vec{x}^{\vec{b}}$ — минимальные представители соответствующих классов. Такой порядок в $P[\vec{x}]/J$ позволяет сформулировать понятие базиса Гребнера в фактор-кольце.

Напомним основные определения согласно [1]. Говорят, что ненулевые многочлены $f_1, f_2, \ldots, f_s \in I$ образуют базис Гребнера идеала I (относительно заданного мономиального порядка), если старший член $LT(g)$ делится на некоторый $LT(f_i)$ для любого $g \in I$. Существует алгоритм построения базиса Гребнера, основанный на критерии Бухбергера. Критерий использует понятия алгоритма деления и S-многочлена. Пусть даны многочлены

$$g(\vec{x}) = \alpha\vec{x}^{\vec{a}} + \cdots, \quad f(\vec{x}) = \beta\vec{x}^{\vec{b}} + \cdots \tag{2}$$

Если для некоторого $\vec{c}$ выполняется $\vec{x}^{\vec{a}} = \vec{x}^{\vec{b}}\vec{x}^{\vec{c}}$, то многочлен $h_1(\vec{x}) = g(\vec{x}) - \alpha\beta^{-1}f(\vec{x})$ называется *результатом* 1*-редукции* многочлена g многочленом f. Продолжая 1-редукцию далее, получим многочлен, не редуцируемый f и называемый *результатом редукции*. Процедура редукции с переносом нередуцируемых мономов в остаток называется *алгоритмом деления*. S*-многочленом* для многочленов (2) называется

$$S(f, g) = \frac{\vec{x}^{\vec{c}}}{\alpha\vec{x}^{\vec{a}}}f - \frac{\vec{x}^{\vec{c}}}{\beta\vec{x}^{\vec{b}}}g, \quad \text{где} \quad \vec{x}^{\vec{c}} = \mathrm{НОК}\,(\vec{x}^{\vec{a}}, \vec{x}^{\vec{b}}).$$

Теорема 1 (Бухбергер). *Многочлены* $f_1, f_1, \ldots, f_s$ *образуют базис Гребнера тогда и только тогда, когда для всех* $i \neq j$ *остаток от деления* $S(f_i, f_j)$ *на* $f_1, f_2, \ldots, f_s$ *равен нулю.*

Для введенного порядка (1) определим базис Гребнера в фактор-кольце. Будем говорить, что $[g_1], [g_2], \ldots, [g_s]$ является базисом Гребнера идеала $I([g_1], [g_2], \ldots, [g_s])$ в $P[\vec{x}]/J$, если $LT(f)$ делится на некоторый $LT(f_i)$ для любого $[f] \in I$. Можно показать, что не все классические определения базиса Гребнера останутся эквивалентными в фактор-кольце. При введенном определении гарантируется существование базиса Гребнера для любого ненулевого идеала. Построить такой базис можно с помощью алгоритма Бухбергера с некоторыми изменениями. Показывается, что эти изменения существенны. Чтобы обосновать критерий Бухбергера в фактор-кольце, необходимо формализовать понятия редукции и алгоритма деления в фактор-кольце и обосновать их корректность. Ниже приведена формулировка критерия для случая, представляющего наибольший интерес с точки зрения решения полиномиальных систем уравнений над конечным полем $\mathrm{GF}(q)$.

Теорема 2. *Набор* $G = \{[g_1], [g_2], \ldots, [g_s]\}$ *является базисом Гребнера в* $P[\vec{x}]/(x_1^q - x_1, x_2^q - x_2, \ldots, x_n^q - x_n))$ *тогда и только тогда, когда*:

1) $\forall i, j \in \{1, 2, \ldots, s\}$ $[S(g_i, g_j)]$ *-остаток от деления на* G *равен нулю*;

2) $\forall i \in \{1, 2, \ldots, s\}$, $\forall j \in \{1, 2, \ldots, n\}$ $[g_i][x_j^{q-m}]$ *-остаток от деления на* G *равен нулю, где* m *– степень, с которой* x_j *входит в старший моном* g_i.

Введенное понятие базиса Гребнера сохраняет справедливой теорему об исключении и утверждение о виде редуцированного базиса Гребнера в случае единственности решения системы уравнений. Аналогичные результаты справедливы в случае произвольного идеала J.

СПИСОК ЛИТЕРАТУРЫ

1. *Кокс Д.*, *Литтл Дж.*, *О'Ши Д.* Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры. М.: Мир, 2000.