Качество генерации псевдослучайных чисел в системах имитационного моделирования OpenGPSS, GPSS World и AnyLogic

Диденко Дмитрий Георгиевич
Старший преподаватель кафедры
ММСА ННК «ІПСА»
Национальный технический университет Украины
«Киевский политехнический институт»
Киев, Украина

1. Большое количество вероятностных распределений

От Бернулли до Вейбула:

- OpenGPSS (29 распределений);
- GPSS World (24 распределения);
- AnyLogic (29 распределений).

2. Тесты псевдослучайных последовательностей

Наборы (батареи) тестов:

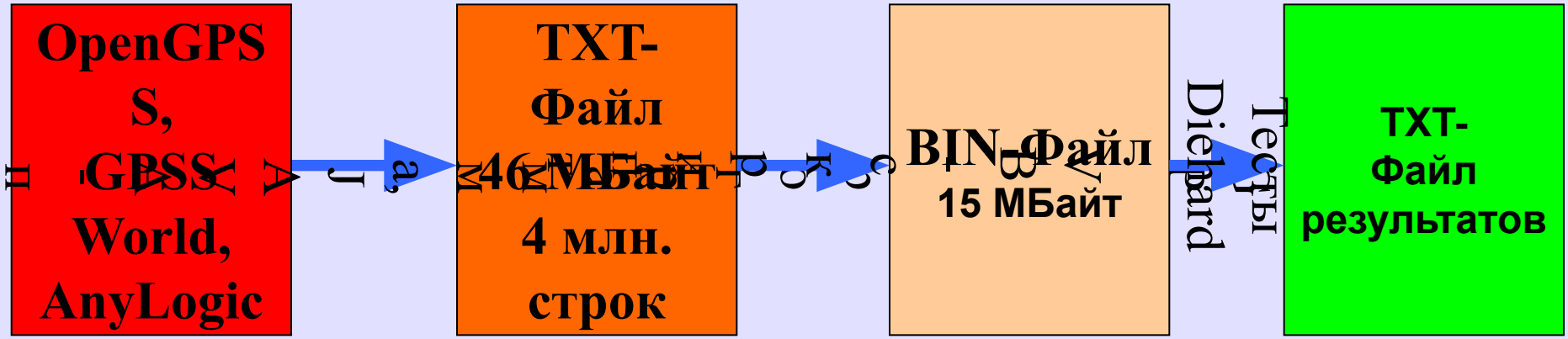
- NIST;
- TEST-U01;
- CRYPT-X;
- The pLab Project;
- DIEHARD;
- ENT.

2. Тесты псевдослучайных последовательностей

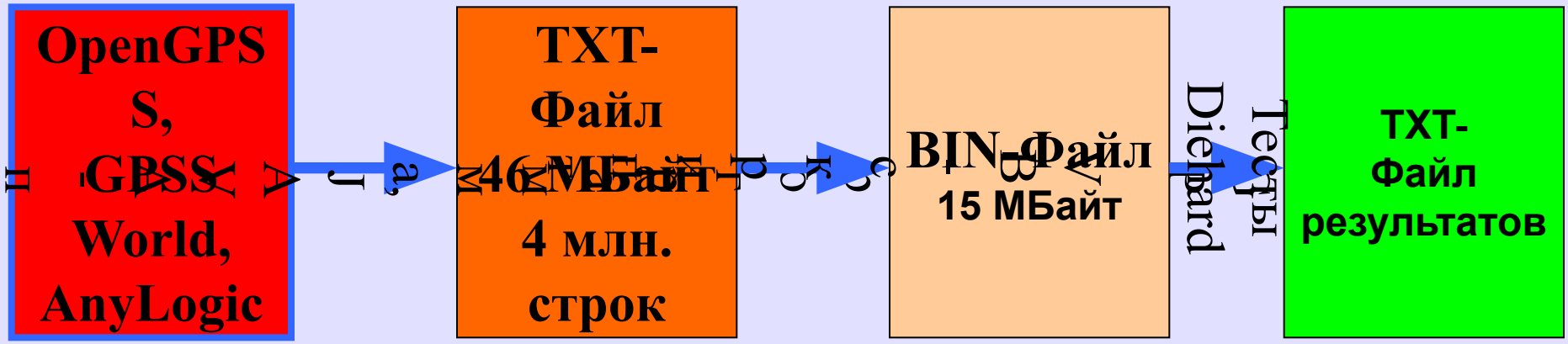
Наборы (батареи) тестов:

- NIST;
- TEST-U01;
- CRYPT-X;
- The pLab Project;
- DIEHARD;
- ENT.

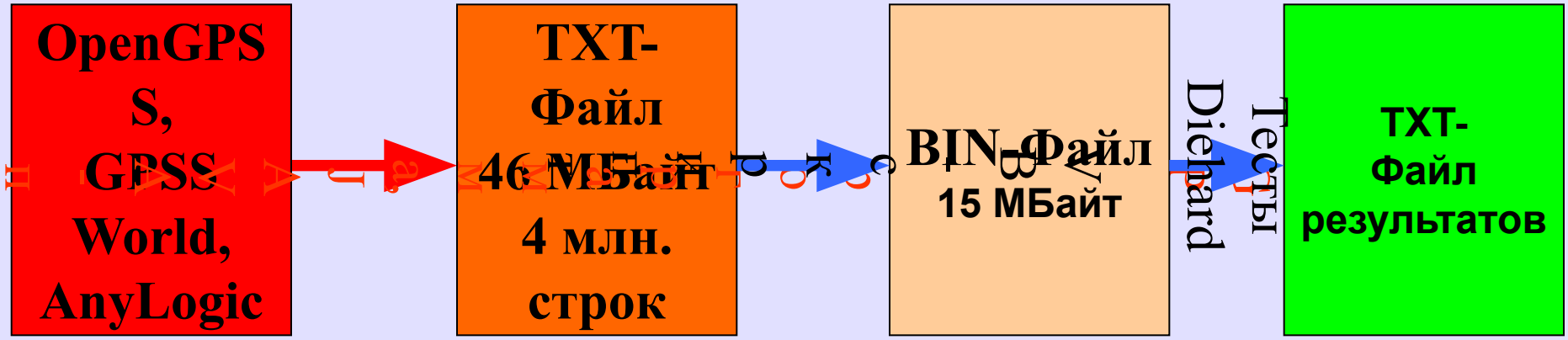
3.1. Схема проведения эксперимента



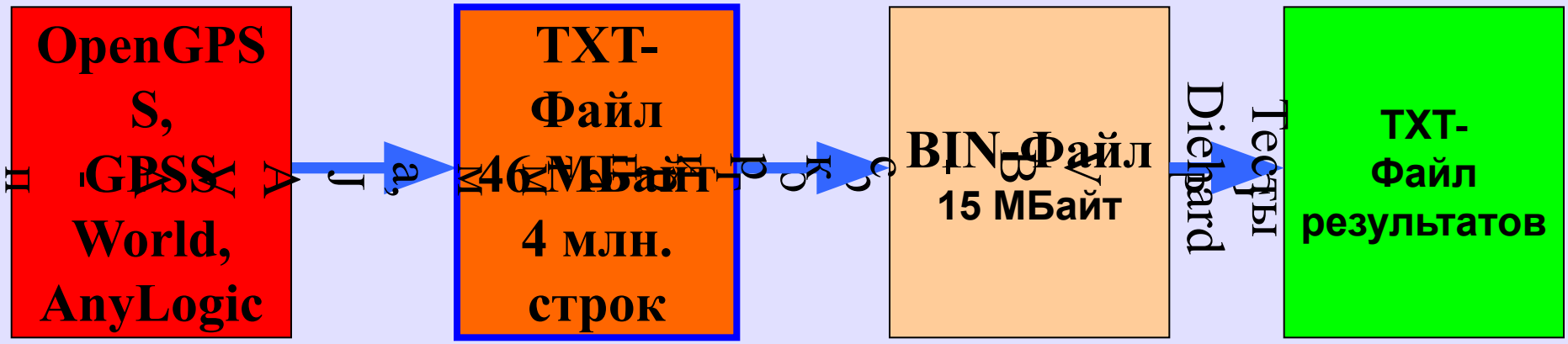
3.1. Схема проведения эксперимента



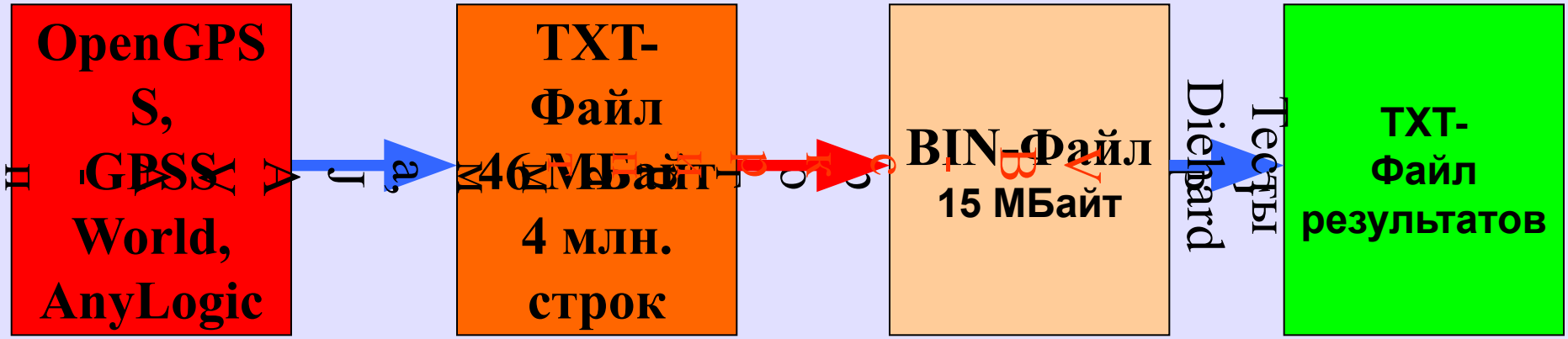
3.1. Схема проведения эксперимента



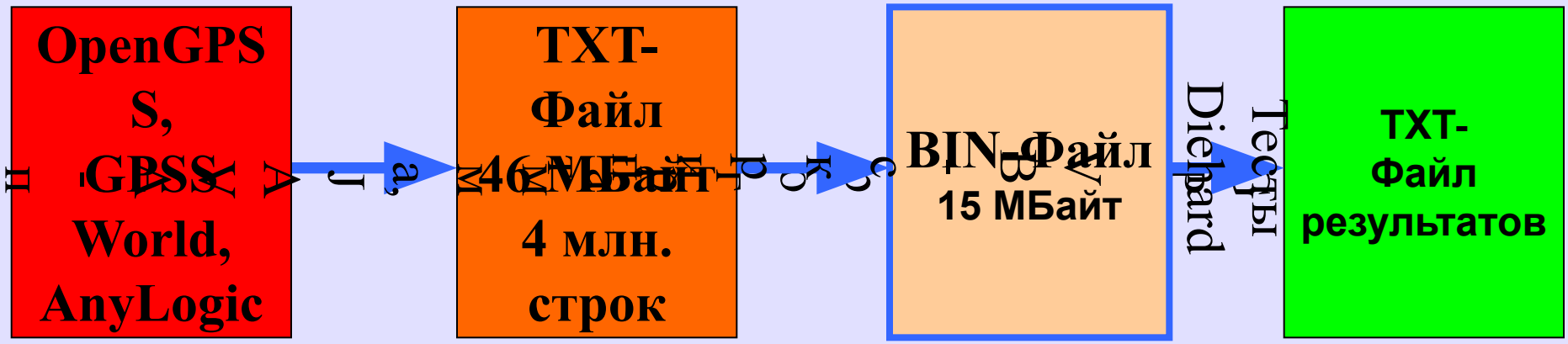
3.1. Схема проведения эксперимента



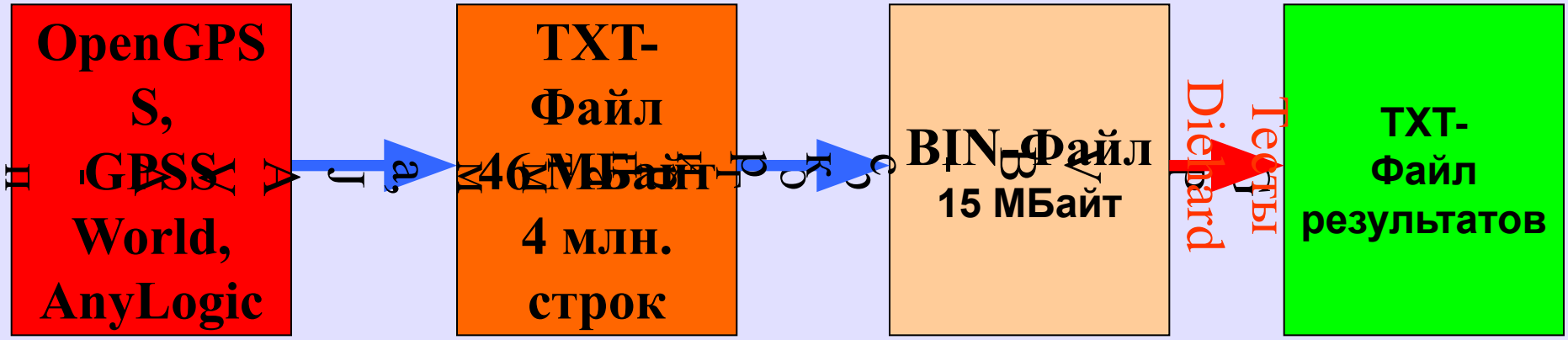
3.1. Схема проведения эксперимента



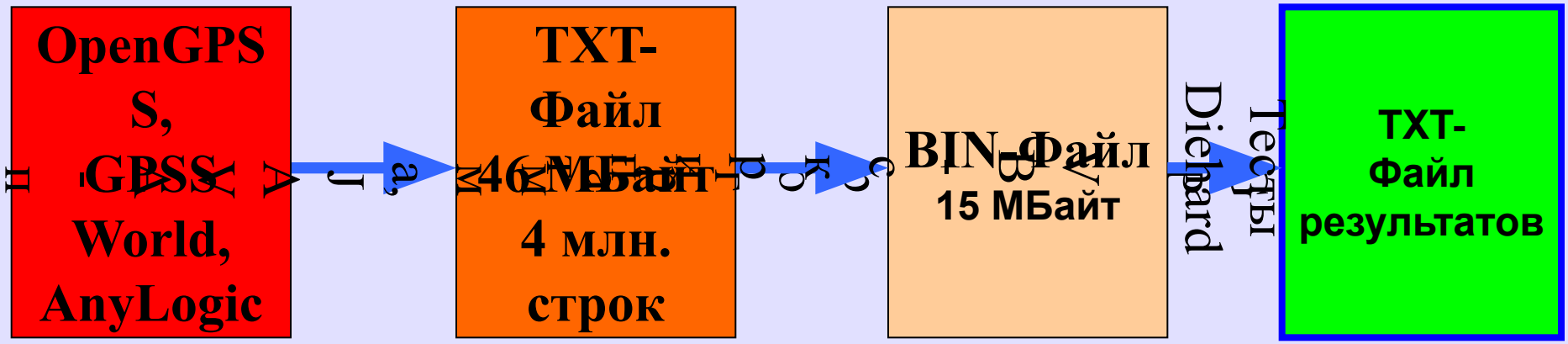
3.1. Схема проведения эксперимента



3.1. Схема проведения эксперимента



3.1. Схема проведения эксперимента



4.1. Тестовая программа для OpenGPSS

```
RMULT 300;начальное смещение
GENERATE 1

;переносим псевдослучайное число в сохраняемую
;величину
SAVEVALUE XN1,RN1
TERMINATE

;временной сегмент
GENERATE 1024
TERMINATE 1
START 1
```

4.2. Тестовая программа для GPSS World

```
FACTORY FUNCTION RN1,C2
0,-0.5/1,0.5
;Scale1 = 2 ^ 32 - 1=4294967295
PLATE VARIABLE FN$FACTORY#4294967295\1
GENERATE 1
WRITE V$PLATE,1
TERMINATE

;генерируем один из транзактов, который будет открывать/закрывать файл
GENERATE 1,,,1
OPEN "d:\test.txt",1,ERROR_BLOCK_1
ADVANCE 4000000;устанавливаем количество сгенерированных чисел
CLOSE 100,1
TERMINATE 1
ERROR_BLOCK_1 TERMINATE 1

RMULT 200
START 1
```

4.3. Тестовая программа для AnyLogic

```
double x;
int z;
for( int i=0; i<4000000; i++ ) { //генерируем 4 млн чисел
  x = uniform(-1,1)*2147483647;
  z = (int)x;
  my_file.println(z);
 }
```

5. Результаты прохождения тестов из пакета DIEHARD

№	Тест	OpenGPSS	GPSS World	AnyLogic
1	Дни рождения	+	-	+
2	Пересекающиеся перестановки	-	+	-
3	Ранги матриц	+/-/-	+/+/+	+/+/+
4	Поток битов	+	-	+
5	Обезьяньи тесты	-	+	+
6	Подсчёт единичек	-/-	-/+	+/+
7	Тест на парковку	-	+	+

6. Результаты прохождения тестов из пакета DIEHARD (продолжение)

№	Тест	OpenGPSS	GPSS World	AnyLogic
8	Тест на минимальное расстояние	-	+	+
9	Тест случайных сфер	+	+	+
10	Тест сжатия	-	+	-
11	Тест пересекающихся сумм	+	+	+
12	Тест последовательностей	+	+	+
13	Тест игры в кости	-/-	+/+	+/+

7. Проверка статистической гипотезы о случайности потока данных

Система моделирования	Количество пройденных тестов	Критерий Хи-квадрат	Анализ результата
OpenGPSS	5	90,00	-
GPSS World	10	29,45	+
AnyLogic	11	28,17	+

Табличное значение критерия Хи-квадрат 36,2

8. Использование встроенного ГПЧ из СУБД Oracle

Работа с системным пакетом dbms_random:

1) начальное смещение для ГПЧ

dbms_random.seed(300);

2) получение следующего числа

a := dbms_random.random;

8. Использование встроенного ГПЧ из СУБД Oracle (продолжение)

Преимущества и недостатки dbms_random:

+ встроенный в Oracle;

+ широкое использование;

- нельзя получить текущее смещение.

9. Способы улучшения ГПЧ

- линейный конгруэнтный метод $X_{n+1} = (aX_n + c) \bmod m$;
- квадратичный конгруэнтный метод $X_{n+1} = (dX_n^2+aX_n+c) \bmod m$;
- генератор на основе объединения путём сложения по mod 2^{32} двух генераторов: запаздывающего генератора Фибоначчи $X_n = X_{n-99}\ X_{n-33} \bmod 2^{32}$ и генератора на основе произведения с переносом $Y_n = 30903\ Y_{n-1}$ carry mod 2^{16};
- генератор М-последовательностей;
- вихрь Мерсена.

10. Модификации Линейного Конгруэнтного Метода

- расширенный конгруэнтный генератор - $X_n = 2^{13} (X_{n-1} + X_{n-2} + X_{n-3}) \bmod (2^{32} - 5)$;
- алгоритм “Marsaglia-Multicarry” (Джордж Марсаглия);
- алгоритм “xor-shift” (Джордж Марсаглия);
- алгоритм Блюма-Блюма-Шуба;
- генератор на базе произведения с переносом - $X_n = (2111111111\, X_{n-4} + 1492\, X_{n-3} + 1778\, X_{n-2} + 5115\, X_{n-1})$ carry mod 2^{32};
- генератор на базе произведения с переносом - $X_n = a\, X_{n-1}$ carry mod 2^{32}.

11. Примеры Линейного Конгруэнтного Метода

№	Источник	m	a	c	Биты
1	Numerical Recipes	2^{32}	1664525	1013904223	0..31
2	Borland C/C++	2^{32}	22695477	1	0..30
3	GNU Compiler Collection	2^{32}	69069	5	16..30
4	glibc (используется в GCC)	2^{32}	1103515245	12345	0..30
5	ANSI C: Open Watcom, Digital Mars, Metrowerks, IBM VisualAge C/C++	2^{32}	1103515245	12345	16..30
6	Borland Delphi, Virtual Pascal	2^{32}	134775813	1	0..31
7	Microsoft Visual/Quick C/C++	2^{32}	214013	2531011	16..30
8	Apple CarbonLib	2^{31}-1	16807	0	0..31

11. Примеры Линейного Конгруэнтного Метода (продолжение)

№	Источник	m	a	c	Биты
9	Microsoft Visual Basic (версия 6 и ниже)	2^{24}	1140671485	12820163	0..23
10	RtlUniform from Native API	2^{31}-1	2147483629	2147483587	0..31
11	MMIX Дональда Кнута	2^{64}	6364136223846793005	1442695040888963407	0..63
12	VAX's MTH$RANDOM (старая версия библиотеки glibc)	2^{32}	69069	1	0..31
13	LC53 в языке программирования Forth	2^{32}-5	2^{32} – 333333333	0	0..31
14	Random class in Java API	2^{48}	25214903917	11	16..47
15	MS Fortran	2^{31}-1	48271	0	0..31

12. Результаты прохождения тестов из пакета DIEHARD

№	Тест	OpenGPSS		GPSS World	AnyLogic
		1.2.1.0	1.2.2.0		
1	Дни рождения	+	-	-	+
2	Пересекающиеся перестановки	-	+	+	-
3	Ранги матриц	+/-/-	+/+/-	+/+/+	+/+/+
4	Поток битов	+	-	-	+
5	Обезьяньи тесты	-	+	+	+
6	Подсчёт единичек	-/-	-/+	-/+	+/+
7	Тест на парковку	-	+	+	+

Диденко Д.Г. © 2011

12. Результаты прохождения тестов из пакета DIEHARD (продолжение)

№	Тест	OpenGPSS		GPSS World	AnyLogic
		1.2.1.0	1.2.2.0		
9	Тест случайных сфер	+	+	+	+
10	Тест сжатия	-	+	+	-
11	Тест пересекающихся сумм	+	+	+	+
12	Тест последовательностей	+	+	+	+
13	Тест игры в кости	-/-	+/+	+/+	+/+

13. Проверка статистической гипотезы о случайности потока данных

Система моделирования	Количество пройденных тестов	Критерий Хи-квадрат	Анализ результата
OpenGPSS 1.2.1.0	5	90,00	-
OpenGPSS 1.2.2.0 MS Fortran	12	24,46	+
GPSS World	10	29,45	+
AnyLogic	11	28,17	+

Табличное значение критерия Хи-квадрат 36,2

14. Настройка ГПЧ в системе OpenGPSS

Настройки - Windows Internet Explorer

http://www.simulation.kiev.ua/index.php?menu=preferenc

Избранное | Настройки | Страница | Безопасность | Сервис

- ГЛАВНАЯ
- ВХОД В СИСТЕМУ
- ЗАДАНИЯ
  - Новое задание
  - Выполнить задание
  - Очистить журнал и выполнить
  - Остановить задание
  - Очистить журнал
  - Удалить задание
  - Снимок
- ДЕМО
- КНИГИ
- СТАТЬИ
- ПЕРСОНЫ
- КОНФЕРЕНЦИИ
  - Календарь конференций
- ДОКУМЕНТАЦИЯ OpenGPSS
  - Публикации по OpenGPSS
  - Новости разработки
  - Пример работы системы
  - Отличия от GPSS/PC
  - Помощь по языку GPSS

/ КЦИМ / Настройки

Настройки

Пользователь	test
E-mail	test
Получать рассылку новостей по почте	Получать
Автообновление заданий каждые	30 сек
Количество цифр после запятой в отчёте	6 цифр
Генератор псевдослучайных чисел	MS Fortran (48271*X) mod (2^31-1). Биты 0..31

ANSI C: Open Watcom, Digital Mars, Metrowerks, IBM VisualAge C/C++ (1103515245*X
Apple CarbonLib (16807*X) mod (2^31-1). Биты 0..31
Borland C/C++ (22695477*X + 1) mod 2^32. Биты 0..30
Borland Delphi, Virtual Pascal (134775813*X + 1) mod 2^32. Биты 0..31
glibc (используется в GCC) (1103515245*X + 12345) mod 2^32. Биты 0..30
GNU Compiler Collection (69069*X + 5) mod 2^32. Биты 16..30
LC53 из языка программирования Forth ((2^32 - 333333333)*X) mod (2^32-5). Биты
Microsoft Visual Basic (версия 6 и ниже) (1140671485*X + 12820163) mod 2^24. Биты
Microsoft Visual/Quick C/C++ (214013*X + 2531011) mod 2^32. Биты 16..30
MMIX Дональда Кнута (6364136223846793005*X + 1442695040888963407) mod 2^
MS Fortran (48271*X) mod (2^31-1). Биты 0..31
Numerical Recipes (1664525*X+1013904223) mod 2^32. Биты 0..31
Random class in Java API (25214903917*X + 11) mod 2^48. Биты 16..47
RtlUniform from Native API (2147483629*X + 2147483587) mod (2^31-1). Биты 0..31
VAX's MTH$RANDOM (старая версия библиотеки glibc) (69069*X + 1) mod 2^32. Биты

Спасибо за внимание

www.simulation.kiev.ua