Алгебраическая симплификация и криптографические мотивы

В. Н. ЛАТЫШЕВ
Московский государственный университет им. М. В. Ломоносова

УДК 512.55

Ключевые слова: алгебраическая симплификация, стандартные базисы идеалов, упорядоченные полугруппы, полугрупповые алгебры, универсальные обёртывающие алгебр Ли, криптография.

Аннотация

С единой точки зрения излагаются общие основы алгебраической симплификации. Определяющим является введённое автором понятие схемы симплификации. В случае алгебр, заданных копредставлением, симплификаторы связаны со стандартным базисом (базисом Грёбнера, базисом Грёбнера—Ширшова) идеала соотношений. Предметом изучения являются алгебры, полученные «деформацией» из полугрупповых алгебр упорядоченных полугрупп. К их числу принадлежат свободные ассоциативные алгебры и универсальные обёртывающие алгебр Ли. Последним уделяется особое внимание. Указываются возможные приложения в криптографии.

Abstract

V. N. Latyshev, Algebraic simplification and cryptographic motives, Fundamentalnaya i prikladnaya matematika, vol. 19 (2014), no. 2, pp. 109—124.

Algebraic simplification is considered from the general point of view. The main notion here is the so-called scheme of simplification due to the author. For a corepresented algebra simplificators are related to the standard basis (Gröbner basis, Gröbner–Shirshov basis) of the ideal of defining relations. We introduce as a main subject for study the class of algebras that may be obtained from ordered semigroup algebras by "deformation" in some sense. This class contains free associative algebras and universal enveloping algebras of Lie algebras. The main attention is paid to the latter algebras. Some possible applications to cryptography are given.

В работе с единой точки зрения излагаются общие основы алгебраической симплификации, нашедшие отражение в различных работах автора.

Определяющим является введённое автором понятие схемы симплификации (см., например, [7]). При этом используются идеи из работ А. И. Ширшова [1], Б. Бухбергера [4], Д. Бергмана [3], Е. С. Голода [5]. В случае задания алгебры образующими и определяющими соотношениями набор симплификаторов задаётся стандартным базисом (базисом Грёбнера, базисом Грёбнера—Ширшова) идеала соотношений. Предметом изучения являются полугрупповые алгебры упорядоченных полугрупп и алгебры, полученные из них путём «деформации»

Фундаментальная и прикладная математика, 2014, том 19, № 2, с. 109—124.

в определённом смысле. К числу таких алгебр принадлежат свободные ассоциативные алгебры, алгебры полиномов, универсальные обёртывающие алгебр Ли. В одно- и двусторонних идеалах алгебр этого класса определяются стандартные базисы. Особенно подробно изучаются стандартные базисы в идеалах универсальных обёртывающих алгебр Ли в духе работы И. Апеля и В. Ласснера [2], где исследуются стандартные базисы односторонних идеалов таких алгебр. Мы предлагаем свою версию изучаемого вопроса и особый упор делаем на двусторонние идеалы. По вычислениям в универсальных обёртывающих алгебрах имеется довольно широкая литература.

В [6] указан способ кодирования сообщений, использующий обратимые элементы групповых алгебр конечных групп. Мы предлагаем аналогичный метод кодирования, использующий возможность одностороннего деления в классе деформированных полугрупповых алгебр упорядоченных полугрупп. «Модельными» примерами здесь являются универсальные обёртывающие алгебры конечномерных алгебр Ли.

1. Схемы симплификации

В математике часто для распознавания отношения эквивалентности, определённого на множестве математических объектов, применяется способ приведения к каноническому виду их символьных кодов (имён): переход к несократимой записи рациональной дроби, нахождение канонического вида квадратичной формы, приведение логической формулы к дизъюнктивному нормальному виду и др.

Под *схемой симплификации* $(M, \leqslant, R)$ мы понимаем множество M символьных выражений (как правило, заданное исчислением), конечное или бесконечное, на котором определён частичный порядок $\leqslant$ с условием минимальности (условием обрыва убывающих цепочек элементов) и которое снабжено фиксированным множеством *симплификаторов* R, элементы которого являются «не повышающими» отображениями множества M в себя, т. е. $rx \leqslant x$ для всех $x \in M$, $r \in R$. Мы будем требовать, чтобы R содержало тождественное отображение.

В конкретных примерах символьные выражения из M являются кодами (именами) математических объектов, частичный порядок $\leqslant$ сравнивает сложность символьных выражений из M, а применение отображений из R упрощает (симплифицирует) символьные коды математических объектов, принадлежащие M. Условие минимальности, которому удовлетворяет порядок $\leqslant$, означает невозможность бесконечного упрощения символьного выражения из M.

Элемент $x \in M$ называется *нормальным*, если он не допускает упрощений, т. е. остаётся на месте после применения симплификаторов: $rx = x$ для всех $r \in R$. Остальные элементы называются *редуцируемыми*. Говорят, что элемент $x \in M$ *редуцируется* к элементу $y \in M$, если $y = r_m \dots r_1 x$, $r_i \in R$,

$i = 1, \ldots, m$. Если при этом элемент y нормален, то он называется *нормальной формой* элемента x и обозначается $\operatorname{nor} x$. В силу условия минимальности, которому удовлетворяет порядок $\leqslant$, всякий элемент множества M обладает нормальной формой, быть может не единственной. Если же элемент $x \in M$ обладает единственной нормальной формой, то она называется его *канонической формой* и обозначается $\operatorname{can} x$. Будем говорить, что схема симплификации обладает свойством *канонизации*, если все элементы множества M имеют каноническую форму. Подмножество $L \subseteq M$ элементов, обладающих канонической формой, инвариантно относительно действия симплификаторов из R. Оно не пусто, поскольку содержит в качестве подмножества множество N всех нормальных элементов. Тем самым определяется схема симплификации $(L, \leqslant, R|_L)$ с канонизацией, которую естественно назвать *подсхемой* схемы $(M, \leqslant, R)$. Иногда бывает удобно рассматривать множество M как полигон над полугруппой отображений $\rho = \langle R \rangle$ множества M в себя, порождённой симплификаторами из R.

На множестве M естественным образом определяются два отношения.

— *Отношение связности* $\sim$. Пару элементов $(x, y) \in M \times M$ назовём непосредственно соотносимой ($x \sim y$), если существует симплификатор $r \in R$, такой что либо $y = rx$, либо $x = ry$. Положим, что пара элементов $(u, v) \in \in M \times M$ находится в отношении $u \sim v$, если она может быть связана цепочкой непосредственных соотносимостей $u \sim z_1 \sim \ldots \sim z_m \sim v$, $z_i \in M$, $i = 1, \ldots, m$. Таким образом, отношение связности симметрично и транзитивно. Оно также рефлексивно, поскольку R содержит тождественное отображение, и потому является эквивалентностью. Отношение связности допускает простую геометрическую интерпретацию, принадлежащую М. Ньюмену. Со схемой симплификации мы связываем её граф Ньюмена [8], обозначаемый нами через Γ, ориентированный и построенный по следующему правилу. Вершинами Γ объявляются элементы множества M, причём из вершины x выходит ребро, кончающееся в вершине $y \neq x$, если $y = rx$ для некоторого симплификатора $r \in R$, т. е. $y < x$. В силу условия минимальности для порядка $\leqslant$ все ориентированные пути в графе Γ конечны. Связные компоненты в графе Γ определяются без учёта ориентации, т. е. две вершины лежат в одной связной компоненте, если они могут быть соединены в Γ «ломаной линией» (неориентированным путём). Легко убедиться, что отношение $x \sim y$, $x, y \in M$, означает, что вершины x и y лежат в одной связной компоненте графа Γ. Элемент $x \in M$ нормален, если он изображается в Γ «минимальной вершиной», т. е. вершиной, из которой не выходит ни одного ребра.

— *Отношение Чёрча—Россера* $\rightsquigarrow$. Два элемента $(x, y) \in M \times M$ считаются соотносимыми, если ρ-орбиты этих элементов имеют непустое пересечение: найдётся $z \in \rho x \cap \rho y$, т. е. $z = \sigma x = \tau y$, $\sigma = \sigma_l \ldots \sigma_1$, $\tau = \tau_m \ldots \tau_1$, $\sigma_i, \tau_j \in R$, $\sigma, \tau \in \rho$. На языке графа Ньюмена Γ это означает, что в Γ существуют ориентированные пути, начинающиеся в вершинах x и y и

кончающиеся в вершине z. Отношение Чёрча—Россера рефлексивно и симметрично, но в общем случае не транзитивно.

Предложение 1. *Следующие условия, наложенные на схему симплификации* $(M, \leqslant, R)$*, равносильны*:

1) *схема симплификации обладает свойством канонизации*;
2) *выполняется условие Чёрча—Россера*: *отношение Чёрча—Россера является эквивалентностью*;
3) *выполняется условие локального слияния*: $r_1 x \rightsquigarrow r_2 x$ *для всех* $x \in M$, $r_1, r_2 \in R$;
4) *всякий класс эквивалентности отношения связности* $\sim$ *обладает единственным нормальным элементом, который в нём является наименьшим*;
5) *отношения связности* $\sim$ *и Чёрча—Россера* $\rightsquigarrow$ *совпадают.*

Доказательство. Докажем импликацию $1) \Longrightarrow 2)$. Необходимо показать транзитивность отношения Чёрча—Россера: из $x \rightsquigarrow y \rightsquigarrow z$ следует, что $x \rightsquigarrow z$. Действительно, $x \rightsquigarrow y$ влечёт $\operatorname{can} x = \operatorname{can} y$ и $y \rightsquigarrow z$ влечёт $\operatorname{can} y = \operatorname{can} z$, откуда получаем, что $\operatorname{can} x = \operatorname{can} z$ влечёт $x \rightsquigarrow z$.

Докажем импликацию $2) \Longrightarrow 3)$. Поскольку R содержит тождественное отображение, то $r_1 x \rightsquigarrow x \rightsquigarrow r_2 x$ влечёт $r_1 x \rightsquigarrow r_2 x$ для всех $x \in M$, $r_1, r_2 \in R$.

Докажем импликацию $3) \Longrightarrow 1)$. Предположим противное: в M существуют «плохие» элементы, не имеющие канонической формы. По условию минимальности в множестве всех плохих элементов должны быть минимальные плохие элементы, пусть $x \in M$ — один из них. Тогда x обладает двумя различными нормальными формами: $\operatorname{nor}_1 x = r_l \dots r_1 x$ и $\operatorname{nor}_2 x = r'_m \dots r'_1 x$, $\operatorname{nor}_1 x \neq \operatorname{nor}_2 x$, $r_i, r'_j \in R$. Без ограничения общности рассуждения можно считать, что $r_1 x < x$ и $r'_1 x < x$. Но тогда элементы $r_1 x$ и $r'_1 x$ обладают каноническими формами ввиду минимальности элемента x. По условию слияния $r_1 x \rightsquigarrow r'_1 x$, откуда следует, что $\operatorname{can} r_1 x = \operatorname{nor}_1 x = \operatorname{can} r'_1 x = \operatorname{nor}_2 x$, т. е. $\operatorname{nor}_1 x = \operatorname{nor}_2 x$, противоречие.

Итак, условия 1)—3) равносильны.

Докажем импликацию $1) \Longrightarrow 4)$. Из условия канонизации вытекает, что любые две соседние вершины графа Γ имеют одну и ту же каноническую форму. Следовательно, все вершины одной и той же связной компоненты имеют одну и ту же каноническую форму, являющуюся единственной её минимальной вершиной. Но это и есть условие 4), сформулированное на языке графа Γ.

Докажем импликацию $4) \Longrightarrow 1)$. Нормальные формы одного и того же элемента множества M лежат в одной связной компоненте графа Γ.

Таким образом, доказана равносильность условий 1)—4).

Докажем импликацию $1) \Longrightarrow 5)$. Импликация $x \rightsquigarrow y \Longrightarrow x \sim y$ очевидна. Обратная импликация $x \sim y \Longrightarrow x \rightsquigarrow y$ вытекает из справедливости импликации $x \sim y \Longrightarrow \operatorname{can} x = \operatorname{can} y$.

Докажем импликацию $5) \Longrightarrow 2)$. Из равенства $\sim \, = \, \rightsquigarrow$ следует, что отношение Чёрча—Россера $\rightsquigarrow$ является эквивалентностью. $\square$

В приложениях основное назначение схем симплификации состоит в построении эффективных методов распознавания отношений эквивалентности. Более точно, если на множестве M определено отношение эквивалентности $\sim$, то полезным оказывается построение схемы симплификации $(M, \leqslant, R)$ со свойством канонизации, в которой несущим множеством является M и при этом выполняется двойная импликация $x \sim y \iff \operatorname{can} x = \operatorname{can} y$, $x, y \in M$. Конечно, здесь имеется в виду, что канонические формы вычисляются с помощью алгоритма. Методология построения таких алгоритмов хорошо формулируется на языке линейных схем симплификации, о которых речь идёт ниже.

Схему симплификации $(M, \leqslant, R)$ будем называть *линейной*, если её несущее множество M является линейным пространством над некоторым полем k, а симплификаторы из R действуют как линейные операторы.

Лемма 1. *Пусть $(M, \leqslant, R)$ — произвольная схема симплификации и $x_1, \ldots, x_m \in M$ — конечное множество элементов. Тогда существует произведение симплификаторов $s \in \rho$, такое что элементы $sx_i \in N$, $i = 1, \ldots, m$, нормальны.*

Доказательство. Проводя индукцию по числу m, можно предположить, что существует произведение симплификаторов $q \in \rho$, такое что $qx_i \in N$, $i = 1, \ldots, m-1$. Существует произведение симплификаторов $t \in \rho$, приводящее элемент qx_m к нормальному виду $(tq)x_m \in N$. Тогда произведение симплификаторов $s = tq$ является искомым. □

Предложение 2. *В любой линейной схеме симплификации $(M, \leqslant, R)$ подмножество элементов $L \subseteq M$, обладающих канонической формой, образует линейное подпространство, инвариантное относительно симплификаторов из R и разлагающееся в прямую сумму инвариантных относительно операторов из R подпространств $L = N \oplus U$, где N — совокупность всех нормальных элементов из M, а U — совокупность всех элементов с нулевой канонической формой.*

Доказательство. Пусть $x, y \in L$, $z = \alpha x + \beta y$, $\alpha, \beta \in k$, $z \in M$. Рассмотрим произвольное произведение симплификаторов $s \in \rho$, приводящее z к нормальной форме $sz \in N$. По лемме 1 существует произведение симплификакторов $t \in \rho$, приводящее элементы sx и sy к нормальным формам $(ts)z = \operatorname{can} x$, $(ts)y = \operatorname{can} y$ соответственно. Отсюда получаем, что $(ts)z = sz = \operatorname{nor} z = \alpha \operatorname{can} x + \beta \operatorname{can} y$. Следовательно, элемент z обладает единственной нормальной формой $\operatorname{can} z = \alpha \operatorname{can} x + \beta \operatorname{can} y \in L$, т. е. $z \in L$. Тем самым доказано, что L — линейное подпространство. Более того, одновременно мы показали, что отображение $\Phi\colon L \to L$, $\Phi\colon z \mapsto \operatorname{can} z$, $z \in L$, пространства L в себя, переводящее всякий элемент в его каноническую форму, является проектором, т. е. линейным идемпотентным оператором $(\Phi^2 = \Phi)$. Следовательно, имеет место прямое разложение $L = \operatorname{Im}\Phi \oplus \operatorname{Ker}\Phi$, где $\operatorname{Im}\Phi = N$ и $\operatorname{Ker}\Phi = U$. □

Следствие 1. *Линейная схема симплификации обладает свойством канонизации, если векторы некоторого базиса её несущего пространства M имеют каноническую форму.*

В линейной схеме симплификации $(M, \leqslant, R)$ со свойством канонизации $(L = M)$ всякий элемент $x \in M$ обладает единственным представлением вида $x = \operatorname{can} x + x_0$, где $\operatorname{can} x \in N$, $x_0 \in U$. Все векторы из M, имеющие общую каноническую форму, образуют целый смежный класс по *O-пространству* U, в котором каноническая форма является наименьшим элементом. В рассматриваемом случае отношение связности совпадает со сравнимостью по модулю U, а действие симплификатора сводится к добавлению некоторого элемента из O-пространства U.

Эти соображения подсказывают методику построения подходящих схем симплификации в приложениях.

Модельный пример. Линейное пространство M над полем k (вообще говоря, бесконечномерное) задано своим базисом $E = \{e_i \mid i \in \mathbb{N}\}$, на котором определён полный порядок $\leqslant$ (порядок с условием минимальности). Этот базис будем называть *выделенным*. Каким-то образом фиксируется подпространство $U \subseteq M$. Требуется построить линейную схему симплификации с несущим пространством M, обладающую свойством канонизации, в которой O-подпространство совпадает с U.

Тем самым ставится задача нахождения эффективной процедуры, распознающей вхождение элемента из M в подпространство U или, что то же самое, распознающей сравнимость двух элементов из M по модулю U.

Введём обозначения, которые сохраним и далее. *Суппортом* $\operatorname{Supp} a$ ненулевого элемента $a \in M$ называется строчка базисных векторов из E, входящих в запись a с ненулевыми коэффициентами и расположенных слева направо в порядке убывания. Наибольший базисный элемент в суппорте $\operatorname{Supp} a$ обозначим через $\bar{a}$. Через ${}^0a$ обозначается результат деления a на его «старший» коэффициент (стоящий при $\bar{a}$).

Теперь приступим к построению искомой линейной схемы симплификации. Для этого нам нужно определить надлежащий частичный порядок на элементах пространства M и систему симплификаторов.

Сравнивать ненулевые элементы пространства M будем лексикографически по их суппортам, считая при этом, что если один суппорт является началом (префиксом) другого суппорта, то более длинный суппорт объявляется старшим. Нулевой элемент считается наименьшим. Таким образом, несравнимыми оказываются различные элементы из M с одинаковыми суппортами. Введённый порядок на M «поднимает» порядок $\leqslant$, определённый на элементах выделенного базиса E, и обозначается тем же символом.

Лемма 2. *Лексикографический порядок на множестве суппортов элементов пространства M удовлетворяет условию минимальности.*

Доказательство. Предположим от противного, что существуют бесконечно убывающие цепочки суппортов, и рассмотрим множество первых (старших) базисных векторов из E в суппортах этих цепочек. В нём есть наименьший элемент $e_{i_0} \in E$. Но тогда существует бесконечно убывающая цепочка суппортов,

каждый из которых начинается вектором e_{i_0}. Вычеркнув его из всех суппортов цепочки, мы получим бесконечно убывающую цепочку суппортов, старшие базисные векторы которых меньше e_{i_0}, противоречие. □

Теперь определим на пространстве M систему симплификаторов, согласованную с введённым на M частичным порядком и такую, чтобы схема симплификации обладала свойством канонизации и O-пространство совпадало с фиксированным подпространством U. Для этого со всяким элементом $u \in U$, $\bar{u} = e_i \in E$, свяжем линейный оператор r_u, действующий на M согласно правилу $r_u e_i = e_i -^0 u$, $r_u e_j = e_j$, $i \neq j$, $e_j \in E$. Назовём его *редукцией* с помощью элемента $u \in U$. Пусть R_v — множество всех редукций с помощью элементов из U. Линейная схема симплификации $(M, \leqslant, R_v)$ является искомой.

Действительно, нулевую нормальную форму имеют лишь элементы из U. Нормальными базисными векторами являются элементы из E, не начинающие суппорты элементов из U. Напротив, старшие базисные векторы элементов из U редуцируются. Линейная оболочка нормальных базисных векторов образует подпространство N нормальных элементов. Построенная схема обладает свойством канонизации, так как если некоторый элемент имеет две нормальные формы, то их разность является ненулевым нормальным элементом, лежащим в U, что невозможно. Согласно предложению 2 имеет место прямое разложение $M = N \oplus U$, где U — O-пространство.

На самом деле можно было построить более простую схему симплификации, решающую ту же задачу, выбрав более «экономично» систему симплификаторов. Рассмотрим подмножество элементов $P \subseteq U$ и множество редукций $R_P \subseteq R_U$, отвечающих элементам множества P. Множество P назовём *полным*, если множества симплификаторов R_P и R_U приписывают любому элементу из M одну и ту же каноническую форму. Множество $P \subseteq U$ является полным в том и только том случае, когда для всякого редуцированного базисного вектора $e_i \in E$ найдётся элемент $v_i \in P$, такой что $\bar{v}_i = e_i$. Если такой элемент v_i единствен, то P является базисом подпространства U, аналогичным ступенчатому базису Гаусса в линейной оболочке линейных форм. При этом нормальные базисные векторы из E играют в этой аналогии роль «свободных переменных». Легко заметить, что если подмножество $P \subseteq U$ полное, то линейная схема симплификации $(M, \leqslant, R_P)$ также решает поставленную задачу.

В приложениях основной задачей является построение такого полного множества $P \subseteq U$, что каноническая форма в линейной схеме симплификации $(M, \leqslant, R_P)$ выполняется с помощью алгоритма.

В алгоритмических вопросах алгебры важное место занимает проблема вхождения элемента в одно- или двусторонний идеал I некоторой алгебры A над полем k. Если в пространстве алгебры A естественным образом определяется выделенный базис E, то решение проблемы вхождения в идеал оказывается возможным при использовании техники схем симплификации, если принять в качестве O-пространства этот идеал $U = I$. Построение хорошего «полного»

подмножества $P \subseteq I$ осуществляется с помощью выбора особой системы порождающих идеала I, называемой его стандартным базисом (базисом Грёбнера, базисом Грёбнера—Ширшова).

В настоящее время существует большое количество классов алгебр (не обязательно ассоциативных и бинарных), в которых находит применение техника алгебраической симплификации. Посвящённая им литература огромна и в полном смысле слова необозрима. Однако лишь небольшое количество этих алгебр пока нашло приложение в реальных вычислениях. Ниже мы делаем попытку объединить эти алгебры в один класс, обратив особое внимание на универсальные обёртывающие алгебр Ли и указывая на некоторые приложения в криптографии. Мы не затрагиваем свободную ассоциативную алгебру и алгебру многочленов, поскольку им посвящено большое количество работ.

2. Деформация полугрупповых алгебр упорядоченных полугрупп и стандартные базисы идеалов

Пусть Λ — упорядоченная полугруппа, умножение в которой обозначается через $\circ$, а порядок через $\leqslant$. Будем предполагать, что порядок $\leqslant$ на Λ удовлетворяет условию минимальности и следующему дополнительному условию: $ab > a$ и $ba > a$ для всех $a, b \neq 1 \in \Lambda$. В частности, если Λ — моноид, то единица в нём — наименьший элемент.

Будем говорить, что алгебра A над полем k получена деформацией из полугрупповой алгебры $k\Lambda$ полугруппы Λ над полем k, если выполняются два условия. Во-первых, совпадают линейные пространства алгебр A и $k\Lambda$, при этом в алгебре A элементы полугруппы Λ считаются выделенным базисом, относительно которого рассматриваются суппорты элементов и старшие базисные векторы. Во-вторых, выполняется условие «типа фильтрации»: $\overline{ab} = a \circ b$ для всех $a, b \in \Lambda$. В частности, в определяемый класс алгебр, конечно, входит и сама полугрупповая алгебра kA, полученная из себя «тривиальной деформацией».

Способом, указанным в разделе 1, на множестве элементов алгебры A можно определить частичный порядок $\leqslant$, сравнивая элементы лексикографически «по суппортам». Этот порядок «продолжает» порядок, определённый на полугруппе Λ, и по лемме 2 удовлетворяет условию минимальности.

Пусть $I \lhd A$ — идеал алгебры A, заданный системой порождающих (базисом) $G = \{g_i \mid i \in \mathbb{N}\}$, в стандартных обозначениях $I = (G)$. Обозначим через R_I систему редукций, действующих на пространстве алгебры A и определённых элементами из I. Тем самым определяется линейная схема симплификации $(A, \leqslant, R_I)$ со свойством канонизации, в которой O-пространством является идеал I (см. раздел 1). Следовательно, имеет место прямое разложение пространства исходной алгебры $A = N \oplus I$, где N — линейная оболочка элементов

полугруппы Λ, не являющихся старшими элементами в суппортах элементов из I.

Теперь рассмотрим множество элементов $P_G = \{ag_ib \mid i \in \mathbb{N},\ g_i \in G,\ a, b \in \Lambda\}$ и через R_G обозначим множество редукций, определённых элементами из P_G. Здесь допускается, что один из элементов a и b или они оба являются пустыми. Линейная схема симплификации $(A, \leqslant, R_G)$ в случае произвольной системы порождающих G идеала I не будет, вообще говоря, обладать свойством канонизации. Но это свойство будет иметь место, если множество элементов $P_G \subseteq I$ будет полным в I (см. раздел 1), т. е. для всякого элемента $u \in I$ найдутся элементы $g_i \in G$ и $a, b \in \Lambda$, такие что $\bar{u} = \overline{ag_ib} = a \circ \bar{g}_i \circ b$. Такая система порождающих идеала называется его *стандартным базисом*. В этом случае канонические формы элементов алгебры A в линейных схемах симплификации $(A, \leqslant, R_I)$ и $(A, \leqslant, R_G)$ совпадают.

Переходим к основной проблеме в рассматриваемом круге вопросов, а именно к нахождению стандартного базиса и идеала, по возможности «наиболее простого», когда идеал задан некоторой произвольной системой порождающих (как правило, конечной).

Сохраняем прежние обозначения. Всякий элемент $u \in I$ обладает *представлением* вида $u = \sum\limits_{i=1}^{m} \lambda_i a_i g_i b_i$, где $\lambda_i \in k$, $g_i \in G$, $a_i, b_i \in \Lambda$, в частности, один из множителей a_i и b_i или они оба могут быть пустыми. Положим $c_i = \overline{a_i g_i b_i} = a_i \circ \overline{g_i} \circ b_i \in \Lambda$. Элемент $c = \max_i c_i \in \Lambda$ называется *параметром* указанного представления элемента u через базис G идеала I. Ясно, что $c \geqslant \bar{u}$. Если $c = \bar{u}$, то, следуя Ф. С. Маколею, представление будем называть *H-представлением*.

Теорема 1. *Следующие условия, наложенные на систему порождающих G идеала I алгебры A над полем k, полученной деформацией из полугрупповой алгебры $k\Lambda$ упорядоченной полугруппы Λ, равносильны*:

1) *G — стандартный базис идеала I*;
2) *всякий элемент идеала I некоторой последовательностью редукций из R_G переводится в 0*;
3) *всякий элемент идеала I обладает H-представлением относительно G*;
4) *разности вида $s = {}^0(a_{i_1} g_i a_{i_2}) - {}^0(a_{j_1} g_j a_{j_2})$, где $\overline{a_{i_1} g_i a_{i_2}} = \overline{a_{j_1} g_j a_{j_2}} = c \in \Lambda$, $a_{i_1}, a_{i_2}, a_{j_1}, a_{j_2}$ принадлежат Λ или пустые символы, $g_i, g_j \in G$, обладают представлениями относительно G с параметрами меньше c*;
5) *линейная схема симплификации $(A, \leqslant, R_G)$ обладает свойством канонизации.*

Доказательство. Импликация 1) $\Longrightarrow$ 2) следует из условия минимальности для порядка $\leqslant$.

Докажем импликацию 2) $\Longrightarrow$ 3). Редуцируя элемент $u \in I$ к нулю, мы на каждом шаге вычитаем элемент из P со старшим элементом из Λ, не большим $\bar{u}$.

Импликация 3) $\Longrightarrow$ 4) верна, поскольку $s \in I$ и $\bar{s} < c$.

Докажем импликацию 4) $\Longrightarrow$ 5). По следствию 1 достаточно доказать, что элементы из Λ имеют каноническую форму. Предположим противное: существуют «плохие» элементы в Λ, не имеющие канонической формы, и $a \in \Lambda$ — один из минимальных плохих элементов. Это означает, что существуют две цепочки редукций из R_G, начинающихся редукциями $r_1, r_2 \in R_G$, приводящие элемент a к различным нормальным формам $\operatorname{nor}_1 a \neq \operatorname{nor}_2 a$. Элементы $r_1 a$ и $r_2 a$ заведомо обладают каноническими формами по выбору элемента $a \in \Lambda$. Поэтому $r_1 \neq r_2$. Но $r_1 a - r_2 a = s \in I$ — элемент из пункта 4). По условию 4) s обладает представлением через G, слагаемые которого имеют нулевую каноническую форму, следовательно, и s имеет каноническую форму $\operatorname{can} s = \operatorname{can}(r_1 a) - \operatorname{can}(r_2 a) = \operatorname{nor}_1 a - \operatorname{nor}_2 a = 0$, противоречие.

Импликация 5) $\Longrightarrow$ 2) справедлива, поскольку в представлении элемента идеала I в виде линейной комбинации элементов из P все слагаемые имеют нулевую каноническую форму.

Импликация 2) $\Longrightarrow$ 1) обосновывается тем, что все старшие элементы из Λ в представлениях элементов идеала I через G оказываются редуцируемыми. $\square$

Элементы s из пункта 4) теоремы 1 называются *s-элементами*. Они играют главную роль во всех алгоритимических вопросах, связанных со стандартными базисами идеалов. Мы видим, что критерием стандартности базиса G идеала I в алгебре A рассматриваемого типа является редуцируемость к нулю относительно G всех s-элементов. Во многих конечно порождённых алгебрах A этого класса выполняется следующее условие: если идеал I обладает конечным базисом G, то существует конечное число так называемых *критических* s-элементов, редуцируемость к нулю которых относительно G влечёт за собой стандартность базиса G. Кроме того, если полугруппа Λ нётерова, то, присоединяя к идеалу I базиса G последовательно не редуцируемые к нулю элементы, мы за конечное число шагов пополним G до стандартного базиса идеала I. Этот метод получил называние алгоритма Бухбергера, хотя точнее было бы называть его алгоритмом Бухбергера—Ширшова. Критические s-элементы есть в свободной ассоциативной алгебре и алгебре полиномов. Этим алгебрам посвящены многие работы. Ниже мы сосредоточим своё внимание на универсальных обёртывающих конечномерных алгебр Ли.

На множестве элементов «базовой» полугруппы Λ определим новый частичный порядок $\succ$: $d = a \circ b \circ c \succ b$, где $a, b, c, d \in \Lambda$ и элементы a, c не являются одновременно пустыми символами. Очевидна импликация $d \succ b \Longrightarrow d > b$, поэтому частичный порядок $\succ$ удовлетворяет условию минимальности. Следуя Анику, минимальные элементы в множестве $\bar{I} = \{\bar{a} \mid a \in I\}$ относительно этого порядка в Λ будем называть *обструкциями* идеала I. Стандартный базис G идеала I называется *редуцированным*, если он удовлетворяет следующим двум условиям:

1) старшие коэффициенты элементов из G равны 1;
2) любой элемент $g_i \in G$ неподвижен относительно редукций, определяемых остальными элементами $G \setminus \{g_i\}$.

Теорема 2. *Всякий идеал $I \lhd A$ деформированной полугрупповой алгебры обладает единственным редуцированным стандартным базисом.*

Доказательство. Пусть G — редуцированный стандартный базис идеала I. Запишем его элементы в виде $g_i = \bar{g}_i - f_i$, где $f_i \in N$ — сумма младших членов (с обратным знаком). Тогда очевидно, что $\bar{g}_i$ — обструкция. Далее, $\bar{g}_i = f_i + g_i$ влечёт $\operatorname{can} \bar{g}_i = \operatorname{can} f_i + \operatorname{can} g_i = f_i$. Таким образом,

$$G = \{g_i = \bar{g}_i - \operatorname{can} \bar{g}_i \mid \bar{g}_i \in \Lambda - \text{обструкция идеала } I\}.$$

Очевидно и обратное, что указанная система элементов является редуцированным стандартным базисом идеала I. □

Стандартный базис одностороннего идеала I в деформированной полугрупповой алгебре A определяется аналогично случаю двустороннего идеала. Например, система порождающих G левого идеала I называется его стандартным базисом, если подмножество элементов $P = \{ag_i \mid g_i \in G,\ a \in \Lambda \cup \varnothing\}$ является полным в I. При этом несложно убедиться, что все основные утверждения, включая теоремы 1 и 2, доказанные для двусторонних идеалов, без труда переносятся на односторонние идеалы.

Предложение 3. *Стандартный базис главного левого идеала $I = (g) \lhd_l A$ деформированной полугрупповой алгебры A, порождённый элементом $g \in A$, состоит из одного этого элемента.*

Доказательство. Элемент $u \in I$ представляется в виде $u = vg$, $v \in A$, при этом единственным образом ввиду отстутствия делителей нуля в A. Тогда $\bar{u} = \overline{vg} = \overline{\bar{v}g} = \bar{v} \circ \bar{g}$. □

Предложение 4. *В деформированной полугрупповой алгебре A возможно однозначное левое (правое) деление с остатком на любой её ненулевой элемент $g \in A$.*

Доказательство. Согласно предложению 3 одноэлементное множество $\{g\}$ является стандартным базисом левого идеала $I = (g) \lhd_l A$. Приведение элемента $u \in A$ алгебры A к каноническому виду относительно I с помощью левых редукций относительно $\{g\}$ даёт нам равенство $u = vg + \operatorname{can} u$, где элемент $\operatorname{can} u$ нормален относительно $\{g\}$ (идеала $I = (g)$). Поскольку «остаток» $\operatorname{can} u$ определён однозначно, то и «левое частное» v также определено однозначно. □

Предложение 5. *Если базовая полугруппа Λ коммутативна, то стандартный базис G двустороннего идеала $I \lhd A$ деформированной полугрупповой алгебры A порождает его одновременно и как левый, и как правый идеал.*

Доказательство. Поскольку в рассматриваемом случае

$$\overline{ag_ib} = a \circ \bar{g}_i \circ b = (a \circ b) \circ \bar{g}_i = \bar{g}_i \circ (a \circ b) = \overline{(a \circ b)g_i} = \overline{g_i(a \circ b)}, \quad a, b \in \Lambda \cup \varnothing,\ \ g_i \in G,$$

то оба подмножества элементов

$$P_l = \{ag_i \mid a \in \Lambda \cup \varnothing,\ g_i \in G\}, \quad P_r = \{g_ia \mid a \in \Lambda \cup \varnothing,\ g_i \in G\}$$

являются полными в I. □

3. Вычисления в универсальных обёртывающих алгебр Ли

Пусть L — n-мерная алгебра Ли с базисом $X = \{x_1, \ldots, x_n\}$, умножение в которой обозначается точкой $\cdot$, U_L — её универсальная обёртывающиая алгебра, содержащая L, базис в которой образуют «коммутативные мономы» вида $x_1^{m_1} \ldots x_n^{m_n}$. Умножение базисных векторов производится с учётом равенства $[x_i, x_j] = x_i x_j - x_j x_i = x_i \cdot x_j \in L$. Свободную абелеву полугруппу $[x]$ (полугруппу коммутативных мономов) упорядочим следующим образом: сначала мономы сравниваются по длине (степени), а если длины равны, то они сравниваются лексикографически по индексам переменных. После этого можно считать, что алгебра U_L получена деформацией в смысле раздела 2 из алгебры полиномов $k[X]$. Заметим, что последнее утверждение неверно, если мономы из $[X]$ упорядочить «чисто лексикографически», поскольку, вообще говоря, не будет выполняться условие «типа фильтрации».

Полугруппа $[X]$ коммутативна, следовательно, стандартный базис идеала $I \lhd U_L$ порождает I и как левый, и как правый идеал (предложение 5). Поэтому при построении стандартных базисов в идеалах алгебры U_L основную роль будут играть односторонние идеалы.

Ближайшей нашей задачей будет показать существование критических s-элементов в конечных системах порождающих односторонних идеалов алгебры U_L. В отличие от работы И. Апеля и В. Лассснера [2], наша версия исходит из общей версии стандартного базиса. Кроме того, мы затрагиваем алгоритмические вопросы, связанные с двусторонними идеалами в алгебре U_L.

Ниже мы используем следующие обозначения и очевидные свойства умножения в U_L.

1. $ab = a \circ b - h_{a,b}$, где $a, b \in [X]$ и $h_{a,b} \in U_L$, $\overline{h_{a,b}} < a \circ b$.
2. Если $I \lhd_l U_L$ — левый идеал, порождённый системой элементов $G = \{g_i \in N\}$, и элемент $u \in I$ обладает представлением (относительно G) с параметром меньше b, $b \in [X]$, то элемент $au \in I$, $a \in [X]$, обладает представлением с параметром меньше $a \circ b \in [X]$.
3. Для фиксированной пары индексов $i, j \in \mathbb{N}$ обозначим $w_{i,j} = \text{Н.О.К.}(\bar{g}_i, \bar{g}_j)$ в полугруппе $[X]$, $w_{i,j} = w_i \circ \bar{g}_i = w_j \circ \bar{g}_j \in [X]$, $w_i, w_j \in [X]$.

Критическим s-элементом, отвечающим паре индексов $i, j \in \mathbb{N}$, называется элемент $s_{i,j} = w_i^0 g_i - w_j^0 g_j = {}^0(w_i g_i) - {}^0(w_j g_j)$. В случае свободной ассоциативной алгебры и алгебры полиномов в определении критического элемента дополнительно предполагается, что $(\bar{g}_i, \bar{g}_j) \neq 1$ в $[X]$.

Предложение 6. *Если все критические s-элементы относительно системы порождающих G левого идеала $I \lhd_l U_L$ обладают представлением с параметром, меньшим параметра их первоначального представления, то и все s-элементы удовлетворяют этому условию.*

Доказательство. В прежних обозначениях произвольный s-элемент, отвечающий паре индексов $i, j \in \mathbb{N}$, имеет вид $s = {}^0(ug_i) - {}^0(vg_j) = u^0 g_i - v^0 g_j$; $u, v \in [X]$, $u \circ \bar{g}_j = v \circ \bar{g}_j = z \in [X]$ — параметр первоначального представления элемента s. В полугруппе $[X]$ справедлива импликация

$$z = \xi \circ w_{i,j} = \xi \circ w_i \circ \bar{g}_i = \xi \circ w_j \circ \bar{g}_j = u \circ \bar{g}_i = v \circ \bar{g}_j \Longrightarrow$$
$$\Longrightarrow u = \xi \circ w_i, \quad v = \xi \circ w_j, \quad \xi \in [X].$$

Из свойства 1 умножения в алгебре U_L получаем

$$\xi w_i = \xi \circ w_i - h_{\xi, w_i} = u - h_u, \quad h_u < u, \quad \bar{h}_u \in U_L,$$
$$\xi w_j = \xi \circ w_j - h_{\xi, w_j} = v - h_v, \quad h_v < v, \quad \bar{h}_v \in U_L,$$

откуда следует, что

$$u = \xi w_i + h_u, \quad v = \xi w_j + h_v.$$

Следуя обозначениям, введённым Ж. Бергманом, обозначим через $I_z \subseteq I$ линейное подпространство элементов, обладающих представлением относительно G с параметром меньше z. Ниже знак сравнения $\equiv$ относится к подпространству I_z. Подставляя выражения элементов u и v из последних равенств в запись элемента s и используя свойство 2 умножения в U_L, мы получаем следующую цепочку сравнений и равенств:

$$s = (\xi w_i + h_u)^0 g_i - (\xi w_j + h_v)^0 g_j \equiv \xi {w_i}^0 g_i - \xi {w_j}^0 g_j = \xi({w_i}^0 g_i - {w_j}^0 g_j) = \xi s_{i,j} \in I_z,$$

поскольку по условию $s_{i,j} \in I w_{i,j}$. □

За конечное число шагов мы можем проверить и редуцируемость к нулю, установив тем самым, является ли G стандартным базисом левого идеала I. Более того, так как базовая полугруппа $[X]$ нётерова, то, если G не является стандартным базисом, с помощью алгоритма Бухбергера G можно пополнить до стандартного базиса за конечное число шагов.

Переходим к описанию стандартных базисов двусторонних идеалов алгебры U_L.

Обозначим через $\operatorname{ad} x_i$ внутреннее дифференцирование U_L, определённое базисным элементом $x_i \in X$: $\operatorname{ad} x_i(u) = [u, x_i] = ux_i - x_i u$, $u \in U_L$. Для краткости такие дифференцирования назовём *элементарными*. Очень важно отметить, что они не повышают максимальную из степеней мономов, входящих в запись элемента из U_L.

Лемма 3. *Левый идеал $I \lhd_l U_L$, замкнутый относительно элементарных дифференцирований, является двусторонним идеалом алгебры $U(L)$.*

Доказательство. Покажем, что I выдерживает умножение на порождающие элементы $x_i \in X$: $u \in I$, $ux_i = x_i u + [u, x_i] \in I$, поскольку $x_i u, [u, x_i] \in I$. □

Систему элементов $G = \{g_i \mid i \in \mathbb{N}\} \subset U_L$ назовём *дифференциально замкнутой*, если её линейная оболочка $\operatorname{Span} G$ замкнута относительно элементарных дифференцирований.

Следствие 2. *Левый идеал $I \lhd_l U_L$, порождённый дифференциально замкнутой системой элементов $G = \{g_i \mid i \in \mathbb{N}\}$, является двусторонним идеалом алгебры U_L.*

Доказательство. По лемме 3 достаточно показать, что I замкнут относительно элементарных дифференцирований. Всякий элемент из идеала I является линейной комбинацией элементов вида $ug_i, u \in U_L$, $g_i \in G$. Имеем $\operatorname{ad} x_j(ug_i) = [ug_i, x_j] = [u, x_j]g_i + u[g_i, x_j] \in I$, поскольку каждое слагаемое правой части равенства лежит в I. □

Лемма 4. *Существует алгоритм, дополняющий конечную систему порождающих $G = \{g_1, \ldots, g_m\}$ двустороннего идеала $I \lhd U_L$ до конечной системы элементов, порождающей I одновременно и как левый, и как правый идеал.*

Доказательство. На первом шаге алгоритма проверяем, не является ли G дифференциально замкнутым, т. е. не лежат ли все коммутаторы вида $[g_i, x_j]$, $i = 1, \ldots, m$, $j = 1, \ldots, n$, в линейной оболочке $\operatorname{Span} G$. Если да, то множество $G_1 = G$ является искомым по лемме 3. Если нет, то существует коммутатор $[g_i, x_j] \notin \operatorname{Span} G$. Полагаем $G_1 = G \cup \{[g_i, x_j]\} \subset I$. Далее к G_1 применяем предыдущее рассуждение и т. д. На каждом шаге мы осуществляем присоединение элементов из конечномерного подпространства элементов алгебры U_L степени не выше D (относительно X), где D — максимальная из степеней элементов множества G. Поэтому описанная процедура обрывается на некотором шаге с номером t, и множество G_t является искомым. □

Предложение 7. *Существует алгоритм, дополняющий конечную систему порождающих G двустороннего идеала $I \lhd U_L$ до его стандартного базиса.*

Доказательство. Сначала, применяя алгоритм из леммы 4, дополняем G до конечной системы элементов H, порождающей I как левый идеал. Затем алгоритмом Бухбергера дополняем H до стандартного базиса как базиса левого идеала. □

4. Возможные криптографические приложения

Основная идея этого пункта заимствована из совместной работы Б. Хёрли и Т. Хёрли [6], где для кодирования сообщений используются обратимые элементы конкретных групповых алгебр. Предлагаемый нами метод кодирования использует алгебры, полученные деформацией из полугрупповых алгебр.

Фиксируем произвольную алгебру A, полученную деформацией из полугрупповой алгебры над полем k. Мы сохраняем все предыдущие обозначения. В качестве основного поля можно взять поле рациональных чисел $\mathbb{Q}$ или конечное поле $\mathbb{F}_q$. Положим, что передаваемое сообщение записывается строкой $w = \alpha_1\alpha_2 \ldots \alpha_d$, $\alpha_i \in k$, из элементов поля k *длины* d.

В распоряжении отправителя (Боб) и получателя (Алиса) имеются следующие секретные данные.

— Алгебра A над полем k, полученная деформацией из полугруппой алгебры $k\Lambda$.
— Эффективная нумерация (перечислительный процесс) элементов базовой полугруппы Λ.
— Кодирующий элемент

$$u = \sum_{j=1}^{m} \beta_j a_j \in A, \quad a_i \in \Lambda, \quad \beta_j \in k.$$

Боб записывает сообщение w в виде элемента

$$\hat{w} = \sum_{i=1}^{d} \alpha_i a_i \in A, \quad a_i \in \Lambda,$$

и осуществляет кодирование

$$\hat{w} \mapsto \hat{z} = \hat{w}u = \sum_{l=1}^{t} \gamma_l a_l \in A, \quad a_l \in \Lambda, \quad \gamma_k \in k,$$

умножая элемент $\hat{w}$ справа на кодирующий элемент u. Алиса получает сообщение в виде строки $z = \gamma_1 \dots \gamma_t$ и восстанавливает элемент $\hat{z}$, пользуясь известной ей нумерацией элементов полугруппы Λ. Поскольку элемент $\hat{z}$ лежит в главном левом идеале, порождённом кодирующим элементом u, он редуцируется относительно u к нулю. Результатом этого процесса редукций является представление $\hat{z} = \hat{w}u$, поскольку левое деление на u единственно в A (предложение 4). Снова пользуясь нумерацией элементов Λ, Алиса восстанавливает сообщение $w = \alpha_1 \dots \alpha_d$.

Богатейший запас примеров деформированных групповых алгебр дают универсальные обёртывающие алгебры, которым посвящён предыдущий раздел. Процесс обнаружения кодирующего элемента весьма труден даже в случае, когда известны алгебра A и нумерация элементов базовой полугруппы Λ, так как в большинстве случаев алгебра A вообще не факториальная. Но и факториальный случай (алгебра полиномов) сложен ввиду большой сложности алгоритмов факторизации.

Литература

[1] Ширшов А. И. О базах свободной алгебры Ли // Алгебра и логика. — 1962. — Т. 1. — С. 14—19.

[2] Apel J., Lassner W. An extension of Buchberger's algorithm and calculations in enveloping fields of Lie algebras // Symbol. Comput. — 1988. — Vol. 6. — P. 361—370.

[3] Bergman G. M. The diamond Lemma for ring theory // Adv. Math. — 1978. — Vol. 6. — P. 178—218.

[4] Buchberger B., Loos R. Algebraic simplification // Computing. — 1982. — Vol. 4. — P. 11—43.

[5] Golod E. S. Standard bases and homology // Algebra Some Current Trends. Proc. of the 5th Nat. School in Algebra held in Varna, Bulgaria, Sept. 24—Oct. 4, 1986. — Berlin: Springer, 1988. — (Lect. Notes Math.; Vol. 1352). — P. 88—95.

[6] Hurley B., Hurley T. Group ring cryptography. — 2011. — arXiv:1104.1724v1[math.GR].

[7] Latyshev V. N. An improved version of standard bases // Formal Power Series and Algebraic Combinatorics. 12th Int. Conf., FPSAC'00, Moscow, Russia, June 2000, Proc. — Berlin: Springer, 2000. — P. 496—505.

[8] Newman M. H. Theories with a combinatorial definition of «equivalence» // Ann. Math. — 1942. — Vol. 43, no. 2. — P. 223—243.