УДК 621.391.15

ЗАМЕТКА О ПОСТРОЕНИИ δ-КОДОВ

Саруханян А. Г.

Приводятся конструкции двух новых классов циклических T-матриц, что приводит к построению матриц Адамара новых порядков.

§ 1. Введение

Один из основных методов построения матриц Адамара, задача существования которых для всех порядков m вида $m=0 (\mathrm{mod}\, 4)$ до сих пор не решена, основан на построении массивов Бомера – Холла, которые, в свою очередь, синтезируются с помощью массивов Геталса – Зейделя и T-матриц [1–3].

В работе [2] задача построения циклических T-матриц сводится к построению четырехсимвольных δ-кодов длины n.

Определение 1 [4]. $(a_i)_{i=1}^n$, $(b_i)_{i=1}^n$, $(c_i)_{i=1}^n$, $(d_i)_{i=1}^n$, $a_i, b_i, c_i, d_i \in \{-1, +1\}$ называются дополнительными последовательностями длины n, если выполняется условие $\sum_{i=j}^{n-j} (a_i a_{i+j} + b_i b_{i+j} + c_i c_{i+j} + d_i d_{i+j}) = 0$, $j = 1, 2, \ldots, n-1$.

Заметим, что пары дополнительных последовательностей называются дополнительными последовательностями Голея [2, 4].

В работах [5, 6] с помощью дополнительных последовательностей Голея и Турина [4] были построены δ-коды длины $3t$, $7t$, $13t$, где $t \in L_1 = \{3, 5, \ldots, 59, 2^a 10^b 26^c + 1\}$, a, b, c – целые неотрицательные числа.

В настоящей заметке приводятся конструкции двух новых классов циклических T-матриц, что приводит к построению матриц Адамара новых порядков.

§ 2. Циклические T-матрицы порядка $2 \cdot 11(2n-1)$, $2(2n-1)$ $(2k+1)$

Из дополнительных последовательностей длины n образуем последовательность векторов $V = \{V_i = (a_i, b_i, c_i, d_i)\}$. Очевидно, что

$$\sum_{i=1}^{n-j} V_i V_{i+j} = 0, \quad j = 1, 2, \ldots, n-1.$$

Если последовательность V образована с помощью $t (t \leqslant 4)$ взаимно ортогональных векторов, то V будем называть $\delta(t, n)$-последовательностью [7, 8]. Если V образована произвольными четырехмерными векторами, то V назовем δ-последовательностью.

Теорема 1. *Пусть существует δ-последовательность длины n. Тогда существует $\delta(4, 2n)$-последовательность.*

Доказательство. Пусть $V = \{(a_i, b_i, c_i, d_i)\}_{i=1}^n$ – δ-последовательность. Докажем, что $P = \{(a_i, a_i, c_i, c_i)_{i=1}^n, (b_i, -b_i, d_i, -d_i)_{i=1}^n\}$ является $\delta(4, 2n)$-последовательностью.

Можно показать, что непериодическая автокорреляционная функция последовательности $Q = \{(x_i)_{i=1}^m, (y_i)_{i=1}^n\}$, $m \leqslant n$ имеет вид

$$(1)\qquad N_Q(j)=\begin{cases}\sum\limits_{i=1}^{m-j}x_ix_{i+j}+\sum\limits_{i=1}^{j}y_ix_{m+i-j}+\sum\limits_{i=1}^{n-j}y_iy_{i+j}, & 1\leqslant j\leqslant m-1,\\ \sum\limits_{i=1}^{m}x_iy_{i+j-m}+\sum\limits_{i=1}^{n-j}y_iy_{i+j}, & m\leqslant j\leqslant n-1,\\ \sum\limits_{i=1}^{m+n-j}x_iy_{i+j-m}, & n\leqslant j\leqslant m+n-1.\end{cases}$$

Теперь, применяя формулы (1) для последовательности P, легко доказать, что $N_P(j)=0$. Очевидно, что последовательность P образована четырьмя взаимно ортогональными векторами. Теорема доказана.

Утверждение 1. *Пусть существуют последовательности Турина длины n. Тогда существует* $\delta(4, 2\cdot 11(2n-1))$*-последовательность.*

Доказательство Пусть $A=(a_i)_{i=1}^{n}$, $B=(b_i)_{i=1}^{n}$, $C=(c_i)_{i=1}^{n-1}$, $D=(d_i)_{i=1}^{n-1}$ — последовательности Турина, $x=(1, 1, 1, 1)$, $y=(1, 1, -1, -1)$ $z=(-1, 1, -1, 1)$, $w=(-1, 1, 1, -1)$.

Рассмотрим последовательность векторов x, y, z, w:

$$X=\{(xa_i)_{i=1}^{n},\ (xc_i)_{i=1}^{n-1},\ (-xa_i)_{i=1}^{n},\ (-xc_i)_{i=1}^{n-1},\ (-xb_{n-i+1})_{i=1}^{n},$$

$$(-xc_i)_{i=1}^{n-1},\ (-xa_i)_{i=1}^{n},\ (xc_i)_{i=1}^{n-1},\ (ya_i)_{i=1}^{n},\ (xd_i)_{i=1}^{n-1},$$

$$(ya_i)_{i=1}^{n},\ (xd_i)_{i=1}^{n-1},\ (ya_i)_{i=1}^{n},\ (xd_i)_{i=1}^{n-1},\ (yb_i)_{i=1}^{n},\ (yd_i)_{i=1}^{n-1},$$

$$(-yb_i)_{i=1}^{n},\ (yc_{n-i})_{i=1}^{n-1},\ (-yb_i)_{i=1}^{n},\ (yd_i)_{i=1}^{n-1},\ (yb_i)_{i=1}^{n},$$

$$(-yd_i)_{i=1}^{n-1},\ (za_i)_{i=1}^{n},\ (zc_i)_{i=1}^{n-1},\ (-za_i)_{i=1}^{n},\ (zd_{n-i})_{i=1}^{n-1},\ (-za_i)_{i=1}^{n},$$

$$(zc_i)_{i=1}^{n-1},\ (za_i)_{i=1}^{n},\ (-zc_i)_{i=1}^{n-1},\ (-zb_i)_{i=1}^{n},\ (-wc_i)_{i=1}^{n-1},$$

$$(-zb_i)_{i=1}^{n},\ (-wc_i)_{i=1}^{n-1},\ (-zb_i)_{i=1}^{n},\ (-wc_i)_{i=1}^{n-1},\ (wb_i)_{i=1}^{n},$$

$$(wd_i)_{i=1}^{n-1},\ (-wb_i)_{i=1}^{n},\ (-wd_i)_{i=1}^{n-1},\ (wa_{n-i+1})_{i=1}^{n},$$

$$(-wd_i)_{i=1}^{n-1},\ (-wb_i)_{i=1}^{n},\ (wd_i)_{i=1}^{n-1}\}.$$

Легко доказать, что X является $\delta(4, 2\cdot 11(2n-1))$-последовательностью.

Утверждение 2. *Пусть существуют последовательности Турина и Голея соответственно длины n и k. Тогда существует* $\delta(4, 2(2n-1)\times(2k+1))$*-последовательность.*

Доказательство. Пусть $A=(a_i)_{i=1}^{n}$, $B=(b_i)_{i=1}^{n}$, $C=(c_i)_{i=1}^{n-1}$, $D=(d_i)_{i=1}^{n-1}$ и $F=(f_i)_{i=1}^{k}$, $G=(g_i)_{i=1}^{k}$ — последовательности Турина и Голея, $x=(1, 1, 0, 0)$, $y=(1, -1, 0, 0)$, $z=(0, 0, 1, 1)$, $w=(0, 0, 1, -1)$. Синтезируем последовательность

$$X=\{\{\{a_i(xf_{k-j+1}+zg_{k-j+1})\}_{i=1}^{n},\ \{c_i(xg_j+zf_{k-j+1})\}_{i=1}^{n-1}\}_{j=1}^{k},$$

$$\{xa_i-zb_i\}_{i=1}^{n},\ \{xd_i-zc_i\}_{i=1}^{n-1},\ \{\{b_i(xg_j+zf_{k-j+1})\}_{i=1}^{n},$$

$$\{d_i(-xf_j+zg_{k-j+1})\}_{i=1}^{n-1}\}_{j=1}^{k},\ \{\{a_i(yf_{k-j+1}+wg_{k-j+1})\}_{i=1}^{n},$$

$$\{c_i(yg_j-wf_j)\}_{i=1}^{n-1}\}_{j=1}^{k},\ \{-ya_i+wb_i\}_{i=1}^{n},\ \{yd_i+wc_i\}_{i=1}^{n-1},$$

$$\{\{-b_i(yg_j+wf_{k-j+1})\}_{i=1}^{n},\ \{d_i(yf_j-wg_{k-j+1})\}_{i=1}^{n-1}\}_{j=1}^{k}\}.$$

Можно показать, что X является $\delta(4,\ 2(2n-1)(2k+1))$-последовательностью.

Следствие 1. *Существуют четыре циклические T-матрицы порядка* $2\cdot11(2n-1)$ *и* $2(2n-1)(2k+1)$, *где* $k=2^a10^b26^c$, $n\in L_2=\{2,\ 3,\ 4,\ \ldots,\ 8,\ 13,\ 15,\ 2^a10^e26^f+1\}$, $a,\ b,\ \ldots,\ f$ *— целые неотрицательные числа.*

Доказательство следствия 1 опирается на утверждения 1, 2, а также на работу [7], где, исходя из $\delta(4,\ n)$-последовательности, приведена конструкция циклических T-матриц.

Ценность следствия 1 заключается в возможности построения циклических T-матриц порядка $2m_1$ и $2m_2$, хотя существование циклических T-матриц порядка $m_1=11(2n-1)$ и $m_2=(2n-1)(2k+1)$ неизвестно.

Следствие 2. *Существуют матрицы Адамара порядка* $8\cdot11(2n-1)m$ *и* $8\cdot(2n-1)(2k+1)m$, *где* m *— порядок существующих матриц типа Вильямсона* [1, 9]. *В частности* $m\in\{3,\ 5,\ 7,\ \ldots,\ 31,\ 33,\ 43,\ 3^a(p+1)/2\}$, *где* a *— целое положительное число,* $p\equiv1\pmod4$ *— степень простого числа.*

Доказательство получается из теорем Купера — Валлиса и Бомера — Холла [1].

ЛИТЕРАТУРА

1. *Wallis W. D., Street A. P., Wallis J. S.* Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices. Lecture Notes in Mathematics. Berlin — New York: Springer-Verlag, 1972. V. 292.
2. *Turyn R. J.* Hadamard Matrices, Baumert-Hall Units, Four-Symbol Sequences, Puls Compression, and Surface Wave Encodings // J. Comb. Theory. 1974. V. 16(A). № 3. P. 313–333.
3. *Саруханян А. Г.* О массивах типа Геталса — Зейделя // Уч. записки Ереван. гос. ун-та. 1979. № 1. С. 12–19.
4. *Robinson P. J., Wallis J. S.* A note on using sequences to construct orthogonal designs // Colloquia Math. Soc. Jánis Bolyai. Combinatorics. Budapest: Akad. Kiado. 1976. V. 18. P. 911–932.
5. *Yang C. H.* Hadamard Matrices and δ-Codes of Length $3n$ // Proc. Amer. Math. Soc. 1982. V. 85. № 3. P. 480–482.
6. *Yang C. H.* Lagrange Identity for Polinomials and δ-Codes of Lengths 7t and 13t // Proc. Amer. Math. Soc. 1983. V. 88. № 4. P. 746–750.
7. *Агаян С. С., Саруханян А. Г.* Обобщенные δ-коды и построение матриц Адамара // Пробл. передачи информ. 1980. Т. 16. № 3. С. 50–59.
8. *Саруханян А. Г.* О построении обобщенных последовательностей с нулевыми автокорреляционными функциями и матриц Адамара // Математические вопросы кибернетики и вычислительной техники. Ереван: Изд-во АН АрмССР, 1984. Т. 12. С. 105–129.
9. *Агаян С. С., Саруханян А. Г.* Рекуррентные формулы построения матриц типа Вильямсона // Мат. заметки, 1981. Т. 30. № 4. С. 603–617.

Поступила в редакцию
2.IV.1985

УДК 621.391.15

ЗАМЕЧАНИЕ О РЕШЕНИИ КВАДРАТНЫХ УРАВНЕНИЙ НАД ПОЛЯМИ ГАЛУА

Квашенников В. В., Яковлев В. Г.

Предлагается формула для решения квадратных уравнений над полями Галуа $GF(2^m)$.

При декодировании алгебраических кодов возникает задача определения корней многочлена над полем Галуа. Значительный интерес представляет решение квадратных уравнений. В [1] получены формулы для