Test of random number generators

Брагінець Я.С.
мПМ-1

Випадкові числа

Випадкові числа — штучно отримана послідовність реалізацій випадкової величини із заданим законом розподілу.

Випадкові генератори

- Швидкі
- Кросплатформені
- Великий період
- Рівномірні
- Незалежні

Способи генерування

Є кілька способів генерування послідовностей випадкових чисел (ГПВЧ):

- за допомогою таблиць випадкових чисел;
- за допомогою спеціальних пристроїв — генераторів випадкових чисел;
- шляхом заміни випадкових чисел послідовністю так званих псевдовипадкових чисел.

Вимоги до ГПВЧ

- із достатньою точністю відтворювати поведінку модельованої випадкової величини із заданим розподілом;
- потребувати мінімальну кількість операцій машини, які необхідні для формування одного випадкового числа.

Завдання

Провести фізичний та статистичні тести заданих генераторів випадкових чисел.

Виконати порівняння якості та визначити більш якісний алгоритм для застосування в прикладних цілях.

Розглянути Алгоритми

- Алгоритм генерації за допомогою лінійної конгруенції (Java's Random class)

  0<= c < m; 0 <= a < m; 0 <= c < m

$$x_n = (ax_{n-1} + c) \bmod m$$

- Вбудований алгоритм мови програмування

Розглянути Алгоритми

- Алгоритм за допомогою побітових зсувів (GFSR)

$$x_n = x_{n-p} \oplus x_{n-q}$$

lagged Fibonacci generator

$$X_i = X_{i-P} \odot X_{i-Q}$$

$$\mathrm{F}(P, Q, \odot),\ P > Q,$$

Статистичні Тести

Перевірити виконання наступних умов:

- **Період –** період повтору згенерованих чисел більший за кількість необхідних чисел
- **Рівномірність –** згенеровані значення мають бути рівномірно розподілені на інтервалі
- **Хі-квадрат –** $\chi^2 = \sum_{i=1}^{M} \frac{(y_i - E_i)^2}{E_i}.$ чим менше тим краще
- **Приховані кореляції –** відсутність прослідковування патерну для будь-яких значеннь $\frac{x_{i+k}}{x_i}$

Статистичні Тести

Перевірити виконання наступних умов:

- **Випадкові блукання, не виконання умови** $\chi^2 > 7.815$
- **Заповнення вузлів решітки –** частка порожніх вузлів має задовольняти відношення e^{-t} t- кількість кроків алгоритму
- **Parking lot test –** відсутність візуальних ліній при спостеріганні заповнених вузлів
- **Короткострокові кореляції** - їх відсутність

$$C(k) = \frac{\langle x_{i+k} x_i \rangle - \langle x_i \rangle^2}{\langle x_i x_i \rangle - \langle x_i \rangle \langle x_i \rangle}$$

Статистичні Тести

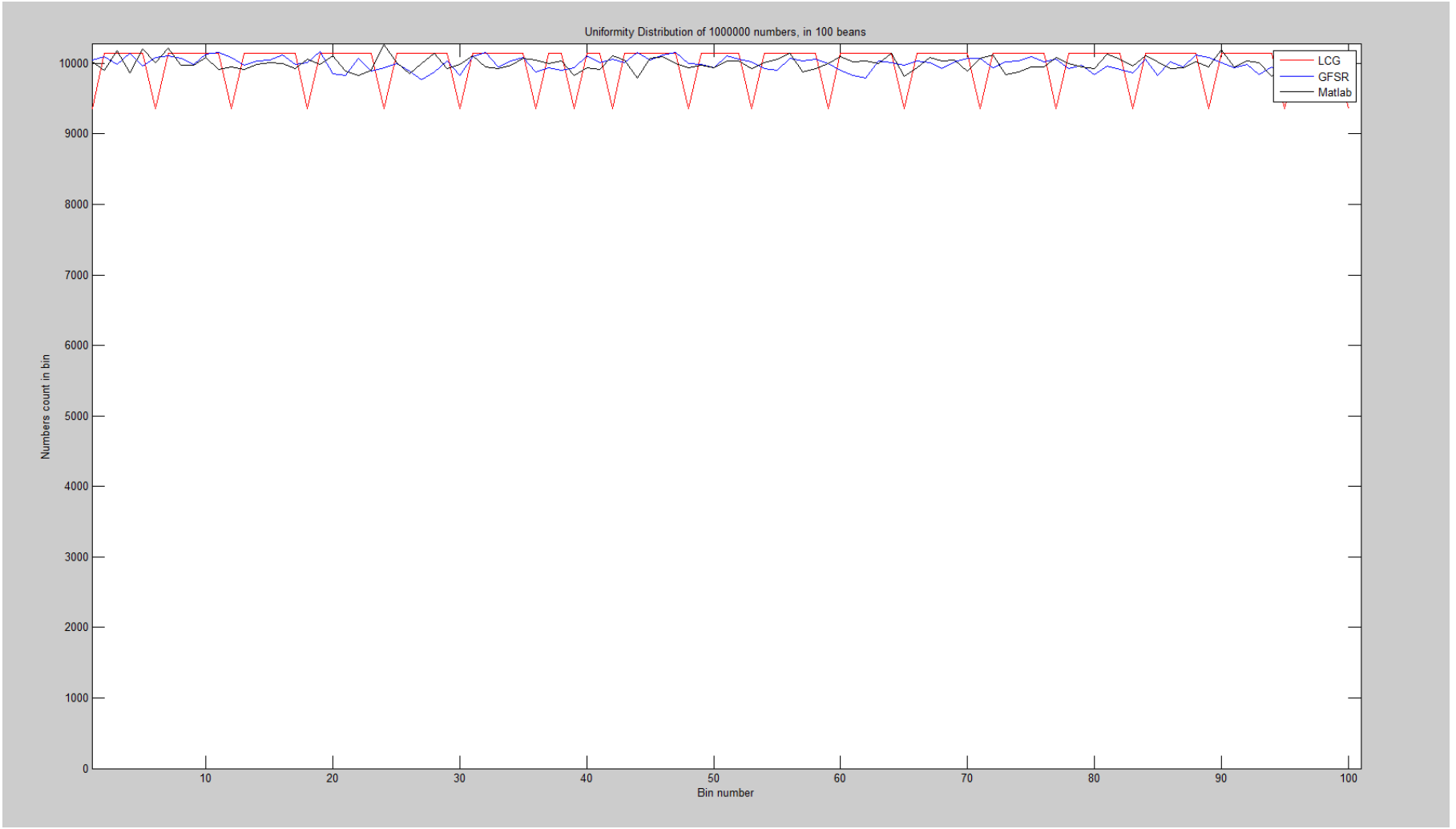
- **Хі-квадрат –** не більше M (M = 100)

```
Chi LGC : 936.877400
Chi GFSR : 127.865200
Chi Matlab : 100.271000
```

- **Випадкові блукання, не викоання** $\chi^2 > 7.815$

```
Random walk for 10 walker, 1000 steps in 100 tests:
Chi LGC : 16.032000
Chi GFSR : 3.536000
Chi Matlab : 3.120000
```

Статистичні Тести Рівномірність

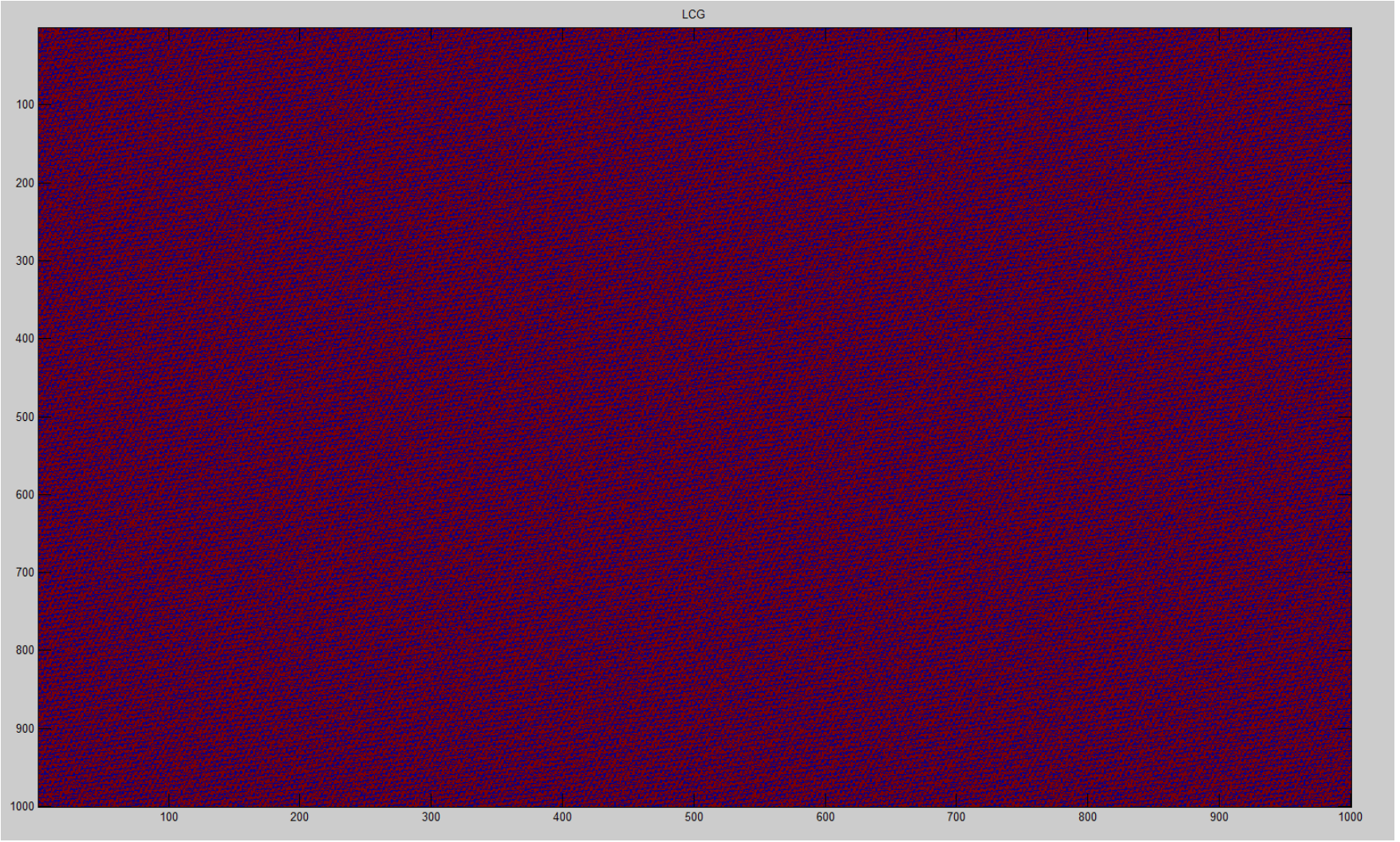


Статистичні Тести Filling Sites

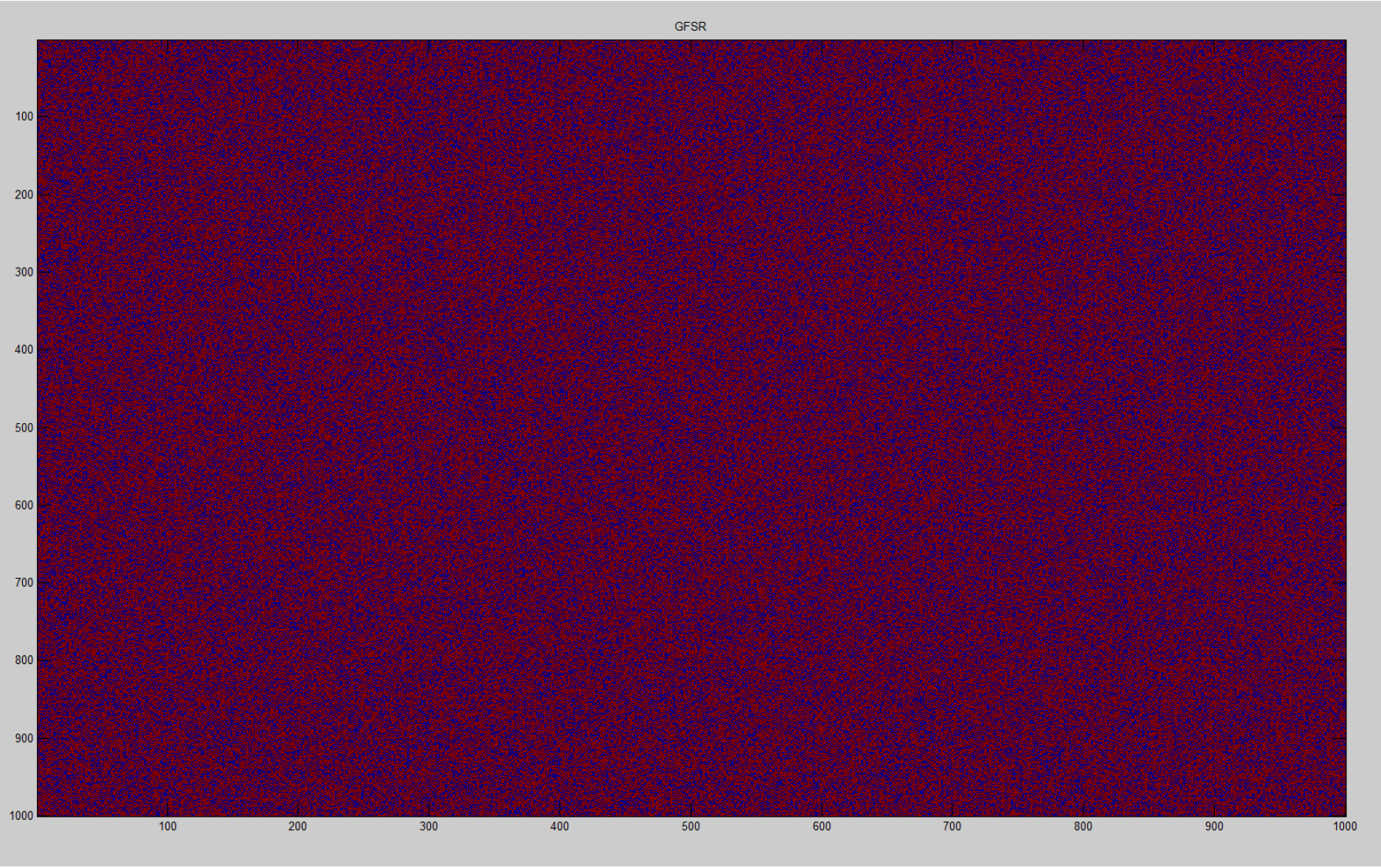
Заповнення вузлів решітки – коефіцієнт зменшення кількості порожніх вузлів має задовольняти відношення e^{-t}, де t- кількість кроків алгоритму заповнення решітки

```
Made 50 steps with lattice size = 10x10
LGC percent of 0 number : 59.434000, expected 60.653066
GFSR percent of 0 number : 60.394000, expected 60.653066
Matlab percent of 0 number : 60.416000, expected 60.653066
```

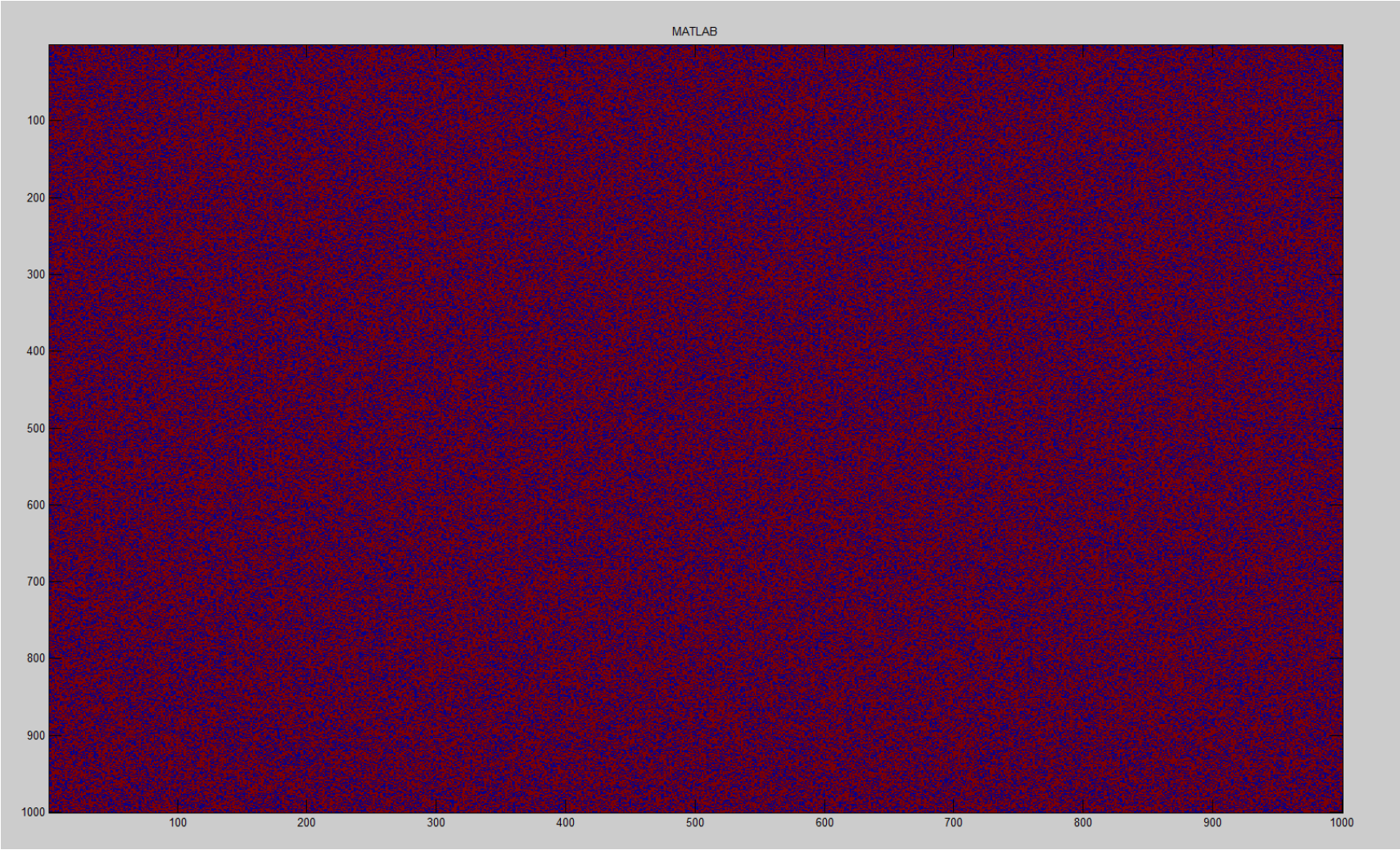
Статистичні Тести **Parking lot test**



Статистичні Тести **Parking lot test**



Статистичні Тести **Parking lot test**



Фізичні Тести

Реалізувати Модель Ізінга використовуючи алгоритми

- **Metropolis –** коли відбувається оборот одного спіну (елементу)
- **Wolf Dynamics** - коли відбувається оборот цілого кластера спінів

Модель Ізінга

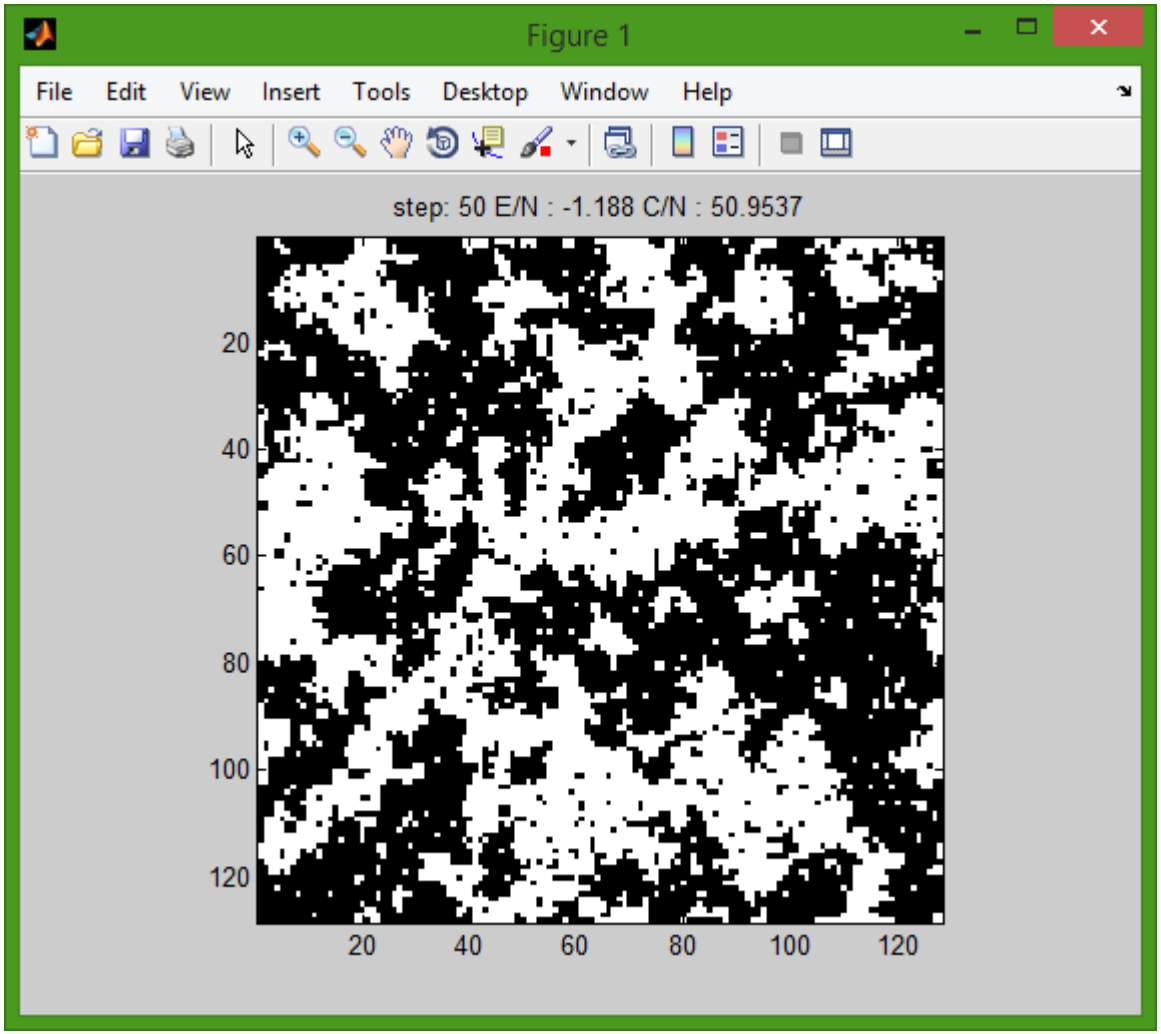
Двовимірна модель описується за допомогою решітки, кожен з вузлів якої – спін, приймає два значення ± 1, напрямлений вверх чи вниз. Частинки у різних вузлах ґратки взаємодіють між собою, причому енергія цієї взаємодії залежить від взаємної орієнтації «спінів».

Буде розглянуто два алгоритми роботи з даною моделлю:

- Метрополісу
- Вольфа

Двовимірна модель має точний аналітичний розв'язок, отриманий Ларсом Онсагером

Модель Ізінга



Модель Ізінга

Модель Ізінга є однією з найбільш поширених фізичних моделей статистичної фізики. За її допомогою досліджують феромагнітні матеріали. Використання даної моделі для тестування ГПВЧ основане на чуттєвості алгоритму Метрополісу та Вольфа до вхідної послідовності псевдовипадкових чисел. Якщо вхідна послідовність має не є істинно випадковою, то критичні індекси системи будуть відмінними від теоретично очікуваних.

Модель Ізінга, Алгоритм Метрополісу

У основі алгоритму Метрополісу полягає використання рівноважної функції канонічного розподілу Pn, і, отже, при застосуванні цього алгоритму повинні вибиратися термодинамічно рівноважні стани системи. Проте немає упевненості, що сформована початкова конфігурація є рівноважною. Щоб уникнути цієї проблеми, необхідно, починаючи з довільної конфігурації спінів (наприклад, усі спини спрямовані вгору), процедуру обчислення середнього проводити тільки після досягнення системою рівноважного стану.

Модель Ізінга, Алгоритм Метрополісу

1. Формуємо початкову (рівноважну) конфігурацію.

2. Випадковим чином вибираємо і пробуємо його перевернути.

3. Обчислюємо зміну енергії системи,

$$DE = 2J \cdot spin[i][j] \cdot (spin\_left + spin\_right + spin\_top + spin\_bottom)$$

4. Якщо $DE \leq 0$, то приймаємо нову конфігурацію і переходимо до кроку 8.

5. Якщо $DE > 0$, то обчислюємо вірогідність переходу $w = \exp(-DE/kT)$.

6. Генеруємо випадкове число r в інтервалі.

7. Якщо $r \leq W$, то нову конфігурацію приймаємо, інакше зберігаємо попередню конфігурацію

8. Визначаємо значення необхідних фізичних величин

9. Повторюємо кроки 2—8 для отримання достатнього числа конфігурацій.

10. Обчислюємо середні по конфігураціях, які статистично незалежні

Модель Ізінга, Алгоритм Вольфа

1. Підготувати початкову конфігурацію, що складається з N спінів.

2. Випадково вибрати спін S_i.

3. Починаючи зі спіну S_i, побудувати навколо нього кластер, який містить спіни такої ж орієнтації та зв'язані один з одним з імовірністю

$P = 1 - e^{-2bJc_ic_j}$.

4. Перевернути всі спіни в цьому кластері.

5. Кінець одного Монте-Карло кроку, зберегти моментальні значення характеристик системи.

6. Повторити кроки 2 до 5 поки не буде зроблено N_{sim} кроків Монте-Карло.

Модель Ізінга, Результати

```
Ising test using GFSR generator and Metropolis. steps : 100000
1   2   3   4   5   6   7   8   9   10
Ratio for E : 0.009119, Mean Energy : -1.453896
Ratio for C : 0.174988, Mean Heat : 1.502717

Elapsed time is 3700.676552 seconds.
```

Metropolis + GFSR

```
Ising test using GFSR generator and Metropolis. steps : 1000000
1   2   3   4   5   6   7   8   9   10
Ratio for E : 0.125459, Mean Energy : -1.441633
Ratio for C : 0.109700, Mean Heat : 1.499927

Elapsed time is 24737.552428 seconds.
```

Модель Ізінга, Результати

```
Ising test using LCG generator and Metropolis. steps : 100000
1   2   3   4   5   6   7   8   9   10
Ratio for E : 0.235481, Mean Energy : -1.475408
Ratio for C : 0.117630, Mean Heat : 1.503688

Elapsed time is 3295.066514 seconds.
```

Metropolis + LCG

```
Ising test using LCG generator and Metropolis. steps : 1000000
1   2   3   4   5   6   7   8   9   10
Ratio for E : -0.024381, Mean Energy : -1.455279
Ratio for C : 0.850149, Mean Heat : 1.506638

Elapsed time is 22830.066365 seconds.
```

Модель Ізінга, Результати

```
Ising test using Matlab generator and Metropolis. steps : 100000
1   2   3   4   5   6   7   8   9   10
Ratio for E : 0.167878, Mean Energy : -1.467145
Ratio for C : 0.680915, Mean Heat : 1.518206

Elapsed time is 3032.945957 seconds.
```

Metropolis + Matlab

```
Ising test using Matlab generator and Metropolis. steps : 1000000
1   2   3   4   5   6   7   8   9   10
Ratio for E : -0.268208, Mean Energy : -1.476887
Ratio for C : -0.033289, Mean Heat : 1.498215

Elapsed time is 21790.010729 seconds.
```

Модель Ізінга, Результати

Metropolis + LCG

```
Ising test using LCG generator and Metropolis. steps : 100000
1   2   3   4   5   6   7   8   9   10
Ratio for E : 0.235481, Mean Energy : -1.475408
Ratio for C : 0.117630, Mean Heat : 1.503688

Elapsed time is 3295.066514 seconds.
```

Metropolis + GFSR

```
Ising test using GFSR generator and Metropolis. steps : 100000
1   2   3   4   5   6   7   8   9   10
Ratio for E : 0.009119, Mean Energy : -1.453896
Ratio for C : 0.174988, Mean Heat : 1.502717

Elapsed time is 3700.676552 seconds.
```

Metropolis + default

```
Ising test using Matlab generator and Metropolis. steps : 100000
1   2   3   4   5   6   7   8   9   10
Ratio for E : 0.167878, Mean Energy : -1.467145
Ratio for C : 0.680915, Mean Heat : 1.518206

Elapsed time is 3032.945957 seconds.
```

Модель Ізінга, Результати

Wolf + LCG

```
Ising test using LCG generator and Wolf. steps : 100000
1   2   3   4   5   6   7   8   9   10
Ratio for E : 8.978691, Mean Energy : -1.986774
Ratio for C : 22.966572, Mean Heat : 0.161191

Elapsed time is 3316.610401 seconds.
```

Wolf + GFSR

```
Ising test using GFSR generator and Wolf. steps : 100000
1   2   3   4   5   6   7   8   9   10
Ratio for E : 5.783534, Mean Energy : -1.914208
Ratio for C : 3.269804, Mean Heat : 1.069799

Elapsed time is 2344.857706 seconds.
```

Wolf + default

```
Ising test using Matlab generator and Wolf. steps : 100000
1   2   3   4   5   6   7   8   9   10
Ratio for E : 7.539575, Mean Energy : -1.959080
Ratio for C : 4.001244, Mean Heat : 1.115727

Elapsed time is 1281.808193 seconds.
```

Висновки GFSR

GFSR генератори можна розглядати як випадок генераторів методом Фібоначчі використовуючи операцію XOR. Дані генератори швидкі та мають великий період. Якість їх випадковості підвищується методом врахування не двох елементів, а більшої кількості. Проте якщо замість XOR використовувати інші бінарні операції то їх якість ще істотніше покращується.

Висновки LCG

LCG добре підходить для більшості завдань, особливо при правильно підібраних параметрах L(1313, 0, 259) , але має кілька дефектів:

Молодші біти отриманих чисел сильно корельовані (залежні), і результат розсіювання впорядкованих пар випадкових чисел в інтервалі (0, 1) має структуру регулярної решітки.

Висновки LCG

Період послідовності сильно залежить від початкових параметрів

Найменші біти не випадкові

Мінімальне випадкове число не 0 а 1

Висновки

В більшості тестів серед пари генераторів краще зарекомендував себе GFSR, тому і не дивно що на даний момент його модифікації одні з найпопулярніших генераторів псевдовипадкових послідовностей. GFSR – досить популярний за швидкодію та якість. Також був протестований вбудований генератор, його якість на рівні GFSR, а в деяких випадках краща.