ТЕОРЕТИКО-ЧИСЛОВОЕ ПРЕОБРАЗОВАНИЕ В ВЫЧИСЛЕНИЯХ С ПРОИЗВОЛЬНОЙ ТОЧНОСТЬЮ

Е.В. Быч, С.А. Семериков
г. Кривой Рог, Криворожский государственный педагогический университет

Умножение двух цифровых строк традиционным ручным методом (в «столбик») – достаточно медленная операция: при умножении двух строк длины N сомножители перемножаются поразрядно, что требует $O(N^2)$ операций. Тем не менее, *все* арифметические операции над числами длины N могут фактически быть выполнены за $O(N*\log N*\log\log N)$ вычислений.

Широко используемым приемом является то, что умножение, по существу – свертка цифр сомножителей, сопровождающаяся некоторой разновидностью переноса. Рассмотрим, например, два способа записи вычисления 456*789:

```
  456                      4  5  6
* 789                    * 7  8  9
 4104                     36 45 54
3648                   32  40 48
3192                28 35  42
------             ------------------
359784             28 67 118 93 54
                3  5  9  7  8  4
```

Слева показан стандартный метод умножения, при котором для получения результата складываются три отдельных коротких (одноразрядных) умножения полных сомножителей (на 9, 8 и 7). Справа показан другой метод (иногда используемый для вычислений «в уме»), при котором сначала вычисляются все одноразрядные перекрестные произведения (например, 8*6=48), которые затем складываются в столбцы для получения неполного результат с переносом (28; 67; 118; 93; 54). Для записи результата проходим справа налево, записывая один наименее значащий разряд и, перенося, старшие в сумму слева (например, 93+5=98, 8 пишем, 9 переносим).

Легко увидеть, что в этом методе суммы в столбцах – компоненты свертки цифровых строк; например, 118=4*9+5*8+6*7. Согласно алгоритму вычисления свертки двух последовательностей [1] быстрым преобразованием Фурье (БПФ), над каждой

последовательностью выполняется БПФ, затем они перемножаются, и над результатом выполняется обратное БПФ. При этом, так как преобразования связаны с плавающей арифметикой, нам нужна достаточная точность для того, чтобы получить точное целое значение каждой составляющей результата при наличии ошибки округления.

Дискретное преобразование Фурье (ДПФ) последовательности $x(N)$ длины N определено как

$$X(k)=\sum_{n=0}^{N-1}x(n)W^{kn}\,. \tag{1}$$

В обычном преобразовании Фурье W определено как

$$W=e^{-\frac{2\pi i}{N}}\,. \tag{2}$$

Обратное преобразование:

$$x(n)=\frac{1}{N}\sum_{k=0}^{N-1}X(k)W^{-kn} \tag{3}$$

Нас интересует не само преобразование, а его свертка. Циклическая свертка двух последовательностей $a(n)$ и $b(n)$ длины N определена как

$$c(n)=a(n)*b(n)=\sum_{k=0}^{N-1}a(k)b(n-k)\,. \tag{4}$$

При этом $a(n)$ и $b(n)$ рассматриваются как циклические последовательности, т.е. $b(-1)=b(N-1)$ и т.д. Теперь свертку можно более эффективно вычислить в обратном пространстве (пространстве Фурье), в котором свертка сводится к линейному (поэлементному) умножению. Для того чтобы вычислить свертку, выполняют Фурье-преобразование сворачиваемых последовательностей, перемножают соответствующие элементы образов и выполняют обратное преобразование.

Прямое (1) и обратное (3) ДПФ может быть вычислено с использованием БПФ. Если $A(k)$ и $B(k)$ – Фурье-преобразования последовательностей $a(n)$ и $b(n)$, то Фурье-преобразование свертки $c(n)$

$$C(k)=A(k)B(k) \tag{5}$$

и $c(n)$ можно вычислить обратным преобразованием. Из (1)

$$C(k)=A(k)B(k)=\sum_{i=0}^{N-1}a(i)W^{ik}\sum_{j=0}^{N-1}b(j)W^{jk}\,. \tag{6}$$

Подставляя (3), получим:

$$\begin{aligned} c(n) &= \frac{1}{N}\sum_{k=0}^{N-1} C(k) W^{-kn} \\ &= \frac{1}{N}\sum_{k=0}^{N-1} W^{-kn} \sum_{i=0}^{N-1} A(i) W^{ik} \sum_{j=0}^{N-1} B(j) W^{jk} \\ &= \sum_{i=0}^{N-1} A(i) \sum_{j=0}^{N-1} B(j) \frac{1}{N} \sum_{k=0}^{N-1} W^{k(i+j-n)} . \end{aligned} \tag{7}$$

Очевидно, что (7) и (4) совпадают тогда и только тогда, когда

$$\frac{1}{N}\sum_{k=0}^{N-1} W^{k(i+j-n)} = \delta(i+j-n) \tag{8}$$

или

$$\sum_{k=0}^{N-1} W^{k(i+j-n)} = N\delta(i+j-n), \tag{8′}$$

где $\delta(n)$ – дискретная дельта-функция (1 при $n=0$ и 0 в противном случае), поэтому сумма в (8′) равна N при $j=n-i$ и 0 в противном случае. Рассмотрим сумму

$$\sum_{k=0}^{N-1} W^{jk} . \tag{9}$$

Очевидно, что при $j=0$ она равна N. В противном случае помножим ее на $(1-W^j)$, результат должен быть равен нулю:

$$\begin{aligned} (1-W^j)\sum_{k=0}^{N-1} W^{jk} &= W^0 + W^j + W^{2j} + \ldots + W^{j(N-1)} \\ &\quad - W^j - W^{2j} - \ldots - W^{j(N-1)} - W^{jN} \\ &= 1 - W^{jN} = 0 \end{aligned} \tag{10}$$

Отсюда $W^{jN}=1$. Так как j было произвольным (фактически $j\neq 0 (\mathrm{mod}\ N)$), то, очевидно, что W должно быть корнем из единицы [2]. В «нормальном» Фурье-преобразовании оно определяется из уравнения (2). Если W ищется как целое или некоторое рациональное или действительное число, этот критерий, несомненно, не может быть удовлетворен. Тем не менее, подходящее W можно найти в кольце вычетов по модулю p, когда p является простым числом вида $p=kN+1$, где k – целое, N – длина преобразования [3]. В этом случае преобразование Фурье называется теоретико-числовым преобразованием (ТП) [4].

Теоретико-числовое преобразование – это обычное дискретное преобразование Фурье, но в другой числовой области. Большинство формул и алгоритмов, применимых к ДПФ, верны и для ТП. Наиболее интересно то, что ТП может быть вычислено, используя «быстрый» алгоритм (быстрое теоретико-числовое преобразование, БТП) подобно тому, как ДПФ может быть вычислено посредством быстрого преобразования Фурье (БПФ). При этом W теперь целое и все вычисления проводятся по модулю p.

Теоретико-числовое преобразование имеет следующие преимущества перед комплексным преобразованием Фурье:

– преобразование действительное;
– поскольку все используемые числа – всегда целые, ошибки округления отсутствуют, что дает возможность преобразования очень длинных последовательностей (порядка $N=2^{46}$) со стандартным 53-битовым разрешением (при использовании целой части типа double);
– вычисления могут быть проделаны «по частям» с восстановлением конечного результата по Китайской теореме вычетов [5].

Недостатки ТП:

– преобразование само по себе бесполезно – оно не имеет физического смысла в отличие от преобразования Фурье, и по большей части полезно только для свертки;
– длинная целая арифметика в большинстве компьютеров медленнее, чем арифметика с плавающей запятой.

1. William H. Press, Saul A. Teukolsky, William T. Vetterling, Brian P. Flannery. Numerical Recipes in C: The Art of Scientific Computing, 2nd Edition. – Cambridge–New York: Cambridge University Press, 1997. – 1009 p.
2. Уткіна С.В., Наришкіна Л.С. Алгебра і числові системи: Навчальний посібник. – К.: Вища школа, 1995. – 304 с.
3. James H. McClellan. Number Theory in Signal Processing. – Englewood Cliffs: Prentice Hall, 1979. – 680 p.
4. Mikko Tommila. Apfloat: A C++ High Performance Arbitrary Precision Arithmetic Package. Version 1.50, 1998.
5. Henry J. Nussbaumer. Fast Fourier Transform and Convolution Algorithms, 2nd ed. – New York: Springer-Verlag, 1982. – 442 p.