использовании групповых операций на рациональных кривых третьей степени $y^3 + xy = x^3 + x^2$ в параметрической форме.

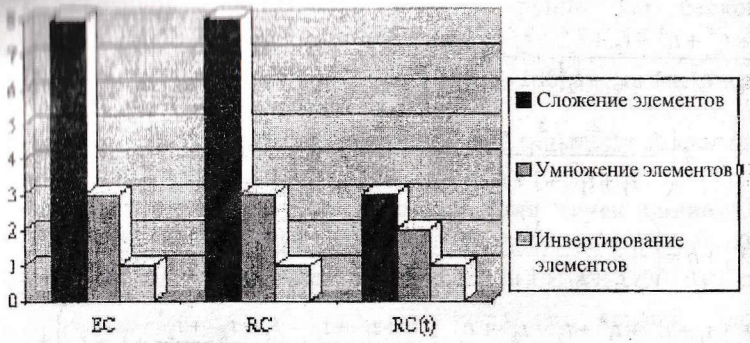

Рис. 2. Вычислительная сложность групповой операции сложения точек эллиптической и рациональных кривых в элементарных операциях над $GF(2^m)$

На рис. 2 представлена сводная диаграмма вычислительной сложности групповых операций сложения точек эллиптической кривой (EC_2), точек рациональной кривой (RC) и точек рациональной кривой (RC) в параметрическом виде ($RC(t)$).

Выводы. Таким образом, на основе параметризации плоской рациональной кривой разработаны быстрые операции сложения точек кривой. Проведенные исследования показали существенное снижение числа операций (в 1,5 – 3 раза), необходимых для сложения точек кривой.

Перспективным направлением дальнейших исследований является разработка быстрых операций удвоения точек, исследование их производительности.

1. *Rivest R.L., Shamir A., Adleman L.M.* A method for obtaining digital signatures and public key cryptosystems // Comm. ACM. – 1978. – P. 120 – 126.
2. ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що грунтується на еліптичних кривих. Формування та перевірка.
3. IEEE P 1363/D11(Draft Version 11) / Standard Specifications for Public key Cryptography / Annex A (Informative). Number-Theoretic Background.
4. *Горбенко И.Д., Збитнев С.И., Поляков А.А.* Сложность арифметических операций в группах точек эллиптических кривых для криптографических операций // Радиотехника. – 2001. – Вып. 119. – С. 32 – 37.
5. *Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А.* Алгоритмические основы эллиптической криптографии: Учебное пособие. – М.: Связь, 2000. – 100 с.
6. *Smart N.* The discrete logarithm problem on elliptic curves of trace one? To appear in Journal of cryptology.

Поступила 16.07.2004 г.

УДК 681.324

Г.А. Кучук, А.А. Пашнев, А.И. Тимочко

МОДЕЛЬ РАСПРЕДЕЛЕНИЯ ВЫЧИСЛИТЕЛЬНЫХ РЕСУРСОВ НЕОДНОРОДНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПО КВАНТАМ ЗАДАННОГО ИНТЕРВАЛА ВРЕМЕНИ

Постановка задачи. В процессе функционирования неоднородных вычислительных сетей (НВС) возникает необходимость в обеспечении распределенной обработки заявок удаленных абонентов НВС в заданные промежутки времени. Достижение максимальной эффективности распределенной обработки заявок удаленных абонентов НВС в заданные промежутки времени, возможно, за счет обеспечения равномерного распределения вычислительных ресурсов (ВР) НВС по квантам заданного интервала времени и нахождения распределения заявок удаленных абонентов по узлам НВС, позволяющего минимизировать среднюю задержку пакета данных в ней [1]. Таким образом, задача повышения эффективности распределенной обработки заявок удаленных абонентов НВС может быть сформулирована так: необходимо построить равномерное распределение ВР НВС по квантам заданного интервала времени и найти такое разбиение множества заявок удаленных абонентов НВС на подмножества и их распределение по узлам НВС в процессе распределенной обработки, чтобы средняя задержка пакета данных в сети принимала минимальное значение и обеспечивалась равномерная загрузка НВС.

Анализ литературы. Для решения указанной задачи возможно использование алгоритма Балаша, метода ветвей и границ, а также метода W, базирующихся на идее последовательного анализа вариантов [2 – 4]. Однако как уже указывалось в [5, 6], все перечисленные методы имеют сравнительно невысокую вычислительную эффективность, что ограничивает решение поставленной задачи числом переменных $h_z \times h_y \le 300$, где h_z – число независимых заявок удаленных абонентов, обрабатываемых в сети; h_y – число узлов НВС. В связи с этим, возникает необходимость в разработке математической модели, позволяющей построить равномерное распределение вычислительных ресурсов неоднородной вычислительной сети по квантам заданного интервала времени и обеспечивающей минимизацию средней задержки пакета данных в сети при распределенной обработке заявок удаленных абонентов для числа переменных $h_z \times h_y > 300$.

Целью статьи является разработка математической модели, позволяющей построить равномерное распределение выделенных вычислительных ресурсов для обработки множества заявок удаленных абонентов НВС по квантам заданного интервала времени и найти такое разбиение множества заявок на подмножества и их распределение по узлам

НВС в процессе распределенной обработки, чтобы средняя задержка пакета данных в сети принимала минимальное значение и обеспечивалась равномерная загрузка НВС для числа переменных $h_z \times h_y > 300$.

Решение задачи построения равномерного распределения выделенных вычислительных ресурсов по квантам заданного временного интервала при обработке заявок отдельных абонентов вычислительной сети подробно рассматривалось в [7]. Исходными данными для решения рассматриваемой задачи являются: T_z – заданный интервал времени, представляющий собой конечный набор квантов, равных 1 с; Z – множество заявок удаленных абонентов НВС. При этом временной интервал T_z представляется в виде отрезка натурального ряда $\{t_{z_1}, t_{z_2}, \ldots, t_{z_i}, \ldots, t_{z_{h_t}}\}$, где t_{z_i} – i-й квант времени, $1 \le i \le h_t$; h_t – число квантов временного интервала T_z. Каждая заявка $z_b \in Z$, $1 \le b \le h_z$, характеризуется параметрами φ_{z_b}, T_{z_b}, где φ_{z_b} – требуемый ВР для обработки заявки z_b; $T_{z_b} = \{t_{z_{b_1}}, t_{z_{b_2}}\}$ – интервал времени, в течение которого необходимо предоставить требуемый вычислительный ресурс; $t_{z_{b_1}}$ – начальный квант временного интервала T_{z_b}; $t_{z_{b_2}}$ – конечный квант временного интервала T_{z_b}.

В результате распределения γ вычислительных ресурсов НВС формируется матрица $M_{\varphi}^{(\gamma)}$, в которой каждой заявке $z_b \in Z$ сопоставляется вектор-строка $\mathrm{m}_{\varphi_b} = (\mathrm{m}_{\varphi_{b,1}}, \ldots, \mathrm{m}_{\varphi_{b,h_t}})$, представляющая собой расписание выделения вычислительных ресурсов НВС для обработки заявки z_b, где компонент $\mathrm{m}_{\varphi_{b,i}}$ определяет выделенный для заявки z_b вычислительный ресурс в i-й квант времени.

Качество распределения γ оценивается с помощью целевой функции $F^{(\gamma)}$ и величины максимального суммарного выделенного ВР, приходящегося на квант заданного временного интервала T_z в распределении γ по всем заявкам множества Z [7]: $m_{\varphi_{\max}}^{(\gamma)} = \max_{i=1,\ldots,h_t} \sum_{b=1}^{h_z} m_{\varphi_{b,i}}$.

При условии равномерного распределения по квантам заданного временного интервала T_z суммарного объема вычислений, необходимого для обработки заявок множества Z, выражение для определения величины минимального суммарного требуемого ВР, приходящегося на квант интервала T_z, примет вид [7]: $\varphi_{z_{\min}} = \frac{1}{h_t} \sum_{b=1}^{h_z} \varphi_{z_b}$. Основой определения целевой функции $F^{(\gamma)}$ служит штраф при выделении заявке $z_b \in Z$ единицы

вычислительного ресурса в i-й квант времени. Если единица ВР для заявки z_b, характеризующейся интервалом времени обработки $T_{z_b} = \{t_{z_{b_1}}, t_{z_{b_2}}\}$, выделена в i-й квант, то соответствующий ей штраф определяется как [7]:

$$s_{t_{b,i}} = \begin{cases} 0, & \text{если } t_{z_{b_1}} \le t_{z_i} \le t_{z_{b_2}}; \\ (t_{z_{b_1}} - t_{z_i}) / \varphi_{z_b}, & \text{если } t_{z_i} < t_{z_{b_1}}; \\ (t_{z_i} - t_{z_{b_2}}) / \varphi_{z_b}, & \text{если } t_{z_i} > t_{z_{b_2}}. \end{cases}$$

Таким образом, для каждой заявки $z_b \in Z$ имеем вектор $s_{t_b} = (\mathbf{s}_{t_{b_1}}, \ldots, \mathbf{s}_{t_{b_{h_t}}})$, у которого компонент $\mathbf{s}_{t_{b_i}}$, $1 \le i \le h_t$, определяет величину штрафа при выделении заявке z_b единицы ВР в i-й квант времени.

Величина штрафа, характеризующего полученное распределение γ выделенных ВР для обработки множества заявок Z, определяет целевую функцию [7]:

$$F^{(\gamma)} = \sum_{b=1}^{h_z} \sum_{i=1}^{h_t} m_{\varphi_{b,i}} \cdot s_{t_{b,i}}.$$

При построении распределения γ ВР по квантам на заданном интервале времени T_z минимизируются величины $F^{(\gamma)}$ и $m_{\varphi_{\max}}^{(\gamma)}$. При этом распределение γ должно удовлетворять следующим условиям:

1) $\forall z_b \in Z$, $\forall t_{z_i} \in T_{z_b}$, $m_{\varphi_{b,i}} \ge 0$, $s_{t_{b,i}} \ge 0$; 2) $\forall z_b \in Z$ $\sum_{i=1}^{h_t} m_{\varphi_{b,i}} \le \varphi_{z_b}$;

3) $\forall t_{z_i} \in T_z$ $\sum_{b=1}^{h_z} m_{\varphi_{b,i}} \le \varphi_{t_i}$,

где φ_{t_i} – суммарный доступный вычислительный ресурс НВС в i-й квант заданного интервала времени T_z.

Полученное равномерное распределение γ описывается с помощью кортежа $\langle Z, \varphi_z, T_z, \varphi_t, M_{\varphi}^{(\gamma)}, F^{(\gamma)}, m_{\varphi_{\max}}^{(\gamma)} \rangle$, где Z – множество заявок удаленных абонентов; $\varphi_z : Z \to N_+$ – функция, указывающая каждой заявке $z_b \in Z$ требуемый вычислительный ресурс для ее обработки; $T_z : Z \to N_+$ – функция, указывающая каждой заявке $z_b \in Z$ интервал времени для ее обработки; $\varphi_t : T_z \to N_+$ – функция, указывающая каждому кванту времени $t_{z_i} \in T_z$ суммарный доступный вычислительный ресурс НВС.

Для каждого вектор-столбца $m_{\varphi_i} = (m_{\varphi_{1,i}}, \ldots, m_{\varphi_{h_z,i}})$ матрицы $M_{\varphi}^{(\gamma)}$,

определяющего выделенный ВР НВС для обработки заявок множества Z в l-м квант заданного интервала времени T_z необходимо найти такое разбиение множества заявок Z на подмножества и их распределение по узлам НВС, чтобы средняя задержка пакета данных в сети принимала минимальное значение. Целевая функция задачи поиска рационального разбиения множества задач Z, обрабатываемых в вычислительной сети, на подмножества и их распределения по узлам $y_a \in Y$, определяется выражением [6]:

$$F^{(\gamma)} = \frac{1}{u_{z_{\max}}} \cdot \sum_{b=1}^{h_z} \sum_{a=1}^{h_y} m_{z_{b,a}} \cdot s_{y_{b,a}}, \qquad (1)$$

где Y – множество узлов НВС; $u_{z_{\max}}$ – независимая от распределения γ величина, определяющая максимальную суммарную интенсивность обмена заявок с узлами вычислительной сети в соответствии с выражением $u_{z_{\max}} = \sum_{b=1}^{h_z} \sum_{i=1}^{h_y} u_{z_{b,i}}$; $u_{z_{b,i}}$ – интенсивность обмена заявки $z_b \in Z$ с узлом $y_i \in Y$; $m_{z_{b,a}}$ – ВР узла y_a, необходимый для обработки заявки z_b; $s_{y_{b,a}}$ – штраф при распределении заявки $z_b \in Z$ на узел $y_a \in Y$, определяемый выражением $s_{y_{b,a}} = \sum_{i=1}^{h_y} \left(u_{z_{b,i}} \cdot h_{wa,i} \right) / \varphi_{z_b}$; $h_{wa,i}$ – длина кратчайшего маршрута между узлами y_a и y_i, определяемая числом каналов ПД, входящих в этот маршрут. Полученное распределение γ должно удовлетворять следующим условиям:

1) $\forall y_a \in Y \left| \sum_{b=1}^{h_z} m_{z_{b,a}} \le \varphi_{y_a} \right.$; 2) $\forall z_b \in Z \left| \sum_{a=1}^{h_y} m_{z_{b,a}} \le \varphi_{z_b} \right.$; 3) $\sum_{a=1}^{h_y} \varphi_{y_a} \ge \sum_{b=1}^{h_z} \varphi_{z_b}$;

4) $s_{y_{b,a}} \ge 0$, $m_{z_{b,a}} \ge 0$ для $1 \le a \le h_y$, $1 \le b \le h_z$,

где φ_{y_a} – доступный вычислительный ресурс узла $y_a \in Y$.

С учетом приведенных условий, задача поиска рационального разбиения множества заявок Z, обрабатываемых в вычислительной сети, на подмножества и их распределения по узлам $y_a \in Y$ может быть сформулирована следующим образом. Пусть заданы множества заявок Z и узлов Y вычислительной сети, определяемые кортежами $\langle Z, \varphi_z, U_z \rangle$ и $\langle Y, \varphi_y, H_w \rangle$, где $\varphi_z = \left(\varphi_{z_1}, \ldots, \varphi_{z_{h_z}} \right)$ – вектор требуемых ВР для обработки множества заявок Z; $U_z = \left\| u_{z_{b,i}} \right\|$ – матрица интенсивностей обмена заявок множества Z с узлами множества Y; $\varphi_y = \left(\varphi_{y_1}, \ldots, \varphi_{y_{h_y}} \right)$ – вектор доступных ВР множества узлов Y вычислительной сети; $H_w = \left\| h_{w_{a,i}} \right\|$ – матрица длин

кратчайших маршрутов между каждой парой узлов НВС y_a и y_i, $1 \le a \le h_y$, $1 \le i \le h_y$. Требуется найти такое распределение γ, удовлетворяющее условиям 1 – 4, чтобы выражение (1) принимало минимальное значение.

Для решения указанной задачи целесообразно использовать метод потенциалов [2], обеспечивающий последовательное выполнение следующих операций: построение базового распределения ВР сети; построение системы потенциалов; проверку базового распределения на рациональность; построение замкнутого контура и перераспределение ВР по контуру с целью минимизации целевой функции $F^{(\gamma)}$. В результате разбиения множества заявок Z, обрабатываемых в НВС, на подмножества и их распределения по узлам множества Y, обеспечивающих минимизацию средней задержки пакета данных в сети, формируется матрица $M_z^{(\gamma)}$, каждый элемент $m_{z_{b,a}}$ которой определяет ВР узла $y_a \in Y$, выделенный для обработки заявки $z_b \in Z$. Результирующее распределение описывается как $\langle Z, \varphi_z, Y, \varphi_y, M_z^{(\gamma)}, F^{(\gamma)} \rangle$.

Выводы. Таким образом, основным, полученным научным и практическим результатом данного исследования является разработанная математическая модель, позволяющая построить равномерное распределение выделенных вычислительных ресурсов для обработки множества заявок удаленных абонентов НВС по квантам заданного интервала времени и найти такое разбиение множества заявок Z на подмножества и их распределение по узлам НВС, чтобы средняя задержка пакета данных в сети принимала минимальное значение и обеспечивалась равномерная загрузка НВС для числа переменных $h_z \times h_y > 300$.

1. *Королёв А.В., Кучук Г.А., Пашнев А.А.* Управление сетевыми ресурсами. – Х.: ХВУ, 2004. – 272 с.
2. *Сергиенко И.В.* Математические модели и методы решения задач дискретной оптимизации. – К.: Наук. думка, 1985. – 520 с.
3. *Максименков А.В.* Распределение задач по машинам сети ЭВМ // Автоматика и вычислительная техника. – 1986. – № 2. – С. 3 – 10.
4. *Максименков А.В.* Основы проектирования информационно-вычислительных систем и сетей ЭВМ. – М.: Радио и связь, 1991. – 319 с.
5. *Пашнев А.А.* Управление обработкой задач в распределенной вычислительной сети // Зб. наук. праць ІПМЕ ім. Г.Є. Пухова. – К.: ІПМЕ. – 2003. – Вип. 22. – С. 136 – 141.
6. *Пашнев А.А., Клименко Л.А.* Математическая модель задачи рационального управления распределенной обработкой задач в ИТС // Системи обробки інформації. – Х.: ХВУ. – 2004. – Вип. 3. – С. 162 – 168.
7. *Пашнев А.А., Кучук Г.А., Лебедева И.А.* Распределение вычислительного ресурса однородной вычислительной сети по квантам заданного интервала времени // Системи обробки інформації. – Х.: ХВУ. – 2004. – Вип. 7 (35). – С. 146 – 153.

Поступила 5.07.2004 г.