MTA Számítástechnikai és Automatizálási Kutató Intézete, Közlemények 25/1982

ИССЛЕДОВАНИЕ ОДНОГО КЛАССА АБЕЛЕВЫХ КОДОВ С ИСПОЛЬЗОВАНИЕМ ЭВМ

П. Лакатош, А. Пете

В теории кодирования важное место занимает вопрос оптимизации связи между расстоянием кода и длинной кодовых слов, т.к. последняя непосредственно влияет на затраты связанные с передачей и исправимостью кодированной информации.

В настоящей статье обсуждается один класс, так называемых абелевых кодов, и попутно наши решаются некоторые интересные сами по себе проблемы, касающиеся векторного пространства над двухэлементным полем.

Пусть G -абелева группа и K поле. Произвольный I идеал групповой алгебры KG будем называть абелевым кодом. Ясно, что если G -конечна, то KG -векторное пространство конечной размерности над K .

Если обозначим через $w(x)$, $x \in I$ вес кодового слова, т.е. число компонентов его отличных от нуля, то вес кода I может быть выражен как

$$d(I) = \min_{0 \neq x \in I} w(x)$$

Пусть $G=(a_1)\times\ldots\times(a_n)$; $a_i^2=1$; $i=1,2,\ldots,n$; и K

поле характеристики отличной от 2. Тогда абелевый код бинарен, и известно что KG -полупростая алгебра, и т.о. для произвольного идеала I представления:

$$KG = I \oplus \bar{I}$$

$$I = I_1 \oplus \dots \oplus I_s \qquad (\bar{I}\text{-дополнительный идеал идеала } I)$$

$$\bar{I} = I_{s+1} \oplus \dots \oplus I_{2^n}$$

где I_j -минимальный идеал генерируемый идемпотентом e_j $(j = 1,2,\dots,2^n)$ однозначны.

Следующая теорема была доказана в [1]:

<u>Теорема:</u> Пусть $\mathcal{H}^* = \{X_{S+1},\dots,X_{2^n}\}$ множества характеров неизоморфных неприводимых представлений соответствующих $e_{s+1},\dots, e_{2^n}$ идемпотентам $\bar{I}$. Если X характер некоторой подгруппы $H \subseteq G$ порядка $2^к$ не может быть получен ограничением системы $\mathcal{H}^*$ на H то

$$X = \sum_{a \in H} X(a^{-1})a \in I$$

По утверждению теоремы в I существует элемент с весом $2^к$ и т.о. $d(I) \leqslant 2^к$.

В дальнейшем подгуппу H со свойствами условий теоремы будем называть подгруппой ассоцированной с системой характеров $\mathcal{H}^*$.

Обозначим при заданных n и $к$ через

- $t(n,к)$ - наибольшее число для которого существует такое множество характеров с количеством элементов $t(n,к)$ для которого может быть определена ассоцированная подгруппа порядка $2^к$.
- $l(n,к)$ - наибольшее число, такое что для любого множества

группы характеров G с числом элементов $l(n,\kappa)$ существует ассоциированная группа порядка 2^{κ}.

- $p(n,\kappa)$ - наименьшее число, для которого существует множество характеров с числом, элементов $p(n,\kappa)$, такое что у него нет ассоциированной подгруппы порядка 2^{κ}.

Ясно что $p(n,\kappa) = l(n,\kappa)+1$; $t(n,\kappa) \geqslant l(n,\kappa)$. В [1] доказываются также следующие утверждения. Пусть

$q(n,\kappa) = \sum_{i=0}^{\kappa} C_n^i$ (C_n^i -комбинаторный коэффициент), тогда:

(1) $d(n,\kappa) < q(n,\kappa)$ если $1 < \kappa < n-1$

$l(n,\kappa) = q(n,\kappa)$ если $\kappa=1$ или $\kappa=n-1$

(2) $p(n,\kappa) \leqslant q(n,\kappa)$ если $1 < \kappa < n-1$

(3) $p(n,\kappa) \leqslant q(n,\kappa) - \sum_{i=1} \sum_{j=i-1} ([\frac{n+j}{2i}]-1)$, $n \geqslant 4$

([a] - обозначает целую часть числа a)

В настоящей статье приводится алгоритм определения вышеупомянутых границ, описанный на языке PL /1, при помощи которого были выполнены конкретные вычисления.

Проблема представляет интерес и с точки зрения комбинаторики т.к. $p(n,\kappa)$ - мощность наименьшего состоящего из векторов длинной 2^{κ} множества, такого, что для любый $\kappa \times 2^n$ бинарной матрицы могут быть выбраны κ векторов, так что составленная из них матрица размерности $2^n \times \kappa$, умноженная на предидущую матрицу даёт в результате обратимую бинарную матрицу.

1.

Прежде чем перейти к обсуждению алгоритма остановимся на нескольких результатах, которые ведут к сокращению времени вычисления. Будем говорить, что множество характеров $\mathcal{H}^*$ к-реализуемо на G , если ни одна из подгруппы группы G порядка 2^n не ассоциируема с $\mathcal{H}^*$.

Пусть $\mathcal{H} = (X_1)X\ldots X(X_n)$, где характеры X_i ($i = 1,2,\ldots,n$) составляют базис $\mathcal{H}$ группы характеров для G . В [1] указывается что для этого базиса всегда может быть выбран такой $a_1, a_2, \ldots, a_n$ базис G , что

$$(4) \qquad X_i(a_j) = \begin{cases} -1 & \text{если } i = j \\ 1 & \text{если } i \neq j \end{cases}$$

Базис G обладающий этим свойством мы будем называть дуальным по отношению к $X_1, \ldots, X_n$ базису.

<u>Лемма 1:</u> Если $\mathcal{H}^1 \subseteq \mathcal{H}$ (H-группа характеров для G) такое множество характеров, что для любого $e \neq g \in G$ существует такой $X \in \mathcal{H}^1$, что $X(g) = -1$, тогда $\mathcal{H}^1$ порождаёт $\mathcal{H}$.

<u>Доказательство:</u> Пусть для $\mathcal{H}^1$ -с заданным свойством $\{\mathcal{H}^1\} = \mathcal{H}^2 \subset \mathcal{H}$, и пусть $\mathcal{H}^2 = (X^{i_1}) X\ldots X(X^{i_e})$, тогда $e < n$ и так базис может быть дополнен элементами $X^{i_{e+1}}, \ldots X^{i_n}$ до базиса $\mathcal{H}$. Пусть дуальным базисом базиса $X^{i_1}, \ldots, X^{i_n}$ будет $b_1 b_2, \ldots b_n$:
Из-за (4) $X^{i_e}(b_n) = 1$ для всех элементов X из $\mathcal{H}^1$. Получая противоречие $\mathcal{H}^2 = \{\mathcal{H}^1\} = \mathcal{H}$, мы приходим к выводу что $\mathcal{H}^1$ со свойствами теоремы и очевидно любое к-реализуемое множество характеров содержит некоторый базис $\mathcal{H}$.

Будем говорить, что в индексе элемента X присутствует i, если в базисном разбиении приводимом в (4) присутствует X_i и обозначим через $X_{i_1 i_2 \ldots i_j}$ характер $X_{i_1} X_{i_2} \ldots X_{i_j}$ ($1 \leqslant i_k \leqslant n$; $k = 1,2,\ldots,j$) .

Замечание: По лемме 1 любое к-реализуемое $\mathcal{H}^*$-множество характеров содержит один из базисов $\mathcal{H}$-группы характеров G , и т.о. всегда достижимо что $\mathcal{H}^*$ содержит характеры с одним индексом.

Действительно, достаточно переиндексировать дуальный базис в соответствии с (4).

<u>Теорема 1:</u> Пусть $\mathcal{H}^*$ 2-реализуемое подмножество группы $\mathcal{H}$ и $1 \leqslant i \leqslant n$, тогда если $\mathcal{H}^*$ содержит одноиндексные характеры, то в индексах элементов $\mathcal{H}^*$ индекс i появляется по крайней мере n-раз.

<u>Доказательство:</u> Достаточно доказать теорему для случая $i=1$. Рассмотрим $\{a_1, b\}$ $b \neq a_1 c, e$; $c, b \in G$ - подгруппу четвёртого порядка. Характер $X \in \mathcal{H}^*$ тогда принимает значение $(-1, \pm 1)$ на генерирующей паре, если $X = X_1 \cdot X'$ и в индексе X' 1 не присутствует.
Пусть $\mathcal{H}^1 = \{X \mid X \in \mathcal{H}^*, \quad X = X_1 \cdot X'\}$. По предположению теоремы $X_1 \in \mathcal{H}^1$. Пусть
$\bar{\mathcal{H}}^1 = \{X \mid X \in \mathcal{H}^1, \ X \neq X_1\}$, очевидно что элементы $\bar{\mathcal{H}}^1$ характеры подгруппы $G^1 = (a_1) X \ldots X (a_n)$. Так как по предположению $\mathcal{H}^*$ реализуемо для любой подгруппы G четвёртого порядка, в том числе реализуемо и для подгруппы генерируемой парой (a_1, b), для произвольного $b \in G^1$ существует такой $X' \in \bar{\mathcal{H}}^1$, для которого $X'(b) = -1$ поэтому по лемме 1 $\bar{\mathcal{H}}^1$ генерирует подгруппу $\mathcal{H}$ порядка 2^{n-1}. Из-за $\mathcal{H}^1 = \bar{\mathcal{H}}^1 \cup \{X_1\}$ и тем самым теорема доказана.

Результаты приводимые в дальнейшем непосредственно направлены на упрощение определения границ для $p(n,k)$ и $l(n,k)$.

<u>Лемма 2:</u> Для $n=5$ и $\mathcal{H}^*$- 13 элементная 2-реализуемся система, то при помощи трансформации базиса может быть достигнуто что $\mathcal{H}^{1'} = \{X_1, X_{12}, X_{13}, X_{14}, X_{15}\} \subset \mathcal{H}^*$ и $\mathcal{H}^*$ со-

держит по крайней мере один характер с индексом 1 не принадлежащий $\mathcal{H}^{1}$[1].

<u>Доказательство:</u> Если n=5 то по теореме 1 если существует 13-элементная 2-реализуемая система, то есть и такая $\mathcal{H}^*$ для которой в индексах элементов $\mathcal{H}^*$ каждый индекс появляется по крайнер мере 5-раз и эта система $\mathcal{H}^*$ содержит и одноиндексные элементы. Предположим теперь, что в индексах элементов системы $\mathcal{H}^*$ каждый из них повтаряется по крайнер мере семь раз. Это возможно лишь тогда если сумма числа индексов равна по крайнер мере 35. Так как индекс главного характера равен нулю вышеупомянутая ситуация возможна лишь если в $\mathcal{H}^*$ кроме X_1, X_2, X_3, X_4, X_5 одноиндексных характеров:

Число различных индексов элементов	Число характеров в $\mathcal{H}^*$ исключая одноиндексные		
5	1	1	1
4	5	5	4
3	2	1	3
2	-	1	-
0	-	-	-

В каждом из трёх случаев X_{1234} принадлежит $\mathcal{H}^*$ и X_{15} не принадлежит $\mathcal{H}^*$.

Выполняя трансформацию $X_1 \to X_{1234}$, $X_i \to X_i$ $(i = 2,3,4,5)$ на $\mathcal{H}^*$ (и соответственно на G) получим что $\mathcal{H}^*$ не содержит X_{1235} и поэтому сумма числа индексов (учитывая и одноиндексные) элементов не достигает 30-ти.

Таким образом можем предположить что существует такой индекс, который в $\mathcal{H}^*$ повторяется по крайнер мере 5 раз, но не более

6-ти раз. Пусть $\mathcal{H}^1$ -множество состоящее из таких $X \in \mathcal{H}^*$ в индексе которых присутствует 1. В теореме 1 мы уже видели, что для множества состоящего из X' для которого $X_1X' \in \mathcal{H}^1$ реализуема любая $G^1 = (a_2) X \ldots X (a_5)$ группа четвёртого порядка и поэтому по лемме 1 группа характеров G^1 содержит один из её базисов.

Подобным образом переиндексированием элементов G и соответственно элементов $\mathcal{H}$ получим

$$\{X_1, X_{12}, X_{13}, X_{14}, X_{15}\} \subset \mathcal{H}^1$$

Так как 5 характеров содержащих 1-й индекс нами даны, то осталось найти восемь или семь характеров не содержащих 1-ого индекса, в зависимости от того, что число характеров содержащих 1 было 5 или 6. Т.о. в нашей программе нужно проверить лишь $C_{16}^{8}+11 \cdot C_{16}^{7} = 138710$ число комбинаций для нахождения реализуемой системы из 13 элементов.

Подобные, ускоряющие поиск предположения могут быть приняты и для случая $n > 5$, при условии принадлежности множеств вида $\mathcal{H}^{1'}$ реализуемой системе.

<u>Лемма 3:</u> Пусть $N=5$ и $\mathcal{H}^*$ - 24 элементная 3-реализуемая система, тогда при помощи трансформации базиса можем достигнуть что $\mathcal{H}^{1'} = \{X_1, X_{12}, X_{13}, X_{14}, X_{15}\} \subset \mathcal{H}^*$ и $\mathcal{H}$ содержит 6 или 7 элементов с индексом 1 не принадлежающих $\mathcal{H}^{1'}$.

<u>Доказательство:</u> Следуя ходу доказательства леммы 1 и используя $p(4,2) = 10$, получим что в реализуемой системе каждый из индексов повторяется 10-ть раз. По доказанным в [1] $p(5,3) \leqslant 25$. Если $p(5,3) = 24$, то так как достижимо что

все характеры с одним индексом содертатся в реализуемом $\mathcal{H}^*$, то максимальная сумма индексов достижима в случае если $\mathcal{H}^*$ содержит

5	шт.	1	индексных характеров
1	шт.	5	"
5	шт.	4	"
10	шт.	3	"
3	шт.	2	"

Т.о. в общей сложности 24 характера имеют максимально 66 индексов и поэтому существует такой индекс который встречается 13 раз. Если система не содержит характера с 5-ю или 4-мя индексами, то элементы этой системы содержат самое больше 64 индекса, и т.о. существует индекс который встречается 12 раз. Если все характеры с 5-ю и 4-мя индексами находятся в $\mathcal{H}^*$, то может быть предположено, что существует такой 2-х индексный характер, каторый не принадлежит системе, ибо в противном случае максимальная сумма индексов составляла бы 59, что противоречиво. Пусть т.о. $X_{12} \in \mathcal{H}^*$, тогда выполняя трансформацию $X_1 \longrightarrow X_{1345}$, $X_i \longrightarrow X_i$ $(i = 2,3,4,5)$ получим систему в которой нет характера с пятью индексами. На основании вышесказанного, можем предположить, что существует такой индекс, который по крайнер мере 10 раз и по меньшей мере 12 раз повторяется.

Следуя обозначениям и ходу рассуждений леммы 2 получим $\{X_1, X_{12}, X_{13}, X_{14}, X_{15}\} \subset \mathcal{H}^1$, $10 \leqslant |\mathcal{H}^1| \leqslant 12$.

Если каждый индекс повторяется точно 10-раз, то либо 0,0,9,9 ,5,1 соответственно 0,1,7,10,5,1 характеры, соответ-

ственно, с числом индексов 5,4,3,2,1,0 содержатся в $\mathcal{H}^*$.
В первом случае можно предположить что $X_{123} \notin \mathcal{H}^*$, и на подгруппе (a_1,a_2,a_3), а во втором случае X_{123} и $X_{124} \notin \mathcal{H}^*$ и на подгруппе (a_1,a_2,a_3,a_4) не может быть получен ограничением системы $\mathcal{H}^*$ характер (-1,-1,-1) . Лемма доказана.

2.

В программе принимаются следующие обозначения:

- Переменные которые не декларируются явно имеют тип соответствующий неявной декларации.
- N обозначается число элементов базиса группы G , а K число элементов базиса рассматриваемых подгрупп.
- Характеры и элементы группы представляются как строки битов длинной N (расположенных в переменных с декларацией FIXED BINARY), так что последние N-битов определяют значения характеров на элементах базиса группы $a_1,\ldots,a_N$ следующим образом: значение бита равно 1, если значение характера -1 и Ø в противном случае.

В массиве KA состоящем из $KO=2^N$ - элементов первые $KH=2^N - N$ - элементы содержат характеры которые не были нами ещё выбраны, т.е. не принадлежат $\mathcal{H}^{1'}$. Заполнение этого массива выполняет:

```
KA(1)=0;
DO I=2 TO KO;
  KA(I)=I-1;
END;
DO I=1 TO KO;
  C1:IF KA(I)=2**(N-1) THEN GOTO C2;
  DO L=1 TO N-1;
```

```
        IF KA(I)=2**(L-1)+2**(N-1) THEN GOTO C2;
      END;
      GOTO C3;
      C2:DO J1=I+1 TO KO;
           KA(J1-1)=KA(J1);
         END;
      GOTO C1;
    C3:END;
```

b)

Располагая в массиве NC элементы группы отличные от единичного, можем определить значение характеров на этих елементах. Значение принимаемые характерами однозначно определяется чётностью суммы общих единиц характеров и элементов группы. Характер принимает значение 1 на элементе группы если сумма чётна и-1 противном случае.

B - двухмерный (KO-1) x (KO-1) массив и B1, B2 - переменные с общим типом BIT(1).

```
DO I=1 TO KO-1;
  NC(I)=I;
END;
DO I=1 TO KO-1;
  DO L=1 TO KH;
    B1='0'B;
    N1=NC(I)&KA(L);
    DO J1=1 TO N;
      IF MOD(N1,2)=1 THEN B3='1'B;
```

```
                ELSE B3='0'B;
      B1=(B1&¬B3)!(¬B1&B3);
      N1=N1/2;
    END;
  B(I,L)=B1;
  END;
END;
```

c)

Далее, определяясь от элементов К1=1 и К2=2 перечислим в лексиграфическом порядке все пары элементов группы, и для предупреждения совпадения порожденных или подгруппе, рассмотрим лищ те пары у которых компонента наименьшего индекса, т.е. бинарно единица с наибольшим позиционным весом, общая. Легко проверить что таким образом могут быть получены (и лищ единожды) все группы четвёртого порядка числа $C^2_{ко-1} : C^2_3$.

Каждой подгруппе Н будут сопоставлены наибольшее 4 строки имеющей КН столбцов матрицы В2 типа **BIT** (1) следующим образом: если некоторый характер Н не может быть задан ограничениями элементов включенных в систему характеров $\mathcal{H}$ [1] на Н , тогда дополним В2 следующей J-той строкой характеризующей подгруппу и характер исследуемой подгруппы так, что В2(J,L)= = '1'B, если L-тый характер из $\mathcal{H}$ редуцируемый к Н , даст исследуемый характер Н, в противном случае В2(J,L) = '0'В .

```
K1=1;K2=2;J=1;
C4:DO L=N TO 1 BY -1;
    IF K2>=2**L THEN DO; LL=L;GOTO Q1; END;
  END;
GOTO C5;
Q1:IF K1<2**LL THEN GOTO C5;
```

```
    IF K1<2**(N-1) THEN GOTO Q3;
    IF (K1&K2-2**(N-1))¬=0 THEN GOTO Q2;
  DO J1=1 TO KH;
    IF B(K1,J1)¬='0'B!B(K2,J1)¬='0'B THEN B2(J,J1)='0'B;
  END;
  J=J+1;
  Q2:IF (K1&¬K2)¬=0 THEN GOTO C5;
  DO J1=1 TO KH;
    IF B(K1,J1)¬='0'B!B(K2,J1)¬='1'B THEN B2(J,J1)='0'B;
  END;
  J=J+1;
  Q3:IF (K1&¬K2)¬=0 THEN GOTO C5;
  DO J1=1 TO KH;
    IF B(K1,J1)¬='1'B!B(K2,J1)¬='0'B THEN B2(J,J1)='0'B;
  END;
  J=J+1;
  C5:IF K2<KO-1 THEN DO;K2=K2+1;GOTO C4;END;
     IF K1<KO-2 THEN DO;K1=K1+1;K2=K1+1;GOTO C4;END;
```

d)

В целях экономии помяти и ускорочения времени вычислений каждые 31 строки B2 помести в одну строку массива M-типа FIXED BINARY (31):

```
J=J-1;
V8:M1=J/31*31+31;
J2=M1/31;
DO I=1 TO J2;
  DO L=1 TO KH;
    DO L1=1 TO 31;
      M(I,L)=B2((I-1)*31+L1,L)+M(I,L)*2;
    END;
```

END;

END;

Последние, ранее не получившие значений, M1-J элэменты массива M содержат '1'B и т.о. размер M не влияет на дальнейшие вычисления.

e)

Из числа характеров не содержащих 1-го индекса, исходя из 2 и 3 леммы, можно выбрать и добавить определённое каличество к N элементному $\mathcal{H}^{1)}$.

Предположим, что в реализуемой системе содержащей KK-элементов содержится L1-L2 характеров без индекса 1. Нужно проверить, что добавляя к $\mathcal{H}^{1)}$.

KA(1),...,KA(KJ) где KJ=KK-N получим ли полную систему характеров, ограничая вышеупомнутую на произвольные подгруппы порядка 2^K, т.е найдём ли 1 в каждой строке при подходящем выборе KJ столбцов матрицы B2. Проверку произведём т.о, что беря дизъюнкцию выбранных столбцов, посмотрим, что из строк M получим ли строку битов представляющую значение $2^{31}-1$.

Так как выбор множества характеров производился в лексикографическом порядке, множество состоящее из первых L1 характеров изменяется лишь тогда, когда следующие после них элементы пробежали по всем выбираемым и содержащим индекс 1 характерам. Целесообразно, т.о., столбцы M разделять на две части, отдельно проверяя ко/2 столбцов относящихся к характерам без индекса 1.

Элемент MS(I ,1) может быть получен дизъюнкцией элементов лежащих на пересечении выбранных по характерам L1 столбцов с I-той строкой матрицы M. MS(I ,2) получаем подобной дизъюнкцией с участием KJ-L1 столбцов.

```
M5=2**31-1;
DO L1=L1 TO L2 BY -1;
  DO L=1 TO L1;
    IN(L)=L;
  END;
  Z1;DO L=L1+1 TO KJ;
    IN(L)=KO/2+L-L1;
    END;
  Z2;DO I=1 TO J2;
       MS(I,1)=0;
       DO J1=1 TO L1;
         MS(I,1)=MS(I,1)!M(I,IN(J1));
       END;
     END;
  Z3;DO I=1 TO J2;
       IF MS(I,1)=K5 THEN GOTO Z7;
       MS(I,2)=0;
       DO J1=L1+1 TO KJ;
         MS(I,2)=MS(I,2)!M(I,IN(J1));
       END;
       IF (MS(I,1)|MS(I,2))=M5 THEN GOTO Z7;
       DO L=KJ TO L1+1 BY -1;
         IF IN(L)<L+KH-KJ THEN GOTO Z4;
```

```
        END;
        GOTO Z5;
        Z4:IN(L)=IN(L)+1;
        DO L=L+1 TO KJ;
          IN(L)=IN(L-1)+1;
        END;
        GOTO Z3;
        Z5:DO L=L1 TO 1 BY -1;
              IF IN(L)<KO/2+L-L1 THEN GOTO Z6;
           END;

        GOTO Z8;
        Z6:IN(L)=IN(L)+1;
        DO L=L+1 TO L1;
          IN(L)=IN(L-1)+1;
        END;
        GOTO Z1;
    Z7:END;
    PUT SKIP EDIT('REALIZALODO RENDSZERT ALKOT AZ ELORE KIVALASZ
    TOTTAKKAL EGYUTT',(KA(IN(L))DO L=1 TO KJ))(A,SKIP,25F(8));
    GOTO Z9;
  Z8:END;
  PUT SKIP EDIT ('MINDEN',KK,'-SZAMU KARAKTERHALMAZHOZ VAN
  ASSZOCIALT ALCSOPORT')(A,F(8),A);
Z9:END;
```

f)

Подобно с) и для случая К=3 мы сможем перечислить образующие элементы всех различных подгрупп порядка 8, так, что представляем их в виде строк битов, для которых компонент с наибольшим индексом общий. Т.к. в каждой такой подгруппе есть четыре элемента с таким свойством (и очевидно любой из них может быть получен произведением оставшихся 3-х) то две различные тройки чисел не будут генерировать одну и ту же группу.

Матрица В2 определяется аналогиено случаю К=2, здесь нужно иследовать 8 характеров для каждой подгруппы.

```
DO I=1 TO 4;
  K(I)=I;
END;
J=1;
C4:DO L=N TO 1 BY -1;
     IF K(4)>=2**L THEN DO; LL=L;GOTO Q1;END;
   END;
GOTO C5;
Q1:IF K(3)<2**LL!K(2)<2**LL THEN GOTO C5;
   IF ((K(4)&¬K(3)!¬K(4)&K(3))&¬K(2)!¬(K(4)&¬K(3)!
   ¬K(4)&K(3))&K(2))¬=K(1) THEN GOTO C5;
                         .
                         .
                         .
```

```
C5:DO L=4 TO 1 BY -1;
      IF K(L)<KO+L-4 THEN GOTO C6;
   END;
GOTO V8;
C6:K(L)=K(L)+1;
   DO L=L+1 TO 4;
      K(L)=K(L-1)+1;
   END;
GOTO C4;
M6=K(1)&K(2)-2**LL;
M7=K(2)&K(3)-2**LL;
M8=K(1)&K(3)-2**LL;
IF LL=4!(K(1)&K(2)&K(3)-16)¬=0 THEN GOTO V1;
DO J1=1 TO KH;
   IF B(K(1),J1)='0'B&B(K(2),J1)='0'B&B(K(3),J1)='0'B
                                THEN B2(J,J1)='1'B;
END; J=J+1;
```

Результаты прогона программы:

N	K	l(n,K)	время/мин
4	2	9	5
5	2	13	50
5	3	24	450

Программа может применяться и в случае $N > 5$, но это ведёт к большим затратам в машинном времени и для К=2,3 Производя небольшие изменения можно определить и реализуемость системы характеров.

Литература

[1] К. Бузаши-А. Пете-П. Лакатош, О кодовых расстояниях одного класса групповых кодов. Проблемы передачи информаций (под редакции)

[2] С.Д. Берман, Полупростые циклические коды. Кибернетика N° 2-3(1967) 21-30.

[3] С.Д. Берман-А.Б. Юданина, Коды с обобшённым мажаритарным декодированием и свёрточные коды. Продлемы передачи информаций т.6. (1970) 6-19.

Ö s s z e f o g l a l ó

Ábel kódok egy osztályának vizsgálata számológép segitségével
Lakatos P., Pető A.

A másodrendű ciklikus csoportok véges direkt szorzatából képzett csoportalgebra ideáljai az Ábel féle kódok fontos osztályát alkotják. Ebben a cikkben leirunk egy PL/1 nyelvű algoritmust, amellyel a csoport bizonyos tulajdonságú karakterrendszereit lehet meghatározni. Ezek alkalmazhatók adott súlyú kódszavak meghatározásához.

S u m m a r y

Investigation of a class of Abelian codes using
computer algorithm

The ideals of the group algebra, which is built on the finite direct product of second order cyclic groups, is an important class of Abelian codes. In this paper we describe a computer algorithm on PL/1 that determines character systems with certain properties of the group. One can use it in determining code words with given weight.