9. Ю р а с о в Н. И. Спектр ферромагнитного резонанса в металлах с коллинеарным магнитным упорядочением // Вестник МГТУ им. Н.Э. Баумана. Сер. “Естественные науки”. – 2000. – № 5. – С. 64–72.
10. Y u r a s o v N. I., Y u r a s o v a L. A., S h e n k a r e n k o A. Y. The influence of spin-orbital magnetic subsystems and binary alloy composition on the FMR in an optical range // The Physics of Metals and Metallography. – 2001. – V. 92. – P. S143–S146.

Статья поступила в редакцию 21.03.2007

Николай Ильич Юрасов родился в 1943 г., окончил в 1966 г. МВТУ им. Н.Э. Баумана и в 1974 г. Московский инженерно-физический институт. Канд. физ.-мат. наук, доцент кафедры “Физика” МГТУ им. Н.Э. Баумана. Автор более 70 научных работ в области физики конденсированного состояния: магнитных и кинетических явлений, интерференционных эффектов, квантовой гравитации и устойчивости тяжелых ядер.

N.I. Yurasov (b. 1943) graduated from the Bauman Moscow Higher Technical School in 1966 and Moscow Institute for Engineering and Physics in 1974. Ph.D. (Phys.-Math.), assoc. professor of “Physics” department of the Bauman Moscow State Technical University. Author of over 70 publications in the field of condense matter physics (magnetic and kinetic phenomena), interference effects, quantum gravitation and heavy nuclei stability.

МАТЕМАТИКА

УДК 621.391.15

В. Е. Г а н т м а х е р, В. А. Е д е м с к и й

КВАЗИОДНОУРОВНЕВЫЕ РАЗНОСТНЫЕ МНОЖЕСТВА

Определены параметры новых разностных множеств, сформированных на основе классов степенных вычетов по простому модулю $p = dR + 1$, $d = 3, 4, 6, 8$, *сбалансированных на несколько близких уровней.*

Известно большое число разностных множеств (РМ) $D(N, K, \lambda)$, где N — модуль, K — порядок множества, сбалансированных на один уровень λ, например: РМ квадратичных вычетов, РМ биквадратичных вычетов и так далее, которые широко применяются в различных областях, в частности, для построения сигналов с хорошими корреляционными свойствами, в теории кодирования, криптографии [1]. Одним из крупных недостатков известных РМ является редкая сетка значений N, для которых существуют РМ. В то же время для целого ряда прикладных задач, например в системах с шумоподобными сигналами, при достаточно больших N и K допустимо, чтобы РМ $D(N, K, \lambda_1, \ldots, \lambda_n)$ было сбалансировано на несколько уровней, при условии, что разница между наибольшим и наименьшим уровнями $\Delta S = \lambda_{\max} - \lambda_{\min}$ не превышает заданного порогового значения $\Delta S_{\max}$ или относительная разность $\gamma = \dfrac{\Delta S}{K}$ не превышает заданного значения $\gamma_{\max}$. Далее такие РМ будем называть квазиодноуровневыми.

В работе [2] изложена теория спектров разностей классов вычетов (СРКВ), которая была эффективно использована для определения параметров новых квазиодноуровневых РМ, сформированных на основе классов степенных вычетов по простому модулю. Там же были найдены несколько правил построения квазиодноуровневых РМ в случае, когда $N = p$ — простое число вида $p = dR + 1$ для $d = 4,\ 6,\ 8$. Одним из недостатков данного подхода является сложность анализа таблиц СРКВ из-за большого числа переменных.

В работах [3, 4] с использованием циклотомических чисел были определены параметры квазиодноуровневых РМ (сбалансированных на два уровня, отличающихся на единицу), которые сформированы на основе классов степенных вычетов для $p = dR + 1$, $d = 4,\ 6,\ 8$.

В работе [5] была предложена методика анализа и синтеза дискретно-кодированных последовательностей, заключающаяся в комплексном использовании теории СРКВ и циклотомических чисел.

Цель настоящей работы заключается в разработке методики расчета параметров квазиодноуровневых РМ (сформированных на основе классов степенных вычетов по простому модулю), которая базируется на комплексном использовании теории СРКВ и циклотомических чисел, а также в определении правил построения новых квазиодноуровневых РМ, в частности в обобщении результатов [2–4] при $p = dR + 1$, $d = 3,\ 4,\ 6,\ 8$.

1. РМ и СРКВ. Обозначим через H_k — класс степенных вычетов с номером k по простому модулю $p{=}dR{+}1$, т.е. $H_k = \left\{\theta^{k+td},\ t{=}\overline{0, R{-}1}\right\}$, где $k = \overline{0, d-1}$, θ — первообразный корень по модулю p; СРКВ классов H_k и H_l обозначим через $S(k, l)$ [2]. Рассмотрим множество $G = \bigcup\limits_{i \in I} H_i$, где I — подмножество множества индексов $\{0, 1, \ldots, d-1\}$, $|I|$ — число элементов в множестве I. При анализе РМ из $C_d^{|I|}$ возможных вариантов наборов индексов для подмножества I будем рассматривать [3] только циклически независимые с порядком $|I| \le \dfrac{d}{2}$.

Согласно работе [2], множество G является РМ $D(p, K, \lambda_1, \ldots, \lambda_n)$, $K = R|I|$, сбалансированным на n уровней, тогда и только тогда, когда его СРКВ имеет n различных гармоник. При поиске квазиодноуровневых РМ необходимо оценить разницу между наибольшей и наименьшей гармониками. Гармоники СРКВ $S(0, k)$ совпадают с циклотомическими числами (k, j), $j = \overline{0, d-1}$ порядка d [5]. Для циклотомических чисел третьего, четвертого, шестого и восьмого порядков существуют формулы, позволяющие выразить их через значения переменных, которые входят в разложение p на сумму квадратов целых чисел [6]. Таким образом, таблица СРКВ будет определяться двумя–четырьмя переменными, что существенно упрощает ее анализ.

Исходя из сказанного выше, получаем методику определения параметров квазиодноуровневых РМ: 1) определение циклически независимых вариантов наборов индексов для выбранного значения d; 2) вычисление гармоник СРКВ, соответствующих множеству G, с использованием формул для циклотомических чисел; 3) определение уровней РМ, вычисление разницы между наибольшим и наименьшим уровнями, сравнение с заданными пороговыми значениями $\Delta S_{\max}$, $\gamma_{\max}$.

Проиллюстрируем применение данной методики для $p = dR + 1$, $d = 3,\ 4,\ 6,\ 8$.

2. Расчет параметров квазиодноуровневых РМ для $d = 3$. Выполним последовательно указанные три шага методики расчета параметров квазиодноуровневых РМ для $d = 3$.

1. При $d = 3$ достаточно рассмотреть единственный вариант, когда $I = \{0\}$.

2. Если $I = \{0\}$, то для анализа РМ необходимо вычислить СРКВ $S(0, 0)$. Используя явные формулы для циклотомических чисел третьего порядка [6], получаем

$$18S(0,0) = (2p - 16 + 2L,\ 2p - 4 - L - 9M,\ 2p - 4 - L + 9M),$$

где $4p = L^2 + 27M^2$, $L = 1 + 3f$, $L,\ M,\ f$ — целые числа.

3. В общем случае (при $d = 3$) РМ $D(p, K, \lambda_1, \lambda_2, \lambda_3)$ сбалансировано на три уровня:

$$\lambda_1 = \frac{2p - 16 + 2L}{18}, \quad \lambda_{2,3} = \frac{2p - 4 - L \pm 9M}{18} \tag{1}$$

Так как $M \neq 0$, то $\lambda_2 \neq \lambda_3$, т.е. РМ не может быть сбалансировано на один уровень и $\Delta S \geq |M|$.

Лемма 2.1. Наибольшая разность между уровнями РМ $\Delta S = |M|$ в том и только в том случае, если $|L - 4| \leq 3|M|$.

Доказательство. Согласно (1), $|\lambda_3 - \lambda_2| = |M|$, тогда наибольшая разность между уровнями РМ ΔS будет равна $|M|$ в том и только в том случае, если $\lambda_2 \le \lambda_1 \le \lambda_3$ ($\lambda_3 \le \lambda_1 \le \lambda_2$), т.е. $2p - 4 - L - 9|M| \le 2p - 16 + 2L \le 2p - 4 - L + 9|M|$. После преобразования получаем неравенство $-3|M| \le L - 4 \le 3|M|$, равносильное неравенству $|L - 4| \le 3|M|$.

Таким образом, лемма 2.1 определяет достаточные условия существования квазиодноуровневых РМ с $\Delta S \le \Delta S_{\max}$. Если $\Delta S_{\max}$ — заданное пороговое значение, то РМ будет квазиодноуровневым при значениях p, удовлетворяющих условиям $|L - 4| \le 3|M|$, $|M| \le \Delta S_{\max}$.

Лемма 2.1 определяет значения p, при которых ΔS достигает наименьшего значения при фиксированном M. Найдем значения p, при которых число уровней РМ минимально.

Теорема 2.1. Если $d = 3$, то множество степенных вычетов H_k является РМ, сбалансированным на два уровня, в том и только в том случае, если $p = 36u^2 - 24u + 7$, где u — целое число; при этом $\Delta S = |2u - 1|$, $\gamma = \dfrac{|2u - 1|}{12u^2 - 8u + 2}$. В остальных случаях РМ сбалансировано на три уровня.

Доказательство. РМ будет сбалансировано на два уровня, если $\lambda_1 = \lambda_2$ или $\lambda_1 = \lambda_3$. Таким образом, должно выполняться равенство $2p - 16 + 2L = 2p - 4 - L \pm 9M$ или $\pm 3M = L - 4$. Тогда $p = L^2 - 6L + 12$, а так как p — простое число, то L — нечетно. Следовательно, $L = 1 + 6u$ и $p = 36u^2 - 24u + 7$ ($4p = (1+6u)^2 + 27(2u-1)^2$). Подставляя $L = 1 + 6u$ и $M = 2u - 1$ в (1) получаем, что $\lambda_1 = \lambda_3 = 4u^2 - 2u$, $\lambda_2 = 4u^2 - 4u + 1$.

В качестве примера в табл. 1 приведены параметры РМ, удовлетворяющих условиям теоремы 2.1.

Таблица 1

Параметры РМ, сбалансированных на два уровня, для $p = 3R + 1$

u	0	1	−1	2	−2	4	5	−6	−8	9	−10	11
p	7	19	67	103	199	487	787	1447	2503	2707	3847	4099
R	2	6	22	34	66	162	262	482	834	902	1282	1366
$\lambda_{\min}$	0	1	6	9	20	49	81	159	272	289	420	441
ΔS	1	1	3	3	5	7	9	10	17	17	21	21
γ	0,5	0,16	0,13	0,08	0,075	0,04	0,03	0,02	0,02	0,018	0,016	0,015

Как следует из таблицы, значения γ быстро убывают с возрастанием $|u|$, в частности справедливо неравенство $\gamma \le \dfrac{1}{5|u|}$ для $u \ne 0$.

Теорема 2.1 определяет достаточные условия существования двухуровневых РМ при $d = 3$. Если $\Delta S_{\max}$ — заданное пороговое значение, то достаточные условия для того, чтобы РМ было квазиодноуровневым, следующие: $p = 36u^2 - 24u + 7$, $|2u - 1| \le \Delta S_{\max}$. При использовании в качестве порогового значения относительной оценки $\gamma_{\max}$ имеем $p = 36u^2 - 24u + 7$, $\dfrac{|2u-1|}{12u^2 - 8u + 2} \le \gamma_{\max}$.

3. Расчет параметров квазиодноуровневых РМ для $d = 4$. Воспользуемся рассмотренной выше методикой расчета параметров квазиодноуровневых РМ для $d = 4$.

1. Выделим циклически независимые варианты подмножеств индексов I для $d = 4$: $I = \{0\}, \{0, 1\}, \{0, 2\}$. Если $I = \{0, 2\}$, то G — хорошо изученное [1, 6] множество квадратичных вычетов. Таким образом, достаточно проанализировать только два первых варианта $\{0\}$ и $\{0,1\}$.

2. Вычислим гармоники СРКВ $S(0, 0), S(0, 1)$ с использованием формул для циклотомических чисел четвертого порядка [6]: для четного R

$$16S(0, 0) = (p - 11 - 6x, p - 3 + 2x + 8y,\ p - 3 + 2x,\ p - 3 + 2x - 8y);$$

$$16S(0, 1) = (p - 3 + 2x + 8y,\ p - 3 + 2x - 8y,\ p + 1 - 2x,\ p + 1 - 2x)$$

и для нечетного R

$$16S(0, 0) = (p - 7 + 2x, p - 3 - 2x,\ p - 7 + 2x,\ p - 3 - 2x),$$

$$16S(0, 1) = (p + 1 + 2x - 8y,\ p - 3 - 2x,\ p - 3 - 2x,\ p + 1 + 2x + 8y),$$

где $p = x^2 + 4y^2$, $x \equiv 1(\mathrm{mod} 4)$, x, y — целые числа. Отметим, что четность y совпадает с четностью R.

3. Из анализа гармоник СРКВ следует, что РМ для $I = \{0\}$ будет иметь два уровня для нечетного R:

$$\lambda_1 = \frac{p - 7 + 2x}{16}, \quad \lambda_2 = \frac{p - 3 - 2x}{16}, \tag{2}$$

и четыре уровня для четного R:

$$\begin{gathered} \lambda_1 = \frac{p - 11 - 6x}{16}, \quad \lambda_2 = \frac{p - 3 + 2x + 8y}{16}, \\ \lambda_3 = \frac{p - 3 + 2x}{16}, \quad \lambda_4 = \frac{p - 3 + 2x - 8y}{16}. \end{gathered} \tag{3}$$

Если же $I = \{0, 1\}$, то СРКВ будет определяться следующим выражением (см. работу [2]): $S(0, 0) + DS(0, 0) + S(0, 1) + S(1, 0)$; здесь D — оператор циклического сдвига Хаффмена.

Для нечетного R РМ имеет следующие уровни:

$$\lambda_{1,2} = \frac{p - 3 \pm 2y}{4}, \tag{4}$$

а для четного R

$$\lambda_{1,2} = \frac{p-5\pm 2y}{4}, \quad \lambda_{3,4} = \frac{p-1\pm 2y}{4}. \tag{5}$$

Теорема 3.1. Если $d = 4$, $I = \{0\}$, то:

1) $\Delta S = \dfrac{|x-1|}{4}$ для нечетного R;

2) $\Delta S = \begin{cases} |y| & \text{при} \quad |x| \le |y|-1, \\ \dfrac{|x|+|y|-1}{2} & \text{при} \quad |x| > |y|-1 \end{cases}$ для четного R.

Доказательство. Если R нечетно, то РМ имеет два уровня для $x \neq 1$ и $\Delta S = \dfrac{|x-1|}{4}$ согласно (2). Утверждение теоремы для четного R следует из (3) и равносильности неравенств $\lambda_2 \le \lambda_1 \le \lambda_4$ ($\lambda_4 \le \lambda_1 \le \lambda_2$) и $|x| \le |y| - 1$.

Так как ΔS при нечетном R зависит только от x, то, задавая различное пороговое значение $\Delta S_{\max} \ge 0$ и фиксируя значение x, можно найти семейства квазиодноуровневых РМ со сколь угодно большим числом элементов.

Следствие 3.1.1. Если $x = 1$, R — нечетное, $I = \{0\}$, то $\lambda_1 = \lambda_2$ и множество биквадратичных вычетов будет РМ, сбалансированным на один уровень ($\Delta S = 0$).

Это известный результат [1].

Следствие 3.1.2. При $x = -3$ или $x = 5$ и нечетном R по теореме 3.1 получаем известный результат для $d = 4$ из работы [3] ($\Delta S = 1$).

Теорема 3.1 обобщает утверждения 6.3.2–6.3.6 из работы [2], в которых существуют ограничения на переменные x, y и $|x-y|$.

Теорема 3.2. Если $d = 4$ и R — нечетное, то множество степенных вычетов $H_k \cup H_{k+1}$ является РМ, сбалансированным на два уровня с $\Delta S = |y|$, а при четном R — на четыре уровня с $\Delta S = |y| + 1$.

Доказательство. Если R нечетно, то теорема следует из (4), так как $y \neq 0$, а если R четно, то из равенства $p - 5 + 2y = p - 1 - 2y$ ($p - 5 - 2y = p - 1 + 2y$) получаем $y = \pm 1$, что невозможно для четного R, т.е. в этом случае все уровни различны. Согласно (5) имеем $\Delta S = |y| + 1$.

Следствие 3.2.1. Если $p = x^2 + 4(2u+1)^2$, то множество степенных вычетов $H_k \cup H_{k+1}$ является РМ, сбалансированным на два уровня, $D\left(p,\ \dfrac{p-1}{2},\ \dfrac{p-5-4u}{4},\ \dfrac{p-1+4u}{4}\right)$.

Следствие 3.2.1 обобщает частный случай ($u = 0$), рассмотренный в работе [4].

Следствие 3.2.2. Если $p = x^2 + 16u^2$, то множество степенных вычетов $H_k \cup H_{k+1}$ является РМ, сбалансированным на четыре уровня, $D\left(p,\ \frac{p-1}{2},\ \frac{p-5}{4} \pm u,\ \frac{p-1}{4} \pm u\right)$.

Следствие 3.2.3. Если $p = x^2 + 16$, то уровни РМ отличаются на единицу: $\lambda_1 = \frac{p-9}{4}$, $\lambda_2 = \frac{p-5}{4}$, $\lambda_3 = \frac{p-1}{4}$, $\lambda_4 = \frac{p+3}{4}$, т.е. $\Delta S = 3$.

Теорема 3.2 позволяет построить большое число квазиодноуровневых РМ с заданным $\Delta S_{\max}$. Например, если $\Delta S_{\max} = 3$, то множество степенных вычетов $H_k \cup H_{k+1}$ будет РМ с $\Delta S \le \Delta S_{\max}$ для следующих значений p: 5, 13, 17, 29, 37, 41, 53, 61, 97, 137, 157, 173, 229, 241, 293, 397, 457, 641, 661, 733, 857, 877, 977, 997, выбранных среди простых чисел, меньших 1000.

Доказанные теоремы определяют достаточные условия существования квазиодноуровневых РМ для $p = 4R + 1$ и расширяют возможности известных способов построения квазиодноуровневых РМ [2–4].

4. Расчет параметров квазиодноуровневых РМ для $d = 6$.

1. Если $d = 6$, то порядок $|I| = 1,\ 2,\ 3$. Определим циклически независимые множества индексов: $I = \{\{0\}, \{0, 1\}, \{0, 2\}, \{0, 3\}, \{0, 1, 2\}, \{0, 1, 3\}, \{0, 1, 4\}, \{0, 2, 4\}\}$. Первые четыре варианта для I были исследованы в работах [5, 8]. Вариант $\{0,1,3\}$ был исследован Холлом [6], а вариант $\{0,1,4\}$ сводится к $\{0,1,3\}$ заменой θ на θ^{-1}. При $I = \{0, 2, 4\}$ получаем множеством квадратичных вычетов [1]. Таким образом, для $d = 6$ представляет новизну лишь один вариант — $I = \{0, 1, 2\}$. Обозначим через $J = (0, 1, 2), (1, 2, 3), (2, 3, 4), (3, 4, 5), (0, 4, 5), (0, 1, 5)\}$ множество троек индексов, порожденное $\{0,1,2\}$ путем циклического сдвига по номерам классов.

2. Если $G = H_0 \cup H_1 \cup H_2$, то, согласно работе [2], его СРКВ определяется выражением

$$S(0,0) + DS(0,0) + D^2S(0,0) + S(0,1) + D^3S(0,1) + \\ + S(0,2) + D^3S(0,2) + D(S(0,1) + D^3S(0,1)).$$

Воспользовавшись формулами для циклотомических чисел шестого порядка [6, 7], рассчитаем гармоники СРКВ. Результаты расчета для нечетного R приведены в табл. 2, а для четного R в табл. 3, в которых $p = A^2 + 3B^2$, $A \equiv 1 (\bmod 3)$, A, B — целые числа. Знак B выбирается в зависимости от первообразного корня θ, а именно, если m — наименьший положительный вычет $ind_\theta 2$ по модулю 3, то $B \equiv -m (\bmod 3)$.

3. Уровни РМ определяются по табл. 2 и 3. Вычислим ΔS.

Таблица 2

Гармоники СРКВ для $p = 6R + 1$ при нечетном R

	$m = 0$	$m = 1$	$m = 2$
$36\lambda_1$	$9p - 27 + 24B$	$9p - 27$	$9p - 27 - 12A + 12B$
$36\lambda_2$	$9p - 27$	$9p - 27 + 12A + 12B$	$9p - 27 + 12A - 12B$
$36\lambda_3$	$9p - 27 - 24B$	$9p - 27 - 12A - 12B$	$9p - 27$

Таблица 3

Гармоники СРКВ для $p = 6R + 1$ при четном R

	$m = 0$	$m = 1$	$m = 2$
$36\lambda_1$	$9p - 45 + 24B$	$9p - 45$	$9p - 45 - 12A + 12B$
$36\lambda_2$	$9p - 45$	$9p - 45 + 12A + 12B$	$9p - 45 + 12A - 12B$
$36\lambda_3$	$9p - 45 - 24B$	$9p - 45 - 12A - 12B$	$9p - 45$
$36\lambda_4$	$9p - 9 + 24B$	$9p - 9$	$9p - 9 - 12A + 12B$
$36\lambda_5$	$9p - 9$	$9p - 9 + 12A + 12B$	$9p - 9 + 12A - 12B$
$36\lambda_6$	$9p - 9 - 24B$	$9p - 9 - 12A - 12B$	$9p - 9$

Теорема 4.1. Если $\{k, l, n\} \in J$ и R — нечетное, то для РМ G максимальная разница между уровнями

$$\Delta S = \begin{cases} \dfrac{4\,|B|}{3} & \text{при } B \equiv 0 (\mathrm{mod} 3), \\ \dfrac{2\,|A \pm B|}{3} & \text{при } B \not\equiv 0 (\mathrm{mod} 3). \end{cases}$$

Доказательство. Если $m = 0$, то согласно первому столбцу табл. 2 $\lambda_3 \leq \lambda_2 \leq \lambda_1$ при $B > 0$ и $\lambda_1 \leq \lambda_2 \leq \lambda_3$ при $B < 0$. Таким образом, $\Delta S = |\lambda_3 - \lambda_1|$ или $\Delta S = \dfrac{4\,|B|}{3}$. Если же $m = 1$, то $\lambda_3 \leq \lambda_1 \leq \lambda_2$ при $A + B > 0$ и $\lambda_2 \leq \lambda_1 \leq \lambda_3$ при $A + B < 0$, тогда $\Delta S = |\lambda_3 - \lambda_2| = \dfrac{2\,|A + B|}{3}$ согласно второму столбцу табл. 2. Аналогично при $m = 2$ величина $\Delta S = \dfrac{2\,|A - B|}{3}$.

Следствие 4.1. Если $p = 4\,(3u - 1)^2 + 3\,(1 + 6u)^2$ или $p = 4\,(2 + 3u)^2 + 3\,(1 + 6u)^2$, то множество степенных вычетов $H_k \cup H_l \cup H_n$ при $\{k, l, n\} \in J$ является РМ, сбалансированным на три уровня, $D\left(p,\ \dfrac{p-1}{2},\ \dfrac{p-3}{4} - 1,\ \dfrac{p-3}{4},\ \dfrac{p-3}{4} + 1\right)$ с $\Delta S = 2$.

Доказательство. Для значений p, определяемых следствием 4.1, $\dfrac{A \pm B}{3} = \pm 1$.

В качестве примера в табл. 4 приведены параметры РМ для значений p, определяемых следствием 4.1.

Таблица 4

Параметры РМ $D\left(p, \dfrac{p-1}{2}, \dfrac{p-3}{4}-1, \dfrac{p-3}{4}, \dfrac{p-3}{4}+1\right)$ **для** $p=6R+1$ **с** $\Delta S=2$ **и** $\gamma=\dfrac{4}{p-1}$

u	-1	1	2	-5	-6	-8	8	0	-1	-3	3	-4	4	-8	8
p	139	163	607	3547	5119	9127	9319	19	79	1063	1567	1987	2659	8563	9907
$3R$	69	81	303	1773	2559	4563	4659	9	39	531	783	993	1329	4281	4953
$\lambda_{\min}$	33	39	150	885	1278	2280	2328	3	18	264	390	495	663	2139	2475

Исследуем теперь случай четного R. (В работе [3] ошибочно полагают, что здесь возможны два уровня.)

Теорема 4.2. Если $\{k,l,n\}\in J$ и R — четное, то для РМ G максимальная разница между уровнями

$$\Delta S=\begin{cases}\dfrac{4\,|B|}{3}+1 & \text{при } B\equiv 0(\mathrm{mod}3),\\ \dfrac{2\,|A\pm B|}{3}+1 & \text{при } B\not\equiv 0(\mathrm{mod}3).\end{cases}$$

Доказательство теоремы 4.2 следует из анализа табл. 3.

Следствие 4.2. Если $p=144u^2-60u+13$ или $p=144u^2+156u+49$, то множество степенных вычетов $H_k\cup H_l\cup H_n$ при $\{k,l,n\}\in J$ является РМ, сбалансированным на четыре уровня, $D\left(p, \dfrac{p-1}{2}, \dfrac{p-9}{4}, \dfrac{p-9}{4}+1, \dfrac{p-9}{4}+2, \dfrac{p-9}{4}+3\right)$ с $\Delta S=3$.

В качестве примера в табл. 5 приведены параметры РМ, сбалансированных на четыре уровня, для значений p, определяемых следствием 4.2.

Таблица 5

Параметры РМ $D\left(p, \dfrac{p-1}{2}, \dfrac{p-9}{4}, \dfrac{p-9}{4}+1, \dfrac{p-9}{4}+2, \dfrac{p-9}{4}+3\right)$ **для** $p=6R+1$ **с** $\Delta S=3$ **и** $\gamma=\dfrac{6}{p-1}$

u	1	-2	3	-4	5	-6	-1	-2	1	-3	2
p	97	709	1129	2557	3313	5557	37	313	349	877	937
$3R$	48	354	564	1278	1656	2778	18	156	174	438	468
$\lambda_{\min}$	22	175	280	637	826	1387	7	76	85	217	232

Доказанные теоремы 4.1 и 4.2 определяют достаточные условия существования квазиодноуровневых РМ с малым значением ΔS и достаточно плотной сеткой значений p.

5. Расчет параметров РМ, сбалансированных на несколько уровней, для $d = 8$.

1. Если $d = 8$, то достаточно рассмотреть следующие циклически независимые варианты наборов индексов:

$$I = \{0\}, \{0, 1\}, \ldots, \{0, 5\}, \{0, 1, 2\}, \{0, 1, 3\}, \{0, 1, 4\}, \{0, 1, 5\}, \{0, 1, 6\}, \{0, 2, 4\}, \{0, 1, 2, 3\}, \{0, 1, 2, 4\}, \{0, 1, 2, 5\}, \{0, 1, 3, 4\}, \{0, 1, 3, 5\}, \{0, 1, 3, 6\}.$$

Как показали проведенные исследования, квазиодноуровневые РМ с наименьшим значением ΔS и наиболее плотной сеткой значений p получаются для двух четверок индексов: $\{0,1,2,5\}$, $\{0,1,3,4\}$; в остальных вариантах существует значение $p_{\max}$, зависящее от $\Delta S_{\max}$, такое, что для всех p, бóльших $p_{\max}$, значение ΔS больше заданного порогового значения $\Delta S_{\max}$, за исключением известного случая, когда РМ определяется множеством восьмеричных вычетов [1].

2. Если $G = H_k \cup H_l \cup H_n \cup H_q$, то ему соответствует СРКВ:

$$S(k, k) + S(l, l) + S(n, n) + S(q, q) + S(k, l) + S(l, k) + S(k, n) + S(n, k) + S(k, q) + S(q, k) + S(l, n) + S(n, l) + S(l, q) + S(q, l) + S(n, q) + S(q, n).$$

Воспользовавшись формулами для циклотомических чисел восьмого порядка [6] и свойствами СРКВ [2], получим, что для нечетного R гармоники СРКВ при $(k, l, n, q) = (0, 1, 2, 5)$ и $(k, l, n, q) = (0, 1, 3, 4)$ определяются согласно табл. 6.

Таблица 6

Гармоники СРКВ для $p = 8R + 1$ при нечетном R

	$y \equiv 0 \pmod 4$	$y \not\equiv 0 \pmod 4$
(0,1,2,5)		
$8\lambda_1$	$2p - 6 + x - 2y - a$	$2p - 6 + x + 2y - a$
$8\lambda_2$	$2p - 10 - 2x + 2a$	$2p - 10$
$8\lambda_3$	$2p - 6 + x + 2y - a$	$2p - 6 + x - 2y - a$
$8\lambda_4$	$2p - 2$	$2p - 2 - 2x + 2a$
(0,1,3,4)		
$8\lambda_1$	$2p - 10$	$2p - 10 - 2x + 2a$
$8\lambda_2$	$2p - 6 + x - 2y - a$	$2p - 6 + x + 2y - a$
$8\lambda_3$	$2p - 2 - 2x + 2a$	$2p - 2$
$8\lambda_4$	$2p - 6 + x + 2y - a$	$2p - 6 + x - 2y - a$

3. Обозначим через H, F наборы четверок индексов, порожденные циклическими сдвигами (0,1,2,5) и (0,1,3,4) по номерам классов:

$H = \{(0, 1, 2, 5);\ (0, 1, 4, 7);\ (0, 3, 4, 5);\ (0, 3, 6, 7)\}$,
$F = \{(0, 1, 3, 4);\ (0, 1, 5, 6);\ (0, 2, 3, 7);\ (0, 4, 5, 7)\}$.

Анализ табл. 6 показывает, что если четверка индексов (k, l, n, q) принадлежит H или F, то ΔS совпадает с линейной комбинацией $x - a$ и y.

Теорема 5.1. При $p = 8R + 1$ и нечетном значении R для РМ степенных вычетов $H_k \cup H_l \cup H_n \cup H_q$, при (k, l, n, q), принадлежащим множествам H или F, справедливы следующие утверждения.

1. Если $p = x^2 + 64 = (x + 4)^2 + 2b^2$ и $(k, l, n, q) \in H$, то $\Delta S = 2$, $\lambda_{\min} = \dfrac{p - 9}{4}$.

2. Если $p = x^2 + 16 = (x - 8)^2 + 2b^2$ и $(k, l, n, q) \in H$ или $p = x^2 + 64 = (x + 4)^2 + 2b^2$, $p = x^2 + 64 = (x + 8)^2 + 2b^2$ и $(k, l, n, q) \in F$, то $\Delta S = 3$, $\lambda_{\min} = \dfrac{p - 9}{4}$.

3. Если $p = x^2 + 256 = (x + 4)^2 + 2b^2$ и $(k, l, n, q) \in H$ или $p = x^2 + 16 = (x - 8)^2 + 2b^2$ и $(k, l, n, q) \in F$, то $\Delta S = 4$, $\lambda_{\min} = \dfrac{p - 13}{4}$.

Доказательство теоремы 5.1 следует из анализа табл. 6.

В качестве примера в табл. 7 приведены параметры РМ, сбалансированного на два уровня, для значений p, определяемых первой формулой теоремы 5.1.

Таблица 7

Параметры РМ $D\left(p, \dfrac{p-1}{2}, \dfrac{p-9}{4}, \dfrac{p-1}{4}\right)$ **для** $p = 8R + 1$ **с** $\Delta S = 2$ **и** $\gamma = \dfrac{4}{p-1}$

u	-1	0	-2	2	3	4
p	73	89	1913	5689	26633	80153
$4R$	36	44	956	2844	13316	40076
$\lambda_{\min}$	16	20	476	1420	6656	20039

Теорема 5.1 определяет достаточные условия существования квазиодноуровневых РМ для $p = 8R + 1$ с малым значением $\Delta S_{\max}$.

Выводы. Предложена методика определения параметров квазиодноуровневых РМ, основанная на комплексном использовании теории СРКВ и циклотомических чисел. Определены параметры новых квазиодноуровневых РМ, сформированных на основе классов степенных вычетов по простому модулю $p = dR + 1$, $d = 3, 4, 6, 8$. Обобщены результаты работ [2–5].

Работа выполнена в рамках гранта РФФИ № 07-01-97615-р_офи 2007 г.

СПИСОК ЛИТЕРАТУРЫ

1. С в е р д л и к М. Б. Оптимальные дискретные сигналы. – М.: 1975. – 200 с.
2. Г а н т м а х е р В. Е., Б ы с т р о в Н. Е., Ч е б о т а р е в Д. В. Шумоподобные сигналы. Анализ, синтез, обработка. – СПб.: Наука и техника, 2005. – 400 с.
3. A r a s u K. T., D i n g C., H e l l e s e n h T., K u m a r P. V., M a r t i n s e n H. M. Almost difference sets and their sequences with optimal autocorrelation // IEEE Trans. Inform. Theory. – 2001. – Vol. 47, № 7. – P. 2934–2943.
4. D i n g C., H e l l e s e t h T., L a m K. Y. Several classes of binary sequences with three-level autocorrelation // IEEE Trans. Inform. Theory. – 1999. – Vol. 45. – P. 2601–2606.
5. Г а н т м а х е р В. Е., Е д е м с к и й В. А. Результаты синтеза пар двоичных последовательностей простого периода с одноуровневой и двухуровневой взаимной корреляцией // Изв. вузов. Радиоэлектроника. – 2006. – Вып. 5. – С. 26–33.
6. Х о л л М. Комбинаторика. – М.: Мир, 1970. – 423 с.
7. W h i t e m a n A. L. The cyclotomic numbers of order twelve // Acta arithmetica. – 1960. – № 6. – P. 53–76.
8. Г а н т м а х е р В. Е., Е д е м с к и й В. А. О ПАКФ двоичных и троичных последовательностей с периодом $p \equiv 1 \bmod 6$ // Вестник НовГУ. Сер. “Технические науки”. – 2005. – № 30. – С. 52–57.

Статья поступила в редакцию 29.03.2007

Владимир Ефимович Гантмахер родился в 1941 г., окончил Ленинградский электротехнический институт. Д-р техн. наук, профессор Новгородского государственного университета. Автор более 200 научных работ в области шумоподобных сигналов и псевдослучайных последовательностей.

V.Ye. Gantmakher (b. 1941) graduated from the Leningrad Institute for Electrical Engineering. D. Sc. (Eng.), professor of the Novgorod State University. Author of more than 200 publications in the field of noise-like signals and pseudo-random series.

Владимир Анатольевич Едемский родился в 1958 г., окончил Ленинградский государственный университет Канд. физ.-мат. наук, доцент Новгородского государственного университета. Автор свыше 30 научных работ в области шумоподобных сигналов, псевдослучайных последовательностей и алгебраической теории чисел.

V.A. Yedemskiy (b. 1958) graduated from the Leningrad State University. Ph. D. (Phys.-Math.), assoc. professor of the Novgorod State University. Author of more than 200 publications in the field of noise-like signals, pseudo-random series and algebraic theory of numbers.