Сложность алгоритмов для разреженных полиномиальных матриц

©М.С.Зуев

Пусть $\mathbb{W}$ - коммутативная область, каждый элемент которой может быть записан в одном машинном слове.

Определение 1. Полином $\sum_{v=1}^{m} c_v x^{v-1} \in \mathbb{W}[x]$, у которого коэффициент c_v отличен от нуля с вероятностью α_v назовем полиномом типа (m, α_v). Если $\alpha_v = \alpha$ для всех v, то будем обозначать тип (m, α). Число α назовем *плотностью* полинома.

Определение 2. Назовем матрицей типа (n, ρ, m, α_k) случайную $n \times n$ матрицу, каждый элемент которой отличен от нуля с вероятностью ρ, а каждый ненулевой элемент – это полином типа (m, α_k). Число ρ назовем *плотностью* матрицы.

Будем обозначать $\mathcal{EA}$ и $\mathcal{EM}$ математическое ожидание числа операций сложения и умножения в алгоритме, а также $\phi(a, b) = a + b - ab$.

Вычислим сложность матричных алгоритмов сложения и умножения с учетом плотности матриц. Будем считать, что для сложения и стандартного умножения полиномов справедливо

$$(m, \alpha_i) + (m, \beta_i) = (m, \phi(\alpha_i, \beta_i))$$

$$(m, \alpha) \times (m, \beta) = (2m - 1, \pi_i^m(\alpha, \beta))$$

$$\mathcal{EA}((m, \alpha) + (m, \beta)) = m\alpha\beta; \tag{1}$$

$$\mathcal{EM}((m, \alpha) \times (m, \beta)) = m^2\alpha\beta;$$

$$\mathcal{EA}((m, \alpha) \times (m, \beta)) = m^2\alpha\beta,$$

где

$$t_i^m = \begin{cases} i & \text{при} \quad 1 \le i \le m \\ 2m - i & \text{при} \quad m \le i \le 2m - 1, \end{cases}$$

$$\pi_i^m(\alpha, \beta) = 1 - (1 - \alpha\beta)^{t_i^m}$$

Для алгоритма сложения полиномиальных матриц справедливо

$$(n, \rho, m, \alpha_v) + (n, \sigma, m, \beta_v) =$$

$$= (n, \phi(\rho, \sigma), m, \phi(\rho\alpha_v, \sigma\beta_v)) \tag{2}$$

Математическое ожидание числа сложений при этом равно

$$\mathcal{EA} = n^2\rho\sigma \sum_{v=1}^{m} \alpha_v\beta_v \tag{3}$$

Для стандартного алгоритма умножения матриц справедливо

$$(n, \rho, m, \alpha) \times (n, \sigma, m, \beta) =$$

$$= (n, 1 - (1 - \rho\sigma)^n, 2m - 1, \eta_v), \tag{4}$$

где

$$q = \rho\sigma(1 - (1 - \alpha)^m)(1 - (1 - \beta)^m),$$

$$\eta_v = 1 - (1 - q\pi_v^m(\alpha, \beta))^n$$

Математическое ожидание количества операций при этом равно

$$\mathcal{EM} = n^3 qM, \tag{5}$$

$$\mathcal{EA} = n^3 qA +$$

$$+ n^2 \sum_{v=1}^{2m-1} ((1 - q\pi_v^m(\alpha, \beta))^n - 1 + nq\pi_v^m(\alpha, \beta)). \tag{6}$$

Будем называть целое число числом типа (w), если оно хранится в w машинных словах. Примем модель

$$(w) + (v) = (max(w, v)), \ \mathcal{EA}((w) + (w)) = w,$$

$$(w) \times (v) = (w + v), \ \mathcal{EM}((w) \times (v)) = vw, \tag{7}$$

$$\mathcal{EA}((w) \times (v)) = vw,$$

для стандартного алгоритма умножения чисел.

Определение 3. Полином $\sum_{v=1}^{m} c_v x^{v-1} \in \mathbb{Z}[x]$, у которого коэффициент c_v отличен от нуля с вероятностью α_v и все ненулевые коэффициенты – это числа типа (w) назовем полиномом типа (m, α_v, w).

Определение 4. Назовем матрицей типа $(n, \rho, m, \alpha_k, w)$ случайную $n \times n$ матрицу, каждый элемент которой отличен от нуля с вероятностью ρ, а каждый ненулевой элемент – это полином типа (m, α_k, w).

Для стандартных алгоритмов умножения полиномов и матриц оценки сложности получаются непосредственно из формул (1), (3), (5), (6).

Данный подход можно использовать для оценки сложности других матричных алгоритмов.

БЛАГОДАРНОСТИ: Работа выполнена при частичной поддержке гранта РФФИ 04-07-90268.

Поступила в редакцию 10 октября 2006 г.