

нии l результатом является 1, а при слишком большом — N). При этом l выбирается методом, похожим на половинное деление. При каждом значении l вычисляется $D(l) = (a^k - 1, N)$, $k = p_1^\alpha p_2^\alpha \dots p_l^\alpha$. Параметр l выбирается следующим образом:

Шаг 1. $l_{\min} := 1$, $l_{\max} := 1$.

Шаг 2. $l_{\max} := l_{\max} \cdot 2$; $l = l_{\max}$.

Шаг 3. Вычислить $D = D(l)$;

— если $D = 1$, то перейти к шагу 2;

— если $D = N$, то перейти к шагу 4;

— если $1 < D < N$ — выход, делитель найден.

Шаг 4. $l_{\min} := l_{\max}/2$; $l_{\text{midl}} := l_{\min} + (l_{\max} - l_{\min})/2$; $l := l_{\text{midl}}$.

Шаг 5. Вычислить $D = D(l)$;

— если $D = 1$, то $l_{\min} := l_{\text{midl}}$; $l_{\text{midl}} := l_{\min} + (l_{\max} - l_{\min})/2$; $l := l_{\text{midl}}$; перейти к шагу 5;

— если $D = N$, то $l_{\max} := l_{\text{midl}}$; $l_{\text{midl}} := l_{\min} + (l_{\max} - l_{\min})/2$; $l := l_{\text{midl}}$; перейти к шагу 5;

— если $1 < D < N$ — выход, делитель найден.

Проведены эксперименты на заранее сформированных массивах чисел, представляющих собой произведение двух простых, с разрядностью 20, 40 и 60 десятичных знаков. Из 10000 чисел разрядностью 20 десятичных знаков были разложены 4250, среднее время на обработку одного числа составило 1,42 с. Разрядность максимального числа, которое было разложено на множители, составляет 60 десятичных знаков:

$$\begin{aligned} &1052808008400417645876606027989867285487720871343057551778083 = \\ &= 123547896523698521452369860571 \cdot 8521456358412963587456325968473, \end{aligned}$$

время разложения — 29 мин 23 с.

ЛИТЕРАТУРА

1. Маховенко Е. Б. Теоретико-числовые алгоритмы в криптографии. М.: Гелиос АРВ, 2006.
2. Климина А. С. Оптимизация выбора параметров для алгоритма Полларда // IV ОМНТК «Молодежь. Техника. Космос». СПб.: БГТУ, 2012. С. 285–286.

УДК 519.688

ПАРАЛЛЕЛЬНЫЙ АЛГОРИТМ ВЫЧИСЛЕНИЯ ФУНКЦИЙ РОСТА В КОНЕЧНЫХ ДВУПОРОЖДЁННЫХ ГРУППАХ ПЕРИОДА 5

А. С. Кузнецова, А. А. Кузнецов, К. В. Сафонов

Представлена параллельная версия алгоритма для вычисления функций роста в конечных двупорождённых группах периода 5.

Ключевые слова: функция роста группы, диаметр Кэли, параллельный алгоритм.

Пусть p — простое число, G — конечная группа экспоненты p . Это значит, что $g^p = e$ для всех $g \in G$. Так как G нильпотентна, то можно найти цепочку подгрупп $G = G_1 \supset \supset G_2 \supset \dots \supset G_n \supset G_{n+1} = e$, в которой G_i нормальны в G , а факторы G_i/G_{i+1} имеют порядок p и лежат в центре G/G_{i+1} .

Пусть для $1 \leq i \leq n$ элемент $a_i \in G_i$, но $a_i \notin G_{i+1}$, тогда каждый элемент группы $g \in G$ можно однозначным образом записать в виде

$$g = a_1^{\gamma_1} a_2^{\gamma_2} \dots a_n^{\gamma_n}, \quad 0 \leq \gamma_i < p. \quad (1)$$

Такое представление элементов группы (рс-представление) можно получить при помощи алгоритма, известного как p -quotient algorithm [1]. Он реализован в системах компьютерной алгебры GAP и Magma. Если $\mathbb{A}$ — порождающее множество группы G , то любой её элемент, записанный в виде слова $\alpha_1\alpha_2\ldots\alpha_s$, где $\alpha_i \in \mathbb{A}$, можно преобразовать к виду (1)

$$\alpha_1\alpha_2\ldots\alpha_s \xrightarrow{pq} a_1^{\gamma_1}a_2^{\gamma_2}\ldots a_n^{\gamma_n}. \quad (2)$$

Процедура (2) даёт возможность решить проблему равенства слов в G . Для вычисления функции роста и диаметра Кэли группы G относительно $\mathbb{A}$ необходимо перечислить все элементы группы в формате минимальных слов [2]. Вычислив количество слов на каждой длине, можно получить функцию роста группы, а максимально возможная длина минимальных слов является диаметром Кэли группы.

Обозначим через $K_s(G)$ множество всех минимальных слов группы G , не превосходящих по длине s ; множество $Q_s(G)$ — элементы $K_s(G)$, записанные в виде правой части (2).

Пусть $s_0 \in \mathbb{N}$ — минимальное число, для которого выполняется $K_{s_0}(G) = K_{s_0+1}(G)$. В этом случае s_0 — диаметр Кэли группы G .

Опишем последовательный алгоритм, вычисляющий функцию роста группы G относительно $\mathbb{A} = \{a_1, a_2, \ldots, a_m\}$:

- 1) $s = 0$, $K_0 = \{e\}$, $Q_0 = \{a_1^0 a_2^0 \ldots a_n^0\}$, $T = K_0$.
- 2) $s = s + 1$, $K_s = K_{s-1}$, $Q_s = Q_{s-1}$, $V = a_1 T \cup a_2 T \ldots \cup a_m T$, $T = \emptyset$, $i = 1$.
- 3) Для $v_i \in V$ $v_i \xrightarrow{pq} \hat{v}_i$. Если $\hat{v}_i \notin Q_s$, то $K_s = K_s \cup \{v_i\}$, $Q_s = Q_s \cup \{\hat{v}_i\}$, $T = T \cup \{v_i\}$.
- 4) Если $i < |V|$, то $i = i + 1$, переход в п. 3, иначе — в п. 5.
- 5) Если $T \neq \emptyset$, то переход в п. 2; иначе — в п. 6.
- 6) Диаметр G равен $s - 1$, $K_{s-1}(G)$ — множество всех минимальных слов группы. Функция роста задаётся формулой $f(j) = |K_j(G)| - |K_{j-1}(G)|$, $1 \leq j \leq s - 1$.

Завершение работы алгоритма.

Для увеличения скорости вычислений алгоритм можно распараллелить следующим образом. Множество Q_s разбивается на p^r непересекающихся классов элементов, где каждый класс однозначно определяется фиксированным набором значений $\gamma_1, \gamma_2, \ldots, \gamma_r$. Параметр r определяется экспериментально и зависит от характеристик мультипроцессорной вычислительной системы.

Пусть $B_0(2, 5, k)$ — максимальная конечная двупорождённая бернсайдова группа периода 5 ступени нильпотентности k . В данном классе групп наибольшей является группа $B_0(2, 5, 12)$, порядок которой равен 5^{34} . Для каждой из $B_0(2, 5, k)$ известны рс-представления, которые несложно получить, используя систему компьютерной алгебры GAP. Положим $\mathbb{A} = \{a_1, a_2\}$ — порождающие элементы $B_0(2, 5, k)$. Для $k \leq 6$ к настоящему времени вычислены функции роста и диаметры Кэли групп $B_0(2, 5, k)$ относительно $\mathbb{A}$. Отметим, что для нахождения функций роста при $k \geq 2$ использовались компьютерные вычисления. В таблице приведены значения порядков групп $B_0(2, 5, k)$, а также их диаметры $D_k(\mathbb{A})$ относительно $\mathbb{A}$.

k	$ B_0(2, 5, k) $	$D_k(\mathbb{A})$	k	$ B_0(2, 5, k) $	$D_k(\mathbb{A})$
1	5^2	8	4	5^8	30
2	5^3	10	5	5^{10}	32
3	5^5	20	6	5^{14}	45

Следующий нерешённый случай — $k = 7$. Поскольку $B_0(2, 5, 7)$ имеет достаточно большой порядок (он равен 5^{18}), для нахождения диаметра данной группы необходимо применять суперкомпьютерные вычисления. В настоящее время идет работа по

программной реализации параллельной версии алгоритма на языке C++ с использованием интерфейса передачи данных MPI. Вычисления будут проводиться на суперкомпьютере Сибирского федерального университета.

ЛИТЕРАТУРА

1. *Halt D., Eick B., and O'Brien E.* Handbook of computational group theory. Boca Raton: Chapman & Hall/CRC Press, 2005.
2. *Кузнецов А. А., Шлёпкин А. К.* Сравнительный анализ бернсайдовых групп $B(2, 5)$ и $B_0(2, 5)$ // Тр. Ин-та математики и механики УрО РАН. 2009. № 2. С. 125–132.

УДК 519.7

КОНВЕЙЕРИЗАЦИЯ КОМБИНАЦИОННЫХ СХЕМ

Ю. В. Поттосин, С. Н. Кардаш

Рассматривается вопрос повышения быстродействия устройства без памяти, преобразующего последовательность дискретных сигналов. Поставлена задача разбиения заданной многоуровневой комбинационной схемы на заданное число каскадов, на выходах которых должны быть поставлены регистры для обеспечения конвейерной обработки поступающих сигналов. Для решения этой задачи используется модель, основанная на представлении комбинационной схемы в виде ориентированного графа.

Ключевые слова: комбинационная схема, конвейеризация, ориентированный граф.

Повышению производительности систем обработки информации всегда уделялось большое внимание. Одним из способов повышения производительности является применение структуры конвейерного типа, который имеет ещё название «трубопровод» (перевод с англ. слова «pipeline») [1]. Подобную структуру образуют несколько независимых процессоров, соединённых между собой последовательно.

При построении систем цифровой обработки сигналов в режиме реального времени широкое распространение получил систолический принцип организации вычислений [2]. Информация в систолическом процессоре распространяется по конвейеру подобно тому, как пульсирует кровь при сокращении систолы сердца. В данной работе излагается попытка найти способ повышения быстродействия путем конвейеризации многоуровневой комбинационной схемы, построенной на основе СБИС.

В многоуровневой схеме устройства задержка складывается из задержек элементов самой длинной цепочки. Пусть на вход комбинационной схемы поступает последовательность p наборов двоичных сигналов. Если T — время задержки схемы, то период смены сигналов не может быть меньше T . Время реакции устройства на данную последовательность в этом случае не меньше pT . Разобьём схему на k каскадов $(C_1, C_2, \dots, C_k)$, и если τ_C — время задержки самого медленно действующего каскада, то $T \leq k\tau_C$. На выходы каждого каскада поставим элементы задержки (триггеры D), пропускающие сигналы с выходов каскада по сигналу синхронизации. Этот же сигнал синхронизации определяет период смены сигналов на входе устройства, который должен быть не меньше суммы двух задержек: задержки τ_C и задержки τ_D элемента D ($\tau_{\text{clock}} \geq \tau_C + \tau_D$). Теперь время реакции устройства на упомянутую последовательность равно $(k + p)\tau_{\text{clock}}$.

Нижняя граница длины p последовательности наборов двоичных сигналов на входе устройства, при которой имеет место ускорение обработки сигналов, определяется