ОБ ЭФФЕКТИВНОСТИ АЛГОРИТМОВ РЕЙДЕРА-ВИНОГРАДА

Владимир Михайлович Чернов (главный научный сотрудник, e-mail: vche@smr.ru)
Учреждение Российской академии наук Институт систем обработки изображений РАН

Аннотация

Доказывается факт существования «исключительных» простых чисел, для которых алгоритмы Рейдера-Винограда вычисления дискретного преобразования Фурье и/или свертки соответствующей длины являются неэффективными. Приводятся достаточные условия «исключительности» в аналитической форме.

Ключевые слова: дискретное преобразование Фурье, циклическая свертка, алгоритм Рейдера-Винограда, вычислительная сложность.

Введение

Хорошо известно [1], что для некоторых простых $p = N$ существуют быстрые алгоритмы дискретного преобразования Фурье (БА ДПФ) с минимальным числом умножений. Синтез таких алгоритмов, как показал Рейдер [2]), сводится к эффективному вычислению циклической свертки длины $(p-1)$. Вычисление свертки эквивалентно параллельному вычислению произведений некоторых полиномов по модулям *циклотомических* полиномов $P_1(t)$, …, $P_d(t)$, где $P_1(t)\ \ldots P_d(t) = t^{p-1} - 1$.

Полуэвристическое нахождение формул «экономного» умножения в полиномиальных кольцах $(\bmod P_j(t))$ является основой метода Винограда [3],[4], в рамках которого получены абсолютные *нижние* оценки мультипликативной сложности БА ДПФ и лишь для некоторых небольших простых чисел p синтезированы БА с хорошими вычислительными характеристиками [5]. Способ сведения ДПФ с простым числом отсчетов к циклической свертке, использующий цикличность мультипликативной группы простого конечного поля, предложен Ч.Рейдером в 1968 г. Без какой-либо общей теории быстрые алгоритмы коротких сверток были впервые описаны в [3]. В 1976 г. Ш.Виноград [4] предложил метод построения алгоритмов коротких сверток и доказал теоремы о сложности рассмотренных алгоритмов свертки для полей комплексных и вещественных чисел. К сожалению, некритическое прочтение работ Ш.Винограда сформировало у определенной части пользователей представление об оптимальности, неулучшаемости БА Винограда и их существовании для всех простых p. Сам Ш.Виноград показал зависимость сложности вычисления свертки от арифметических свойств поля, в котором производятся вычисления. В настоящее время оптимальные алгоритмы ДПФ известны для простых $p = 2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19$ (см., например, [5]).

В данной статье показывается, что уже традиционное сведение вычисления ДПФ простой длины p к свертке длины $(p-1) = s$, в случае, когда s «плохо» факторизуется, может приводить к «быстрым» алгоритмам, сложность которых выше тривиального (непосредственного) вычисления ДПФ.

1. Некоторые примеры

Пример 1. Рассмотрим вычисление дискретной круговой свертки

$$z(m) = (x * y)(m) = \sum_{n=0}^{p-1} x(n)\ \ y(m-n) \qquad (1)$$

вещественных последовательностей с периодом p=47. Пусть $M(N)$ и $C(N)$ – мультипликативные сложности вычисления N-точечного ДПФ вещественного массива и N-точечной круговой свертки вещественных последовательностей, соответственно; $C^*(N)$ - мультипликативная сложность вычисления свертки вещественной и комплексной последовательностей. Примем типичное для БА Рейдера-Винограда соглашение, что вычисление ДПФ комплексного массива требует в два раза больше умножений, чем вещественного [1]. Будем также считать, что умножение комплексных чисел реализуется посредством трех вещественных умножений.

1. Вычисление 47-точечной свертки по стандартной спектральной схеме требует вычисления двух 47-точечных ДПФ вещественных массивов, одного (обратного) ДПФ комплексного массива и $3 \cdot 47 = 141$ вещественных умножений для реализации умножения 47 спектральных компонент. Таким образом, справедливо равенство:

$$C(47) = 4M(47) + 141. \qquad (2)$$

2. Вычисление 47-точечного ДПФ, согласно основной идее метода Рейдера, сводится к вычислению 46-точечной свертки вещественной с комплексной последовательностью значений базисных функций ДПФ, что предполагает, по крайней мере, вычисление двух 23-точечных сверток функций указанного вида. Поэтому из (2) следует

$$C(47) = 2 \cdot 4 \cdot C^*(23) + 141.$$

3. Так как число 23 также простое, то вычисление 23-точечных сверток опять сводится к вычислению 23-точечных ДПФ и дополнительным умножениям спектральных компонент. Так как ДПФ подпоследовательностей значений базисных функций 47-точечного ДПФ могут быть выполнены заранее, то справедливо равенство

$$C^*(23) = 3M(23) + 3 \cdot 23,$$

откуда, с аналогичной аргументацией, получаем:

$$
\begin{aligned}
&C(47)\geq\\
&\geq 24M(23)+141+3\cdot 8\cdot 23\geq 693+48\ \ C^*(11)\geq\\
&\geq 693+48\left(3M(11)+33\right)=2277+144\ \ C^*(10)\geq\\
&\geq 2277+288\ \ C(5).
\end{aligned}
\tag{3}
$$

Лучший из известных алгоритмов вычисления 5-точечной свертки содержит 10 вещественных умножений [6]. Поэтому из (3) следует $C(47)\geq 5157$. В то же время, прямой метод вычисления правой части равенств (1) для $m=0,\ \ldots,\ 46$ требует $47\cdot 47=2209$ умножений, то есть приблизительно в 2 раза меньше. Основными причинами парадоксального результата в рассмотренном выше примере является существование «достаточно длинной» цепочки простых чисел

$$
\begin{aligned}
&p_1=5,\ p_2=2p_1+1=11,\ p_3=2p_2+1=23,\\
&p_4=2p_3+1=47
\end{aligned}
\tag{4}
$$

и практически безальтернативная необходимость вычисления свертки простой длины спектральными методами. Общий результат о «исключительных» простых числах p, для которых, по всей видимости, не существует удовлетворительных алгоритмов вычисления ДПФ и свертки длины p, описывается следующим утверждением.

Теорема 1. *Пусть p_0 - простое, $d_0,\ \ldots,\ d_k$ - такие натуральные числа, что $p_{t+1}=d_t p_t+1$ - также простые числа. Пусть $w=d_k\ldots\ d_0p_0$. Тогда справедливо неравенство*

$$
M(p_{k+1})\geq\frac{w}{\max\limits_{0\leq j\leq k}\{d_j\}}\left(2\cdot 4^k-1\right).
\tag{5}
$$

Доказательство. Аргументация аналогична рассуждениям Примера 1. Для любого $t=1,\ \ldots,\ k$ справедливы неравенства:

$$
M(p_{t+1})=C^*(d_tp_t)\geq d_tC^*(p_t)\geq 4d_tM(p_t)+3p_t\ .
\tag{6}
$$

Кроме того, для $t=0$ аналогично (6) имеем

$$
M(p_1)=C^*(d_0p_0)\geq d_0C^*(p_0)\geq 2d_0C(p_0).
\tag{7}
$$

Нижние оценки Винограда для $C(p_0)$ имеют вид $C(p_0)\geq 2p_0-\tau$, где τ - число неприводимых многочленов $P_j(z)$ в разложении многочлена Рейдера [1]:

$$
z^{p_0-1}-1=P_1(z)\ldots P_\tau(z).
\tag{8}
$$

Число τ зависит от поля, над которым рассматривается разложение (8) (см., например [2]), но в любом случае $\tau\leq p_0$. Поэтому $C(p_0)\geq p_0$.

Утверждение теоремы получается редукцией неравенства (6) с учетом соотношений (7)-(8) и очевидного неравенства $p_{t+1}\leq d_td_{t-1}\ldots d_0p_0$.

Действительно

$$
\begin{aligned}
&M(p_{k+1})\geq 4d_kM(p_k)+3p_k\geq\\
&\geq 4d_kM(p_k)+3d_{k-1}\ldots d_0p_0\geq\\
&\geq 4^2d_kd_{k-1}M(p_{k-1})+\\
&+4\cdot 3d_kd_{k-2}\ldots d_0p_0+3d_{k-1}\ldots d_0p_0\geq\\
&\geq 4^k\cdot 3d_kd_{k-1}\ldots d_1M(p_1)+\\
&+3\sum_{s=0}^{k-1}4^s\left(d_{k-s}\right)^{-1}d_k\ldots d_0p_0\geq\\
&\geq\frac{w}{\max\limits_{0\leq j\leq k}\{d_j\}}\left(2\cdot 4^k-1\right).
\end{aligned}
$$

Проводимое ниже следствие дает достаточно грубые, но легко проверяемые неравенства, характеризующее «исключительные» простые числа, для которых, как и в Примере 1, последовательное применение метода Рейдера приводит к алгоритмам ДПФ (или свертки), мультипликативная сложность которых выше, чем при непосредственном вычислении соответствующих сумм.

Следствие 1. Пусть p_0 - простое, $d_0,\ \ldots,\ d_k$ - такие натуральные числа, что $p_{t+1}=d_tp_t+1$ - также простые числа.

Если справедливо неравенство

$$
\frac{6k-1}{4}\geq\log_2 p_{k+1},
\tag{9}
$$

то справедливо и неравенство

$$
M(p_{k+1})\geq 2p_{k+1}^2.
\tag{10}
$$

Доказательство. Так как

$$
\max_{0\leq j\leq k}\{d_j\}\leq\frac{w}{p_0\,2^k},
$$

то

$$
\frac{w}{\max\limits_{0\leq j\leq k}\{d_j\}}\ \left(2\cdot 4^k-1\right)\geq p_0\,2^k\left(2\cdot 4^k-1\right)\geq 2\cdot 2^k\cdot 4^k-2^k.
$$

Поэтому из неравенства

$$
8^k\ \geq\ p_{k+1}^2+2^k
\tag{11}
$$

следует неравенство (5). Но

$$
\begin{aligned}
&\log_2\left(p_{k+1}^2+2^k\right)=\\
&=2\log_2 p_{k+1}+\log_2\left(1+\frac{2^k}{p_{k+1}^2}\right)\leq 2\log_2 p_{k+1}+\frac{1}{2},
\end{aligned}
$$

откуда легко следует (6).

Аналогичное неравенство справедливо и для вычисления p-точечной свертки при «исключительных» простых p.

Следствие 2. Пусть p_0 - простое, $d_0,\ \ldots,\ d_k$ - такие натуральные числа, что $p_{t+1}=d_tp_t+1$ - также простые числа, $k\geq 4$. Тогда, если справедливо неравенство

$$
\frac{6k+5}{4}\geq\log_2 p_{k+1},
\tag{12}
$$

то справедливо и неравенство

$$C(p_{k+1}) \geq p_{k+1}^2. \qquad (13)$$

Доказательство. В силу неравенства

$$C(p_{k+1}) = 4 \;\; C(p_{k+1}) + p_{k+1} \geq 4 \;\; M(p_{k+1}),$$

Примера 1, доказательство неравенства (13) проводится аналогично доказательству неравенства (10) предыдущего следствия.

Пример 2. Пусть $p_0 = 2$; $p_{t+1} = d_t p_t + 1$, где $d_0 = 2$, $d_1 = 2$, $d_2 = 8$, $d_3 = d_4 = d_5 = d_6 = d_7 = 2$. Тогда $p_8 = 2879$ - простое число, все p_t $(t = 0, \ldots, 7)$ также простые. Неравенство (12) в этом случае выполняется:

$$\frac{6k+5}{4} = 11,75 \geq 11,55 \geq \log_2 2879.$$

2. О плотности исключительных простых чисел в натуральном ряду

Анализируя вышесказанное, автор считает возможным высказать предположение, что «плохих» простых чисел, которые порождают такие натуральные *N*, что для этих длин не существует эффективных алгоритмов вычисления ДПФ и свертки, бесконечно много, но встречаются они весьма редко. Первая часть предположения базируется исключительно на субъективном авторском мнении.

Гипотеза. *Существует бесконечно много конечных множеств натуральных чисел* $d_0, \ldots, d_k$ *и таких простых* p_0, *что числа* $p_{t+1} = d_t p_{t+1}$ *также являются простыми, причем для* p_{k+1} *выполняются неравенства* (9)-(10) *или* (12)-(13).

Вторая часть предположения (о редкости «плохих» простых) базируется на вполне определенных количественных результатах.

Определение. Если простое p таково, что число $q = 2p+1$ также простое, то число p называется простым числом Софи Жермен.

Простые числа (4) как раз и являются простыми Софи Жермен. Первыми такими простыми являются числа 2, 3, 5, 11, 23, 29, 41, 53, 83, 89, 113, 131. Конечно или бесконечно множество простых Софи Жермен в настоящее время неизвестно. Известна только гипотетическая асимптотическая оценка количества $S(N)$ простых Софи Жермен, на превосходящих данного N:

$$S(N) \sim 2C_2 \frac{N}{(\ln N)^2}, \qquad (14)$$

где $C_2 \approx 0,6601618158...$ - так называемая «константа простых близнецов». Оценка (14) достаточно хорошо согласуется с результатами численных экспериментов [10]-[12].

Разумеется, даже в случае справедливости оценки (14) нельзя утверждать бесконечность множества чисел, для которых справедлива Гипотеза (число $q = 2p+1$ может быть и простым, а для простого p, простого Софи Жермен, «хорошо» факторизуется число $(p-1)$). Простые числа $q = 2p+1$ для простых чисел p Софи Жермен можно охарактеризовать и так: число $(q-1)$ имеет «аномально мало» простых делителей (всего два). Простые числа с аномально малым количеством делителей у числа $(q-1)$ рассматривались в работе [7]. Косвенным подтверждением высказанного в Гипотезе предположения о редкости «исключительных» простых и «плохих» натуральных, ими порожденных, явилась бы информация о количестве «обобщенных простых Софи Жермен», при которых $q = kp+1$ также простое при некотором четном k и количественная информация о «редкости» простых q с «аномально малым» числом простых делителей у числа $(q-1)$.

Обозначим $\mathrm{N}(p \leq x; \mathfrak{A})$ число простых $p \leq x$, для которых выполняется условие $\mathfrak{A}$. Справедливы следующие утверждения [7],[8].

Теорема 2. *Для четного* k, $2 \leq k < x$ *справедливо неравенство:*

$$\mathrm{N}(p \leq x;\ p-1 = kq,\ q \text{ - простое}) = O\left(\frac{x}{\ln^2\left(x/k\right)}\right).$$

Пусть далее $\nu(n)$ - число различных простых делителей числа n. Известно ([8], с.188), что «нормальное» число простых делителей числа n равно $\ln\ln n$, то есть, за исключением $o(x)$ значений n, $n \leq x$, выполняются неравенства

$$(1-\varepsilon)\ln\ln n < \nu(n) < (1+\varepsilon)\ln\ln n.$$

Следующая теорема показывает, что числа $(p-1)$ ведут себя так же, как и все натуральные.

Теорема 3. *Для любого* $\varepsilon > 0$ *выполняется асимптотическое равенство*

$$\mathrm{N}\left(p \leq x; (1-\varepsilon)\ln\ln x < \nu(p-1) < (1+\varepsilon)\ln\ln n\right) =$$

$$= \frac{x}{\ln x} + o\left(\frac{x}{\ln x}\right).$$

Заключение

В работе показано существование «исключительных» простых чисел. Возникает естественный вопрос о синтезе эффективных алгоритмов вычисления ДПФ именно для исключительных длин преобразований. Следует отметить, что сам С.Виноград в главе монографии [2] указал на возможность снижения сложности предложенных им алгоритмов ниже теоретической нижней границы при использовании процессоров, производящих вычисления с элементами поля констант, отличного от поля дей-

ствительных чисел. Другим паллиативным решением является использование представления данных в «нетрадиционных» системах счисления [14]. В частности, возможность использования таких систем для вычисления свертки Примера 1 рассмотрена в [15].

Благодарности

Работа выполнена при поддержке Российского фонда фундаментальных исследований (проект №09-01-00511-а).

Литература

1. **Блейхут, Р.** Быстрые алгоритмы цифровой обработки сигналов / Р.Блейхут; пер.с англ. – М.: Мир, 1987. – 448 с.
2. **Макклеллан, Дж. Х.** Применение теории чисел в цифровой обработке сигналов / Дж.Х. Маккеллан, Ч.М. Рейдер; пер.с англ. – М.: Радио и связь, 1983. – 263 с.
3. **Winograd, S.** On Computing the Discrete Fourier Transform / S. Winograd // Proc. Nat. Acad. Sci. USA. – 1976. – Vol.73. – P.1005-1006.
4. **Winograd, S.** On the Discrete Fourier Transform / S. Winograd // Math. Comp. – 1978. – Vol. 32. – P. 175-199.
5. **Власенко, В. А.** Методы синтеза быстрых алгоритмов свертки и спектрального анализа сигналов / В.А. Власенко, Ю.П. Лаппа, Л.П. Ярославский. – М.: Наука, 1990. – 180 с.
6. **Нуссбаумер, Г.** Быстрое преобразование Фурье и алгоритмы вычисления сверток / Г. Нуссбаумер; пер.с англ. – М.: Радио и связь, 1985. – 248с.
7. **Erdös, P.** On the normal number of prime factors of *p-1* and some related problems concerning Euler's φ-function / P. Erdös // Quart. J. Oxford. – 1935. – Vol.6. – P.205-213.
8. **Prachar, K.** Primzahlverteilung / K.Prachar. – Springer-Verlag, Berlin, 1957.
9. **Winograd, S.** Arithmetic complexity of computations / S. Winograd. – SIAM, 1980. – 93p.
10. **Dubner, H.** Large Sophie Germain Primes / H. Dubner. // Math. Comput. – 1996. – Vol. 65. –P. 393-396.
11. **Indlekofer, K. H.** Largest Known Twin Primes and Sophie Germain Primes / K. H. Indlekofer, A. Járai // Math. Comput. – 1999. – Vol. 68. – P. 1317-1324.
12. **Ribenboim, P.** Sophie Germain Primes / P. Ribenboim // The New Book of Prime Number Records. – New York, Springer-Verlag, 1996. – P. 329-332.
13. **Chernov, V.M.** Data Algorithms: Galois vs. Rader and Winograd / V.M.Chernov // Pattern Recognition and Image Analysis. – 2003. – Vol. 13(1) . – P. 5–7.
14. **Чернов, В.М.** Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований / В.М.Чернов. – М.: Физматлит, 2007.
15. **Chernov, V.** Fast algorithm for «error-free» convolution computation using Mersenne-Lucas codes / V. Chernov // Chaos, Solitons and Fractals. – 2006. – Vol. 29. – P. 372-380.

References

1. **Blahut, R.E.** Fast algorithms for Digital Signal Processing / R.E. Blahut. – Addison-Wesley, 1985.
2. **McClellan, J.H.** Number Theory in Digital Signal Processing / J.H. McClellan, C.M. Rader. – Prentice-Hall, New Jersey, 1979.
3. **Winograd, S.** On Computing the Discrete Fourier Transform / S. Winograd // Proc. Nat. Acad. Sci. USA. – 1976. – Vol.73. – P.1005-1006.
4. **Winograd, S.** On the Discrete Fourier Transform / S. Winograd // Math. Comp. – 1978. – Vol. 32. – P. 175-199.
5. **Vlasenko, V.A.** Methods of Fast Convolution Algorithms Synthesis and Spectral Signal Analysis / V.A. Vlasenko, Yu.P. Lappa, L.P. Yaroslavsky. – Moscow, Science, 1990. – 180 p. – (In Russian).
6. **Nussbaumer, H.J.** Fast Fourier Transform and Convolution Algorithms / H.J. Nussbaumer. – Springer-Verlag, Berlin, 1982.
7. **Erdös, P.** On the normal number of prime factors of *p-1* and some related problems concerning Euler's φ-function / P. Erdös // Quart. J. Oxford. – 1935.– Vol.6. – P. 205-213.
8. **Prachar, K.** Primzahlverteilung / K.Prachar. – Springer-Verlag, Berlin, 1957.
9. **Winograd, S.** Arithmetic complexity of computations / S. Winograd. – SIAM, 1980. – 93p.
10. **Dubner, H.** Large Sophie Germain Primes / H. Dubner. // Math. Comput. – 1996. – Vol. 65. –P. 393-396.
11. **Indlekofer, K. H.** Largest Known Twin Primes and Sophie Germain Primes / K. H. Indlekofer, A. Járai // Math. Comput. – 1999. – Vol. 68. – P. 1317-1324.
12. **Ribenboim, P.** Sophie Germain Primes / P. Ribenboim // The New Book of Prime Number Records. – New York, Springer-Verlag, 1996. – P. 329-332.
13. **Chernov, V.M.** Data Algorithms: Galois vs. Rader and Winograd / V.M.Chernov // Pattern Recognition and Image Analysis. – 2003. – Vol. 13(1) . – P. 5–7.
14. **Chernov, V.M.** Arithmetic methods of fast discrete orthogonal transform synthesis / V.M. Chernov. – Moscow, Fizmatlit, 2007. – (In Russian).
15. **Chernov, V.** Fast algorithm for «error-free» convolution computation using Mersenne-Lucas codes / V. Chernov // Chaos, Solitons and Fractals. – 2006. – Vol. 29. – P. 372-380.

ON EFFICIENCY OF RADER-WINOGRAD ALGORITHMS

Vladimir Mikhailovich Chernov[1] (chief researcher, e-mail: vche@smr.ru)
[1] Image Processing Systems Institute of the RAS

Abstract

It is proved the existence of «exclusive» prime numbers, for which Rader-Winograd algorithms of discrete Fourier transform and/or convolution computation for corresponded lengths are not effective. The sufficient conditions of «exclusiveness» are given in analytical form

Key words: discrete Fourier transform, cyclotomic convolution, Rader-Winograd algorithm, computational complexity.

В редакцию поступила 7.12.2009 г.