АНАЛИТИЧЕСКИЕ И ЧИСЛЕННЫЕ МЕТОДЫ ИССЛЕДОВАНИЙ В МАТЕМАТИКЕ И ИХ ПРИЛОЖЕНИЯ

UDK 517.977

DIRECTIONAL DERIVATIVES OF VALUE FUNCTIONS IN PARAMETRIC NONLINEAR PROGRAMMING

Alexey Leschov, Leonid Minchenko
BSUIR, Minsk

We study the problem of existence and calculation of directional derivatives of value functions in the nonlinear mathematical programming problems which depend on parameters. This is one of the important problems in the theory of mathematical programming with perturbations of parameters [1,2]. We obtain sufficient conditions for existence and explicit formulas for calculating the directional derivatives of the first and second orders, under weaker hypotheses than those traditionally assumed.

We consider a mathematical programming problem $NLP(x)$ depending on a parameter $x \in R^n$:

$$f(x,y) \to \inf_y,$$

$$y \in F(x) = \{y \in R^m \mid h_i(x,y) \le 0,\ \ i \in I,\ \ h_i(x,y) = 0,\ \ i \in I_0\},$$

where $I = \{1,\dots,s\}$, $I_0 = \{s+1,\dots,p\}$, and all functions $f(x,y)$, $h_i(x,y)$ $i = 1,\dots,p$ are assumed to be twice continuously differentiable.

For the multivalued mapping F defined above by the constraints of $NLP(x)$, we use the notation

$$domF = \{x \in R^n \mid F(x) \ne \varnothing\},\ grF = \{(x,y) \mid y \in F(x),\ \ x \in R^n\}.$$

Consider the value function

$$\varphi(x) = \inf\{f(x,y) \mid y \in F(x)\}$$

and the solution set of the problem $NLP(x)$

$$\omega(x) = \{y \in F(x) \mid f(x,y) = \varphi(x)\},\ x \in R^n.$$

Fix a value $x^0 \in domF$ of the parameter for the rest of the paper. We assume that the set $\omega(x^0 + t\bar{x})$ is nonempty and uniformly bounded for all sufficiently small numbers $t \ge 0$, that is there exist a number $t_0 > 0$ and a bounded set $Y_0 \subset R^m$ such that $\omega(x^0 + t\bar{x}) \subset Y_0$ for all $t \in [0,t_0]$.

In the sequel, for arbitrary chosen $x \in domF$, $y \in F(x)$, $y^0 \in F(x^0)$ and $(\bar{x},\bar{y}) \in \mathrm{R}^n \times \mathrm{R}^m$, we denote the pairs (x,y), (x^0,y^0) and $(\bar{x},\bar{y})$ by symbols z, z^0 and $\bar{z}$, respectively.

Consider the Lagrange function

$$L(z,\lambda) = f(z) + \langle \lambda, h(z) \rangle, \text{ where } \lambda = (\lambda_1,\dots,\lambda_p),\ h = (h_1,\dots,h_p).$$

Following [2, 3] introduce the lower Dini derivatives of the multivalued mapping F at the point z^0 in the direction $\bar{x}$:

$$DF(z^0;\bar{x}) = \{\bar{y} \in R^m \mid y^0 + t\bar{y} + o(t) \in F(x^0 + t\bar{x}),\ \forall t > 0\}$$

$$D^2F(z^0,\bar{z};\bar{x}) = \{\bar{v} \in R^m \mid y^0 + t\bar{y} + t^2\bar{v} + o(t^2) \in F(x^0 + t\bar{x}), \forall t > 0\}$$

and the sets

$$\Gamma(z^0;\bar{x}) = \{\bar{y} \in R^m \mid \langle \nabla h_i(z^0), \bar{z}\rangle \le 0,\ i \in I(z^0),\ \langle \nabla h_i(z^0), \bar{z}\rangle = 0,\ i \in I_0,\ \bar{z} = (\bar{x}, \bar{y})\}$$

$$\Gamma^2(z^0, \bar{z}; \bar{x}) = \{\bar{v} \in R^m \mid \langle \nabla_y h_i(z^0), \bar{v}\rangle + \frac{1}{2}\langle \bar{z}, \nabla^2 h_i(z^0)\bar{z}\rangle \le 0,\ i \in I^2(z^0, \bar{z}),$$

$$\langle \nabla_y h_i(z^0), \bar{v}\rangle + \frac{1}{2}\langle \bar{z}, \nabla^2 h_i(z^0)\bar{z}\rangle = 0,\ i \in I_0\},$$

where

$$I^2(z^0, \bar{z}) = \{i \in I(z^0) \mid \langle \nabla h_i(z^0), \bar{z}\rangle = 0\},\ I(z^0) = \{i \in I \mid h_i(z^0) = 0\},$$

$$I^a(z^0, \bar{z}) = \{i \in I^2(z^0, \bar{z}) \mid \langle \nabla_y h_i(z^0), \bar{v}\rangle + \frac{1}{2}\langle \bar{z}, \nabla^2 h_i(z^0)\bar{z}\rangle = 0,\ \forall \bar{v} \in \Gamma^2(z^0, \bar{z}; \bar{x})\}.$$

The main idea of our paper is to propose a new regularity-like condition (see the definition below) which allows to extend significantly the known results [1] about differential properties of value functions.

Definition 1. We say that the relaxed Mangasarian-Fromovitz condition in the direction $\bar{x}$ (briefly $RMF_{\bar{x}}$) holds at the point $z^0 = (x^0, y^0) \in grF$ iff $\Gamma(z^0; \bar{x}) \ne \varnothing$ and the system of (R^{m+1})-vectors

$$\begin{pmatrix} \nabla_y h_i(z) \\ \langle \nabla_x h_i(z), \bar{x}\rangle \end{pmatrix},\ i \in I_0 \cup I^a(z^0, \bar{x})$$

has constant rank near z^0.

The next theorem gives us sufficient conditions for the directional differentiability of multivalued mappings.

Theorem 1. Let $RMF_{\bar{x}}$ hold at the point z^0. Then $DF(z^0; \bar{x}) = \Gamma(z^0; \bar{x}) \ne \varnothing$.

Definition 2. Let $\bar{y} \in \Gamma(z^0; \bar{x})$. We say that the relaxed second order Mangasarian-Fromovitz condition at the point z^0 along the vector $\bar{z} = (\bar{x}, \bar{y})$ in the direction $\bar{x}$ (briefly, $RMF^2_{\bar{x}}(\bar{z})$) holds iff $\Gamma^2(z^0, \bar{z}; \bar{x}) \ne \varnothing$ and the system

$$\begin{pmatrix} \nabla_y h_i(z) \\ \langle \nabla_x h_i(z), \bar{x}\rangle \end{pmatrix},\ i \in I_0 \cup I^a(z^0, \bar{z})$$

has constant rank for all z in some neighbourhood of the point z^0.

Theorem 2. Let $\bar{y} \in \Gamma(z^0; \bar{x})$. If the condition $RMF^2_{\bar{x}}(\bar{z})$ holds at the point $z^0 = (x^0, y^0)$ along the vector $\bar{z} = (\bar{x}, \bar{y})$ then $D^2F(z^0, \bar{z}; \bar{x}) = \Gamma^2(z^0, \bar{z}; \bar{x}) \ne \varnothing$.

Denote $\Phi(z^0, \bar{z}, \bar{v}) = \langle \nabla_y f(z^0), \bar{v}\rangle + \frac{1}{2}\langle \bar{z}, \nabla^2 f(z^0)\bar{z}\rangle$.

Theorem 3. Let $RMF_{\bar{x}}$ and strong second order sufficient condition in the direction $\bar{x}$ ($SSOSC_{\bar{x}}$) hold at all points $z^0 = (x^0, y^0)$, where $y^0 \in \omega(x^0)$. Then

1) the function φ is differentiable at the point x^0 in the direction $\bar{x}$ and

$$\varphi'(x^0; \bar{x}) = \min_{y^0 \in \omega(x^0)} \min_{\bar{y} \in \Gamma(z^0; \bar{x})} \langle \nabla f(z^0), \bar{z}\rangle = \min_{y^0 \in \omega(x^0)} \max_{\lambda \in \Lambda(z^0)} \langle \nabla_x L(z^0, \lambda), \bar{x}\rangle$$

2) the following formula is valid

$$D^2_+\varphi(x^0; \bar{x}) = \inf_{y^0 \in \omega(x^0, \bar{x})} \inf_{\bar{y} \in \Gamma^*(z^0; \bar{x})} \inf_{\bar{v} \in \Gamma^2(z^0, \bar{z}; \bar{x})} 2\Phi(z^0, \bar{z}, \bar{v}) =$$

$$= \inf_{y^0 \in \omega(x^0, \bar{x})} \inf_{\bar{y} \in \Gamma^*(z^0; \bar{x})} \sup_{\lambda \in \Lambda^2(z^0, \bar{x})} \langle (\bar{x}, \bar{y}), \nabla^2_{zz} L(z^0, \lambda)(\bar{x}, \bar{y})\rangle.$$

References

1. Bonnans, J.F. Perturbations analysis of optimization problems / J.F. Bonnans, A. Shapiro. – New York: Springer-Verlag, 2000.
2. Luderer, B. Multivalued analysis and nonlinear programming problems with perturbations / B. Luderer, L. Minchenko, T. Satsura. – Dordrecht: Kluwer Acad. Publ., 2002. – 222 p.
3. Minchenko, L.I. Parametric nonlinear programming problems under relaxed constant rank regularity condition / L. Minchenko, S. Stakhovski // SIAM Journal on Optimization. – 2011. – Vol. 21. – N 1.

УДК 511.1

ПРОСТЫЕ ЧИСЛА МЕРСЕННА

Аксамит М.В., Былинович В.Н.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск
Научный руководитель: Стройникова Е.Д.

Основная теорема арифметики гласит, что всякое натуральное число $n > 1$ можно представить в виде произведения простых множителей:

$$n = p_1 * p_2 * \dots * p_m,$$

где $p_1, p_2, \dots, p_m$ – простые числа.

Разложение натурального числа на составляющие его простые множители называется факторизацией числа. В настоящий момент неизвестен такой алгоритм факторизации, который мог бы разложить любое большое число на простые множители за полиномиальное время. Благодаря этому простые числа нашли широкое применение в криптографии. Например, RSA: для того, чтобы взломать данный шифр, нужно разложить большое число n, известное по открытому ключу, на простые множители, которых всего два. В том же алгоритме RSA для генерации ключей требуется найти большие простые числа, что на сегодняшний день гораздо проще факторизации.

Небольшие простые числа из начала списка простых можно получить с помощью таких несложных алгоритмов, как решето Эратосфена, Сундарама или Аткина. Но на практике, как правило, нужны числа более высоких порядков. Тут на помощь приходят тесты на простоту – алгоритмы, проверяющие, является ли число простым. Но само число сначала нужно сгенерировать.

Существует ряд чисел специального вида, простоту которых можно доказать эффективными алгоритмами и за полиномиальное время:

Числа Мерсенна – самые большие из известных простых чисел, очень распространены благодаря существованию эффективного теста на простоту Люка–Лемера, однако бесконечность таких чисел до сих пор не доказана. Их можно представить в виде

$$M_p = 2^p - 1,$$

где p – простое число. Замечание: простоты числа p недостаточно для доказательства простоты числа Мерсенна. Для этого существует специальный алгоритм: тест Люка – Лемера для чисел Мерсенна. Тест основывается на том, что простота числа M_p влечет за собой простоту числа p. Пусть p – простое число, большее либо равное трем. Зададим последовательность:

$$L_0 = 4,$$
$$L_{n+1} = L_n^2 + 2.$$

Тогда M_p простое тогда и только тогда, когда $L_{p-2} \equiv 0 \ (mod\ M_p)$.

При реализации теста вычисляют не сами значения $L_0, L_1, \dots, L_k$, длина которых растет по экспоненте, а только их остатки от деления на M_p.