Доклады БГУИР
2007 *январь–март* *№ 1 (17)*

ЭЛЕКТРОНИКА

УДК 621.391.26

ОПТИМИЗАЦИЯ ЦИФРОВОЙ ОБРАБОТКИ СИГНАЛОВ С ИСПОЛЬЗОВАНИЕМ СТРУКТУРНЫХ АЛГОРИТМОВ ДЛЯ МАТРИЦ НЕКОТОРЫХ КОДОВ ЯКОБИ

Е.Д. СТРОЙНИКОВА

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 28 ноября 2006

Рассмотрены кодовые последовательности Якоби, соответствующие групповым разностным множествам типа Адамара, с блоковыми длинами $N=2^r-1$. Установлена конечность множества численных значений блоковых длин для последовательностей такого вида. Исследованы структурные особенности и свойства данных последовательностей, а также соответствующих кодовых циркулянтных матриц и матриц инцидентности симметричных блок-схем. Для указанных матриц приведены быстрые алгоритмы векторно-матричного умножения, которые могут быть использованы в мультипроцессорных системах цифровой обработки сигналов. Применение новой факторизации матриц Адамара типа Сильвестра и принципа "двойки" обеспечивает наименьшую сложность вычислений и сокращение временных затрат.

Ключевые слова: оптимизация сложности вычислений векторно-матричного умножения, разностное множество, симметричная блок-схема, кодовая последовательность, бинарная циркулянтная матрица кодовых слов, факторизация.

Введение

Многие задачи цифровой обработки сигналов (ЦОС) с формальной точки зрения представляют собой задачи умножения матриц на векторы (например, декодирование по методу максимального правдоподобия, согласованная и трансверсальная фильтрация, синхронизация, корреляционная обработка, спектральный анализ) [1, 2]. В такой постановке оптимизация процедуры обработки сводится к сокращению объема вычислений. Тем самым уменьшаются временные затраты на векторно-матричные вычисления. Алгоритмы умножения, позволяющие сократить число арифметических операций по сравнению с традиционным строчно-столбцовым методом, называют быстрыми. Общепринятый метод решения задачи минимизации векторно-матричных вычислений – факторизация матриц в произведение слабозаполненных множителей [1, 2]. Таким образом, актуальной является проблема отыскания общих методов оптимизирующей факторизации, применение потенциала перестановочных матриц, а также разработка методов факторизации различных, важных для приложений классов матриц.

Качество алгоритма умножения матрицы на вектор оценивается коэффициентом сложности S, который равен отношению количества операций для вычисления этого произведения к числу строк матрицы [1, 2]. В случаях умножения на вектор матриц бинарных и троичных сигналов с элементами $0, \pm 1$ речь идет о сокращении аддитивной сложности вычислений. Следует отметить, что учет структурных свойств матриц может привести

к резкому сокращению объема вычислений. В частности, для матриц Адамара типа Сильвестра порядков 2^r известны быстрые алгоритмы с коэффициентами сложности r [1] и $0{,}875r$ [2], которые лишь незначительно отличаются от нижней границы Капорина $S_K \geq 0{,}63r$ [1]. Наименьшей аддитивной сложностью обладают алгоритмы, основанные на комбинации процедур быстрого преобразования Адамара (БПА) и декодирования полного кода [1, 2]. На основе алгоритмов вычисления БПА конструируются высокоскоростные и эффективные декодеры. Процессоры БПА легко реализуются на универсальных и специализированных микропроцессорах ЦОС или в виде программ для универсальных ЭВМ.

Применение нелинейных сигналов с хорошими корреляционными свойствами позволяет обеспечить высокую криптостойкость и помехозащищенность систем передачи информации [2]. В классе периодических бинарных фазоманипулированных сигналов с одно- и двухуровневыми периодическими функциями автокорреляции (ПФА) квадратично-вычетные (КВ) кодовые последовательности (КП), КП Холла и Якоби позволяют построить на их основе импульсные последовательности, оптимальные по минимаксному критерию и поэтому широко применяемые в системах связи, радиолокации и телеметрии [3–5]. Можно указать на следующие аналогии в структурах и свойствах М-последовательностей и вышеуказанных семейств КП при соответствии последних разностным множествам типа Адамара [6] (М-последовательности всегда соответствуют разностным множествам типа Адамара в силу значений своих ПФА [2, 3, 5–7]) и блоковых длинах $N=2^r-1$. Разностные множества для всех данных КП являются одноуровневыми и имеют одни и те же параметры: $v=N=2^r-1$, $k=2^{r-1}-1$, $\lambda=2^{r-2}-1$ [3–6]. Матрицы, полученные дополнением первой строкой и первым столбцом, состоящими из 1, соответствующих матриц инцидентности симметричных блок-схем [4–7] в алфавите {1, –1}, являются нормализованными матрицами Адамара порядка 2^r [6]. В случаях цикличности разностных множеств, что справедливо при таких N для М-последовательностей, КП Холла, КВ КП [8] и КП Якоби, как будет показано ниже, при некоторых значениях N, ПФА КП является одноуровневой, принимающей одинаковые значения: $R_\mu(m)=-1$ для $1 \leq m < N$ [2–5]. Более подробно здесь будут рассмотрены КП Якоби, соответствующие разностным множествам типа Адамара, с блоковыми длинами $N=2^r-1$, а также вопрос об оптимизации сложности векторно-матричного произведения для бинарных матриц кодов Якоби со словами такого типа.

Численные значения блоковых длин вида 2^r-1 КП Якоби, соответствующих разностным множествам типа Адамара

Воспользуемся следующим утверждением, которое позволяет также установить тот факт, что численные значения блоковых длин вида 2^r-1 КВ КП являются простыми числами Мерсенна [8].

Лемма. *В равенстве* $2^k-1=p^s$, *где* p *— простое нечетное число,* k, s *— натуральные числа,* k *является простым числом, а* $s=1$.

Доказательство. Рассмотрим равенство $2^k-1=p^s$. Если $k=2l$ — четное число, то $2^k-1=(2^l-1)(2^l+1)=p^s$. $2^l-1>1$ при $l>1$ и $2^l-1=1$ при $l=1$, $2^l+1>1$ для любых натуральных l. По свойству простых чисел, если $l>1$, то p делит 2^l-1 и 2^l+1 одновременно, что невозможно, поскольку $(2^l+1, 2^l-1)=1$. Если $l=1$, то $k=2$, $p=2^2-1=3$ и $s=1$.

Пусть теперь k нечетно. Предположим, что $k=m\cdot n$ — составное число. Тогда $p^s=(2^m-1)(2^{m(n-1)}+2^{m(n-2)}+\ldots+2^m+1)$ и $2^m-1>1$, так как $m>1$. По свойству простых чисел $2^m-1 \equiv 0 \pmod p$ и $2^{m(n-1)}+2^{m(n-2)}+\ldots+2^m+1 \equiv 0 \pmod p$. Из последнего сравнения следует, что $n \equiv 0 \pmod p$. Аналогично можно показать, что любой отличный от 1 делитель числа k делится на p. Значит, $k=p^l$, $l>1$. Поскольку $2^k-1=p^s$, то $2^k \equiv 1 \pmod p$. Значит, по свойству порядка элемента мультипликативной циклической группы поля Галуа $GF(p)^*$ порядок элемента 2 делит k. С другой стороны, порядок элемента 2 делит порядок группы $GF(p)^*$, т.е. $p-1$. Но так как $(p^l, p-1)=1$, получаем противоречие. Значит, k не может быть составным числом, а только нечетным простым числом.

Было показано выше, что при $k=2$ $s=1$. Пусть теперь k — нечетное простое число. Из равенства $2^k-1=p^s$ получаем, что $p^s \equiv -1 \pmod 8$. Если s — четное число, то последнее

сравнение невозможно, так как квадрат любого нечетного числа сравним с 1 по модулю 8. Пусть теперь s – нечетное число, $s>1$, тогда равенство $p^s+1=2^k$ невозможно, поскольку $p^s+1=(p+1)(p^{s-1}-p^{s-2}+\ldots-p+1)$ и $p+1\equiv 0 \pmod 2$, а $p^{s-1}-p^{s-2}+\ldots-p+1\equiv 1 \pmod 2$. Итак, $s=1$. Лемма доказана.

Теорема. *Блоковые длины вида* 2^r-1 *КП Якоби, соответствующих разностным множествам типа Адамара, могут принимать только два значения:* 15 *и* 63.

Доказательство. Длиной КП Якоби, соответствующей групповому разностному множеству в самом общем случае, может быть число вида $N=p^s\cdot q^t$, где p и q — простые нечетные числа, причем $q^t=p^s+l$ [2, 3, 6]. В аддитивной группе $GF(p^s)\oplus GF(q^t)$, являющейся прямой суммой $GF(p^s)$ и $GF(q^t)$, разностное множество D образуется из следующих пар: 1) (c, d), где c и d — ненулевые квадраты, 2) (g, h), где g и h — не квадраты; 3) $(u, 0)$ [6]. Тогда D содержит $k=(N-l+1)/2$ элементов. Но поскольку D является разностным множеством типа Адамара, $k=(N-1)/2$ [6], что указывает на уравновешенность КП Якоби, так как k равно числу символов КП, равных 1. Следовательно, $l=2$.

В равенстве $2^r-1=(u-1)(u+1)$ обозначено $u-1=p^s$, $u+1=q^t$. Откуда получаем $2^r=u^2$, следовательно, $u=2^k$ и $r=2k$ — четное число. Таким образом, $2^k-1=p^s$, что возможно, согласно лемме, только в случае, когда $s=1$ и k — простое число. При $k=2$ получаем $2^k-1=3$, $2^k+1=5$, значит, $N=15$. При нечетном простом k $2^k+1\equiv 0 \pmod 3$, откуда имеем $2^k+1=q^t=3^t$, следовательно, $3^t-1=2^k$ и $3^t\equiv 1 \pmod 8$, что возможно только при четном $t=2n$. Тогда $3^{2n}-1=(3^n-1)\cdot(3^n+1)=2^k$, откуда $3^n-1=2^v$, $3^n+1=2^w$. Поскольку $2^w-2^v=2^v(2^{w-v}-1)=2$, то $v=1$, $w=v+1=2$, следовательно, $n=1$, а $t=2$. В этом случае получаем единственное значение $k=3$, поэтому $2^k-1=7$, $2^k+1=9$, значит, $N=63$. Теорема доказана.

Данная теорема позволяет установить конечность множества численных значений (всего два значения) блоковых длин вида 2^r-1 КП Якоби типа Адамара.

Теоретический анализ структурных особенностей КП Якоби

В самом общем случае для построения КП Якоби $\mu=\{\mu_i, i=0, 1,\ldots, N-1\}$ с блоковой длиной $N=p^s\cdot q^t$ одно из правил кодирования может быть сформулировано следующим образом:

$$\mu_i=\begin{cases}1 \text{ при } i\equiv 0 \pmod{q^t},\\ -1 \text{ при } i\equiv 0 \pmod{p^s},\ i\not\equiv 0 \pmod{q^t},\\ \psi_1(i)\cdot\psi_2(i) \text{ при } i\not\equiv 0 \pmod{p^s},\ i\not\equiv 0 \pmod{q^t},\end{cases} \qquad (1)$$

где $\psi_1(i)$ и $\psi_2(i)$ равны значениям квадратичных характеров ненулевых элементов полей Галуа $GF(p^s)$ и $GF(q^t)$, стоящих на i-х позициях, приведенных по модулям p^s и q^t согласно китайской теореме об остатках (КТО) [1, 6]. Причем элементы полей могут быть, например, упорядочены в p- и q-ичных системах счисления в соответствии с разложениями по базисам над $GF(p)$ и $GF(q)$, состоящим из степеней примитивных элементов. Нужно отметить, что в данном случае количество способов упорядочения определяется числом примитивных элементов полей Галуа. Такое упорядочение используется при вычислении элементов матриц Джекобстола, которые фигурируют в методе Пейли построения матриц Адамара [7]. Для $s=1$, $t=2$, например, это выглядит следующим образом:

$GF(p)$: 0, 1,…, $p-1$;
$GF(q^2)$: 0, 1,…, $q-1$, β, $\beta+1$,…, $\beta+q-1$,…, $(q-1)\beta$, $(q-1)\beta+1$,…, $(q-1)\beta+q-1$,

где β — примитивный элемент $GF(q^2)$.

По КП Якоби (1) однозначно строится разностное множество D, описанное выше в доказательстве теоремы и состоящее из всех элементов аддитивной группы $W=GF(p^s)\oplus GF(q^t)$, соответствующих порядковым номерам символов КП, равных 1. В указанной группе операция сложения задается по правилу: $(a, b)+(c, d)=(a+c, b+d)$, где a, $c\in GF(p^s)$, b, $d\in GF(q^t)$. При построении симметричной блок-схемы каждый блок C_i имеет ту же мощность, что и D, и получается путем сложения всех элементов D с фиксированным элементом группы g_i,

представляющим собой соответствующую номеру i упорядоченную пару, i=0, 1,…N–1, g_0= (0, 0), g_1= (1, 1). В случае s=t=1 группа W является циклической с образующим элементом g_1 и изоморфна циклической аддитивной группе классов вычетов по модулю N согласно КТО. Во всех остальных случаях группа W не является циклической, поскольку характеристики полей $GF(p^s)$ и $GF(q^t)$ равны соответственно p и q, откуда $(p\cdot q)g_i=g_0$ для любого $g_i\in W$, в то время как $p\cdot q<N$. Поэтому только при s=t=1 соответствующая КП (1) симметричная блок-схема может быть отождествлена с блок-схемой классов вычетов по модулю N и имеет циклический автоморфизм $\alpha: i\to i+1$, $C_i\to C_{i+1}$, который переставляет как элементы, так и блоки по циклу длины N. Итак, важно отметить, что только в случае s=t=1 разностное множество и порожденная им симметричная блок-схема являются циклическими, а соответствующая матрица инцидентности — циркулянтной. Исходя из критериев существования КП с одно- и двухуровневой ПФА — существования соответствующих одно- и двухуровневых циклических разностных множеств [3], можно заключить, что КП Якоби (1) с такими ПФА могут существовать лишь при s=t=1. И в этом случае КП (1) обладают одноуровневой ПФА $R_\mu(m) = -1$ для $1\le m <N$ при $q = p+2$ и двухуровневой — при $q = p+4$ [3].

Определения и свойства изоморфизмов блок-схем, разностных множеств и КП [3, 6] позволяют заключить, что те же самые замечания касаются и изоморфных (1) КП Якоби. Для вышеуказанных разностного множества D и симметричной блок-схемы существует единственный класс изоморфных коэффициентов T, состоящий из всех пар (y, z) из W, где y, z — ненулевые элементы с различными значениями квадратичных характеров ψ_1 и ψ_2 соответственно. Все коэффициенты из T приводят к одному и тому же разностному множеству, поэтому для КП (1) существует единственная изоморфная КП $\eta=\{\eta_i, i=0, 1,\ldots, N-1\}$ со следующим правилом кодирования:

$$\eta_i = \begin{cases} 1 \text{ при } i \equiv 0 \pmod{q^t}, \\ -1 \text{ при } i \equiv 0 \pmod{p^s},\ i \not\equiv 0 \pmod{q^t}, \\ -\psi_1(i)\cdot\psi_2(i) \text{ при } i \not\equiv 0 \pmod{p^s},\ i \not\equiv 0 \pmod{q^t}. \end{cases} \qquad (2)$$

При N=15 и N=63 для КП Якоби (1) существует в каждом конкретном случае единственная изоморфная КП (2) — инверсно-изоморфная. Это следует из того, что $-g_1=(-1,-1)\in T$, поскольку в случае N=15 $\psi_1(-1)$ и $\psi_2(-1)$ соответственно равны значениям символов Лежандра $\left(\frac{-1}{3}\right)=-1$, $\left(\frac{-1}{5}\right)=1$, а в случае N=63 $\psi_1(-1)=\left(\frac{-1}{7}\right)=-1$, $\psi_2(-1)=\psi_2(2)=\psi_2(\beta^4)=1$ для любого примитивного элемента β поля $GF(3^2)$.

При N=63, поскольку s=1, t=2, для КП (1) и (2) разностные множества и порожденные ими симметричные блок-схемы не являются циклическими, соответствующие матрицы инцидентности не являются циркулянтными, а ПФА являются пятиуровневыми, независимо от выбора примитивного элемента β поля $GF(3^2)$, как показывают непосредственные вычисления. Поэтому при N=63 симметричные циркулянтные матрицы КП Якоби и матрицы инцидентности симметричных блок-схем не могут быть получены из соответствующих циркулянтных матриц М-последовательностей при таких же N с помощью перестановок строк и столбцов. Поскольку для симметричных матриц указанные перестановки задаются одним правилом, и это бы означало существование изоморфизмов соответствующих блок-схем, что противоречило бы свойствам изоморфизмов. В данном случае КП (1) и (2) в алфавите {0, 1} после преобразования $1\to 0$, $-1\to 1$ не могут быть представлены над полем $GF(2)$ даже в виде суммы М-последовательностей с такими же блоковыми длинами, как это было сделано в [8] для КВ КП, в силу того что полиномы степеней N–1 с коэффициентами при x^i, равными символам КП, не являются идемпотентами кольца $R_N[x]=GF(2)[x]/(x^N-1)$ [7] по причине невыполнения условий $\mu_i=\mu_{2i}$ и $\eta_i=\eta_{2i}$ для всех i=0, 1,…, N–1. Действительно, если β — корень полинома $f(x)=x^2+2x+2$, то $\mu_1=\mu_2=\mu_4=\mu_8=1$, $\mu_{16}=-1$, если β — корень полинома $g(x)=x^2+x+2$, то $\mu_1=\mu_2=1$, $\mu_4=-1$, то же самое для КП η, только знаки меняются на противоположные.

Строение КП Якоби с блоковыми длинами N =15 и их циркулянтных матриц

При N=15, поскольку s=t=1, p=3, q=5, для КП (1) и (2) разностные множества и порожденные ими симметричные блок-схемы являются циклическими, соответствующие матрицы инцидентности — циркулянтными, а ПФА — одноуровневыми, $R_\mu(m) = -1$ для $1 \le m < 15$. В данном случае КП (1) и (2) являются М-последовательностями [3], что можно доказать аналитически по аналогии с КВ КП в [8].

Согласно правилу кодирования (1), получаем КП μ:

μ_0=1, μ_1=1, μ_2=1, μ_3= –1, μ_4=1, μ_5=1, μ_6= –1, μ_7= –1, μ_8=1, μ_9= –1,
μ_{10}=1, μ_{11}= –1, μ_{12}= –1, μ_{13}= –1, μ_{14}= –1. (3)

В данном случае $\psi_1(i) = \left(\frac{i}{3}\right)$, $\psi_2(i) = \left(\frac{i}{5}\right)$ — символы Лежандра и $\psi_1(i) \cdot \psi_2(i) = \left(\frac{i}{15}\right)$ — символ Якоби. Поскольку $\left(\frac{2}{15}\right) = 1$, $\mu_{2i} = \mu_i$ для всех символов КП (3), причем порядковые номера вычисляются как классы вычетов по модулю 15. КП (3) можно поставить в соответствие полином $J(x)$ с коэффициентами a_i, $i = \overline{0, N-1}$, из поля Галуа $GF(2)$ по правилу:

$$a_i = \begin{cases} 0, \mu_i = 1, \\ 1, \mu_i = -1. \end{cases} \quad (4)$$

$J(x) = x^3 + x^6 + x^7 + x^9 + x^{11} + x^{12} + x^{13} + x^{14}$.

Поскольку $J^2(x) = J(x^2) = J(x)$, $J(x)$ — идемпотент кольца полиномов $R_N[x]$. Поэтому существует однозначное представление $J(x) = \sum_s b_s \theta_s(x)$, где $b_s \in GF(2)$, $(N, s)=1$, $\theta_s(x)$ — примитивные идемпотенты кольца $R_N[x]$ [7]. В случае N=15 существует два примитивных идемпотента $\theta_1(x)$ и $\theta_7(x)$, соответствующих циклотомическим классам C_1={1,2,4,8} и C_7={7,14,13,11}. Пусть γ — примитивный элемент поля $GF(2^4)$, являющийся корнем примитивного полинома x^4+x+1. Тогда по формуле для коэффициентов $\theta_s(x)$ $\varepsilon_i = \sum_{j \in C_s} \gamma^{-ij}$, $i = \overline{0, N-1}$, получаем, что $J(x) = \theta_7(x)$. Как известно, $\theta_s(x)$ порождают коды максимальной длины (КМД) [7], следовательно, циклический код Якоби, порожденный $J(x)$, является КМД, а значит, КП (3) является М-последовательностью, ее циркулянтная матрица A_1 или, что то же самое, матрица инцидентности соответствующей симметричной блок-схемы является матрицей ненулевых слов КМД в алфавите {1, –1}. Тогда после перестановки в матрице A_1 строк в соответствии с возрастанием первых четырех символов в двоичной системе счисления, согласно преобразованию (4) и перестановке столбцов $i \to \gamma^{i-1}, i = \overline{1,15}$, с записью номера в двоичной системе счисления, согласно разложению по базису $\{1, \gamma, \gamma^2, \gamma^3\}$, получится матрица $H_{16}^{/}$, отличающаяся от матрицы Адамара типа Сильвестра H_{16} отсутствием строки и столбца с нулевыми номерами [1, 2]. Таким образом, $H_{16}^{/} = P_1 \cdot A_1 \cdot Q_1$, $A_1 = P_1^{-1} \cdot H_{16}^{/} \cdot Q_1^{-1}$, P_1, P_1^{-1}, Q_1, Q_1^{-1} — перестановочные матрицы, которые соответствуют перестановкам координат входного и выходного векторов и при умножении на вектор не требуют выполнения арифметических операций.

Согласно правилу кодирования (2) КП, η имеет следующий вид:

η_0=1, η_1= –1, η_2= –1, η_3= –1, η_4= –1, η_5=1, η_6= –1, η_7=1, η_8= –1, η_9= –1,
η_{10}=1, η_{11}=1, η_{12}= –1, η_{13}=1, η_{14}=1. (5)

Данной КП по правилу (4) ставится в соответствие полином $J^*(x)$, который также является идемпотентом кольца $R_N[x]$, и $J^*(x) = \theta_1(x)$. Поэтому циклический код Якоби, порожденный $J^*(x)$, является КМД, КП (5) — М-последовательностью. По аналогии с A_1 получаем симметрическую циркулянтную матрицу A_2, после перестановки строк в которой

в соответствии с возрастанием первых четырех символов в двоичной системе счисления и перестановки столбцов $i \to \gamma^{1-i}, i = \overline{1,15},$ с записью номера в двоичной системе счисления, согласно разложению по базису {1, γ, γ^{-1} γ^{-2}, γ^{-3}}, также получится матрица $H_{16}^{/}$. Таким образом, $H_{16}^{/} = P_2 \cdot A_2 \cdot Q_2$, $A_2 = P_2^{-1} \cdot H_{16}^{/} \cdot Q_2^{-1}$, где P_2, P_2^{-1}, Q_2, Q_2^{-1} — перестановочные матрицы, которые соответствуют перестановкам координат входного и выходного векторов.

Быстрые алгоритмы векторно-матричного умножения для циркулянтов КП Якоби или КМД при *N* =15, основанные на БПА

Строки матрицы-циркулянта КП длиной *N* получают с помощью всевозможных циклических сдвигов КП на одну позицию влево либо вправо, очевидно, что размерность такой матрицы равна *N*×*N*. Умножение матрицы-циркулянта КП, полученной первым (вторым) способом, на вектор является фактически операцией вычисления циклической свертки (периодической корреляционной функции) двух последовательностей [1]. Циркулянтные матрицы в первом и во втором случаях отличаются друг от друга перестановками строк в обратном порядке, за исключением строки с нулевым номером. Поэтому такие матрицы могут быть получены друг из друга при помощи умножения перестановочной матрицы, отличающейся от единичной матрицы перестановкой строк $i \to N-i$, i=1,…, N–1, и не требующей выполнения арифметических операций при умножении на вектор. Поэтому число арифметических операций при умножении первой и второй матриц на векторы одинаково. В дальнейшем ограничимся рассмотрением первого случая.

Матрицы Адамара типа Сильвестра широко применяются в теории и практике ЦОС, помехоустойчивой передачи информации. Они служат основой БПА, декодирования и поиска последовательностей Уолша (Рида-Маллера), применяются в теории бент-функций [1, 2, 7]. Эти матрицы строятся рекуррентно:

$$H_1 = [1],\ H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},\ H_{2^r} = \begin{bmatrix} H_{2^{r-1}} & H_{2^{r-1}} \\ H_{2^{r-1}} & -H_{2^{r-1}} \end{bmatrix} = H_2 \otimes H_{2^{r-1}} = \underbrace{H_2 \otimes H_2 \otimes \ldots \otimes H_2}_{r},$$

где r — натуральное число, $\otimes$ — знак тензорного произведения матриц. Еще в 1958 г. И. Дж. Гуд показал, что матрицы, являющиеся тензорными степенями других матриц, могут быть факторизованы в произведение слабозаполненных матриц. В частности, это касается и матриц Адамара типа Сильвестра, метод Гуда лежит в основе классического варианта БПА [1, 2, 7].

Используя матрицу Адамара типа Сильвестра H_{2^r}, можно записать дискретное преобразование Уолша–Адамара в следующей форме:

$$\bar{b} = H_{2^r}\ \bar{s}, \qquad (6)$$

где $\bar{s} = (s(0), s(1), \ldots, s(2^r - 1))^{\mathrm{T}}$ и $\bar{b} = (b(0), b(1), \ldots, b(2^r - 1))^{\mathrm{T}}$ — соответственно векторы-столбцы отсчетов сигнала и спектральных коэффициентов. Вычисление преобразования (6) требует при обычном строчно-столбцовом методе выполнения $2^r(2^r-1)$ операций сложения-вычитания. Для построения БПА в классическом варианте матричное равенство (6) записывается в следующем виде:

$$\begin{bmatrix} b(0) \\ b(1) \\ \vdots \\ b(2^{r-1}-1) \\ b(2^{r-1}) \\ \vdots \\ b(2^{r}-1) \end{bmatrix} = \begin{bmatrix} H_{2^{r-1}} & H_{2^{r-1}} \\ H_{2^{r-1}} & -H_{2^{r-1}} \end{bmatrix} \cdot \begin{bmatrix} s(0) \\ s(1) \\ \vdots \\ s(2^{r-1}-1) \\ s(2^{r-1}) \\ \vdots \\ s(2^{r}-1) \end{bmatrix}, \text{ откуда } \begin{bmatrix} b(0) \\ b(1) \\ \vdots \\ b(2^{r-1}-1) \end{bmatrix} = H_{2^{r-1}} \cdot \begin{bmatrix} s(0)+s(2^{r-1}) \\ s(1)+s(2^{r-1}+1) \\ \vdots \\ s(2^{r-1}-1)+s(2^{r}-1) \end{bmatrix},$$
$$\begin{bmatrix} b(2^{r-1}) \\ b(2^{r-1}+1) \\ \vdots \\ b(2^{r}-1) \end{bmatrix} = H_{2^{r-1}} \cdot \begin{bmatrix} s(0)-s(2^{r-1}) \\ s(1)-s(2^{r-1}+1) \\ \vdots \\ s(2^{r-1}-1)-s(2^{r}-1) \end{bmatrix}, \quad (7)$$

Из этих выражений следует, что вычисление 2^r-точечного преобразования сводится к предварительному суммированию (вычитанию) входных данных и последующему вычислению двух 2^{r-1}-точечных преобразований. Процедуру снижения размерности преобразования можно продолжить, согласно (7), до получения двухточечного преобразования. Для этого потребуется r шагов. На каждом шаге производится 2^r сложений и вычитаний, поэтому общее количество операций равно $r \cdot 2^r$. В результате этого число узлов графа на каждой итерации остается постоянным и равным 2^r, а вычислительный процесс заканчивается через r итераций. Рассмотренный алгоритм БПА можно трактовать как разложение (факторизацию) матрицы H_{2^r} в произведение r слабозаполненных множителей порядка $2^r \times 2^r$, содержащих в каждой строке и каждом столбце только два ненулевых элемента. Граф алгоритма имеет регулярную структуру и строится из пары базовых операций сложения и вычитания, необходимой для вычисления произведения H_2 на вектор, которая получила название "бабочка" (см. рис. 1). Крылья такой бабочки уменьшаются вдвое на каждой последующей итерации. Существуют и другие формы факторизации, приводящие к такому же результату.
что позволяет отдельно вычислить первую и вторую половины спектра.

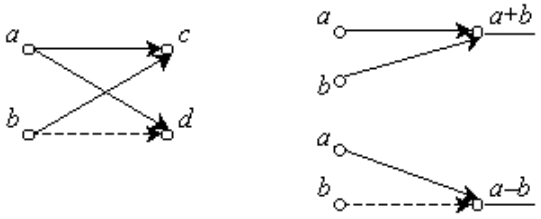

Рис. 1. Пара базовых операций "бабочка" графа классического БПА

Сложность умножения матриц A_1 и A_2 на вектор определяется аддитивной сложностью умножения матрицы $H_{16}^{/}$ на вектор, уменьшить которую позволяет БПА для умножения H_{16} на вектор. Поскольку размерность матрицы H_{16} на единицу больше размерности входного вектора, то для согласования размерностей длина входного вектора увеличивается на единицу. Итак, алгоритм можно разбить на следующие этапы: 1) координаты входного вектора подвергаются перестановке, задаваемой Q_1^{-1} или Q_2^{-1}; 2) полученный после этого вектор дополняется нулевой координатой $s(0)=0$; 3) вычисляется произведение H_{16} на данный вектор, используя БПА, причем координату $b(0)$ на последней итерации вычислять не нужно; 4) в полученном векторе-произведении переставляются координаты в соответствии с P_1^{-1} или P_2^{-1}. При использовании классического БПА для $r=4$, согласно (7), количество операций сложения-вычитания равно $4 \cdot 2^4 - 3 = 61$, поскольку на 1-й итерации отсутствуют вычисления суммы и разности $s(0) \pm s(8) = \pm s(8)$ и на 4-й итерации отсутствует вычисление одной суммы для получения $b(0)$. В данном случае выигрыш в числе операций по сравнению с прямым методом умножения $w_1 = (15 \cdot 14)/61 \approx 3{,}443$ раза, коэффициент сложности $S_1 = 61/15 \approx 4{,}067$.

В [2] была предложена новая явная факторизация матриц Адамара типа Сильвестра, которая позволяет выполнить декодирование циклического кода Рида-Маллера с меньшей в среднем на 12,5%, чем $r \cdot 2^r$,сложностью при ориентации на аппаратную реализацию декодера и использовании схем программируемой логики. Результат базируется на факторизации определенного класса тензорных произведений матриц и использовании принципа "двойки". Данный принцип может быть сформулирован следующим образом: "в двоичной системе счисления для любого натурального числа k умножение на 2^k арифметической операцией можно не считать". Принцип "двойки" учитывает тот факт, что вычисления на ЭВМ

осуществляются в двоичной системе счисления и умножение на 2 есть лишь разрядный сдвиг, не требующий ни временных, ни аппаратурных затрат.

Матрицу H_4 можно представить в виде произведения следующих слабозаполненных сомножителей:

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 2 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix}. \quad (8)$$

При разложении (8) с использованием принципа "двойки" аддитивная сложность умножения H_4 на вектор, как и в [2], равна 7 вместо 8 согласно (7). Данный вариант БПА, как и вариант из [2], позволяет вычислить произведение H_4 на вектор за три итерации вместо двух согласно (7). Тем не менее здесь на 1-й итерации требуется выполнение двух операций, на 2-й — одной операции вместо выполнения четырех операций на 1-й итерации в классическом варианте БПА. Следует отметить, что программная реализация БПА при факторизации (8) является более выигрышной по сравнению с аналогичной из [2], поскольку отсутствуют перестановки координат векторов, полученных на всех итерациях, и на 1-й итерации нужно производить запоминание двух нововведенных координат $s^1(4)$ и $s^1(5)$ вместо трех. Граф вычислений показан на рис. 2, где использованы обозначения из рис. 1.

Согласно [2], справедлива следующая факторизация матрицы H_{16}:

$$H_{16} = U \cdot V \cdot U \cdot V = (U \cdot V)^2 = \left(\begin{bmatrix} E^{11} & E^{21} & E^{31} & E^{41} \\ E^{12} & E^{22} & E^{32} & E^{42} \\ E^{13} & E^{23} & E^{33} & E^{43} \\ E^{14} & E^{24} & E^{34} & E^{44} \end{bmatrix} \cdot \begin{bmatrix} H_4 & O & O & O \\ O & H_4 & O & O \\ O & O & H_4 & O \\ O & O & O & H_4 \end{bmatrix} \right)^2, \quad (9)$$

где E^{ij} — матрица порядка 4×4, в которой элемент e_{ij}=1, а остальные равны нулю, O — нулевая матрица порядка 4×4. Матрица U в факторизации (9) является перестановочной матрицей и не требует выполнения арифметических операций при умножении на вектор. На рис. 3 приведен соответствующий граф вычислений. Граф второго варианта БПА для H_{16} имеет регулярную структуру (рис. 3), следовательно, алгоритм может быть реализован в два этапа, каждый из которых имеет три итерации в соответствии с (9), (8) и рис. 2. Поскольку после умножения на вектор матрицы V на каждом из двух этапов выполняется одна и та же перестановка координат выходного вектора в соответствии с матрицей U, можно исключить перестановки в программной реализации, заменив их непосредственным вычислением соответствующих координат выходного вектора на последней итерации. На каждом из этапов умножение матриц H_4 на соответствующие отрезки вектора может осуществляться параллельно для сокращения временных затрат. Таким образом, на 1-й и 4-й итерациях данного алгоритма выполняется 8 операций сложения-вычитания, на 2-й и 5-й – 4 операции сложения, на 3-й и 6-й – 16 операций сложения вычитания, в то время как на каждой из четырех итераций традиционного БПА выполняется 16 операций сложения-вычитания.

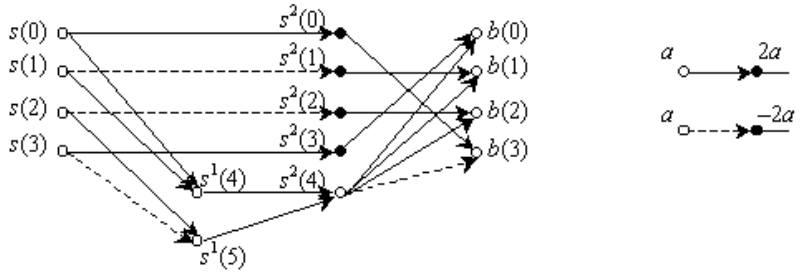

Рис. 2. Граф БПА с использованием новой факторизации H_4

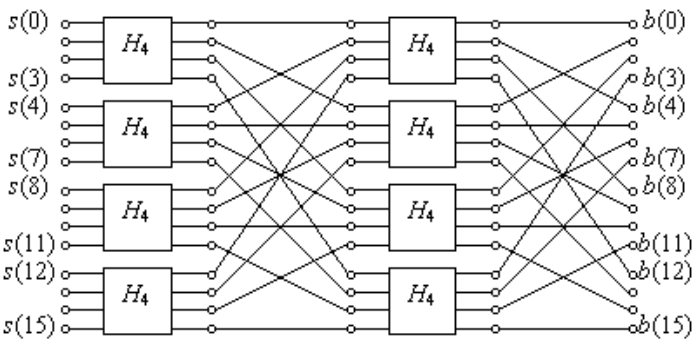

Рис. 3. Граф БПА с использованием факторизации (9) для H_{16}

При использовании варианта БПА, задаваемого (9), факторизации (8) и принципа "двойки" количество операций сложения-вычитания при умножении матрицы $H_{16}^{/}$, а значит, и A_1, A_2, на вектор будет равно 8·7–3=53, что примерно на 13% меньше, чем при первом варианте с использованием классического БПА. Действительно (см. также рис. 2, 3), так как $s(0)=0$, не требуется вычисления одной суммы на 1-й итерации: $s^1(4)=s(1)$, и так как $s^2(0)=s(0)=0$, на 3-й итерации не требуется вычисления одной разности: $b(3)=-s^2(4)$. На 6-й итерации не требуется вычислять одну сумму для получения координаты $b(0)$. В данном случае выигрыш в числе операций по сравнению с прямым методом умножения $w_2=(15\cdot14)/53\approx3{,}962$ раза, коэффициент сложности $S_2=53/15\approx3{,}533$. Итак, $S_2<S_1$, $S_2/S_1\approx0{,}869$.

Быстрые алгоритмы векторно-матричного умножения для циркулянтов и матриц инцидентности симметричных блок-схем КП Якоби при N =63

Рассмотрим циркулянтные матрицы A_1 и A_2 КП Якоби μ и η при N=63 и матрицы инцидентности соответствующих симметричных блок-схем B_1 и B_2. Умножения матриц B_1 и B_2 на векторы можно рассматривать по аналогии с диадной сверткой как вычисление сверток специального вида, когда номера отсчетов представляются, согласно КТО, как элементы-пары вышеописанной группы W, упорядоченные соответствующим образом в 7-ичной и 3-ичной системах счисления. Выполним в матрицах A_i, B_i перестановки строк и такие же перестановки столбцов в соответствии с КТО и внешним упорядочением по второй координате, а внутренним упорядочением по первой координате: (0,0), (1,0), …, (6,0),…, (0,8), (1,8),…, (6,8). Тогда $A_i = PA_i^* P^T$, $B_i = PB_i^* P^T$, $i=1,2$, где P — соответствующая перестановочная матрица, матрицы A_i^*, B_i^* имеют блочно-циркулянтную структуру. Разделяя данные матрицы на 9 вертикальных блоков по 7 соседних столбцов и применяя теорему оптимизирующей факторизации матриц [2], получаем следующие разложения:

$$A_1^* = K \cdot L = \begin{bmatrix} G & F & F & F^{/} & F^{/} & F & F^{/} & F & F^{/} \\ F & F & F^{/} & F^{/} & F & F^{/} & F & F^{/} & G \\ F & F^{/} & F^{/} & F & F^{/} & F & F^{/} & G & F \\ F^{/} & F^{/} & F & F^{/} & F & F^{/} & G & F & F \\ F^{/} & F & F^{/} & F & F^{/} & G & F & F & F^{/} \\ F & F^{/} & F & F^{/} & G & F & F & F^{/} & F^{/} \\ F^{/} & F & F^{/} & G & F & F & F^{/} & F^{/} & F \\ F & F^{/} & G & F & F & F^{/} & F^{/} & F & F^{/} \\ F^{/} & G & F & F & F^{/} & F^{/} & F & F^{/} & F \end{bmatrix} \cdot diag\left(\underbrace{M,\ldots,\ M}_{9} \right), \text{ где } M = \begin{bmatrix} 1 & \ldots & 1 \\ & Q_7 & \\ -2E_7 & -Q_7 & \end{bmatrix},$$

$$Q_7 = \begin{bmatrix} -1 & 1 & 1-1 & 1-1-1 \\ 1 & 1-1 & 1-1-1-1 & \\ 1-1 & 1-1-1-1 & 1 & \\ -1 & 1-1-1-1 & 1 & 1 \\ 1-1-1-1 & 1 & 1-1 & \\ -1-1-1 & 1 & 1-1 & 1 \\ -1-1 & 1 & 1-1 & 1-1 \end{bmatrix}, \quad B_1^* = J \cdot L = \begin{bmatrix} G & F & F & F^{/} & F^{/} & F & F^{/} & F & F^{/} \\ F & F & G & F^{/} & F & F^{/} & F & F^{/} & F^{/} \\ F & G & F & F & F^{/} & F^{/} & F^{/} & F^{/} & F \\ F^{/} & F^{/} & F & F^{/} & F & F^{/} & G & F & F \\ F^{/} & F & F^{/} & F & F^{/} & F^{/} & F & F & G \\ F & F^{/} & F^{/} & F^{/} & F^{/} & F & F & G & F \\ F^{/} & F & F^{/} & G & F & F & F^{/} & F^{/} & F \\ F & F^{/} & F^{/} & F & F & G & F^{/} & F & F^{/} \\ F^{/} & F^{/} & F & F & G & F & F & F^{/} & F^{/} \end{bmatrix} \cdot diag\left(\underbrace{M,\ldots,\ M}_{9} \right), \qquad (10)$$

где матрица G состоит из семи 1-х строк единичной матрицы порядка 15, F – из 2-й – 8-й ее строк, F' – из 9-й – 15-й ее строк, Q_7 – циркулянтная матрица КВ КП, E_7 – единичная матрица порядка 7. В разложениях A_2^*, B_2^* матрица M отличается перестановкой местами блоков Q_7 и $-2E_7-Q_7$. Данные факторизации справедливы, когда примитивный элемент поля $GF(3^2)$ β является корнем полинома $g(x)$. Если β — корень полинома $f(x)$, то матрицы K и J в соответствующих разложениях отличаются одинаковыми перестановками $\begin{pmatrix}012345678\\012678345\end{pmatrix}$ столбцов и строк, состоящих из блоков F, F', G.

После перестановок строк $\begin{pmatrix}01234567\\04125376\end{pmatrix}$ и столбцов $\begin{pmatrix}1234567\\4216375\end{pmatrix}$, согласно [1, 2], матрица Q_7, дополненная строкой с нулевым номером, состоящей из единиц, являющаяся также матрицей КМД в алфавите $\{1, -1\}$ [3, 8], преобразуется в матрицу H_8', отличающуюся от матрицы Адамара типа Сильвестра H_8 отсутствием столбца с нулевым номером, состоящего из единиц. При использовании БПА для умножения H_8' на вектор входной вектор дополняется координатой $s(0)=0$. В случае классического БПА для $r=3$, согласно (7), количество операций сложения-вычитания равно $3\cdot2^3-2=22$, поскольку на 1-й итерации отсутствуют вычисления суммы и разности $s(0)\pm s(4)=\pm s(4)$. Для матрицы H_8, согласно [1, 2], справедлива следующая факторизация:

$$H_8=\begin{bmatrix}E_4 & E_4\\ E_4 & -E_4\end{bmatrix}\cdot\begin{bmatrix}H_4 & O\\ O & H_4\end{bmatrix}, \qquad (11)$$

где E_4 — единичная матрица порядка 4, O — нулевая матрица порядка 4×4. Соответствующий граф вычислений приведен на рис. 4, где использованы обозначения из рис. 1. При использовании варианта БПА, задаваемого (11), факторизации (8) и принципа "двойки" количество операций сложения-вычитания при умножении матрицы H_8' на вектор равно 5+7+8=20, поскольку $s(0)=0$ (см. также рис. 2, 4).

При умножении матрицы M на вектор в соответствии с ее разложением $M=\begin{bmatrix}1 & \dots & 1\\ & Q_7 & \\ & -Q_7 & \end{bmatrix}-2\cdot\begin{bmatrix}0 & \dots & 0\\ & \dots & \\ 0 & \dots & 0\\ & E_7 & \end{bmatrix}$ в целом потребуется выполнить 22+7=29 операций сложения-вычитания и 7 операций умножения на 2 в традиционном варианте. При использовании принципа "двойки" и нового варианта БПА для умножения M на вектор потребуется выполнить только 20+7=27 аддитивных операций. Умножение же матрицы L на вектор потребует выполнить $29\cdot9=261$ операцию сложения-вычитания и 63 операции умножения на 2 в традиционном и соответственно $27\cdot9=243$ аддитивные операции в новом варианте. Итак, последний вариант является более предпочтительным. При умножении матрицы L на вектор все 9 матриц M могут умножаться на соответствующие отрезки вектора параллельно для повышения скорости обработки.

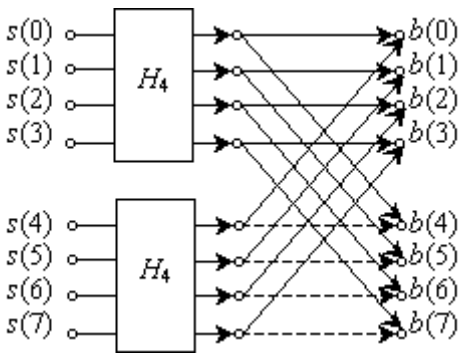

Рис. 4. Граф БПА с использованием факторизации (11) для H_8

Далее, согласно (10), на полученный вектор умножаются соответственно матрицы K или J. Матрица J может быть разделена на 3 вертикальных блока по 45 соседних столбцов, и, снова применяя теорему об оптимизирующей факторизации, получим разложение:

$$J=\begin{bmatrix} E_7 & O & O & O & O & O & O & O & E_7 & O & O & O & O & O & O & E_7 & O \\ O & E_7 & O & O & O & O & O & O & O & E_7 & O & O & O & O & O & O & E_7 \\ O & O & E_7 & O & O & O & O & O & O & O & E_7 & O & O & O & E_7 & O & O \\ O & O & O & E_7 & O & O & O & O & O & O & E_7 & O & E_7 & O & O & O & O & O \\ O & O & O & O & E_7 & O & O & O & O & O & O & E_7 & O & E_7 & O & O & O & O \\ O & O & O & O & O & E_7 & O & O & O & E_7 & O & O & O & O & E_7 & O & O & O \\ O & O & O & O & E_7 & O & E_7 & O & O & O & O & O & O & O & O & E_7 & O & O \\ O & O & O & O & O & E_7 & O & E_7 & O & O & O & O & O & O & O & O & E_7 & O \\ O & O & O & E_7 & O & O & O & O & E_7 & O & O & O & O & O & O & O & O & E_7 \end{bmatrix} \cdot diag(R,R,R), R=\begin{bmatrix} G & F & F \\ F & F & G \\ F & G & F \\ F' & F' & F \\ F' & F & F' \\ F & F' & F' \end{bmatrix}, \quad (12)$$

где O — квадратная матрица порядка 7, состоящая из нулей. Таким образом, умножение матрицы J на вектор требует выполнения 12·7·3+18·7=378 операций сложения. При умножении матрицы J на вектор все 3 матрицы R могут умножаться на соответствующие отрезки вектора параллельно. Причем все строки внутри каждого из блоков, состоящего из семи соседних строк, всех матриц R и затем все такие строки последующей матрицы из факторизации могут умножаться на соответствующие отрезки векторов параллельно для повышения скорости обработки. Применив к матрице K перестановку блоков столбцов $\begin{pmatrix} 012345678 \\ 036147258 \end{pmatrix}$, получим матрицу, аналогичную по структуре матрице J, для которой может быть использована подобная факторизация. Поэтому при умножении матрицы K на вектор также потребуется выполнить 378 операций сложения.

Итак, суммарное количество аддитивных операций при вычислении векторно-матричного произведения для всех матриц A_i^*, B_i^*, а также A_i, B_i, $i=1,2$, согласно данному алгоритму, с использованием представленной оптимизирующей факторизации (10), (12), нового варианта БПА (8), (11) и принципа "двойки" равно 243+378=621. Выигрыш в числе операций по сравнению с прямым методом умножения составляет w=(63·62)/621≈6,290 раза, коэффициент сложности S=621/63≈9,857. Следует отметить, что выполнение в матрицах A_i, B_i перестановок строк и таких же перестановок столбцов в соответствии с КТО при внешнем упорядочении по первой координате, внутреннем упорядочении по второй координате: (0,0), (0,1), …, (0,8),…, (8,0), (8,1),…, (8,6), с последующим разделением данных матриц на 7 вертикальных блоков по 9 соседних столбцов и применение соответствующей оптимизирующей факторизации, даже с учетом нового варианта БПА и принципа "двойки", приводит к большему объему вычислений, чем в описанном здесь случае. Соответствующие коэффициенты сложности при этом приближенно равны 10,556 при 665 аддитивных операциях для матриц A_i и 10,222 при 644 аддитивных операциях для матриц B_i. Это обусловлено тем, что после применения теоремы оптимизирующей факторизации в блочно-диагональной матрице блоки, состоящие из 9 соседних столбцов, требуется делить еще на 3 вертикальных блока по 3 столбца, чтобы применить БПА для H_4 к матрице H_4', отличающейся от матрицы H_4 отсутствием столбца с нулевым номером.

Сравнительный анализ вычислительной сложности алгоритмов

В [2, 9] отмечается, что при использовании теорем оптимизирующей факторизации в общем случае не известен способ переупорядочения столбцов и строк матрицы, приводящий к оптимальному алгоритму, с другой стороны, учет тонкой структуры матрицы может привести к резкому сокращению объема вычислений. Последнее утверждение оказывается справедливым для матриц-циркулянтов и матриц инцидентности симметричных блок-схем КП Якоби типа Адамара с блоковыми длинами N=15, 63, как показывают вышеприведенные структурные алгоритмы векторно-матричного умножения. Одним из важнейших свойств сигнальных матриц, определяющим возможность факторизации со значительным сокращением вычислительных затрат, является связь с матрицами Адамара типа Сильвестра [1, 2]. Однако, как отмечается в [10], для перспективных нелинейных сигналов не известна связь их матриц с матрицами Адамара–Сильвестра и, следовательно, невозможна обработка на основе БПА.

Здесь же эта задача была решена для циркулянтных матриц и матриц инцидентности симметричных блок-схем КП Якоби типа Адамара с блоковыми длинами вида 2^r-1, и установлена связь данных матриц с матрицами Адамара типа Сильвестра при построении соответствующих быстрых алгоритмов векторно-матричного умножения.

В работе [9] приведен универсальный алгоритм факторизации прямоугольных бинарных матриц с элементами ±1, имеющий меньшие вычислительные затраты для циркулянтных матриц, чем двукратное преобразование Фурье при $N<1024$ и алгоритм Агарвала-Кули при $N<360$. Данный алгоритм основан на теореме оптимизирующей факторизации [2] и последовательном делении первого сомножителя факторизации на вертикальные блоки, состоящие из пар соседних блоков, полученных на предыдущем шаге, до тех пор, пока все сомножители разложения будут содержать не более 2 ненулевых элементов в каждой строке. В случае нечетного числа блоков последний блок остается не объединенным с другими. На первом шаге данного алгоритма в блоки объединяются попарно соседние столбцы. В [9] дано также значение верхней границы коэффициента сложности $S_{алг1}\le 3+N/4$ для бинарных квадратных матриц с числом строк $N\le 2^{15}$, причем можно дать более точную оценку: $S_{алг1}\le 2{,}75-3/N+N/4$. При сравнении для $N=15$ $S_2\approx 3{,}533$ алгоритма факторизации матриц A_1 и A_2, использующего (8), (9), с $S_{алг1}\le 6{,}3$ при более точной оценке получаем, что S_2 меньше верхней границы $S_{алг1}$ примерно в 1,783 раза, или на 43,921%. Сравнивая для $N=63$ $S\approx 9{,}857$ алгоритмов факторизации матриц A_1, A_2, B_1, B_2, использующих (8), (10)–(12), с $S_{алг1}\le 18{,}452$ при более точной оценке, получаем, что S меньше верхней границы $S_{алг1}$ примерно в 1,872 раза, или на 46,580%.

Согласно теореме оптимизирующей факторизации [2], процедура умножения факторизованной матрицы на вектор представляется в виде выполнения внутренней (умножение на вектор матриц-блоков) и внешней (сложение результатов внутренних вычислений) процедур. В работе [10] представлен алгоритм факторизации произвольных бинарных квадратных матриц с элементами ±1 на основе оптимизации блочного разбиения матриц и переупорядочения строк подматриц при выполнении внутренней факторизации по коду Грея, т.е. в таком порядке, чтобы любые две соседние строки отличались только одной координатой. Для длин $2^r<N<2^{r+1}$ при $3\le r\le 8$ оптимальный размер блока, согласно [10], может быть определен как $m=\lceil \log_2 N+0{,}5\rceil-1$, где $\lceil x\rceil$ – наименьшее ближайшее целое число к x. Оценка верхней границы коэффициента сложности вычисления векторно-матричного произведения с использованием алгоритма из [10]:

$$S_{алг2}\le \frac{2^{m-1}-2}{m}+\left\lfloor \frac{N}{m}\right\rfloor, \qquad (13)$$

где $\lfloor x\rfloor$ — наибольшее ближайшее целое число к x. Сравнение с известными ранее алгоритмами показывает, что использование данного алгоритма обеспечивает уменьшение оценки верхней границы сложности в некоторых случаях до 25%. Установлено, что с ростом размерности N значение $S_{алг2}$ приближается к значению верхней границы, причем для некоторых размерностей циркулянтов нелинейных бинарных сигналов эти значения практически совпадают. При сравнении для $N=15$ $S\approx 3{,}533$ алгоритма факторизации матриц A_1 и A_2, использующего (8), (9), с $S_{алг2}\le 5{,}667$ из (13) при $m=3$ получаем, что S_2 меньше верхней границы $S_{алг2}$ примерно в 1,604 раза, или на 37,657%. Сравнивая для $N=63$ $S\approx 9{,}857$ алгоритмов факторизации матриц A_1, A_2, B_1, B_2, использующих (8), (10)–(12), с $S_{алг2}\le 15{,}8$ из (13) при $m=5$ получаем, что S меньше верхней границы $S_{алг2}$ примерно в 1,603 раза, или на 37,614%.

Заключение

Установлена конечность множества численных значений блоковых длин вида 2^r-1 КП Якоби, соответствующих групповым разностным множествам типа Адамара. Исходя из общих замечаний о КП Якоби, были сделаны соответствующие заключения о тонких структурах и свойствах КП типа Адамара с блоковыми длинами $N=2^r-1$, а также их циркулянтных матриц и матриц инцидентности соответствующих симметричных блок-схем.

С использованием примитивных идемпотентов кольца полиномов над двоичным полем Галуа показано, что только КП Якоби при N=15 являются М-последовательностями, а соответствующие циклические коды – КМД. Приведены быстрые алгоритмы векторно-матричного умножения для циркулянтов КП Якоби с N=15, 63 и матриц инцидентности симметричных блок-схем, основанные на структурной связи данных матриц с матрицами Адамара типа Сильвестра и общей теореме оптимизирующей факторизации. Причем алгоритмы с использованием принципа "двойки" имеют наименьшую сложность и кроме выигрыша в вычислениях уменьшают количество обращений к памяти, хранящей промежуточные результаты, что приводит к реальному существенному сокращению времени декодирования при микропроцессорной реализации. Сравнительный анализ коэффициентов сложности показывает, что представленные алгоритмы с учетом принципа "двойки" позволяют решать задачи ЦОС с меньшими вычислительными затратами, чем алгоритмы факторизации бинарных матриц В.В. Лосева, С.В. Мальцева из [9] и Р.П. Богуша из [10].

THE OPTIMIZATION OF DIGITAL SIGNAL PROCESSING WITH THE USE OF STRUCTURAL ALGORITHMS FOR SOME JACOBI CODES MATRICES

E.D. STROINIKOVA

Abstract

Jacobi codes sequences connected with Hadamard difference sets and having block lengths $N=2^r-1$ are considered. It is established that the set of numerical values of such sequences block lengths is finite. Structural features and properties of these sequences and also of corresponding circulant codes matrices and incidence matrices of symmetric block-schemes are investigated. Fast algorithms of vector-matrix multiplication for given matrices which may be applied in multiprocessor systems of digital signal processing are produced. The use of a new factorization of Hadamard-Sylvester matrices and the principle of "two" guarantees the minimal quantity of calculations and a reduction of time disbursements.

Литература

1. *Лосев В.В.* Микропроцессорные устройства обработки информации. Алгоритмы цифровой обработки: Учеб. пособие для вузов. Минск, 1990.
2. *Дворников В.Д., Конопелько В.К., Липницкий В.А.* Теория и практика низкоскоростных кодов. Минск, 2002.
3. *Свердлик М.Б.* Оптимальные дискретные сигналы. М., 1975.
4. *Пелехатый М.И.* // Радиотехника и электроника. 1970. Т. 15, № 7. С. 1428–1439.
5. *Пелехатый М.И.* // Радиотехника и электроника. 1971. Т. 16, № 5. С. 788–796.
6. *Холл М.* Комбинаторика / Пер. с англ. М., 1970.
7. *Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А.* Теория кодов, исправляющих ошибки / Пер. с англ. М., 1979.
8. *Стройникова Е.Д.* // Вестн. Военной академии Республики Беларусь. 2004. № 4(5). С. 62–69.
9. *Лосев В.В., Мальцев С.В.* // Радиотехника и электроника. 1992. Т. 37, № 12. С. 2190–2198.
10. *Богуш Р.П.* Корреляционная обработка бинарных изображений и сигналов с использованием факторизации матриц: Дис. … канд. техн. наук. Новополоцк, 2001.