УДК 004.056

МЕТОД ФОРМУВАННЯ ПРАВИЛ ПЕРЕСТАНОВОК

В. А. Лужецький, д.т.н., професор,
І. С. Горбенко, аспірант
Вінницький національний технічний університет

Запропоновано метод формування правил перестановок. Існуючі генератори ПВП не забезпечують формування псевдовипадкової перестановки довільної множини елементів так, щоб кожен елемент з'являвся один раз, а підбір параметрів генераторів є досить складним.

Ідея методу полягає в тому, що множина чисел розбивається на підмножини, з яких здійснюється вибір. Розбиття можливе на підмножини постійного або змінного розміру. У випадку змінного розміру підмножин значення розмірів s_i формує довільний генератор ПВЧ. Якщо $s_i < N$, де N – кількість чисел у послідовності, тоді s_i приймається у якості розміру наступної підмножини k_i, а значення N зменшується на s_i та процес розбиття продовжується. Інакше $k_i := N$ та процес розбиття завершується. У обох випадках поточна кількість підмножин збільшується на 1.

Вибір підмножин та вибір елементів з підмножин може здійснюватись у детермінованому або псевдовипадковому порядку. Детермінований порядок вибору підмножин передбачає вибір за формулою:

$$n_i = \begin{cases} (a \cdot i + b) \bmod N \\ N - ((a \cdot i + b) \bmod N) \end{cases}$$

де $i = 0, 1, \ldots, (N - 1)$. Для вибору елементів з підмножини формула набуває вигляду:

$$n_{ij} = \begin{cases} ((a_i \cdot i + b_i) \bmod n_i) + n_{i0} \\ n_{i0} - ((a \cdot i + b) \bmod n_i) \end{cases}$$

При псевдовипадковому виборі індекси підмножин та елементів формуються деяким генератором ПВЧ. Оскільки можуть виникати повторення чисел, вводяться допоміжні параметри – індикатор перестановки та регістр прапорців. Початкове значення індикатора перестановки $I_i = k_i$. Вибір елемента з підмножини здійснюється лише якщо $I_i > 0$. При кожному виборі індикатор I_i зменшується на 1. На основі окремих індикаторів формується загальний індикатор:

$$I = I_0 \vee I_1 \vee ... \vee I_{N-1}.$$

Якщо $I = 0$, це свідчить про завершення процесу формування перестановок. При псевдовипадковому виборі елементів використовується регістр прапорців, який вказує, які елементи не були вибрані. Початковий стан регістру прапорців $2^{k_i} - 1$. При спробі вибору елементу на регістр накладається відповідна даному елементу маска і вибір здійснюється, якщо результат операції не дорівнює 0. Після вибору елементу відповідний біт регістру встановлюється рівним 0. Оскільки розмір підмножини може бути постійним (C) або змінним (V), а порядок вибору підмножин та порядок вибору елементів з підмножини – детермінованим (D) або псевдовипадковим (R), можливі 8 методів формування перестановок: CDD, VDD, CRD, VRD, CDR, VDR, CRR, VRR. З точки зору випадковості найкращими є останні три методи. Сформовані ними послідовності мають найменші коефіцієнти автокореляції першого та другого порядків, однак їм характерні суттєві часові витрати. Запропонований метод забезпечує формування псевдовипадкової перестановки множини елементів довільного обсягу, де кожен елемент гарантовано з'являється один раз. Підбір параметрів є досить простим.