ՀԱՅԿԱԿԱՆ ՍՍՀ ԳԻՏՈՒԹՅՈՒՆՆԵՐԻ ԱԿԱԴԵՄԻԱՅԻ ԶԵԿՈՒՅՑՆԵՐ
ДОКЛАДЫ АКАДЕМИИ НАУК АРМЯНСКОЙ ССР
LXXIII 1981 2

УДК 519.6

МАТЕМАТИКА

А. К. Матевосян

# Быстрые алгоритмы вычисления положительно и отрицательно обернутых $(m_1, m_2 \ldots, m_n)$-сверток

(Представлено чл.-корр. АН Армянской ССР Р .Р.Варшамовым 24/III 1981)

1. Пусть $a=[a_0, a_1, \ldots, a_{N-1}]^T$ и $b=[b_0, b_1, \ldots, b_{N-1}]^T$ есть два $N$-мерных, $N=m_1 \cdot m_2 \cdot \ldots \cdot m_n$, комплексных вектора, а $i \underset{m}{\ominus} j$—поразрядное вычитание по модулю чисел $i$ и $j$ в системе счисления с основаниями $m_1, m_2, \ldots, m_n$ [1].

Определение 1. *Положительно обернутой $(m_1, m_2, \ldots, m_n)$-сверткой векторов $a$ и $b$ назовем такой вектор $c=[c_0, c_1, \ldots, c_{N-1}]^T$, что*

$$c_i=\sum_{j=0}^{i} a_j \bar{b}_{i \underset{m}{\ominus} j}+\sum_{j=i+1}^{N-1} a_j \bar{b}_{i \underset{m}{\ominus} j}. \tag{1}$$

Замечание 1. Понятие положительно обернутой $(m_1, m_2, \ldots, m_n)$-свертки совпадает:

а) при $n=1$ с циклической положительно обернутой сверткой, введенной А. Ахо, Дж. Хопкрофтом, Дж. Ульманом [2];

б) при $n>1$ с $m$-сверткой, введенной в работе [1] А. М. Трахтманом и В. А. Трахтманом;

в) при $n=2$ $m$-свертка переходит в диадную свертку [1].

Определение 2. *Отрицательно обернутой $(m_1, m_2, \ldots, m_n)$-сверткой векторов $a$ и $b$ назовем такой вектор $d=[d_0, d_1, \ldots, d_{N-1}]^T$, что*

$$d_i=\sum_{j=0}^{i} a_j \bar{b}_{i \underset{m}{\ominus} j}-\sum_{j=i+1}^{N-1} a_j \bar{b}_{i \underset{m}{\ominus} j}. \tag{2}$$

Замечание 2. Понятие отрицательно обернутой $(m_1, m_2, \ldots, m_n)$-свертки при $n=1$ совпадает с циклической отрицательно обернутой сверткой, введенной в работе [2] А. Ахо, Дж. Хопкрофтом и Дж. Ульманом.

Из задач прикладного характера [1,3,4] возникает задача построения алгоритмов вычисления $(m_1, m_2, \ldots, m_n)$-сверток, требующих выполнения существенно меньшего числа операций по сравнению с общепринятым алгоритмом умножения вектора на матрицу, требующим $N^2$ операций умножения и $N(N-1)$ операций сложения.

В работах [2,5,6], [2] и [1] построены алгоритмы вычисления соответственно циклической, отрицательно обернутой циклической и $m$-сверток за число операций $\ll N^2$. Большинство указанных быстрых алгоритмов базируются на методе быстрого преобразования Фурье (БПФ) [7] и его обобщении—быстром преобразовании по системам Виленкина—Крестенсона (БПВК) [1]. Отметим также, что единственным оптимальным алгоритмом по числу операций умножения является алгоритм вычисления диадной свертки, основанный на быстром преобразовании Уолша (БПУ) [1] и требующий $N$ операций умножения и $3N\log_2 N$ операций сложения.

В настоящей работе доказана теорема о связи между положительно и отрицательно обернутыми $(m_1, m_2, \ldots, m_n)$-свертками, из которой, в частности, вытекает теорема, доказанная А. Ахо, Дж. Хопкрофтом и Дж. Ульманом ([2], стр. 289); предлагается единый подход к рекуррентному построению быстрых алгоритмов вычисления положительно и отрицательно обернутых $(m_1, m_2, \ldots, m_n)$-сверток, превосходящих по скорости известные алгоритмы; найдено необходимое и достаточное условие существования алгоритмов вычисления $(m_1, m_2, \ldots, m_n)$-сверток. Построен алгоритм вычисления циклической положительно обернутой свертки векторов длины $N=2^n$, превосходящий по скорости выполнения почти вдвое алгоритм, приведенный в работе [2].

Перейдем к изложению результатов настоящей работы.

2. Обозначим через $V$ оператор, ставящий в соответствие вектору $a$ с компонентами $a_k$, $k=0, 1, \ldots, N-1$, $N=m_1 \cdot m_2 \cdot \ldots \cdot m_n$, вектор $V[a]$ с компонентами $a_k \cdot v_j^{k_{n-j}}$, $k=0, 1, \ldots, N-1$, если $m_1 \ldots m_{j-1} \leqslant k \leqslant m_1 \ldots m_j - 1$, где $k_j$—разрядные коэффициенты числа $k$ в системе счисления с основаниями $m_1, m_2, \ldots, m_n$, а $v_j = \exp(-i\pi/m_j)$.

Теорема 1. *Пусть вектор $z$ есть положительно (отрицательно) обернутая $(m_1, m_2, \ldots, m_n)$-свертка $x$ и $y$, тогда вектор $V[z]$ есть отрицательно (положительно) обернутая $(m_1, m_2, \ldots, m_n)$-свертка векторов $V[x]$ и $\overline{V[y]}$.*

Из теоремы 1 как частный случай, при $n=1$, вытекает теорема, 7.2 [2].

Следствие 1. *Пусть построен алгоритм вычисления положительно (отрицательно) обернутой $(m_1, m_2, \ldots, m_n)$-свертки с характеристиками $D_0$ (число операций умножения) и $D_1$ (число операций сложения), тогда можно построить алгоритм вычисления отрицательно (положительно) обернутой $(m_1, m_2, \ldots, m_n)$-свертки с характеристиками $D_0+3(N-1)$ и $D_1$.*

Анализ всех известных быстрых алгоритмов вычисления сверток показывает, что они имеют следующую структуру:

$$\left.\begin{array}{l}\text{этап 1—вычисление векторов:}\\ A=Z_1\cdot a^T,\quad B=Z_2\cdot b^T,\\ \text{этап 2—поэлементное умножение векторов } A \text{ и } B:\\ C_l=A_l\cdot B_l,\\ \text{этап 3—вычисление искомого вектора } c:\\ c=Z_3\cdot C^T.\end{array}\right\} \tag{3}$$

Пусть $Z_i=\{z^i_{kj}\}$, $i=1, 2$, есть матрицы порядка $p\times N$, а $Z_3=\{z^3_{kj}\}$—порядка $N\times p$, $I_N$—единичная матрица порядка $N$, $\otimes$—кронекерово произведение ([1]). Возникает вопрос: каким условиям должны удовлетворять матрицы $Z_i$, чтобы подстановка их в (3) приводила к алгоритму вычисления $(m_1, m_2, \ldots, m_n)$-свертки?

Теорема 2. *Для того чтобы матрицы $Z_i$ приводили к алгоритму вычисления положительно обернутой $(m_1, m_2, \ldots, m_n)$-свертки, необходимо и достаточно, чтобы*

$$\sum_{k=1}^{p} z^1_{kj} z^2_{ks} z^3_{ik} = \begin{cases} 1, & \text{если } i\underset{m}{\ominus} j=s,\\ 0, & \text{если } i\underset{m}{\ominus} j\neq s.\end{cases} \tag{4}$$

Пусть матрицы $Z_i(m_k)$, $i=1, 2, 3$, $k=1, 2, \ldots, n$, приводят к алгоритмам вычисления циклической положительно обернутой свертки векторов длины $m_k$ с характеристиками $D_0(m_k)$ и $D_1(m_k)$. Обозначим через $Z_i$, $i=1, 2, 3$, следующие матрицы:

$$\left.\begin{array}{l} Z_1=\left[\prod\limits_{l=n-1}^{1} I_{p_{n-l+1}\ldots p_n}\otimes Z_1(m_{n-l})\otimes I_{m_1\ldots m_{n-l-1}}\right]\cdot\left[Z_1(m_n)\otimes I_{N/m_n}\right],\\ Z_2=\left[\prod\limits_{l=n-1}^{1} I_{p_{n-l+1}\ldots p_n}\otimes Z_2(m_{n-l})\otimes I_{m_1\ldots m_{n-l-1}}\right]\cdot\left[Z_2(m_n)\otimes I_{N/m_n}\right],\\ Z_3=\left[Z_3(m_n)\otimes I_{N/m_n}\right]\cdot\left[\prod\limits_{l=1}^{n-1} I_{p_{n-l+1}\ldots p_n}\otimes Z_3(m_{n-l})\otimes I_{m_1\ldots m_{n-l-1}}\right]. \end{array}\right\} \tag{5}$$

Теорема 3. *Матрицы $Z_i$, $i=1, 2, 3$, при подстановке их в* (3) *приводят к алгоритму вычисления положительно обернутой $(m_1, m_2, \ldots, m_n)$-свертки с характеристиками* $D_0=\prod\limits_{k=1}^{n} D_0(m_k)$ *и* $D_1=\sum\limits_{k=1}^{n} D_1(m_k)\cdot\left[\prod\limits_{j>k} D_0(m_j)\right]\cdot\left[\prod\limits_{j<k} m_1\ldots m_j\right]$.

Разложение (5) позволяет строить быстрореализуемые на ЭВМ процедуры выполнения алгоритма.

Замечание 3. Если матрицы $Z_i(m_k)$ являются матрицами Фурье порядка $m$, то алгоритм теоремы 3 совпадает с алгоритмом вычисления $m$-свертки, приведенным в работе ([1]), а разложение (5) задает алгоритм БПВК.

Перейдем к рассмотрению циклической свертки векторов длины $N$. Если $N=p_1 \cdot p_2 \ldots p_n$, где числа $p_i$ попарно взаимно-просты, то алгоритм вычисления положительно обернутой циклической свертки сводится к алгоритму вычисления $(p_1, p_2, \ldots p_n)$-свертки, рассмотренному выше. Если $N=p^n$, то, как и в случае $(m_1, m_2, \ldots, m_n)$-сверток, циклическую свертку векторов длины $p^n$ можно представить в виде комбинации циклических сверток векторов длины $p^{n-1}$. Пусть построен алгоритм вычисления циклической свертки векторов длины $p$ с характеристиками $D_0(p)$ и $D_1(p)$, а $A(p)$ и $B(p)$ обозначают константы

$$A(p)=D_1(p)+\frac{D_1(p)+p^2-p}{D_0(p)+(p^2-3p)/2}\cdot p,$$

$$B(p)=\frac{D_1(p)+p^2-p}{D_0(p)+(p^2-3p)/2}.$$

Справедлива

Теорема 4. *Существует алгоритм вычисления циклической свертки векторов длины $p^n$ с характеристиками*

$$D_0(p^n)=D_0(p)\cdot\left(D_0(p)+\frac{p^2-p}{2}\right)^{n-1}$$

*и*

$$D_1(p^n)=A(p)\cdot\left(D_0(p)+\frac{p^2-p}{2}\right)^{n-1}-B(p)\cdot p^n.$$

Алгоритм теоремы 4 обобщает на случай произвольного $p$ метод, приведенный в работе [6] для $p=2$. Для оценки построенного алгоритма выберем $p=3$ и воспользуемся алгоритмом С. Винограда [5] с характеристиками $D_0(3)=4$ и $D_1(3)=21$. Тогда алгоритм теоремы 4 будет иметь характеристики $D_0(3^n)=4\cdot 7^{n-1}$ и $D_1(3^n)=42\cdot 7^{n-1}-7\cdot 3^n$ и будет эффективнее алгоритма, основанного на БПФ для $N\leqslant 243$ и для $N\leqslant 2.187$, если свертываемые вектора действительны.

Перейдем к циклической свертке векторов длины $N=2^n$.

Теорема 5. *Существует алгоритм вычисления положительно обернутой циклической свертки векторов длины $2^n$ с характеристиками $D_0(2^n)=(3n-4)\cdot 2^{n-1}+3$ и $D_1(2^n)=3n2^n$.*

Доказательство теоремы 5 основано на том, что положительно обернутая циклическая свертка векторов длины $2^n$ сводится к одной положительно обернутой свертке векторов длины $2^{n-1}$ и одной отрицательно обернутой циклической свертке векторов длины $2^{n-1}$.

Построенные в работах [2] и [6] алгоритмы вычисления циклической свертки векторов длины $2^n$ имеют характеристики $D_0(2^n)=12+(3n-8)2^n$, $D_1(2^n)=3n2^n$ и $D_0=2\cdot 3^{n-1}$, $D_1=22\cdot 3^{n-1}-8\cdot 2^n$ соответственно, причем второй алгоритм эффективнее первого по числу операций умножения для $N\leqslant 128$, но требует выполнения несколько большего числа операций сложения. Алгоритм теоремы 5 эффективнее почти вдвое по числу операций умножения первого из вышеуказанных алгоритмов при одинаковом числе операций сложения и эффективнее второго алгоритма при $N \geqslant 64$.

Замечание 4. Все алгоритмы, построенные в настоящей работе, имеют вид (3). Отметим также, что матрицы $Z_i$ алгоритма теоремы 5 совпадают по структуре с матрицами Уолша.

Автор выражает признательность С. С. Агаяну за постановку задачи и помощь при выполнении работы.

Вычислительный центр
Академии наук Армянской ССР
и Ереванского государственного университета

Ա. Կ. ՄԱԹԵՎՈՍՅԱՆ

## Դրական և բացասական $(m_1, m_2, \dots, m_n)$-փաթեթների հաշվման արագ ալգորիթմներ

Դիցուք $a=[a_0, a_1, \dots, a_{N-1}]^T$ և $b=[b_0, b_1, \dots, b_{N-1}]^T$ $N=m_1 \cdot m_2 \cdot \dots \cdot m_n$, կոմպլեքս վեկտորներ են, $i \underset{m}{\ominus} j$—հանում ըստ կարգի։ $a$ և $b$ վեկտորների դրական (բացասական) $(m_1, m_2, \dots, m_n)$-փաթեթ կկոչենք $c=[c_0, c_1, \dots, c_{N-1}]^T$ վեկտոր, որի կոորդինատները որոշվում են հետևյալ կերպ։

$$c_i=\sum_{j=0}^{i} a_j \bar{b}_{i \underset{m}{\ominus} j} \pm \sum_{j=i+1}^{N-1} a_j \bar{b}_{i \underset{m}{\ominus} j}$$

Աշխատանքում առաջարկվում է դրական և բացասական $(m_1, m_2, \dots, m_n)$-փաթեթների հաշվման արագ ալգորիթմների կառուցման ընդհանուր մեթոդ։ Կառուցված ալգորիթմները գերազանցում են իրենց արագությամբ փաթեթների հաշվման հայտնի արագ ալգորիթմները։ Մասնավորապես, $N=2^n$ չափանի վեկտորների ցիկլիկ փաթեթի հաշվումը երկու անգամ ավելի արագ է կատարվում, քան ընդունված Ֆուրյեի արագ ձևափոխության վրա հիմնված ալգորիթմով։

### ЛИТЕРАТУРА—ԳՐԱԿԱՆՈՒԹՅՈՒՆ

[1] *А. М. Трахтман, В. А. Трахтман*, Основы теории дискретных сигналов на конечных интервалах, Сов. радио, М., 1975. [2] *А. Ахо, Дж. Хопкрофт, Дж. Ульман*, Построение и анализ вычислительных алгоритмов, Мир, М., 1979. [3] *А. Розенфельд*, Распознавание образов и обработка изображений, Мир, М., 1975. [4] *Л. Рабинер, Б. Гоулд*, Теория и применение цифровой обработки сигналов, Мир, М., 1978. [5] *S. Winograd*, Math. of Computation, v. 30, 141 (1978). [6] *D. Pitassi*, EMC—16, № 3 (1971). [7] *J. Cooley, J. Tuckey*, Math. Comp, v. 19 (1965).