УДК 669.78.27

В.Е.Гантмахер, В.А.Едемский

О ДВОИЧНЫХ И ТРОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЯХ С КВАЗИОДНОУРОВНЕВОЙ ПЕРИОДИЧЕСКОЙ АВТОКОРРЕЛЯЦИОННОЙ ФУНКЦИЕЙ ДЛЯ $p \equiv 1 \bmod 4$

The necessary and sufficient conditions of existence of binary and ternary successions with quasi-single-level by a periodic autocorrelation function for the period $p \equiv 1 \bmod 4$ are presented.

Введение

В [1,2] разработана теория спектров разности классов вычетов в простом поле Галуа. Эта теория была эффективно использована для синтеза новых регулярных правил кодирования полностью уравновешенных троичных псевдослучайных последовательностей с периодом $p \equiv 1 \bmod 4$ [3,4]. Правила были получены обобщением результатов расчета на ЭВМ. В данной статье находятся необходимые и достаточные условия для применения вышеупомянутых правил. Исследования проводятся с использованием спектров разности классов вычетов (СРКВ) и циклотомических чисел.

Определения и обозначения

Пусть $p = 1 + 4R$ — простое число и $p > 5$. Обозначим через θ первообразный корень простого поля Галуа $GF(p)$. Тогда все ненулевые элементы $GF(p)$ можно упорядочить по степеням θ и разбить на четыре непересекающихся класса

$$H_k = \{\theta^{k+4t}, k = \overline{0,3}; t = \overline{0, R-1}\}.$$

Рассмотрим правила построения дискретно-кодированных последовательностей (ДКП), при которых каждому из классов ставится в соответствие какое-либо число из множества $\{0,\pm 1\}$, и изучим корреляционные свойства получаемых последовательностей. В [1] было показано, что для этих целей удобно использовать математический аппарат спектров разностей классов вычетов. Напомним основные определения и соотношения.

СРКВ H_k и H_l будет матрица строка из четырех чисел $S(k,l) = (s_0, s_1, s_2, s_3)$, где s_i — число элементов множества $\{\theta^{l+4t} - \theta^k; t = \overline{0, R-1}\}$, принадлежащих H_i.

В [1] показано, что если двоичные последовательности (ДП) сформированы по правилу

$$U_x(i) = \begin{cases} 1, \text{если } i \in H_k, \\ 0, \text{если } i \notin H_k, \end{cases} \quad U_y(i) = \begin{cases} 1, \text{если } i \in H_l, \\ 0, \text{если } i \notin H_l, \end{cases} \tag{1}$$

то для периодической автокорреляционной функции (ПАКФ) ДКП X справедливо соотношение

$$\lambda_x(\tau) \Leftrightarrow S(k,k), \tag{2}$$

а для периодической взаимнокорреляционной функции X и Y

$$r_{x,y}(\tau) \Leftrightarrow S(k,l). \tag{3}$$

Аналогично, если $Z = X \pm Y$, то

$$\lambda_z(\tau) = S(k,k) + S(l,l) \pm S(k,l) \pm S(l,k). \tag{4}$$

Следовательно, изучение ПАКФ и ПВКВ в этом случае сводится к исследованию СРКВ.

В [1] исследованы свойства СРКВ и, в частности, было показано, что

$$S(k,l) = D^k S(0, <l-k>_4), \tag{5}$$

где $<l-k>_4$ — наименьший положительный вычет по модулю 4, а D — оператор циклического сдвига Хаффмена. Таким образом, как ПАКФ, так и ПВКФ ДКП, сформированных по правилу кодирования (1), определяются $S(0,j)=(s_{0j},s_{1j},s_{2j},s_{3j})$. В этом случае s_{ij} является числом решений сравнения $\theta^{j+4t}-1\equiv\theta^{i+4s} \bmod p$ для $t,s=\overline{0,R-1}$, т.е. совпадает с циклотомическим числом (j,i). В [5] приведены явные формулы циклотомических чисел для этого случая.

Для $p\equiv 1 \bmod 4$ справедливо $P=x^2+4y^2$, $x\equiv\langle 1\rangle_4$. Запишем следующие соотношения, связывающие СРКВ и циклотомические числа.

Для $R\equiv 0 \bmod 2$

$$\begin{aligned} S(0,0)&=((0,0),(0,1),(0,2),(0,3)),\\ S(0,1)&=((0,0),(0,3),(1,2),(1,2)),\\ S(0,2)&=((0,2),(1,2),(0,2),(1,2)), \end{aligned} \tag{6}$$

где

$$\begin{aligned} 16(0,0)&=p-11-6x,\\ 16(0,1)&=p-3+2x+8y,\\ 16(0,2)&=p-3+2x,\\ 16(0,3)&=p-3+2x-8y,\\ 16(1,2)&=p+1-2x. \end{aligned} \tag{7}$$

Для $R\equiv 1 \bmod 2$

$$\begin{aligned} S(0,0)&=((0,0),(1,0),(0,0),(1,0)),\\ S(0,1)&=((0,1),(1,0),(1,0),(0,3)),\\ S(0,2)&=((0,2),(0,3),(0,0),(0,1)), \end{aligned} \tag{8}$$

где

$$\begin{aligned} 16(0,0)&=p-7+2x,\\ 16(0,1)&=p+1+2x-8y,\\ 16(0,2)&=p+1-6x,\\ 16(0,3)&=p+1+2x+8y,\\ 16(1,2)&=p-3-2x. \end{aligned}$$

Сразу же заметим, что $R=y^2+2t+4t^2$, т.е. четность y совпадает с четностью R.

Двоичные последовательности с одноуровневыми (квазиодноуровневыми) ПАКФ и ПВКФ

Пусть ДП X сформирована по правилу кодирования (1). Для иллюстрации метода докажем заново известный результат.

Лемма 1. ДП X имеет одноуровневую ПАКФ тогда и только тогда, когда $p=4(2u+1)^2+1$. В этом случае $\lambda(\tau)=u(u+1)$.

Доказательство. Согласно (2) и (5) можно считать, что $k=0$ и $\lambda(\tau)\Leftrightarrow S(0,0)$. Таким образом, необходимым и достаточным условием одноуровненности $\lambda(\tau)$ будет равенство компонент $S(0,0)$. Согласно (6) и (7) для четного R это невозможно. Для нечетного R должно выполняться равенство $(0,0)=(1,0)$. Последнее означает, что $x=1$ и $y=2u+1$. Тогда $\lambda=(p-5)/4=u(u+1)$. Это известное разностное множество биквадратичных вычетов.

Лемма 2. ДП X имеет двухуровневую ПАКФ тогда и только тогда, когда $p=4(2u+1)^2+(1+4t)^2$ для $t\neq 0$. В этом случае $\lambda(\tau)\in\{u(u+1)+t(t+1),\ u(u+1)+t^2\}$.

Доказательство. Если R нечетно, то $y = 2u + 1,$ и согласно (8) $\lambda(\tau)$ всегда имеет два уровня. Если же R четно, то согласно (6) и (7) $\lambda(\tau)$ имеет минимум три уровня.

Следствие 1. Если $p = 4(2u+1)^2 + 3^2$ или $p = 4(2u+1)^2 + 5^2,$ то уровни ПАКФ отличаются на 1.

Рассмотрим теперь пару ДП X и $Y,$ сформированных по правилу кодирования (1). В общем случае рельеф ПВКФ может иметь четыре уровня. Изучим наиболее интересные случаи.

Теорема 1. Пара ДП X и Y имеет одноуровневую ПВКФ тогда и только тогда, когда $p = 16u^2 + 1$ и $|k - l| = 2.$ В этом случае $\lambda = u^2.$

Доказательство. Согласно (3) и (5) можно считать, не нарушая общности, что $k = 0$ и $l = 1$ или $l = 2.$ Следовательно, как и в лемме 1, все сводится к анализу $S(0,1)$ или $S(0,2).$

СРКВ $S(0,1)$ не может иметь одинаковых компонент, так как $(0,1) \neq (0,3).$

Исследуем $S(0,2).$ Если R четное, из (6) и (7) следует $(0,2) = (1,2),$ т.е. $x = 1$ и $y = 2u.$ Тогда $\lambda(\tau) = (p-1)/16 = u^2.$ Для нечетного R равенство невозможно. Теорема доказана.

Теорема 2. Пара ДП X и $Y,$ сформированных по правилу кодирования (1), имеет двухуровневую ПВКФ тогда и только тогда, когда:

1) $p = 16u^2 + (1+4t)^2,\ t \neq 0;\ |k-l| = 2.$ В этом случае $\lambda(\tau) \in \{u^2 + t^2, u^2 + t(t+1)\};$

2) $p = 16u^2 + (1 \pm 4u)^2 = 32u^2 \pm 8u + 1;\ |k-l| = 1.$ В этом случае $\lambda(\tau) \in \{u^2, u(u \pm 2)\}.$

Доказательство. Как и в предыдущей теореме, необходимо провести анализ СРКВ $S(0,1)$ и $S(0,2).$

При $R \equiv 0 \bmod 2$ согласно (6) в $S(0,2)$ всегда две компоненты, если $x \neq 1.$ Если же R нечетное, то в $S(0,2)$ всегда $(0,1) \neq (0,3).$ Приравнивая к этим уровням остальные, получаем противоречие.

Исследуем теперь СРКВ $S(0,1).$ Если R четное, то из (6) следует либо $(0,1) = (1,2),$ либо $(0,3) = (1,2),$ т.е. $p - 1 - 2x = p - 3 + 2x \pm 8y$ или $4 - 4x = \pm 8y,$ тогда $t = \pm u$ и $p = 16u^2 + (1 \pm 4u)^2.$ Уровни $\lambda(\tau)$ вычисляются согласно (7). Если же R нечетное, то либо $(1,0) = (0,1),$ либо $(1,0) = (0,3),$ т.е. $p - 3 - 2x = p + 1 + 2x \pm 8y$ или $-16t = 16u + 8,$ что невозможно.

Следствие 2. Если $p = 16u^2 + 3$ или $p = 16u^2 + 5,$ то рельеф $\lambda(\tau) = \{u^2 + 1, u^2 + 2\}$ для $|k - l| = 2.$

Аналогично, если взять $Z = X + Y,$ то для $|k - l| = 2$ можно получить согласно (4) хорошо известный результат о рельефе ПАКФ, так как в этом случае Z соответствует множеству квадратичных вычетов.

Троичные квазиортогональные последовательности

Рассмотрим теперь троичные последовательности (ТП), сформированные по следующему правилу кодирования:

$$U(i) = \begin{cases} 1, \text{ если } i \in H_k, \\ -1, \text{ если } i \in H_l, \\ 0 \text{ в остальных случаях.} \end{cases}$$

Согласно (4) и (5) в данном случае можно считать, не нарушая общности, что $|k - l| = 1,2.$

Теорема 3. Если $|k - l| = 1,$ то $r(\tau)$ имеет два уровня тогда и только тогда, когда $p = 4(2u+1)^2 + (1+4t)^2.$ В этом случае $\lambda(\tau) \in \{u, -u-1\}.$

Доказательство. Можно считать, что $k = 0$ и $l = 1.$ Тогда согласно (4) $r(\tau) \Leftrightarrow S(0,0) + DS(0,0) - S(0,1) - S(1,0).$

Если R четно, т.е. $y = 2u,$ то $r(\tau)$ имеет уровни

$$u_1 = (0,0) + (0,3) - 2(0,1) = \frac{1 - x - 3y}{2},\ \ u_2 = (0,1) + (0,0) - 2(0,3) = \frac{1 - x + 3y}{2},$$

$$u_3 = (0,2) + (0,1) - 2(1,2) = \frac{1 - x + y}{2},\ \ u_4 = (0,3) + (0,2) - 2(1,2) = \frac{1 - x + y}{2}.$$

Двухуровневая ПАКФ в этом случае невозможна.

Если же R нечетно, т.е. $y = 2u + 1,$ то

$$u_1 = (0,0) - (0,1) = \frac{y-1}{2} = u,\ \ u_2 = (0,0) - (0,3) = -\frac{y+1}{2} = -u - 1,\ \ u_3 = u_1,\ \ u_4 = u_2.$$

Последнее и доказывает теорему.

Теорема 4. Если $|k - l| = 2$ и $p = 4y^2 + (1 + 4t)^2,$ то $r(\tau)$ всегда имеет два уровня.

Доказательство. Как и в теореме 3, достаточно проанализировать компоненты СРКВ: $(u_1, u_2, u_3, u_4) = S(0,0) + D^2 S(0,0) - S(0,2) - S(2,0).$

Если R четно, то

$$u_1 = (0,0) - (0,2) = -\frac{x+1}{2} = -2t - 1,\ \ u_2 = (0,1) - (0,3) - 2(1,2) = \frac{x-1}{2} = 2t,\ \ u_3 = u_1,\ \ u_4 = u_2.$$

Если же R нечетно, то

$$u_1 = (0,0) - (0,2) = \frac{x-1}{2} = 2t,\ \ u_2 = 2(1,0) - (0,3) - (0,1) = -\frac{x+1}{2} = -2t - 1,\ \ u_3 = u_1,\ \ u_4 = u_2.$$

В обоих случаях получаем требуемые уровни.

Заключение

Данные результаты дают необходимые и достаточные условия для ряда регулярных правил формирования двоичных последовательностей с квазиодноуровневыми ПАКФ и ПВКФ, а также определяют регулярные правила построения полностью уравновешенных квазиортогональных троичных последовательностей с двухуровневой ПАКФ.

1. Гантмахер В.Е. // Тр. 2-й Междунар. науч.-техн. конф. «Актуальные проблемы фундаментальных наук». М., 1994. С.В40-В43.
2. Гантмахер В.Е. // Вестник НовГУ. Сер.: Естеств. и техн. науки. 1995. №1. С.81-87.
3. Гантмахер В.Е. // Вестник НовГУ. Сер.: Естеств. и техн. науки. 1998. №10. С.77-81.
4. Гантмахер В.Е. // Вестник НовГУ. Сер.: Естеств. и техн. науки. 1999. №13. С.76-80.
5. Холл М. Комбинаторика. М.: Мир, 1970. 423 с.