7. S. L. Krivoi, "A search algorithm for invariant relations in programs," Kibernetika, No. 5, 12-18 (1981).
8. B. Wegbreit, "The synthesis of loop predicates," Comm. ACM, No. 2, 102-112 (1974).
9. S. Katz and Z. Manna, "Logical analysis of programs," Comm. ACM, No. 4, 188-206 (1976).
10. V. S. Kostyrko, "The analysis of computer programs," in: Methodology and Experience with Problems of Quality Control Automation [in Russian], Izd. Inst. Kibern., Akad. Nauk UkrSSR, Kiev (1978), pp. 38-49.
11. V. R. Pratt, "Semantical consideration of Floyd—Hoare logic," Proc. 17th Ann. Symp. on Foundations of Computer Science, Houston, Springer, Berlin (1976), pp. 109-121.
12. V. S. Kostyrko, "A procedure for proving program correctness," Kibernetika, No. 1, 50-58 (1978).
13. C. A. R. Hoare, "A note on the for statement," BIT, No. 3, 80-86 (1972).

GENERATION OF INTEGRAL CHARACTERISTICS OF SYMMETRIC-RANGE RESIDUE CODES

A. A. Kolyada and M. Yu. Selyaninov

UDC 681.14

In the residue number system (RNS) with the bases $m_1, m_2, \ldots, m_k$ are, the number A from the symmetric range

$$D_k^- = \left\{-\left[\frac{1}{2}M_k\right], \ -\left[\frac{1}{2}M_k\right]+1, \ldots, \right] \times \frac{1}{2}M_k[-1\right\},$$

where $M_k = \prod_{i=1}^{k} m_i$, [X] and]X[are, respectively, the nearest integers to X on the left and on the right, has the same residue representation as its complement code $A_g \in D_k = \{0, 1, \ldots, M_k - 1\}$ mod M_k, defined as

$$A_g = \begin{cases} A, & \text{if} \quad A \geqslant 0, \\ A + M_k, & \text{if} \quad A < 0. \end{cases}$$

Operations on numbers from the range D_k^- normally use the integral characteristics of nonpositional codes (rank, nucleus, coefficients of mixed-radix representation, etc.) corresponding to the elements of the set D_k, and not D_k^-. This increases the complexity of many nonmodular operations in RNS, primarily multiplication and division. In order to overcome this weakness of the traditional construction of modular arithmetic, a symmetric RNS has been proposed, whose code is easily converted into symmetric mixed-radix code [1]. By using the latter instead of the ordinary code, we manage to speed up the execution of some RNS operations, such as division [2, 3].

In this article, we consider the generation of the most useful symmetric integral characteristics of residue code, i.e., characteristics corresponding to the range D_k^-, by the method of signed numbers using the operation of restriction of the interval-residue code [4-6]. Unlike the k-step recursive procedure generating the symmetric mixed-radix code [1], the proposed algorithm is strictly parallel. Its running time is 1 + $]\log_2 k[$ modular operations.

We introduce the following notation: $|X|_m$ is the least nonnegative remainder congruent with X mod m; $|X|_m^-$ is the least absolute value remainder congruent with X modulo

$$m \left(-\frac{1}{2}m \leqslant |X|_m^- < \frac{1}{2}m\right);$$

$$[X]^- = \begin{cases} [X], & \text{if} \quad X < [X] + \frac{1}{2}; \\ [X] + 1, & \text{if} \quad X \geqslant [X] + \frac{1}{2}; \end{cases}$$

Translated from Kibernetika, No. 4, pp. 20-24, July-August, 1986. Original article submitted February 1, 1984.

$$\alpha_{i,l} = |AM_{i,l}^{-1}|_{m_i},$$

$$M_{i,l} = \frac{M_l}{m_i} M_l = \prod_{j=1}^{l} m_j \, (i, l = 1, 2, \ldots, k);$$

$m_1, m_2, \ldots, m_k$ is a system of pairwise relatively prime moduli.

The relevant integral characteristics of nonpositional code are defined as follows.

Definition 1. The symmetric rank and nucleus of an integer A in the system with the moduli $m_1, m_2, \ldots, m_l$ ($l > 1$) are, respectively, the integers $\rho_l^-(A)$ and $\eta_l^-(A)$ satisfying the relationships

$$\begin{aligned} |A|_{M_l}^- &= \sum_{i=1}^{l} M_{i,l}\alpha_{i,l} - \rho_l^-(A) M_l, \\ |A|_{M_l}^- &= \sum_{i=1}^{l-1} M_{i,l-1}\alpha_{i,l-1} + \eta_l^-(A) M_{l-1}. \end{aligned} \tag{1}$$

Definition 2. The symmetric interval number of l-th order of an integer A with respect to the moduli $m_0 = 1$, $m_1, m_2, \ldots, m_l$ ($l \geqslant 0$) is $N_l^-(A) = [A/M_l]^-$, $M_0 = 1$.

Definition 3. The symmetric mixed-radix representation of the number $A \in D_k^-$ with respect to the moduli $m_1, m_2, \ldots, m_k$ is a representation of the form

$$A = \sum_{i=1}^{k} a_i^- M_{i-1}, \tag{2}$$

where a_i^- is an integer coefficient satisfying the inequality $-m_i/2 \leqslant a_i^- < m_i/2$ ($i = 1, 2, \ldots, k$).

Repeating the manipulations of [7-9] for the rank $\rho_l(A)$ and the nucleus $\eta_l(A)$ of the number $A \in D_l$, we prove the following theorem.

THEOREM 1. In the RNS with the moduli $m_1, m_2, \ldots, m_l$ ($l > 1$), the rank $\rho_l^-(A)$ and the symmetric nucleus $\eta_l^-(A)$ of any integer satisfy the formulas

$$\rho_l^-(A) = \hat{\rho}_l(A) + \theta_l^-(A), \tag{3}$$

$$\eta_l^-(A) = \hat{\eta}_l(A) - m_l\theta_l^-(A), \tag{4}$$

where

$$\hat{\rho}_l(A) = \left[\frac{1}{m_l} \sum_{i=1}^{l} \left[\frac{m_l\alpha_{i,l}}{m_i}\right]\right], \tag{5}$$

$$\hat{\eta}_l(A) = \left|\alpha_{l,l} - \sum_{i=1}^{l-1} \frac{\alpha_{i,l-1}}{m_i}\right|_{m_l}, \tag{6}$$

$\theta_l^-(A)$ is Amerbaev's symmetric correction defined by

$$\theta_l^-(A) = -\left[\frac{1}{m_l}\left(\left[\frac{|A|_{M_l}^-}{M_{l-1}}\right] - \rho_{l-1}(A)\right)\right],$$

$\rho_{l-1}(A)$ is the normalized rank of A in the RNS with the moduli $m_1, m_2, \ldots, m_{l-1}$ [7, p. 142].

Remark. The rank $\rho_{l-1}(A)$ of any integer A satisfies the inequality $0 \leqslant \rho_{l-1}(A) \leqslant l - 2$ [7], and since

$$\min_{X \in D_l^-} \left[\frac{X}{M_{l-1}}\right] \geqslant -\frac{m_l + 1}{2},$$

the above expression for $\theta_l^-(A)$ implies that this quantity takes only two values 0 and 1, if $m_l > 2(l - 2)$.

Definition 4. The interval-residue representation of an integer A in the system with the moduli $m_1, m_2, \ldots, m_{l-1}$ is a representation of the form

$$A = \sum_{i=1}^{l-} M_{i,l-1}\alpha_{i,l-1} + \dot{I}_{l-1}(A) M_{l-1}, \tag{7}$$

where the integer $\dot{I}_{l-1}(A)$ is called the interval index of A. The characteristic $J_l(A) = [\dot{I}_{l-1}(A)/m_l]$ is called the nuclear interval index of A with respect to the modulus m_l ($l > 1$).

We thus obtain the following theorem.

THEOREM 2. In the RNS with the moduli $m_1, m_2, \ldots, m_l$, the l-th order symmetric interval number of any integer A satisfies the relationship

$$N_l^-(A) = J_l(A) + \theta_l^-(A), \quad l = 2, 3, \ldots, k. \tag{8}$$

Proof. From (7) we find that

$$\dot{I}_{l-1}(A) = \frac{A}{M_{l-1}} - \sum_{i=1}^{l-1} \frac{M_{i,l-1}\alpha_{i,l-1}}{M_{l-1}},$$

and therefore using (6) and our notation we obtain

$$|\dot{I}_{l-1}(A)|_{m_l} = \left|\alpha_{l,l} - \sum_{i=1}^{l-1} \frac{\alpha_{i,l-1}}{m_i}\right|_{m_l} = \hat{\eta}_l(A),$$

where A is an integer. Then, by Euclid's lemma from divisibility theory and Definition 4, we represent the interval index $\dot{I}_{l-1}(A)$ of A in the form

$$\dot{I}_{l-1}(A) = \hat{\eta}_l(A) + J_l(A) m_l. \tag{9}$$

Substituting (9) in (7) and applying (1) and (4), we obtain

$$A = \sum_{i=1}^{l-1} M_{i,l-1}\alpha_{i,l-1} + (\hat{\eta}_l(A) + J_l(A) m_l) M_{l-1} = \sum_{i=1}^{l-1} M_{i,l-1}\alpha_{i,l-1} + \hat{\eta}_l(A) M_{l-1} - \theta_l^-(A) M_l +$$

$$+ \theta_l^-(A) M_l + J_l(A) M_l = \sum_{i=1}^{l-1} M_{i,l-1}\alpha_{i,l-1} + \eta_l^-(A) M_{l-1} + (J_l(A) + \theta_l^-(A)) M_l = |A|_{M_l}^{-} + (J_l(A) + \theta_l^-(A)) M_l,$$

whence follows the sought result (8).

THEOREM 3. The coefficient a_l^- of the symmetric representation of $A \in D_k^-$ in the mixed-radix number system with the bases $m_1, m_2, \ldots, m_k$ satisfies the formula

$$a_l^- = |J_{l-1}(T_l(A)) + \theta_{l-1}^-(A)|_{m_l}^{-}, \tag{10}$$

where

$$T_l(A) = \sum_{i=1}^{l-1} M_{i,l-1}\alpha_{i,l-1} + \hat{\eta}_l(A) M_{l-1}, \tag{11}$$

$$l = 3, 4, \ldots, k.$$

Proof. Using (4) to compare (1) and (11), we see that

$$|T_l(A)|_{M_l}^{-} = |A|_{M_l}^{-}. \tag{12}$$

Then, applying the modified Euclid's lemma and (2), we may write

$$T_l(A) = N_l^-(T_l(A)) M_l + |A|_{M_l}^{-} = N_l^-(T_l(A)) M_l + a_l^- M_{l-1} + \sum_{i=1}^{l-1} a_i^- M_{i-1}.$$

Hence it follows that

$$N_{l-1}^-(T_l(A)) = N_l^-(T_l(A)) m_l + a_l^-.$$

Expressed in terms of the least absolute value remainders, mod m_l, this leads to an important formula for the l-th digit of the symmetric mixed-radix code of $A \in D_k^-$:

$$a_l^- = |N_{l-1}^-(T_l(A))|_{m_l}^{-}, \quad l = 2, 3, \ldots, k. \tag{13}$$

Now in order to obtain (10) from (13), it suffices to apply Theorem 2 [see (8)] and equality (12).

From Theorems 1-3 we see [see (3)-(6), (8), (10)] that generation of the sought symmetric integral characteristics of residue codes [$\rho_l^-(A)$, $\eta_l^-(A)$, $N_l^-(A)$, a_l^-] reduces to computing some approximate values of these characteristics [$\hat{\rho}_l(A)$, $\hat{\eta}_l(A)$, $\hat{N}_l(A) = J_l(A)$, $\hat{a}_l = |J_{l-1}(T_l \times (A))|_{m_l}$] and finding the corresponding Amerbaev's symmetric corrections. We will show that these characteristics may be generated by the method of signed numbers, based on the operation of restriction of interval-residue representations of the numbers $T_l(A)$ ($l = 3, 4, \dots, k$).

Using the relation

$$m_{l-1}\alpha_{i,l-1} = \alpha_{i,l-2} + \left[\frac{m_{l-1}\alpha_{i,l-1}}{m_i}\right] m_i \tag{14}$$

which follows from Euclid's lemma, we can easily transform (11) to the form

$$T_l(A) = \sum_{i=1}^{l-2} M_{i,l-2}\alpha_{i,l-2} + \hat{\eta}_{l-2}(A) M_{l-2} + J_{l-1}(T_l(A)) M_{l-1}, \tag{15}$$

where

$$\hat{\eta}_{l-1}(A) = \left|\sum_{i=1}^{l-1}\left[\frac{m_{l-1}\alpha_{i,l-1}}{m_i}\right]\right|_{m_{l-1}}, \tag{16}$$

$$\hat{\rho}_{l-1}(A) = \left[\frac{1}{m_{l-1}}\sum_{i=1}^{l-1}\left[\frac{m_{l-1}\alpha_{i,l-1}}{m_i}\right]\right], \tag{17}$$

$$J_{l-1}(T_l(A)) = \hat{\rho}_{l-1}(A) + \hat{\eta}_l(A), \tag{18}$$

$$\hat{\eta}_l(A) = \left|\sum_{i=1}^{l}\left[\frac{m_l\alpha_{i,l}}{m_i}\right]\right|_{m_l}. \tag{19}$$

Note that (6) and (19) are equivalent, since by (14)

$$\left|\left[\frac{m_l\alpha_{i,l}}{m_i}\right]\right|_{m_l} = \left|-\frac{\alpha_{i,l-1}}{m_i}\right|_{m_l}.$$

Let us now consider the generation of Amerbaev's symmetric corrections.

Definition 5. Numbers of the form

$$Z_l^-(A) = T_l(A) - \frac{1}{2}M_l,\ l = 1, 2, \dots, k, \tag{20}$$

where $T_1(A) = |A|_{m_1}$ and $T_l(A)$ ($l = 2, 3, \dots, k$) are defined by (11), are called signed numbers.

THEOREM 4. If $m_l > 2(l - 2)$ ($l = 2, 3, \dots, k$), then for Amerbaev's symmetric correction $\theta_l^-(A)$, where $A \in D_k^-$, we have

$$\theta_l^-(A) = \begin{cases} 0, & \text{if } Z_l^-(A) < 0, \\ 1, & \text{if } Z_l^-(A) \geqslant 0. \end{cases}$$

Proof. Adding and subtracting $\theta_l^-(A) M_l$ in the right-hand side of (11) and then using (1) and (4), we represent $T_l(A)$ in the form

$$T_l(A) = |A|_{\overline{M}_l} + \theta_l^-(A) M_l,\ l = 2, 3, \dots, k.$$

Then from (20)

$$Z_l^-(A) = |A|_{\overline{M}_l} + \left(\theta_l^-(A) - \frac{1}{2}\right) M_l. \tag{21}$$

The sought result now may be obtained from (21) if we note that $-M_l/2 \leqslant |A|_{\overline{M}_l} < M_l/2$ and the correction $\theta_l^-(A)$ takes only two values, 0 or 1, since $m_l > 2(l - 2)$ (see remark).

This relationship between Amerbaev's symmetric corrections and the signs of the signed numbers (20) is a key element in the proposed method of generating integral characteristics of nonpositional codes. The following lemma also plays an important role in this method.

LEMMA. Let the moduli $m_2, m_3, \dots, m_k$ of the RNS be odd numbers, and $m_i > 2(i-2)$ $(i > 4)$, then:

1) for all $l = 3, 4, \dots, k$, $J_{l-1}(T_{l-1}(A)) > \frac{m_{l-1}}{2}$ implies $Z^-(A) \geqslant 0$, and $J_{l-1}(T_l(A)) < \frac{m_l - 1}{2}$ implies $J_l^-(A) < 0$;

2) if $\hat{\eta}_2(A) > \frac{m_2 - 1}{2}$, then $Z_2^-(A) \geqslant 0$, and if $\hat{\eta}_2(A)^2 < \frac{m_2 - 1}{2}$, then $Z_2^-(A) < 0$;

3) the number $Z_1^-(A)$ and the remainder $|A|^-_{m_1}$ have the same sign.

Proof. Substituting (15) in (20), we obtain

$$Z_l^-(A) = T_{l-1}(A) + \left(J_{l-1}(T_l(A)) - \frac{m_l}{2}\right) M_{l-1}. \tag{22}$$

Adding and subtracting $\theta_{l-1}^-(A) M_{l-1}$ in the right-hand side of (22) and using (1) and (4), we represent the signed number $Z_l^-(A)$ $(l = 3, 4, \dots, k)$ in the form

$$Z_l^-(A) = |A|^-_{M_{l-1}} + \left(J_{l-1}(T_l(A)) + \theta_{l-1}^-(A) - \frac{m_l}{2}\right) M_{l-1}. \tag{23}$$

First let $J_{l-1}(T_l(A)) > \frac{m_l - 1}{2}$.

Since the modulus m_l $(l = 2, 3, \dots, k)$ is odd, the number $\frac{m_l - 1}{2}$ is an integer; therefore, $J_{l-1}(T_l(A)) \geqslant \frac{m_l - 1}{2} + 1$ and regardless of the particular value of the correction $\theta_{l-1}^-(A)$ (whether 0 or 1) we have the inequality $J_{l-1}(T_l(A)) + \theta_{l-1}^-(A) - \frac{m_l}{2} \geqslant \frac{1}{2}$, and thus also $Z_l^-(A) \geqslant 0$ [see (23)]. If $J_{l-1}(T_l(A)) > \frac{m_l - 1}{2}$, then as in the previous case we obtain $J_{l-1}(T_l(A)) + \theta_{l-1}^-(A) - \frac{m_l}{2} < -\frac{1}{2}$, which reduces (23) to $Z_l^-(A) < 0$.

Parts 2 and 3 of the lemma are proved similarly, using the numbers

$$Z_2^-(A) = |A|_{m_1} + \left(\hat{\eta}_2(A) - \frac{m_2}{2}\right) m_1 \tag{24}$$

and

$$Z_1^-(A) = |A|_{m_1} - \frac{m_1}{2}.$$

From (22) and (24) we see that in case of indeterminacy, when $J_{l-1}(T_l(A)) = \frac{m_l - 1}{2}$ $(l = 3, 4, \dots, k)$ or $\hat{\eta}_2(A) = \frac{m_2 - 1}{2}$, the signed number $Z_l^-(A)$ $(l = 2, 3, \dots, k)$ coincides with the number $Z_{l-1}^-(A)$, so that the procedure of restriction of the interval-residue representations of the numbers $T_3(A), T_4(A), \dots, T_k(A)$ described by (16)-(19) in conjunction with the above lemma makes it possible to determine the signs of all the signed numbers (20), and hence also Amerbaev's symmetric corrections $\theta_l^-(A)$ $(l = 2, 3, \dots, k)$.

The preceding discussion suggests the following algorithm to generate the symmetric integral characteristics of the residue code $(\alpha_1, \alpha_2, \dots, \alpha_k) = (|A|_{m_1}, |A|_{m_2}, \dots, |A|_{m_k})$ of the number $A \in D_k^-$.

1. For all $l = 3, 4, \dots, k + 1$ compute $\hat{\eta}_{l-1}(A)$ and $\hat{\rho}_{l-1}(A)$ [see (16) and (17)].

2. Use (10), (11), (13), (18) to determine approximate values of the k − 1 highest-order digits in the mixed-radix code of the number A:

$$\hat{a}_2 = \hat{\eta}_2, \quad \hat{a}_l = |\hat{\rho}_{l-1}(A) + \hat{\eta}_l(A)|_{m_l}, \quad l = 3, 4, \dots, k,$$

and generate the characteristics

$$S_1 = \begin{cases} 0, & \text{if } \alpha_1 < \frac{m_1}{2}; \\ 1, & \text{if } \alpha_1 \geqslant \frac{m_1}{2}, \end{cases}$$

$$S_2 = \begin{cases} 0, & \text{if} \quad \hat{\eta}_2(A) \leqslant \frac{m_2 - 1}{2}; \\ 1, & \text{if} \quad \hat{\eta}_2(A) > \frac{m_2 - 1}{2}, \end{cases}$$

$$S_l = \begin{cases} 0, & \text{if} \quad \hat{\rho}_{l-1}(A) + \hat{\eta}_l(A) \leqslant \frac{m_l - 1}{2}; \\ 1, & \text{if} \quad \hat{\rho}_{l-1}(A) + \hat{\eta}_l(A) > \frac{m_l - 1}{2}, \quad l = 3, 4, \ldots, k; \end{cases}$$

$$H_l = \begin{cases} 0, & \text{if} \quad \hat{a}_l \neq \frac{m_l - 1}{2}; \\ 1, & \text{if} \quad \hat{a}_l = \frac{m_l - 1}{2}, \quad l = 2, 3, \ldots, k. \end{cases}$$

3. Apply the lemma and Theorem 4 to generate Amerbaev's symmetric corrections by the rule

$$\theta_1^-(A) = S_1, \quad \theta_l^-(A) = \overline{H}_l S_l V H_l \theta_{l-1}^-(A), \quad l = 2, 3, \ldots, k,$$

or in parallel form

$$\theta_l^-(A) = S_l \overline{H}_l V S_{l-1} \overline{H}_{l-1} H_l V S_{l-2} \overline{H}_{l-2} H_{l-1} H_l V \ldots V S_2 \overline{H}_2 \overline{H}_3 \ldots H_l V S_1 H_2 H_3 \ldots H_l, \quad l = 2, 3, \ldots, k.$$

4. Use (3), (4), (10), (13) to compute the sought symmetric integral characteristics of the residue code: the rank $\rho_k^-(A)$, the nucleus $\eta_k^-(A)$, the coefficients

$$a_1^- = |\alpha_1|_{m_1}^-, \quad a_l^- = |\hat{a}_l + \theta_{l-1}^-(A)|_{m_l}^-, \quad l = 2, 3, \ldots, k, \tag{25}$$

of the mixed-radix code.

The l-th order symmetric interval number $N_l^-(A)$ of A (l = 1, 2,...,k − 1) is determined by the k − l highest-order digits of the mixed-radix representation:

$$N_l^-(A) = a_{l+1}^- + a_{l+2}^- m_{l+1} + \ldots + a_k^- m_{l+1} m_{l+2} \ldots m_{k-1}.$$

If the mixed-radix code of A is not generated, the characteristic $N_l^-(A)$ (l = 2, 3,..., k − 1) may be obtained by computing from (7) the residue code of the nuclear interval index $J_l(A)$ in the system with the moduli m_{l+1}, m_{l+2},...,m_k and then using (8).

Under conditions of maximum parallelism, the proposed algorithm generating the symmetric integral characteristics of the residue code required 1 +]log₂ k[modular operations.

Our results lead to the following conclusions.

1. The symmetric integral characteristics of residue codes, like their known analogs [10], have the same structure, which is largely determined by Amerbaev's symmetric corrections.
2. The method of signed numbers provides a universal and efficient apparatus for generating symmetric integral characteristics of residue codes.
3. The existing generators of integral characteristics of nonpositional codes [5, 6] may be easily adapted for use with symmetric-range residue codes.

LITERATURE CITED

1. N. S. Szabo and R. I. Tanaka, Residue Arithmetic and Its Application to Computer Technology, McGraw-Hill, New York (1967).
2. E. Kinoshita, H. Kosako, and Y. Kojima, "General division in the symmetric residue number system," IEEE Trans., Comp., 22, No. 2, 134 (1973).
3. D. K. Banergi, Cheung To-Yat, and V. Ganesan, "A high-speed division method in residue arithmetic," Proc. 5th Symp. Comput. Arithmetic (Ann Arbor, May 18-19, 1981), New York (1981), pp. 158-164.
4. A. A. Kolyada, "Algorithms in generalized RCS arithmetic," Vestn. Belorus. Univ., Ser. 1, No. 1, 6-12 (1980).
5. A. A. Kolyada and L. Zh. Ivashkova, Soviet Patent No. 800989," A Device to Find the Rank of a Number," Byull. Izobret., No. 4 (30 Jan. 1981).
6. A. A. Kolyada, Soviet Patent No. 968802, "A Device to Generate Positional Characteristics of Nonpositional Code," Byull. Izobret., No. 39 (23 Oct. 1982).

7. V. M. Amerbaev, Theoretical Fundamentals of Machine Arithmetic [in Russian], Nauka, Kazakh. SSR, Alma-Ata (1976).
8. A. A. Kolyada and F. S. Pilipovets, "On the distribution of Amerbaev's correction to the approximate rank of a number in a RCS," Vestnik Belorus. Univ., Ser. 1, No. 3, 12-16 (1982).
9. A. A. Kolyada, "On the nucleus of a number in residue class systems," Kibernetika, No. 3, 124-126 (1982).
10. A. A. Kolyada and V. K. Kravtsov, "On a method of generation of positional characteristics of nonpositional code," in: Int. Conf. on Math. Methods in Op. Res. (Sofia, Oct. 24-29, 1983), ANB, Sofia (1983), pp. 39-41.

MINIMIZATION METHODS FOR FUNCTIONS ON SIMPLE SETS

V. S. Mikhalevich, N. N. Redkovskii,
and A. E. Perekatov

UDC 519.6

INTRODUCTION

Historically, the main efforts in the development of numerical methods of nonlinear programming concentrated on the solution of nonlinear programming problems in general form. A whole arsenal of such methods is currently available, including penalty function methods, different versions of the linearization method, etc. Yet the use of general methods is not necessarily justified in many special cases.

In this article, we consider special optimization methods for the solution in a number of common problems. These are primarily minimum seeking problems on sets of "simple" structure [1]. Let E^n be an Euclidean space, and x the elements in this space with the components x^i, i = 1,...,n. Simple sets are a parallelepiped $\{x: a_i \leqslant x^i \leqslant b_i\}$, a ball $\{x: \|x\| \leqslant R\}$, a sphere $\{x: \|x\| = R\}$, a simplex $\{x: x^1 + \ldots + x^n = 1,\ x^i \geqslant 0\}$, and so on. In the development of any mathematical model, these constraints naturally arise before the introduction of other more constraints.

The existing approaches to the construction of special numerical methods of minimizing f(x) on such sets may be divided into two groups. In one group, the direction of descent p_k in the scheme $x_{k+1} = x_k + \alpha_k p_k$ is projected onto the set D on which the minimum is sought. The step α_k is chosen so that the sequence x_k does not leave the set D. One of the first studies in this direction is [2]. This approach is developed in [3, 4] mainly for parallelepiped constraints.

The methods of the other group first construct a nonlinear transformation $x = \varphi(z)$, such that $x \in D$ for any $z \in E^n$. The minimum of f(x) on D is sought by applying to $f[\varphi(z)]$ the methods of unconstrained minimization over z.

The relevance of both groups of methods is attributable to the fact that the iterative sequences x_k generated by the various algorithms remain inside the feasible region D. This is a very important aspect if the variables $x \notin D$ are devoid of concrete physical meaning in the particular mathematical model. Methods ensuring that $x_k \in D$ in each iteration is preferred to other algorithms if the solution of the optimization problem may stop by hitting a time limit, before the computations stop algorithmically. Algorithms ensuring $x_k \in D$ make it possible to dispense with additional efforts to correct the approximate solution x_* and to ensure the inclusion $x_* \in D$.

The use of the transformations $x = \varphi(z)$ for minimizing f(x) on D was first considered in detail in [5]. In order to eliminate the constraint $x \in D$, the following transformations were used in [5]:

$$\text{for} \quad D = \{x: x^i \geqslant 0\} \quad x^i = [z^i]^2, \quad x^i = \exp[z^i], \quad x^i = |z^i|;$$

$$\text{for} \quad D = \{x: 0 \leqslant x^i \leqslant 1\} \quad x^i = \sin^2 z^i, \quad x^i = [\exp(z^i) + \exp(-z^i)]^{-1}\exp(z^i);$$

$$\text{for} \quad D = \{x: a_i \leqslant x^i \leqslant b_i\} \quad x^i = a_i + (b_i - a_i)\sin^2 z^i.$$

Translated from Kibernetika, No. 4, pp. 25-35, July-August, 1986. Original article submitted June 7, 1985.