УДК 519.8

Н. Г. Журбенко, канд. физ.-мат. наук

Институт кибернетики имени В. М. Глушкова НАН Украины, г. Киев

ОБ ОДНОМ СЕМЕЙСТВЕ МОДИФИКАЦИЙ *R*-АЛГОРИТМА

Рассматривается семейство модификаций *r*-алгоритма — субградиентного алгоритма с преобразованием пространства. В отличие от *r*-алгоритма в предлагаемых модификациях значения коэффициентов растяжения пространства вычисляются в процессе работы алгоритма. Алгоритмы могут использоваться с постоянным шаговым множителем. Приводится результат исследования численной эффективности одного алгоритма рассматриваемого семейства.

Ключевые слова: *негладкая оптимизация, субградиент, преобразование пространства, численная эффективность.*

Введение. Более 40 лет назад был разработан субградиентный алгоритм минимизации с растяжением пространства в направлении разности двух последовательных градиентов — *r*-алгоритм [1]. Практика использования *r*-алгоритма показывает, что до настоящего времени он является одним из наиболее эффективных алгоритмов негладкой оптимизации. Однако теоретическое исследование эффективности алгоритма далеко не закончено. Основная проблема теоретического обоснования *r*-алгоритм состоит в согласованном выборе значений коэффициента растяжения пространства и шагового множителя. В работе приводится описание семейства модификаций *r*-алгоритма — $r(\sigma)$-алгоритмы. Величины коэффициентов растяжения пространства на итерациях $r(\sigma)$-алгоритмов не постоянны, они вычисляются в процессе его работы. Алгоритмы не требуют использования процедуры одномерного спуска по направлению.

Численная схема r-алгоритма. Рассматривается задача безусловной минимизации субдифференцируемой функции $f(x)$ в R^n. Будем обозначать $\partial f(x)$ множество субградиентов функции $f(x)$ в точке x.

В r-алгоритме используется оператор растяжения пространства [2] $R(\eta) = (\alpha - 1)\eta\eta^T + I$, где $\eta \in R^n$. α — направление и коэффициент растяжения пространства, $|\eta| = 1$, $\alpha \geq 0$. Вычислительная схема r-алгоритма применительно к задаче отыскания безусловного минимума функции $f(x)$ состоит в следующем.

0-ый шаг алгоритма (инициализация). Выбираем начальное приближение x_0 и невырожденное линейное преобразование B_0. Вы-

числяем: $g(x_0) \in \partial f(x_0)$; $g_0^* = B_0^* g(x_0)$ (субградиент в преобразованном пространстве $Y_0 = B_0^{-1} X \equiv A_0 X$, X — исходное пространство). Пусть на шаге k алгоритма $(k = 0,1,2,\ldots)$ получены определенные значения векторов x_k, g_k^* (субградиент в преобразованном пространстве) и матрицы B_k. ($A_k = B_k^{-1}$ — матрица преобразования пространства).

$(k+1)$-ый шаг алгоритма $(k = 0,1,2,\ldots)$.

Вычисляем:

1) h_{k+1} — шаговый множитель, $h_{k+1} \geq 0$.
2) $x_{k+1} = x_k - h_{k+1} B_k g_k^* / |g_k^*|$;
3) $g(x_{k+1}) \in \partial f(x_k)$. (субградиент в точке x_{k+1});
4) $\tilde{g}_{k+1}^* = B_k^* g(x_{k+1})$ (субградиент в преобразованном пространстве $Y_k = A_k X$);
5) $\eta_{k+1} = (\tilde{g}_{k+1}^* - g_k^*)/|\tilde{g}_{k+1}^* - g_k^*|$ (направление растяжения пространства Y_k);
6) $\alpha_{k+1} \geq 1, \beta_{k+1} = 1/\alpha_{k+1}$ (α_k коэффициент растяжения пространства Y_k);
7) $B_{k+1} = B_k R_{\beta_{k+1}}(\eta_k)$, (обратный оператор преобразования пространства $Y_{k+1} = A_{k+1} X = B_{k+1}^{-1} X$);
8) $g_{k+1}^* = R_{\beta_{k+1}}(\eta_{k+1}) \tilde{g}_{k+1}$ $(g_{k+1}^* = B_{k+1}^* g(x_k)$. (субградиент в преобразованном пространстве $Y_{k+1} = A_{k+1} X = B_{k+1}^{-1} X$).

Переходим к $(k+2)$-му шагу алгоритма, или прекращаем работу при выполнении критерия останова.

В r-алгоритме значения коэффициентов растяжения пространства (параметр r-алгоритма) выбираются одинаковыми на всех итерациях: $\alpha_k = \alpha > 1$. На практике рекомендуется это значение выбирать порядка 2.0. Величина шагового множителя определяется процедурой минимизации («спуска») по направлению $-B_k g_k^* / |g_k^*|$. Обычно применяемые процедуры «спуска» являются достаточно грубой реализацией алгоритма локализации минимума по направлению. Наиболее часто используется процедура адаптивной регулировки шаговых множителей [1]. Эта процедура определяется параметрами $0 < q_1 \leq 1$, $q_2 \geq 1$ и целым числом $L \geq 2$. Эти величины являются параметрами (константами) алгоритма.

Вычислительная схема $r(\sigma)$-алгоритмов. Вычислительная схема предлагаемых алгоритмов соответствует приведенной схеме

r-алгоритма. Отличие состоит лишь в следующем. Вместо оператора растяжения $R_\alpha(\eta)$ будет использоваться следующий оператор

$$\tilde{R}(\tilde{\eta}) = (\alpha - 1)\tilde{\eta}\tilde{\eta}^T + I, \qquad (1)$$

где $\tilde{\eta} \in R^n$, σ — нормирующий множитель, $\sigma \in R^1$, $\sigma > 0$. В отличие от оператора $R_\alpha(\eta)$, вектор $\tilde{\eta}$ не нормирован, то есть выполнение условия $|\tilde{\eta}| = 1$ не требуется. Различные варианты алгоритма будут определяться выбором нормирующего множителя σ.

Остановимся на простейших свойствах оператора $\tilde{R}_\sigma(\tilde{\eta})$: $\tilde{R}^* = \tilde{R}$; $\tilde{R}^{-1}(\tilde{\eta}) = -\left(\sigma / (1 + \sigma\tilde{\eta}^2)\right)\tilde{\eta}\tilde{\eta}^T + I$; $\tilde{R}_\sigma(0) = I$.

Пусть $|\tilde{\eta}| \neq 0$ и $\eta = \tilde{\eta} / |\tilde{\eta}|$. Тогда $\tilde{R}(\tilde{\eta}) = R_\alpha(\eta) + I$, где

$$\alpha = 1 + \sigma |\tilde{\eta}|^2 . \qquad (2)$$

Таким образом, если $\tilde{\eta} \neq 0$, то оператор $\tilde{R}_\sigma(\tilde{\eta})$ является оператором растяжения по направлению $\tilde{\eta} / |\tilde{\eta}|$. Значение коэффициента растяжения определяется (2). Значение нормирующего множителя σ будет определяться на основании субградиентов $\tilde{g}^*_{k+1}, g^*_k$: $\sigma_{k+1} = \sigma(\tilde{g}^*_{k+1}, g^*_k)$. Естественным требованием на функцию $\sigma(g_1, g_2)$ будет выполнение условия (условия «однородности») $\sigma(\mu g_1, \mu g_2) = \sigma(g_1, g_2) / \mu^2$, где $\mu \in R^1, \mu > 0$. Это условие обеспечивает независимость работы алгоритма от множителя на целевую функцию.

Легко видеть, что алгоритм $r(\sigma_0)$: $\sigma_0(g_1, g_2) = 1/|g_2 - g_1|^2$ фактически является r-алгоритмом с коэффициентом растяжения равным 2. Отметим, что именно это значение рекомендуется на практике использования r-алгоритм.

Выбирая различные нормирующие множители σ, мы будем получать различные алгоритмы рассматриваемого класса. В данной работе рассматривается $r(\sigma_1)$-алгоритм с нормирующим множителем $\sigma_1(g_1, g_2) = 1/|(g_2 | * | g_1|)$.

Численная эффективность $r(\sigma)$-алгоритмов. Приведем результаты численных исследований эффективности алгоритма $r(\sigma_1)$ в сравнении с r-алгоритмом. Результаты численных исследований эффективности других вариантов алгоритм $r(\sigma)$ приведены в [3, 4]. В качестве тестовых задач рассматривались задачи минимизации функций: $f(x) = \sum_{i=1}^{n} \rho_n^{i-1} |x_i|$, где параметр ρ_n выбирался в зависимости от раз-

мерности задачи n по формуле $\rho_n = 10^{6/(n-1)}$. Начальная точка $x_i = 1.0,\ \ i = 1,2,...n.$ Критерий останова: $f_k \le 10^{-6}$, где f_k — значение функции на итерации останова k.

Результаты решения тестовых задач минимизации функций $f(x)$ приведены в таблице, где приняты следующие обозначения: n — размерность пространства переменных; k — номер итерации, на которой алгоритм прекратил работу; kg — количество вычислений субградиента; $\alpha_{\max}$ — максимальное значение коэффициента растяжения; α_{avrg} — среднее значение коэффициента растяжения; r — результаты работы r-алгоритма с параметрами $q_1 = q_2 = 1$. В алгоритмах отмеченных символом «*» используется постоянная величина шага (в преобразованном пространстве). В алгоритмах, не отмеченных символом «*», используется адаптивная регулировка шаговых множителей *r*-алгоритма.

Таблица

Минимизация функции $f(x)$

Параметры / Алгоритм	n	k	k_g	$\alpha_{\max}$	α_{avrg}
r_1	100	1536	1554	5.38	4.49
r_1^*	100	1540	1541	5.76	4.49
r	100	3256	3264	2.00	2.00
r_1	500	7847	7873	5.19	4.58
r_1^*	500	7850	7851	5.19	4.58
r	500	16850	16864	2.00	2.00

Выводы. $r(\sigma)$-алгоритмы являются модификациями r-алгоритма. Вычислительная схема $r(\sigma)$-алгоритмов с постоянным шагом существенно проще схемы r-алгоритма. Величины коэффициентов растяжения пространства на итерациях $r(\sigma)$-алгоритмов не постоянны, они вычисляются в процессе его работы. Алгоритмы могут использоваться с постоянным шаговым множителем. Численные эксперименты показали достаточно высокую эффективность $r(\sigma)$-алгоритмов. Их эффективность не уступает эффективности r-алгоритма

Список использованной литературы:

1. Шор Н. З., Журбенко Н. Г. Метод минимизации, использующий операцию растяжения пространства в направлении разности двух последовательных градиентов. *Кибернетика*. 1971. № 3. С. 51-59.

2. Шор Н. З. Методы минимизации недифференцируемых функций и их применение. К.: Наук. думка, 1979. 208 с.
3. Журбенко Н. Г.Об одной модификации *r*-алгоритма. Материалы III Международной конференции *Математическое моделирование, оптимизация и информационные технологии*. Кишинеу: Эврика, 2012. С. 355–361.
4. Журбенко Н. Г., Чумаков Б. М. Программное управление коэффициентами растяжения *r*-алгоритма. *Теорія оптимальних рішень*. Київ: Ін-т кібернетики ім. В. М. Глушкова НАН України, 2012. С. 113–118.

Is considered the family of minimization algorithms using space dilation operation along the direction of the difference of two successive subgradients. In contrast to r-algorithm, in the proposed modifications the values of dilation coefficients are calculated in the process of algorithm. The algorithms can be used with a constant step size. Is the result of the study of the numerical efficiency of the algorithm considered family.

Key words: *nonsmooth optimization, subgradient, the transformation of the space, numerical efficiency.*

Получено 15.03.2017

УДК 681.3.06:006.354

Л. В. Ковальчук*, д-р техн. наук,
Н. В. Кучинська,** канд. техн. наук

*Інститут СЗР України, м. Київ,
**Національний технічний університет України «КПІ», м. Київ

ОЦІНКИ ПРАКТИЧНОЇ СТІЙКОСТІ МОДИФІКАЦІЙ НОВИХ СТАНДАРТІВ БЛОКОВОГО ШИФРУВАННЯ ВІДНОСНО ЦІЛОЧИСЕЛЬНОГО РІЗНИЦЕВОГО КРИПТОАНАЛІЗУ

Отримані науково обґрунтовані оцінки практичної стійкості до цілочисельного різницевого криптоаналізу ГОСТ-подібних та «Калина»-подібних блокових шифрів, проведено статистичний порівняльний аналіз отриманих значень з відповідними параметрами для випадкових вузлів заміни.

Ключові слова: *різницевий, диференціальний криптоаналіз, блокові шифри, стійкість, s-блоки, вузли заміни.*

Вступ. Сьогодні симетричні блокові алгоритми шифрування є основним криптографічним засобом забезпечення конфіденційності при обробці інформації у сучасних інформаційно-телекомунікаційних системах. За останні кілька років у країнах СНД прийнято низку власних стандартів блокових шифрів, а саме СТБ 34.101.31-2011 (Білорусь), ГОСТ Р 34.12 2015 (РФ) та ДСТУ 7624:2014 «Калина» (Україна). Варто зауважити, що в стандарті ГОСТ Р 34.12 2015 визначено

