Об одном вычислительном свойстве конечных циклических групповых алгебр и многочленов применительно к теории кодирования

Р. М. АНТОНЯН, А. М. АНТОНЯН (Ереван)

Общепринятый способ задания циклических кодов ([1]) предусматривает наличие так называемого порождающего элемента, который может иметь вид либо многочлена над алфавитом кода, либо идемпотента соответствующей групповой алгебры конечной циклической группы над упомянутым алфавитом. По теории Веддерберна—Артина ([2]) каждый идемпотент классически полупростой (вполне приводимой, полупростой артиновой) алгебры разлагается в сумму неразложимых идемпотентов. Из изложенного следует достаточность задания неразложимых идемпотентов для описания всех идемпотентов классически полупростой алгебры.

§ 1. Прямое вычисление неразложимых идемпотентов

Введем в рассмотрение некоторые объекты, необходимые для дальнейших рассуждений и выводов. Пусть F есть поле из двух элементов, G представляет собой группу нечетного порядка n, $n>1$, ζ — образующая группы G, а FG — групповая алгебра группы G над полем F. Рассмотрим элемент

$$\zeta^t+\zeta^{2t}+\zeta^{2^2t}+\ldots+\zeta^{2^{r-1}t} \tag{1}$$

алгебры FG, где t есть произвольное натуральное число, причем $2^r t \equiv t \pmod n$ и $2^i t \not\equiv t \pmod n$ для всех i из множества $\{1, 2, \ldots, r-1\}$. Непосредственной проверкой нетрудно убедиться в том, что вышеприведенный элемент является идемпотентом алгебры FG. Ф. Дж. Мак—Вильямс называет такие идемпотенты тривиальными ([3]), однако термин «циклотомические» представляется нам более удачным с точки зрения отражения сущности рассматриваемого объекта.

Множество всех различных идемпотентов вида (1) обозначим через $\{a_i|i\in I\}$, причем $a_0=1$. Для дальнейших рассмотрений нам понадобится

Лемма. а) *Произвольный идемпотент алгебры FG может быть задан в виде суммы элементов множества $\{a_i|i\in I\}$;*

б) *любая сумма элементов множества* $\{a_i|i\in I\}$ *есть некоторый идемпотент алгебры* FG.

Доказательство. Каждый элемент алгебры FG может быть записан в виде многочлена $f(\zeta)$ от образующей ζ группы G с коэффициентами из поля F. Если $f(\zeta)$ есть идемпотент алгебры FG, то выполняется соотношение

$$f^2(\zeta) = f(\zeta^2) = f(\zeta)$$

в силу двоичности поля F, то есть, автоморфизм $\zeta \to \zeta^2$ группы G индуцирует всего лишь перестановку одночленов в многочлене $f(\zeta)$. Отсюда следует, что из присутствия в $f(\zeta)$ одночлена ζ^t вытекает содержание в $f(\zeta)$ одночленов $\zeta^{2t}, \zeta^{2^2 t}, \ldots, \zeta^{2^{r-1}t}$, что и завершает доказательство пункта а).

б) Справедливость второй части леммы следует из факта, что сумма любых идемпотентов классически полупростой алгебры снова есть идемпотент этой алгебры.

Хорошо известно ([4]), что классически полупростая групповая алгебра конечной группы G разлагается в прямую сумму одномерного и фундаментального идеалов, причем одномерный идеал порождается идемпотентом

$$\frac{1}{|G|}\sum_{g\in G} g, \tag{2}$$

а фундаментальный — идемпотентом, причем фундаментальный идеал состоит из всех элементов, вес Ли ([1]) которых является сравнимым с нулем по модулю характеристики основного поля, а одномерный — из элементов, скалярно кратных (2).

В нашем случае одномерный идеал содержит один единственный ненулевой элемент, то есть (2), а порождающий фундаментальный идеал идемпотент имеет вид

$$\sum_{i=1}^{n-1} \zeta^i, \tag{3}$$

причем нетрудно видеть, что элемент (3) совпадает с суммой всех элементов множества $\{a_i|i\in I\}$.

Преобразуем множество $\{a_i|i\in I\}$ следующим образом: для каждого i, $i\in I$, обозначим через b_i элемент a_i, если a_i имеет четный вес Хэмминга, либо $\sum_{i=0}^{n-1} \zeta^i + a_i$, в противном случае. Сформулируем основное утверждение этого параграфа.

Теорема 1. *Максимальное ненулевое произведение элементов множества* $\{b_i|i\in I\}$ *есть неразложимый идемпотент алгебры* FG.

Доказательство. Легко убедиться в справедливости леммы для множества $\{b_i|i\in I\}$. Рассмотрим максимальное ненулевое произведение элементов b_i, $i\in I$. Допустим, оно имеет вид

$$b_{i_1} \cdot b_{i_2} \cdot \ldots \cdot b_{i_k}. \tag{4}$$

Если элемент (4) не есть неразложимый идемпотент алгебры FG, то умножим его на произвольный неразложимый идемпотент из его разложения, к примеру, на e. Тогда элемент

$$b_{i_1} \cdot b_{i_2} \cdot \ldots \cdot b_{i_k} \cdot e \tag{5}$$

есть неразложимый идемпотент алгебры FG. По лемме, идемпотент e разлагается в сумму некоторых элементов множества $\{b_i | i \in I\}$. Из максимальности произведения (4) вытекает, что элемент (5) разлагается в сумму нескольких экземпляров элемента (4), так как все остальные слагаемые равны нулю. Отсюда и из двоичности поля F следует справедливость равенства

$$e = b_{i_1} \cdot \ldots \cdot b_{i_k} \cdot e = b_{i_1} \cdot \ldots \cdot b_{i_k}$$

и доказательство теоремы завершено.

§ 2. Формулы связи неприводимых многочленов и неразложимых идемпотентов полупростых факторалгебр алгебры многочленов над конечными полями

В литературе ([1]) описан способ задания циклических кодов в виде идеалов факторалгебры $F[X]/\mathrm{Id}(X^n-1)$ алгебры многочленов $F[X]$ над конечным полем F, $|F|=q$, причем n взаимно просто с q. Порождающими элементами этих идеалов являются с одной стороны идемпотенты алгебры $F[X]/\mathrm{Id}(X^n-1)$, а с другой — делители двучлена X^n-1. Так как произвольный идемпотент классически полупростой алгебры разлагается в сумму неразложимых идемпотентов, а каждый многочлен алгебры $F[X]$ — в произведение неприводимых многочленов, задача нахождения формул связи неразложимых идемпотентов и неприводимых многочленов представляет интерес. Нижеследующее утверждение решает эту задачу для несколько более широкого класса алгебр.

Теорема 2. *Пусть $f(X)$ — произвольный сепарабельный многочлен из $F[X]$ ненулевой степени n. Пусть также*

$$\pi\colon\ F[X] \to F[X]/\mathrm{Id}\, f(X) —$$

канонический эпиморфизм, а $f_1(X), \ldots, f_r(X)$ — неприводимые делители многочлена $f(X)$ над полем F. Тогда множество

$$\left\{1 - f_i^k(\pi(X)) \middle| k = \underset{1 \leqq i \leqq r}{\text{н.о.к.}} (q^{\deg f_i(X)} - 1),\ i = 1, \ldots, r\right\}$$

является максимальной ортогональной системой неразложимых идемпотентов алгебры $F[X]/\mathrm{Id}\, f(X)$.

Доказательство. Покажем, что алгебра $F[X]/\mathrm{Id}\, f(X)$ полупроста. Действительно, пусть существует многочлен $g(X) \in F[X]$, $\deg g(X) < \deg f(X)$, такой, что

$$\exists t \in \mathbf{N}(g^t(X) \equiv 0 \mod f(X)).$$

Это означает, что $g^t(X)$ делится на $f(X)$. Но $g(X)$ не делится на $f(X)$, а это

противоречит сепарабельности многочлена $f(X)$. Легко видеть, что все нильпотентные элементы принадлежат радикалу Джекобсона $\mathrm{Rad}\,(F[X]/\mathrm{Id}\,f(X))$. Покажем теперь, что в алгебре $F[X]/\mathrm{Id}\,f(X)$ каждый простой идеал максимален. Действительно, пусть $a\in F[X]/\mathrm{Id}\,f(X)$, a не нильпотентен. Пусть также $T=\{a, a^2, a^3, \ldots\}$. В силу конечности алгебры $F[X]/\mathrm{Id}\,f(X)$ множество T конечно и содержит идемпотент e. По известным кольцевым построениям ([2]) множество $F[X]/\mathrm{Id}\,f(X)\setminus T$ содержит хотя бы один простой идеал P, являющийся максимальным относительно этого свойства. Тогда алгебра $(F[X]/\mathrm{Id}\,f(X))/P$ есть конечная область целостности, являющаяся полем. Отсюда вытекает, что P — максимальный идеал и $\mathrm{Rad}\,(F[X]/\mathrm{Id}\,f(X))=0$, так как в алгебре $F[X]/\mathrm{Id}\,f(X)$ нет нильпотентных элементов, то есть, наша алгебра полупроста.

В силу полупростоты алгебра $F[X]/\mathrm{Id}\,f(X)$ распадается в прямую сумму минимальных двусторонних идеалов, являющихся полями, что следует из коммутативности $F[X]/\mathrm{Id}\,f(X)$. Обозначим $F[X]/\mathrm{Id}\,f(X)$ и $\pi(X)$ через R и ζ соответственно. Тогда по известной теореме об изоморфизмах ([2]) множество $\{f_i(\zeta)\cdot R|\ \ i=1, \ldots, r\}$, где $\pi(f(X))=f(\zeta)$, совпадает с множеством максимальных идеалов алгебры R. Рассмотрим последовательность

$$f_i(\zeta),\ f_i^2(\zeta),\ f_i^3(\zeta),\ \ldots \tag{6}$$

элементов идеала $f_i(\zeta)\cdot R$ для некоторого фиксированного i. Эта последовательность не содержит нуля, так как для любого натурального числа j имеет место равенство

$$f_i^j(\zeta)R=(f_i(\zeta)R)^j=f_i(\zeta)R$$

в силу идемпотентности любого идеала в полупростой артиновой алгебре.

Последовательность (6) с некоторого момента начинает циклиться из-за конечности числа элементов идеала $f_i(\zeta)\cdot R$. Следовательно, существуют натуральные числа l и t, такие, что

$$f_i^l(\zeta)=f_i^t(\zeta).$$

Без ограничения общности можно предположить, что $l>t$. Тогда

$$f_i^t(\zeta)\cdot f_i^{l-t}(\zeta)=f_i^l(\zeta)=f_i^{2(l-t)}(\zeta)\cdot f_i^l(\zeta)$$

и $f_i^{2(l-t)}(\zeta)-f_i^{l-t}(\zeta)$ аннулирует ненулевой идеал $f_i(\zeta)\cdot R$ классически полупростой алгебры R и одновременно принадлежит ему. Из [2] вытекает, что $L(R)$ есть структура с дополнениями. Отсюда следует, что элемент

$$f_i^{2(l-t)}(\zeta)=f_i^{l-t}(\zeta)$$

принадлежит дополнению идеала $f_i(\zeta)\cdot R$ в структуре $L(R)$. Но пересечение идеала с его дополнением равно нулю, откуда получается равенство

$$f_i^{2(l-t)}(\zeta)-f_i^{l-t}(\zeta)=0$$

и $f_i^{l-t}(\zeta)$-идемпотент, порождающий максимальный идеал в R. Для любого идемпотента e коммутативного кольца R с единицей имеет место разложение Пирса

$$R=eR\oplus(I-e)R$$

кольца R в прямую сумму звоих идеалов. Из

$$R = f_i^{l-t}(\zeta) \cdot R \oplus \left(I - f_i^{l-t}(\zeta)\right) \cdot R$$

вытекает, что элемент $I - f_i^{l-t}(\zeta)$ является идемпотентом, порождающим минимальный идеал в R. Легко показать, что любой неразложимый идемпотент из R можно представить в подобном виде.

Пусть теперь $f_i^k(\zeta)$-идемпотент алгебры R. Так как R разлагается в прямую сумму полей, порядки мультипликативных групп которых суть

$$q^{\deg f_j(X)} - 1, \quad j = 1, \ldots, r,$$

то одним из выражений для k будет

$$k = \underset{1 \leqq j \leqq r}{\text{н.о.к.}} \left(q^{\deg f_j(X)} - 1\right),$$

что и завершает доказательство теоремы.

Искомое утверждение для циклических кодов с основанием F получается заменой в формулировке теоремы 2 многочлена $f(X)$ на $X^n - 1$, где n — натуральное число, взаимно простое с q.

В обозначениях теоремы 2 приведем обратное утверждение.

Теорема 3. *Пусть множество* $\{e_1, \ldots, e_t\}$ *есть максимальная ортогональная система неразложимых идемпотентов алгебры* R. *Тогда система*

$$\{\text{н.о.д.}\left(1 - e_i, f(X)\right) \mid i = 1, \ldots, t\}$$

представляет собой множество всех неприводимых делителей многочлена $f(X)$.

Доказательство. Пусть M есть максимальный идеал алгебры R. Тогда в множестве $\{e_1, \ldots, e_t\}$ содержится элемент e, такой, что

$$M = (1 - e) \cdot R.$$

С другой стороны, существует неприводимый делитель $g(X)$ многочлена $f(X)$, такой, что

$$M = g(\zeta) \cdot R.$$

Элементами идеала $g(\zeta) \cdot R$ являются многочлены $r(\zeta)$, такие, что $r(X)$ делится на $g(X)$ и $\deg r(X) < \deg f(X)$. Отсюда вытекает существование многочлена $r_1(X)$, такого, что

$$r_1(X) = 1 - e.$$

Так как $M = g(\zeta) \cdot R = r_1(\zeta) \cdot R$, то

$$g(X) = \text{н.о.д.}\left(g(X), f(X)\right) = \text{н.о.д.}\left(r_1(X), f(X)\right),$$

что и требовалось доказать.

Теоремы 1 и 3 в совокупности представляют собой алгоритм разложения двучленов на неприводимые множители над полем из двух элементов.

Литература

[1] Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн, Теория кодов, исправляющих ошибки. *М.* «*Связь*», 1979 г.
[2] И. Ламбек, Кольца и модули. М. «*Мир*», 1971 г.
[3] F. J. MacWilliams. Binary codes which are ideals in the group algebra of an Abelian group. *BSTJ*, **49** (1970), 18.
[4] Ч. Кэртис, И. Райнер, Теория представлений конечных групп и ассоциативных алгебр. *М.* «*Наука*», 1969 г.

(Поступило 6. окт. 1983.)