ЗАСТОСУВАННЯ ПОТОКОВИХ SIMD-РОЗШИРЕННЬ ПРОЦЕСОРА В ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

Соловей О.С., Рисований О.М.

Національний технічний університет "Харківський політехнічний інститут", м. Харків

Генерація псевдовипадкових чисел – одна з найстаріших задач обчислювальної техніки. У багатьох випадках задачі моделювання мають використовувати генератор більйони разів, що робить час їх роботи прямозалежним від часу роботи генератора.

Незважаючи на це, більшість мов програмування, мають у стандартних бібліотеках один з старіших методів генерації — лінійний конгруентний метод, який не забезпечує високої швидкості.

Більшість ідей (xorshift, fastrand) спрямовані, на вдосконалення математичної частини алгоритму. Я хочу запропонувати використання SIMD-розширень процесора, що дозволить скоротити число тактів процесора, необхідних для роботи генератора.

SSE дозволяє робити паралельні обчислення для чотирьох 32-бітних значень одночасно, що дозволяє прискорити обчислення майже у відповідну кількість разів. (ще незначну кількість тактів займає розділення 128-бітного значення, що не займає багато часу, бо виконуються бітовими логічними операціями зсуву та маски).

Порівняння методів генерації здійснювалося методом генерації 100000 чисел, програмою написаною на мові C, та скомпільованої компілятором Intel 11.1. Час генерації підраховано процесорним лічильником тактів, за допомогою інструкції RDTSC. Затримки використання лічильника, команд вводу/виводу та ін. Не враховувалися, через однаковість для всіх методів генерації. Код програми розміщено у мережі інтернет за адресою http://pastebin.com/Vb7gCTAJ.

Метод	**Середній час генерації, тактів**	**СКВ**
SSE	3,55	288,84
CLASSIC	85,91	287,93
FAST	6,25	288,4
XORRAND	8,06	287,85

Як видно з результатів, наведених у таблиці, використання SSE дозволяє досягти високої швидкості генерації, проте слід враховувати, що використання є виправданим, тільки за умови потреби, щонайменше у чотирьох числах за одну умовну ітерацію.