ИНФОРМАТИКА

УДК 621.396

МЕТОД БЫСТРОГО ОПРЕДЕЛЕНИЯ ФАЗЫ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ЯКОБИ

канд. техн. наук С.В. МАЛЬЦЕВ, Р.Н. БАСАЛАЙ
(Полоцкий государственный университет)

Разработан метод быстрого определения фазы шумоподобных сигналов на основе последовательностей Якоби, предложена аппаратная реализация алгоритма синхронизации, оценена помехоустойчивость алгоритма.

Сигналы на основе последовательностей Якоби обладают хорошими корреляционными свойствами и высокой эквивалентной линейной сложностью [1]. Эти особенности позволяют использовать их в качестве синхросигналов для радиотехнических систем связи с кодовым разделением каналов. При практической реализации радиотехнических систем связи, использующих кодовое разделение каналов, качество работы системы в целом определяется временем вхождения в синхронизм.

Вхождение в синхронизм (устранение неопределенности по фазе) является сложной задачей, особенно для больших длин принимаемого шумоподобного сигнала. Для ее решения могут использоваться традиционные методы прямого последовательного поиска фазы [2, 3]. Однако такие методы обработки имеют большую вычислительную сложность и, как следствие, значительные временные затраты. В ряде случаев хорошей альтернативой методу прямого поиска фазы сигнала может быть метод, использующий структурные особенности конкретной последовательности, в данном случае – Якоби.

Последовательность Якоби длиной L формируется следующим образом:

$$b_{hq}(i)=\begin{cases} b_{pq}(i)=\left\{\left(\dfrac{i}{p}\right)\cdot\left(\dfrac{i}{q}\right), \text{ если } НОД\left[i, L\right]=1; \\ 1, \text{ если } i \equiv \bmod q; \qquad 0 \le i < L \\ -1 \ - \text{ в других случаях,} \end{cases} \tag{1}$$

где p, q – простые числа, $p < q$; *НОД* – наибольший общий делитель; $L = pq$.

Последовательности Якоби в своей основе являются композицией двух компонент, образованных из q и p последовательностей квадратичных вычетов, длиной p и q соответственно:

$$\begin{cases} QR_p(i)=\left(\dfrac{i}{p}\right), \ 0 \le i < p; \\ QR_q(i)=\left(\dfrac{i}{q}\right), \ 0 \le i < q. \end{cases} \tag{2}$$

Методы обработки, использующие структурные свойства сложных последовательностей, для извлечения информации о фазе каждой составляющей предложены в [4]. На основе такого подхода становится возможным вычислить фазу последовательности Якоби и существенно снизить вычислительную сложность алгоритма, по сравнению с методами прямого поиска.

В ходе исследований обнаружено, что информацию о фазе каждой из компонент QR_p и QR_q последовательности Якоби можно получить, вычисляя корреляционную сумму вида:

$$S_x(i)=\sum_{j=0}^{pq-1} b_{pq}(i+j)\cdot QR_x(j), \ 0 \le i < p\cdot q, \tag{3}$$

где x – p или q соответственно.

Выражение (3) описывает вычисление корреляции анализируемой последовательности Якоби со сдвигом i и последовательности, образованной компонентами QR_p (или QR_q), которые повторяются q (или p) раз соответственно.

Пример 1. Вычислим корреляционную сумму $S_q(i)$ для последовательности Якоби длиной 15 ($p = 3$, $q = 5$), со сдвигом $i = 0$:

$I = 0$	j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	
	$b_{15}(i + j)$	1	1	1	–1	1	1	–1	–1	1	–1	1	–1	–1	–1	–1	
	$QR_5(j)$	1	1	–1	–1	1	1	1	–1	–1	1	1	1	–1	–1	1	
	$b_{15}(j)\times QR_5(j)$	1	1	–1	1	1	1	–1	1	–1	–1	1	–1	1	1	–1	$S_5(0) = 9 + (–6) = 3$

То есть для вычисления (3) требуется сложить поразрядные произведения отсчетов входной последовательности Якоби и последовательности квадратичных вычетов.

Установлено, что корреляционные суммы (3) $S_p(i)$ и $S_q(i)$, $0 \le i < pq$, обладают свойством:

$$\begin{aligned} S_p(i) &= S_p(i \bmod p) = \begin{cases} -p, \text{ если } QR_p(i) = 1; \\ q, \text{ если } QR_p(i) = -1; \end{cases} \\ S_q(i) &= S_q(i \bmod q) = \begin{cases} -q, \text{ если } QR_q(i) = -1; \\ p, \text{ если } QR_q(i) = 1. \end{cases} \end{aligned} \tag{4}$$

То есть вычисление корреляционных сумм (3) дает информацию о распределении вычетов/невычетов в каждой из компонент QR_p и QR_q, формирующих данную последовательность Якоби, по которому можно установить их фазы, а затем и фазу последовательности Якоби.

Пример 2. Значения корреляционных сумм $S_p(i)$ и $S_q(i)$ для различных сдвигов i последовательности Якоби длиной 15 ($p = 3$, $q = 5$):

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$QR_3(i)$	1	1	–1	1	1	–1	1	1	–1	1	1	–1	1	1	–1
$S_3(i)$	–3	–3	5	–3	–3	5	–3	–3	5	–3	–3	5	–3	–3	5
$QR_5(i)$	1	1	–1	–1	1	1	1	–1	–1	1	1	1	–1	–1	1
$S_5(i)$	3	3	–5	–5	3	3	3	–5	–5	3	3	3	–5	–5	3

Видно, что значения сумм (3) точно повторяют структуру распределения вычетов/невычетов в компонентах QR_p и QR_q.

Для полного определения структуры компонент QR_p и QR_q с учетом фазовой неопределенности, потребуется всего p и q вычислений суммы (3) соответственно. Для больших p и q общее количество вычислений корреляционной суммы будет значительно меньше, чем при определении фазы методами прямого поиска (так как $p + q << pq$).

Определение фаз компонент QR_p и QR_q можно осуществлять как традиционными методами, так и предложенным в [5 – 7] методом дихотомии, если p и q являются числами вида $4k + 1$, что дополнительно снижает вычислительную сложность алгоритма определения фазы.

Пусть P и Q – фазы компонент QR_p и QR_q соответственно. Очевидно, что при этом P является значением фазы последовательности Якоби по mod p, а Q – фазой последовательности Якоби по mod q. Тогда фаза последовательности Якоби φ выражается через найденные фазы компонент – последовательностей квадратичных вычетов – следующим образом:

$$\begin{cases} \varphi = P + pm; \\ \varphi = Q + qk, \end{cases} \tag{5}$$

где $m, k \in \mathbf{Z}$ (неизвестные).

Преобразуем (5):

$$pm - qk = (Q - P). \tag{6}$$

Выражение (6) представляет собой линейное диофантово уравнение с двумя неизвестными. В [8] показано, что данное уравнение разрешимо, если *НОД* $[p, q] = 1$ (p и q взаимно просты).

Так как p и q – простые числа, значит, уравнение (6) всегда имеет решение (бесконечное число пар решений). Практический интерес представляют значения неизвестных, удовлетворяющие неравенствам: $0 \le m < q$, $0 \le k < p$.

Алгоритмы решения линейных диофантовых уравнений вида (6) предложены в [9], например, алгоритм Эвклида. После решения уравнения (6) фаза последовательности Якоби может быть вычислена из (5).

Реализацию алгоритма Эвклида и последующие вычисления при определении фазы последовательности Якоби в устройстве синхронизации целесообразно реализовать программно.

Рассмотрим одну из возможных аппаратных реализаций блока разложения последовательности Якоби b_{pq} на составляющие QR_p и QR_q для $p = 3$, $q = 5$ (рис. 1).

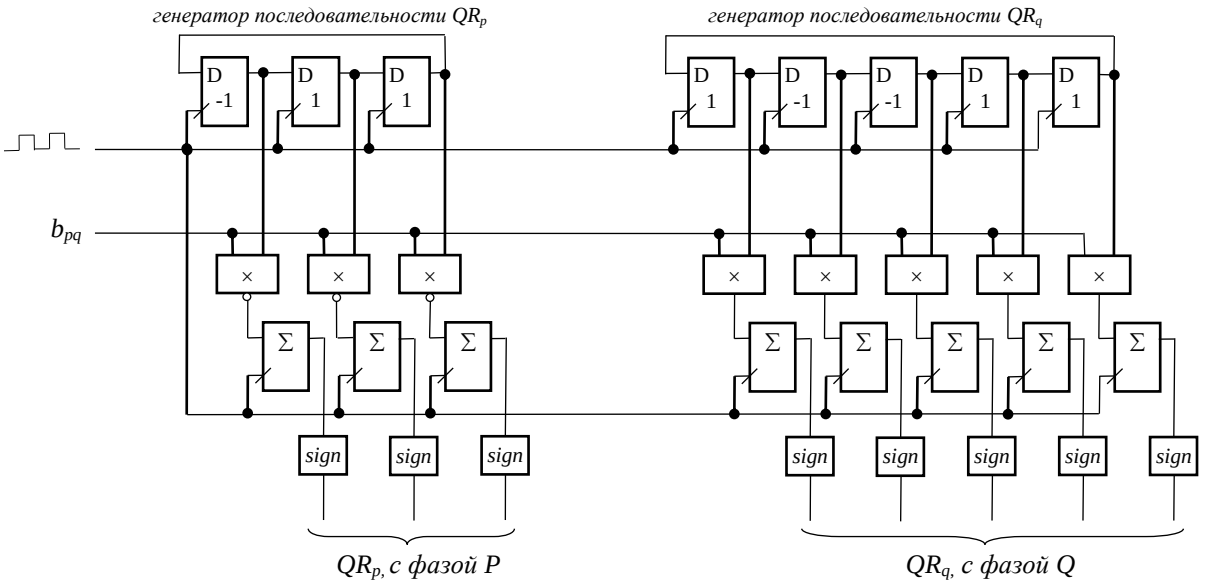

Рис. 1. Блок разложения последовательности Якоби b_{pq} на компоненты QR_p и QR_q:
D – D-триггер (цифрой обозначено начальное состояние);
Σ – накапливающий сумматор; sign – блок определения знака

Входная последовательность Якоби поступает на вход b_{pq} блока с каждым тактовым импульсом поразрядно. На триггерах D-типа реализованы два генератора последовательностей QR_p и QR_q и всех возможных их циклических сдвигов. В блоке происходит одновременное вычисление корреляционных сумм (3) $S_p(i)$, $0 \le i < p - 1$ и $S_q(i)$, $0 \le i < q - 1$, которое заканчивается на $p \times q$-м такте работы (т.е. когда на вход блока поступит последний разряд входной последовательности Якоби). Полученные значения при помощи блока получения знака результата преобразуются в значения разрядов последовательностей QR_p и QR_q с неизвестными фазами P и Q соответственно. Значения фаз P и Q могут быть найдены при дальнейшей обработке. Если p и (или) q являются числами вида $4k + 1$, то для дальнейшей обработки можно использовать разработанные устройства определения фазы последовательностей квадратичных вычетов методом дихотомии [10, 11].

Как правило, вычисление корреляционной суммы (3) осуществляется для последовательности Якоби, которая содержит ошибки вследствие наличия шумов в канале передачи. Поэтому важной характеристикой метода является устойчивость предлагаемого алгоритма к наличию ошибок.

Простейший анализ (3) показывает, что с каждой дополнительной как одиночной, так и пакетной ошибкой в последовательности Якоби значение корреляционной суммы будет изменяться на ±2 единицы. Очевидно, что в первую очередь может быть утеряна информация о распределении вычетов/невычетов в QR_p (так как $p < q$). То есть максимальное число ошибок в последовательности Якоби, при котором возможно восстановить структуру компонент QR_p и QR_q, а значит и определить фазу последовательности Якоби, составляет:

$$r = \frac{p-1}{2}. \tag{7}$$

Максимальная доля ошибок (частота битовых ошибок) в принятой последовательности, при которой возможно с вероятностью 100 % восстановить структуру компонент QR_p и QR_q, определяется как

$$BER = \frac{p-1}{2pq} \approx \frac{1}{2q}. \tag{8}$$

Параметром, ограничивающим устойчивость алгоритма синхронизации к ошибкам в принимаемой последовательности, является значение коэффициента p (7). Поэтому при выборе из ряда близких по длине кодовых последовательностей предпочтение следует отдавать таким, у которых значение коэффициента p больше. Для увеличения доли ошибок (8), которая определяет допустимое отношение сигнал/шум в канале передачи, значение коэффициента q следует выбирать как можно ближе к p. Выполнение последнего условия также способствует улучшению периодической автокорреляционной функции кодовой последовательности Якоби [1].

Однако практический интерес представляет не число ошибок в принимаемой последовательности, а то отношение сигнал/шум в канале передачи, при котором еще обеспечивается возможность синхронизации и которое приводит к возникновению такого числа ошибок. На рисунке 2 приведены зависимости максимальной доли ошибок и отношения сигнал/шум в канале передачи при фазовой манипуляции [2] для последовательностей Якоби, образованных простыми числами в диапазоне 3…199 (длины последовательностей Якоби 15…39203).

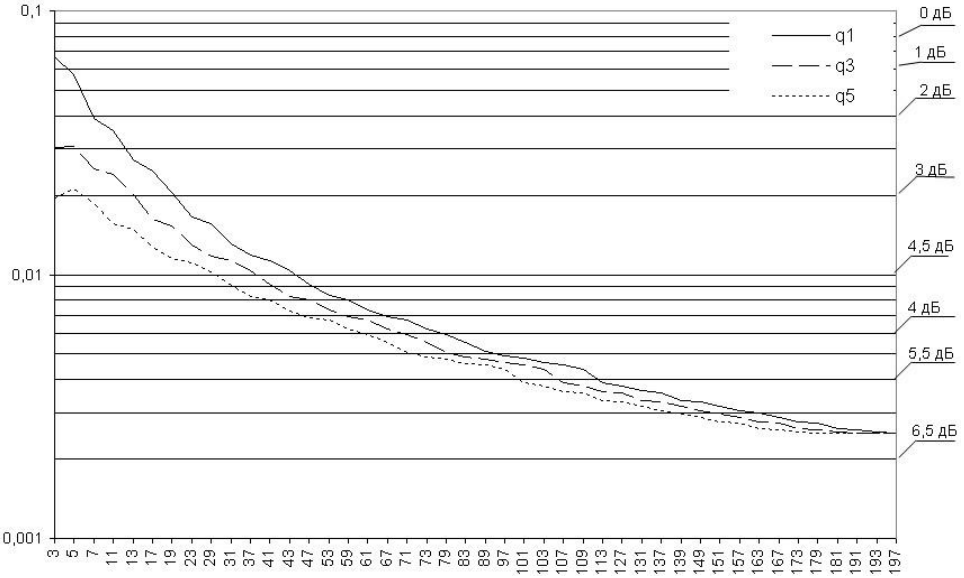

Рис. 2. Максимальная доля ошибок (ось ординат – слева) и отношение сигнал/шум в канале передачи (ось ординат – справа) при фазовой манипуляции для последовательностей Якоби, образованных простыми числами p (ось абсцисс) и q, обеспечивающая 100 %-ную вероятность определения структуры компонент QR_p и QR_q. Линиями q1, q2 и q3 обозначены соответствующие параметры для последовательностей Якоби, у которых коэффициент q является первым, третьим и пятым числом соответственно после коэффициента p в ряду простых чисел

Увеличение числа ошибок в принятой последовательности больше уровня, приведенного в (7), снижает вероятность точного определения структуры компонент QR_p и QR_q (вероятность синхронизации), однако не исключает ее возможность. Аналитическое описание зависимости вероятности правильного определения фазы от числа ошибок и от их распределения в последовательностях Якоби неизвестно. Вероятность точного определения структуры компонент QR_p и QR_q и определения фазы от числа ошибок была получена экспериментально для некоторых последовательностей Якоби (рис. 3).

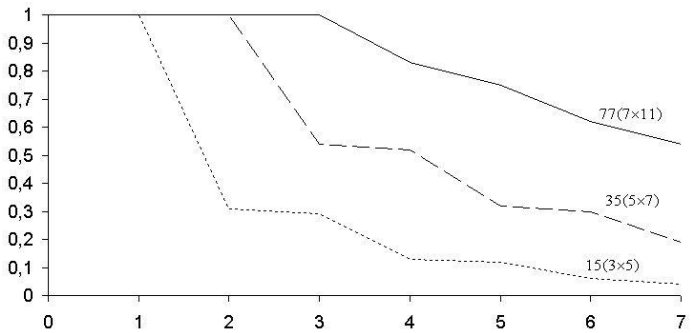

Рис. 3. Вероятность правильного определения фазы при различном числе ошибок для последовательностей Якоби длиной pq = 15(3×5), pq = 35(5×7), pq = 77(7×11)

Анализ графика (см. рис. 3) свидетельствует, что даже при числе ошибок, превышающем пороговый уровень (7), синхронизация последовательности Якоби возможна с достаточно высокой вероятностью. Например, для последовательности $pq = 77$ и при числе ошибок, вдвое превышающем (7), синхронизация возможна с вероятностью около 60 %. Это можно использовать при работе устройства синхронизации при уровне шумов, превышающем пороговое значение. При этом для определения фазы последовательности Якоби может потребоваться несколько попыток в зависимости от вероятности правильного декодирования фазы при различном числе ошибок.

ЛИТЕРАТУРА

1. Green, D.H. and Green, P.R. Modified Jacoby Sequences, IEEE Proc // Comput. Digit. Tech. – 2000. – № 147. – P. 241 – 251.
2. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 384 с.
3. Варакин Л.Е. Поиск шумоподобных сигналов по времени и частоте в системах связи // Электросвязь. – 1981. – № 3. – С. 44 – 45.
4. Лосев В.В., Бродская Е.Б., Коржик В.И. Поиск и декодирование сложных дискретных сигналов / Под ред. В.И. Коржика. – М.: Радио и связь, 1988. – 224 с.
5. Мальцев С.В., Богуш Р.П. Синхронизация квадратично-вычетных последовательностей методом дихотомии // Известия Белорусской инженерной академии. – 2002. – Т. 1 № 2(14). – С. 20 – 22.
6. Басалай Р.Н., Мальцев С.В. Способ уменьшения вычислительной сложности алгоритма синхронизации последовательностей квадратичных вычетов // Актуальные проблемы радиоэлектроники: научные исследования, подготовка кадров: Сб. науч. ст.: В 3 ч. – 2005. Ч. 1 – С. 15 – 19.
7. Басалай Р.Н. Нахождение сумм Якобшталя для двухуровневых последовательностей квадратичных вычетов // Труды молодых специалистов Полоцкого гос. ун-та. Сер. Промышленность. – 2005. – Вып. 11. – С. 73 – 75.
8. Девенпорт Г. Высшая арифметика. Введение в теорию чисел. – М.: Наука, 1965. – 176 с.
9. Бугаенко В.О. Уравнения Пелля. – М.: МЦНМО, 2001 – 32 с.
10. Пат. РБ № 2280 на полезную модель, МПК G 06 F 5/01. Устройство вычисления величины задержки последовательности квадратичных вычетов / Р.Н. Басалай, С.В. Мальцев; Заявка № u20050222; Заявл. 18.04.05.
11. Пат. РБ № 2281 на полезную модель, МПК G 06 F 5/01. Устройство определения величины задержки последовательности квадратичных вычетов / Р.Н. Басалай, С.В. Мальцев; Заявка № u20050222; Заявл. 18.04.05.