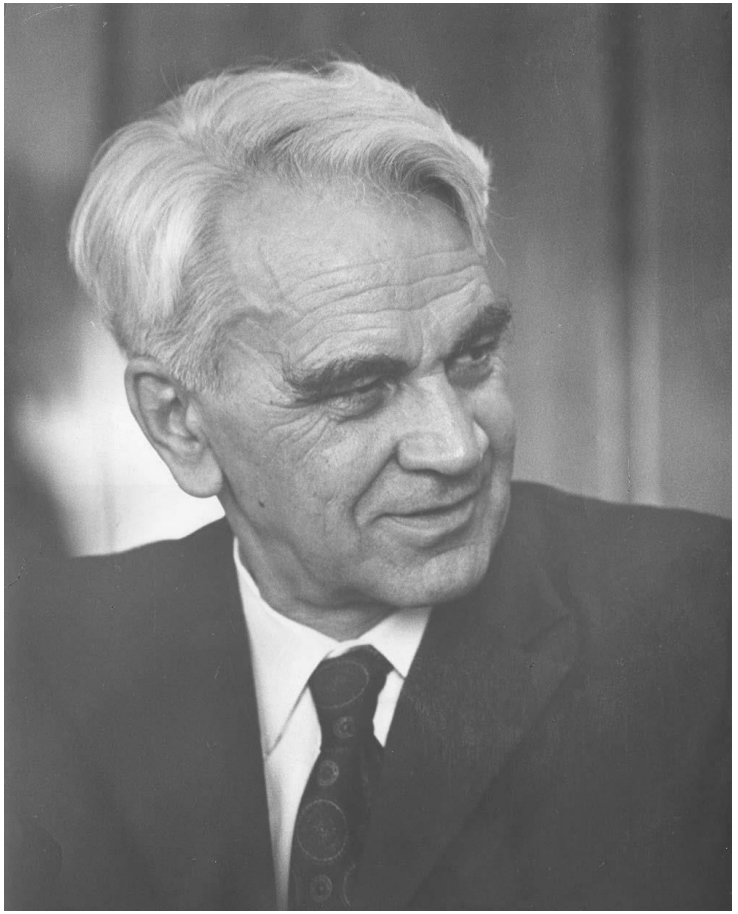
Псевдослучайные числа для расчетов на многопроцессорных системах

Якобовский Михаил Владимирович
проф., д.ф.-м.н.
Институт прикладной математики
им. М.В.Келдыша РАН, Москва

Мстислав Всеволодович Келдыш



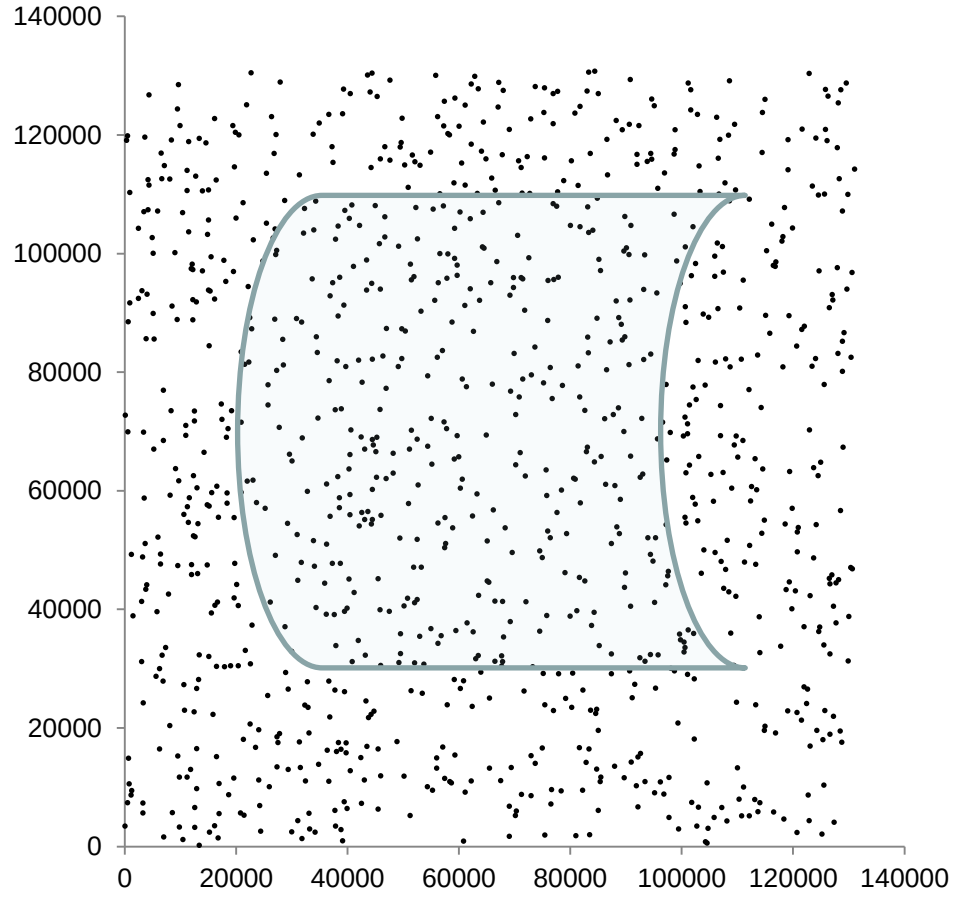
10 февраля 1911 г. - 24 июня 1978 г.

Три К — Курчатов, Келдыш и Королев 1956г

Применение последовательностей случайных и псевдослучайных чисел

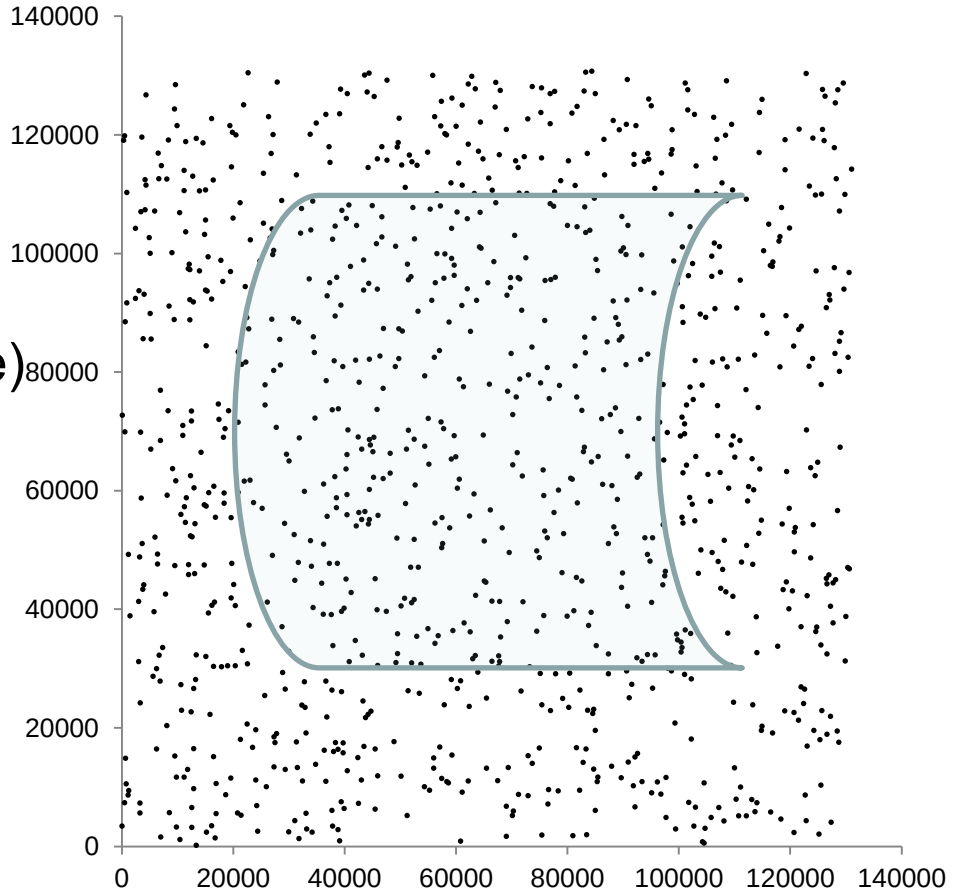
- Численное моделирование
  - Методы молекулярной динамики
  - Генетические алгоритмы
- Численные методы
  - Многомерная многоэкстремальная оптимизация
  - Определение многомерных интегралов
- Принятие решения
- Игры
- Лотереи
- …

Определение площади фигуры



Последовательный алгоритм

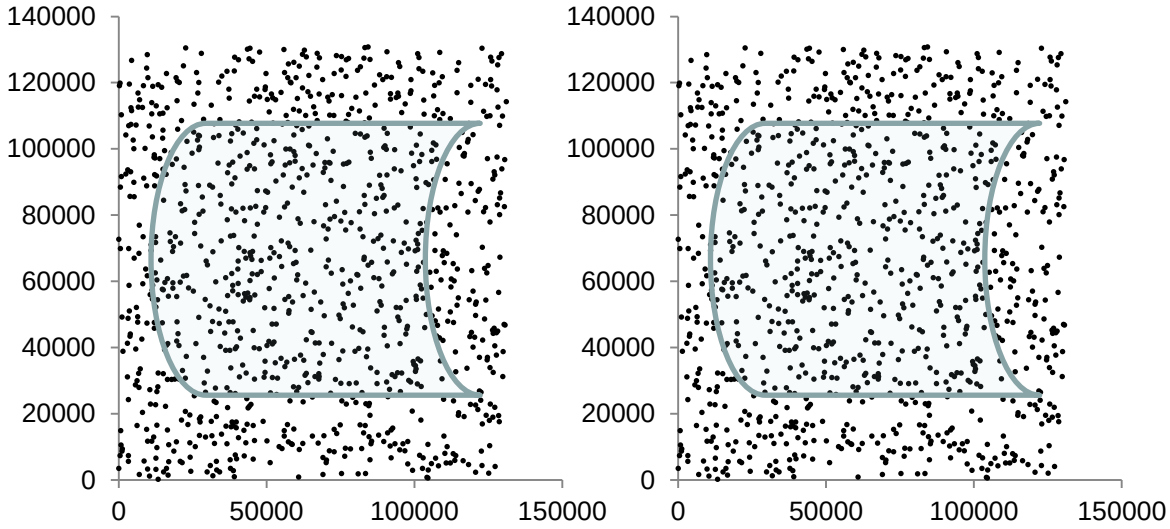
```
M=0;
for(i=0;i<N;i++)
{
X=rand();
Y=rand();
Если (точка (X,Y) принадлежит фигуре)
        то M++;
}
S=130000*130000*M/N;
```



Параллельный алгоритм для P процессоров

1. Каждый процессор определяет число m_{rank} «своих» N/P точек, попавших внутрь фигуры
2. Найдем общее число точек, попавших внутрь фигуры

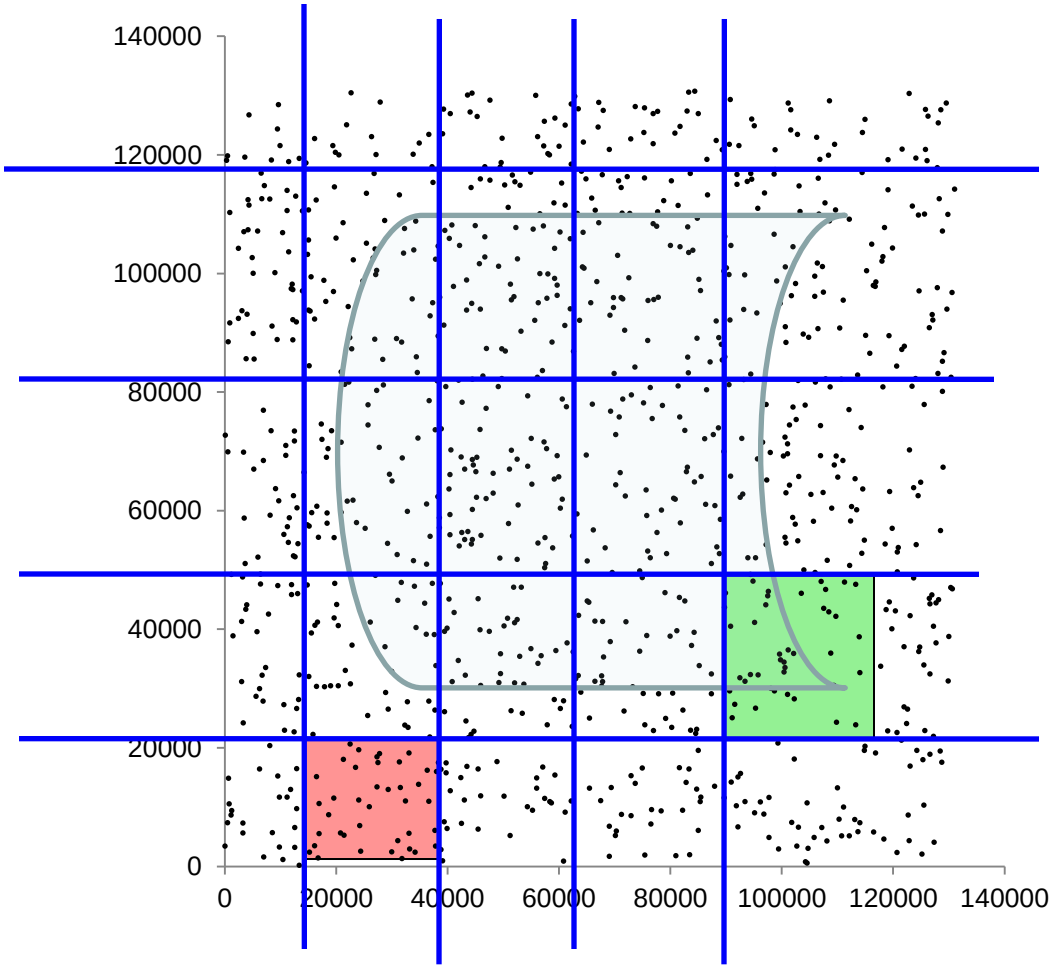
$$M = \sum_{rank=0}^{P-1} m_{rank}$$



3. S=S0*M/N;

Другой параллельный алгоритм, на основе метода геометрического параллелизма

- Возможен большой дисбаланс нагрузки



Вопросы

Должен ли ответ параллельной программы в точности совпадать с ответом последовательной версии?

НЕТ

Где взять нужное количество разных «своих» элементов?

Физический генератор?

Нельзя обеспечить вопроизводимость.

Как обеспечить уверенность в сохранении свойств генератора?

ДА

Каким образом на каждом из процессоров вычислить значения именно «своих» элементов, не вычисляя значений чужих?

Брать на процессоре с номером rank числа с номерами rank+P*I

Как вычислять каждое P-ое число?

Вычислять на процессоре с номером rank числа из диапазона

(2N/P)*rank … (2N/P)*(rank+1)-1

Как попасть в начало диапазона?

«Аппаратный» генератор СЧ

Инструкция *rdrand*. Архитектура Ivy Bridge

http://www.securitylab.ru/analytics/435181.php

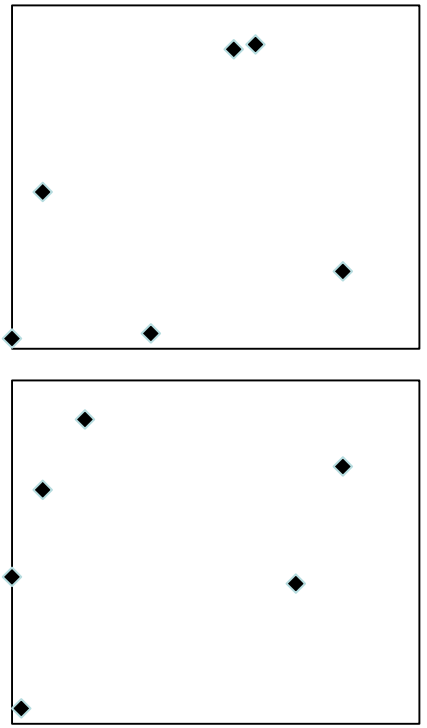
*unsigned int __builtin_ia32_rdrand32_step (unsigned int *);*

http://gcc.gnu.org/onlinedocs/gcc/X86-Built-in-Functions.html#X86-Built-in-Functions

**THE INTEL® RANDOM NUMBER GENERATOR
CRYPTOGRAPHY RESEARCH, INC. WHITE PAPER
PREPARED FOR INTEL CORPORATION Benjamin Jun and
Paul Kocher April 22, 1999**

Нарушение идентичности размещения точек

- Если брать на процессоре с номером rank числа с номерами rank+P*j, то
  - При P=1: (0,1), (2,3), (4,5), (6,7), (8,9), (10,11)
  - При P=2:
    - У первого процесса: (0,2), (4,6) (8,10)
    - У второго процесса: (1,3), (5,7), (9,11).
- Идентичность точек нужна:
  - Для получения одинакового результата
  - Для упрощения отладки
  - Для сохранения свойств последовательности
    - x1 x2 x3 x4 x5 x6 x7 x8 x9 …
    - x2 x4 x6 x8 x10 …



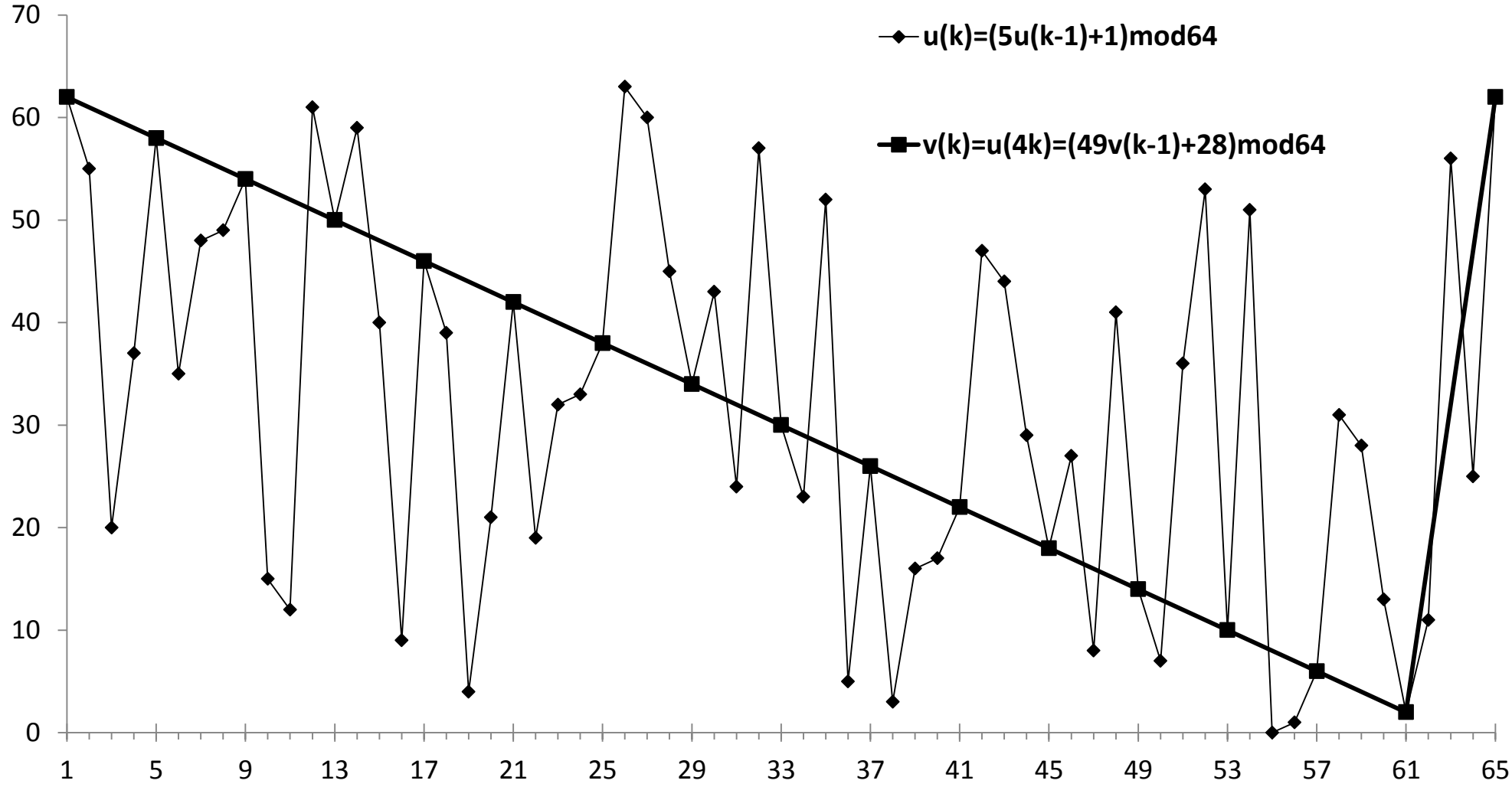
Метод *leapfrog* генерации последовательности псевдослучайных чисел

- Один процессор
- 1 3 7 9 2 5 3 5 6 1 4 2 6 8 9 5

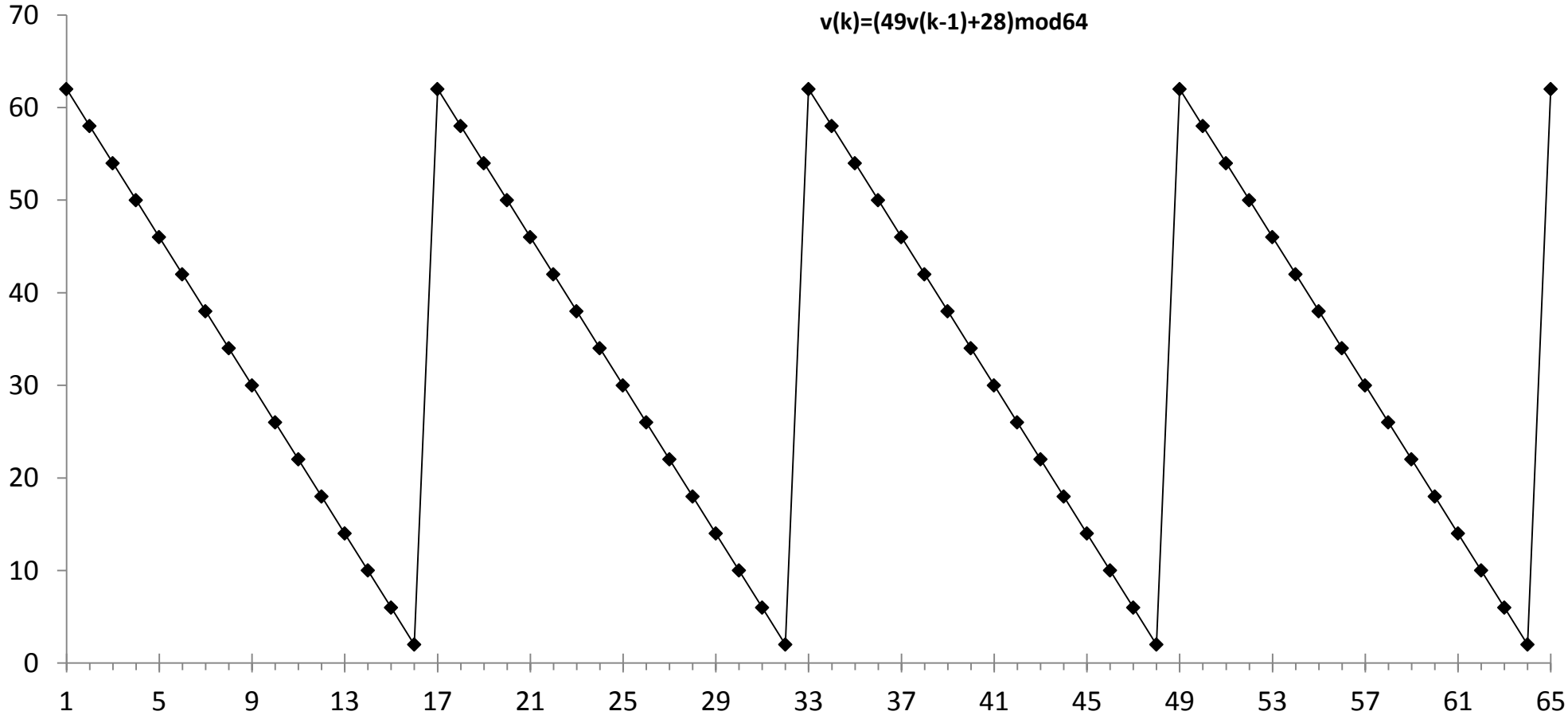
- Два процессора
- 1 7 2 3 6 4 6 9
- 3 9 5 5 1 2 8 5

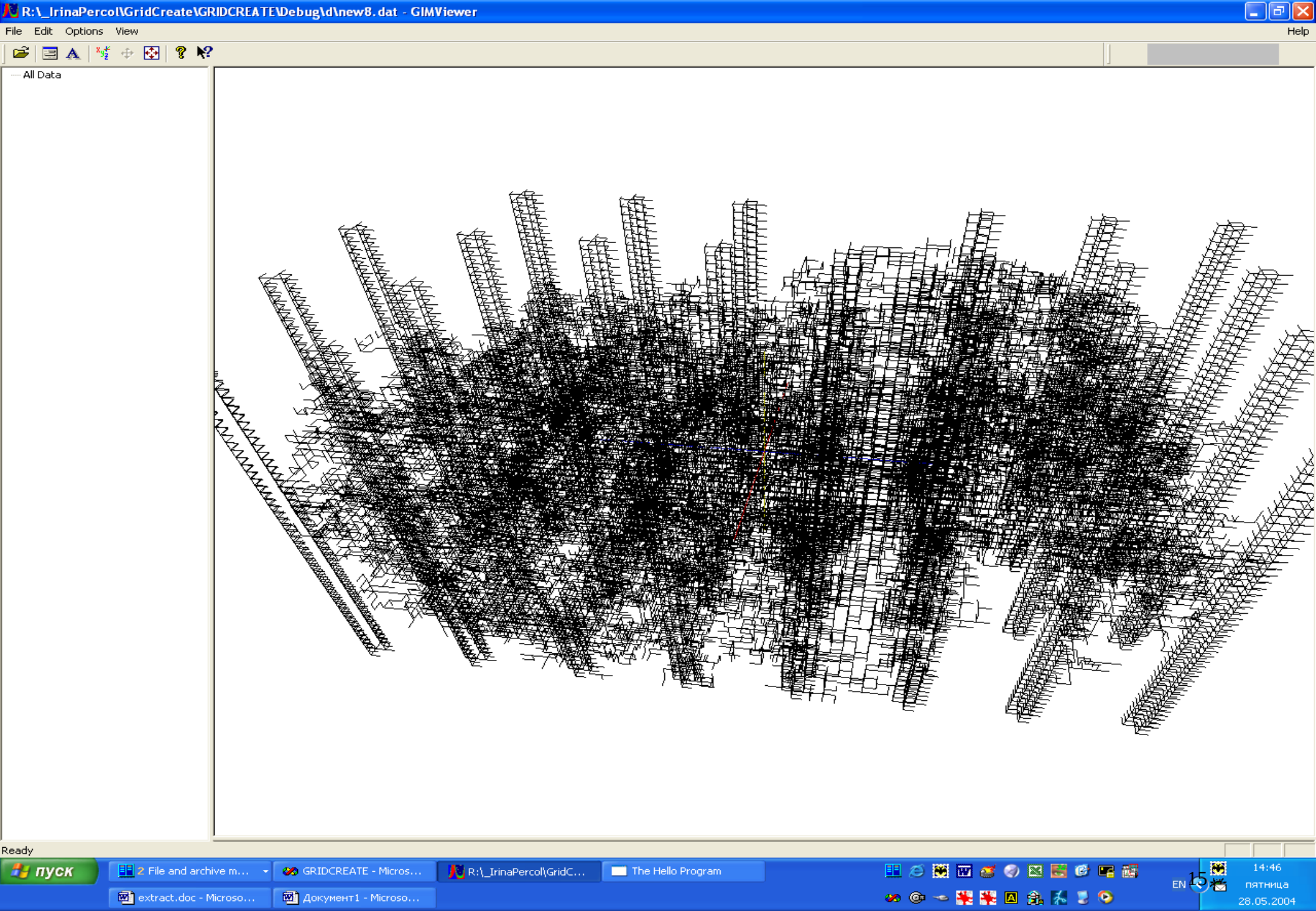
- Три процессора
- 1 3 7 9 2 5 3 5 6 1 4 2 6 8 9 5
- 1 **3** 7 9 **2** 5 3 **5** 6 1 **4** 2 6 **8** 9 5
- 7 5 6 2 9

Метод *leapfrog* генерации последовательности псевдослучайных чисел

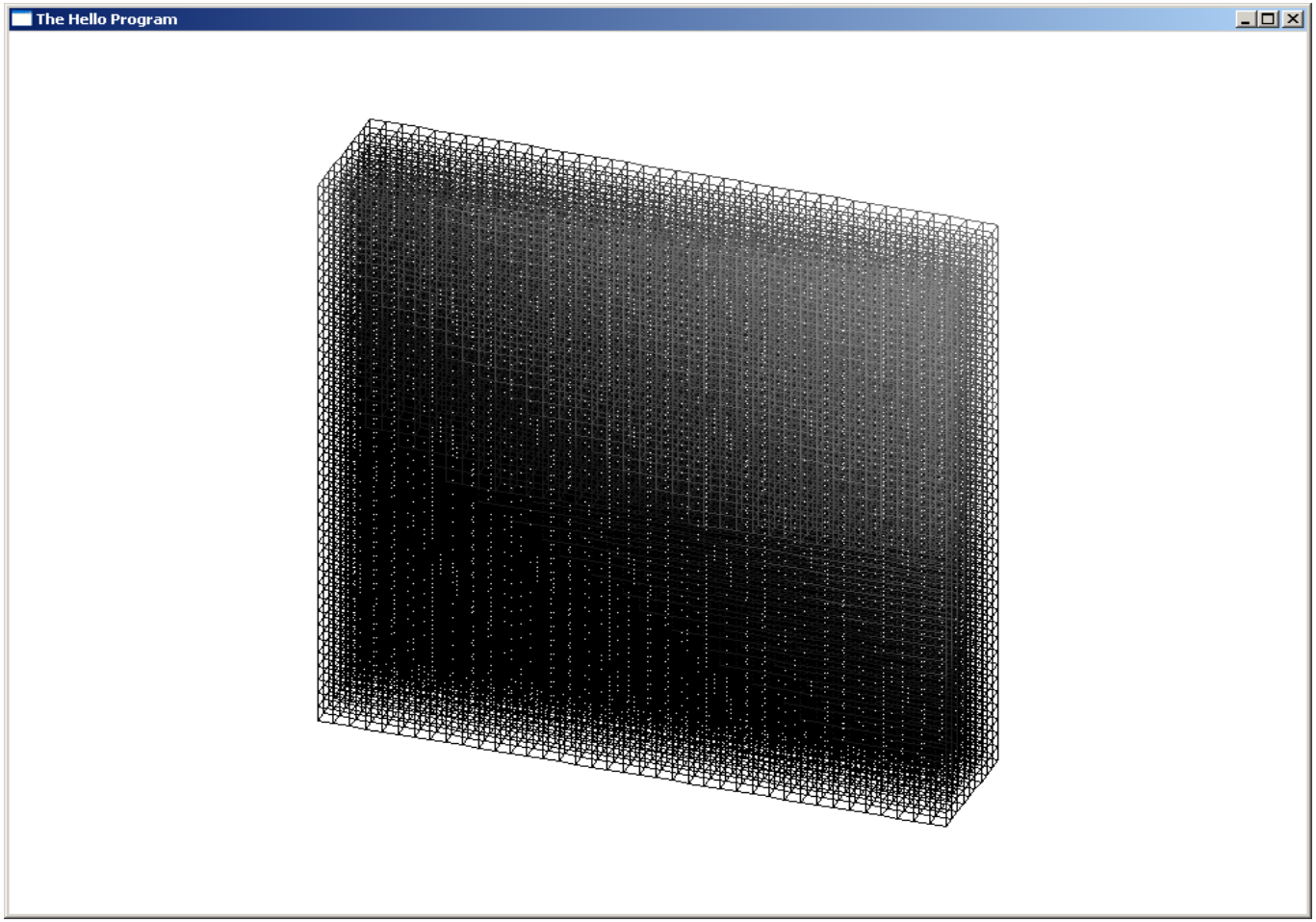


Слу чай ная пос ледов ате льность ……

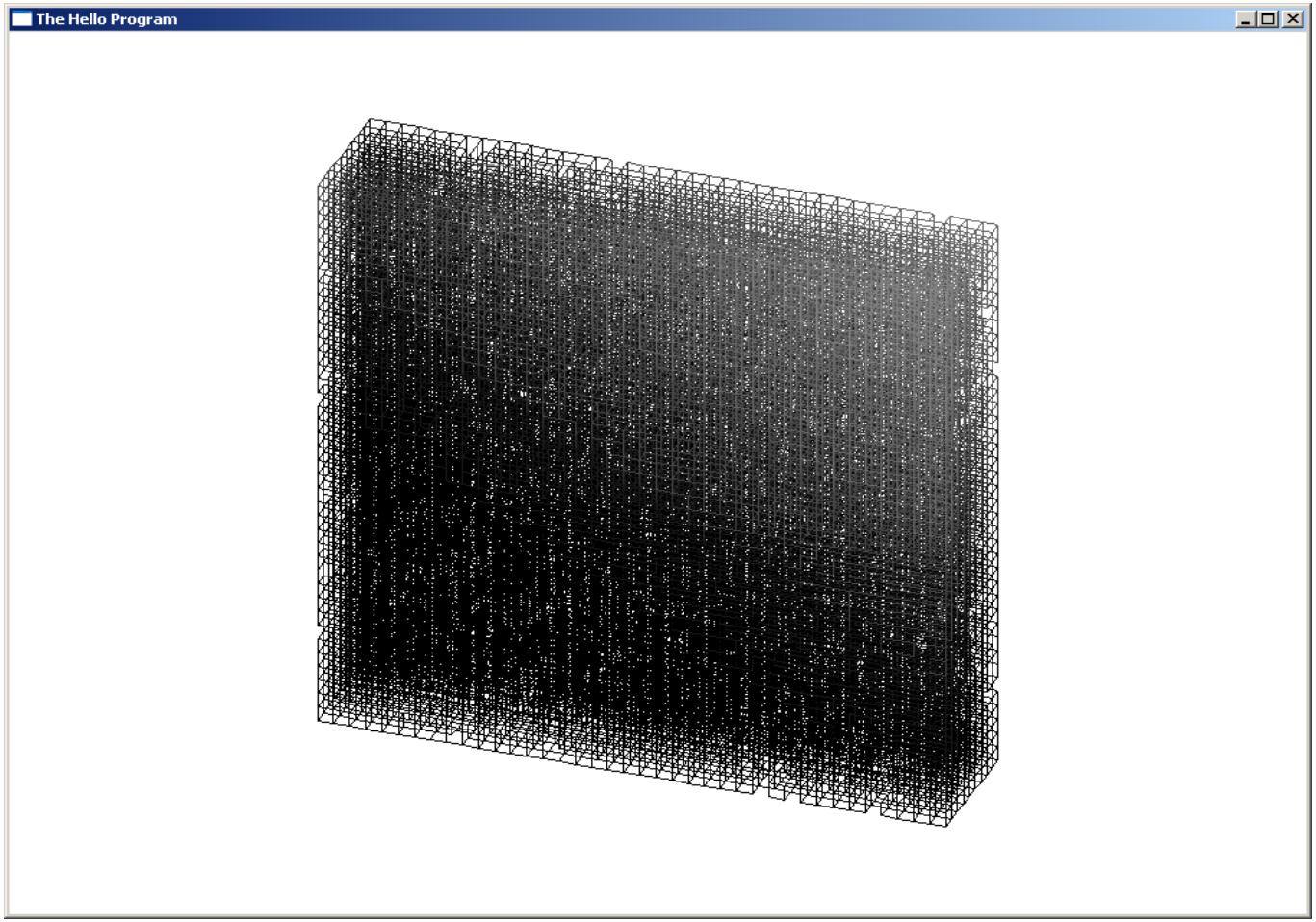



R:_IrinaPercol\GridCreate\GRIDCREATE\Debug\d\new8.dat - GIMViewer
File Edit Options View Help
All Data
Ready
пуск
2 File and archive m...
GRIDCREATE - Micros...
R:_IrinaPercol\GridC...
The Hello Program
extract.doc - Microso...
Документ1 - Microso...
EN
14:46
пятница
28.05.2004

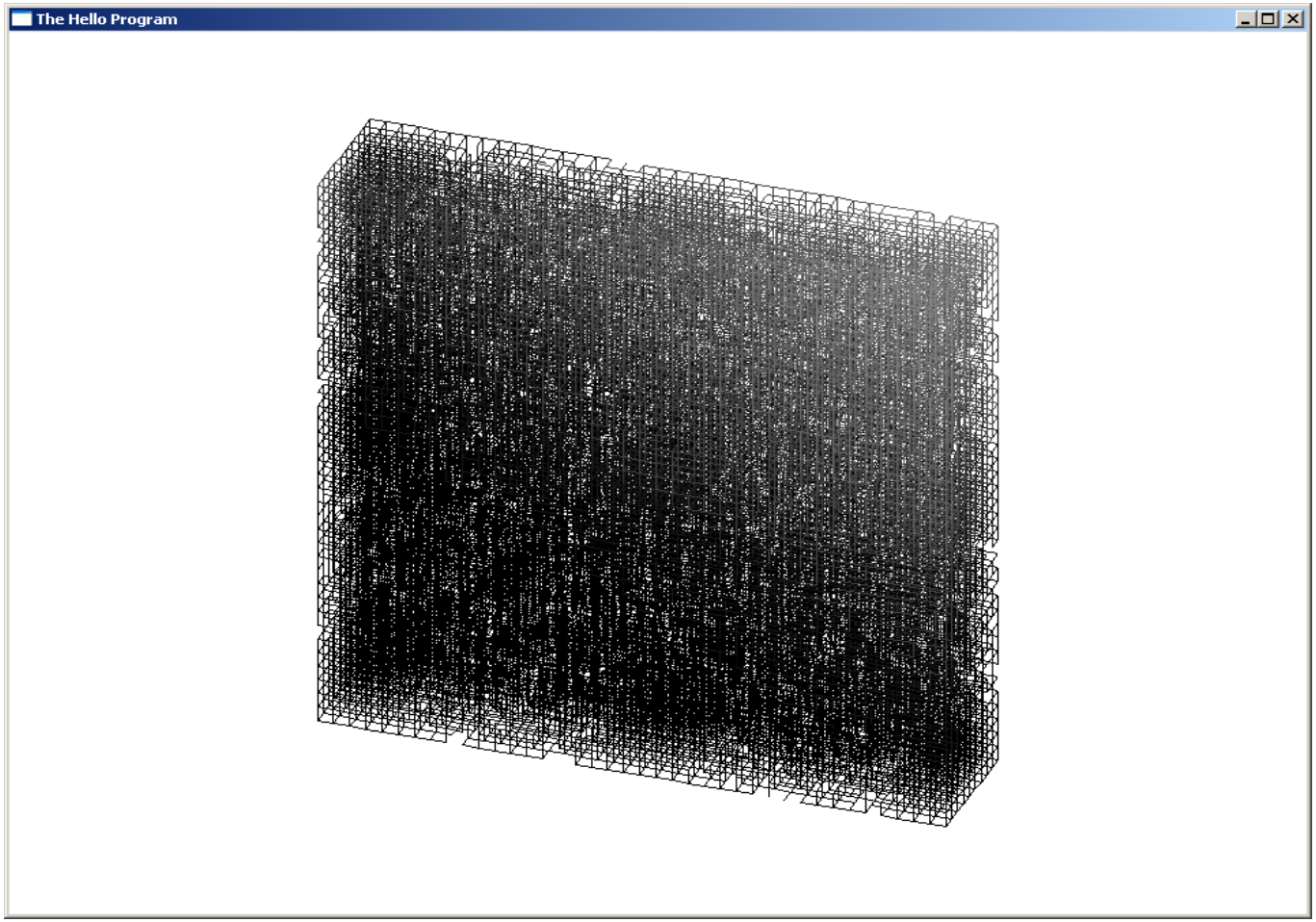
Решетка p=100%



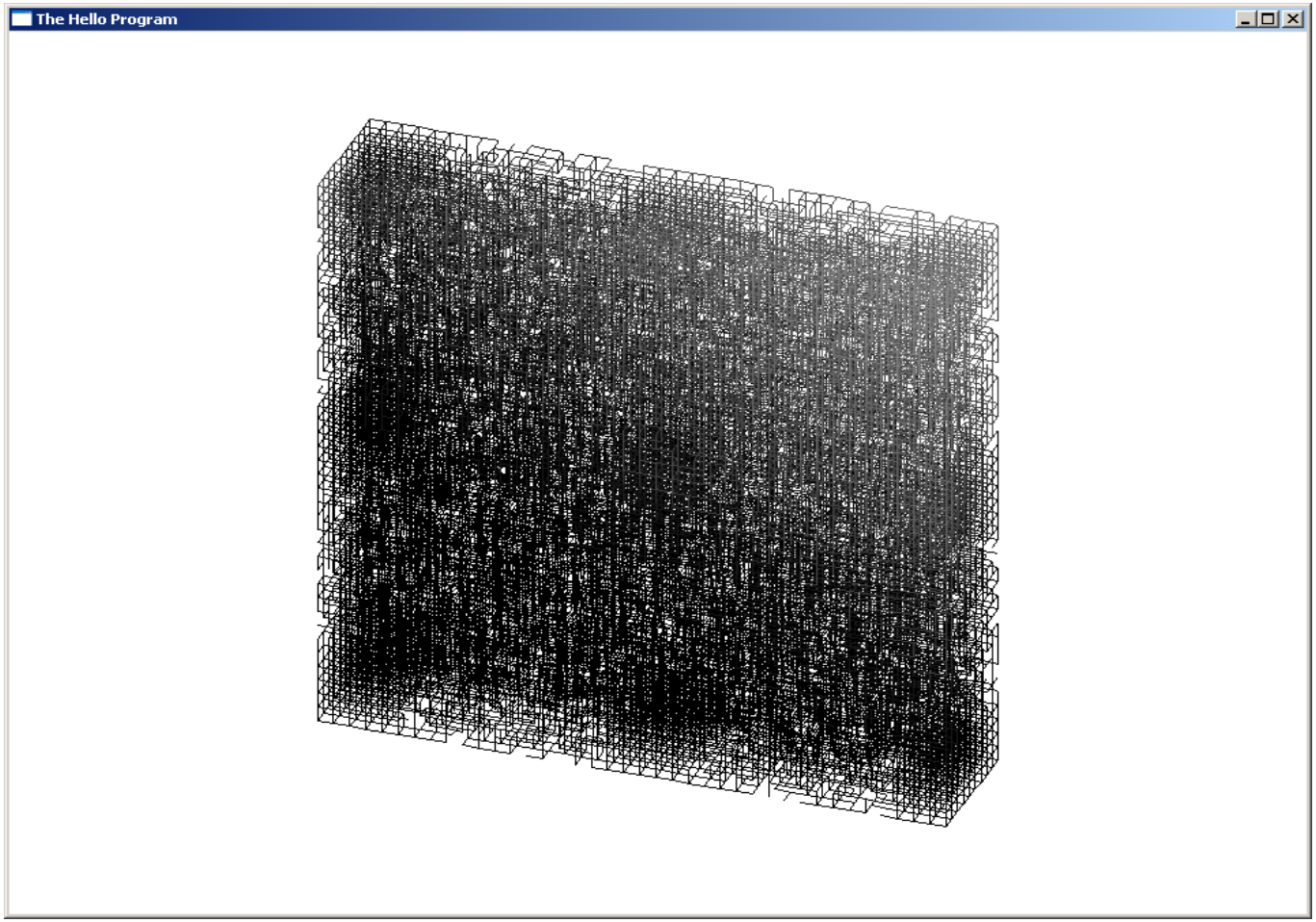
Перколяционная решетка p=90%



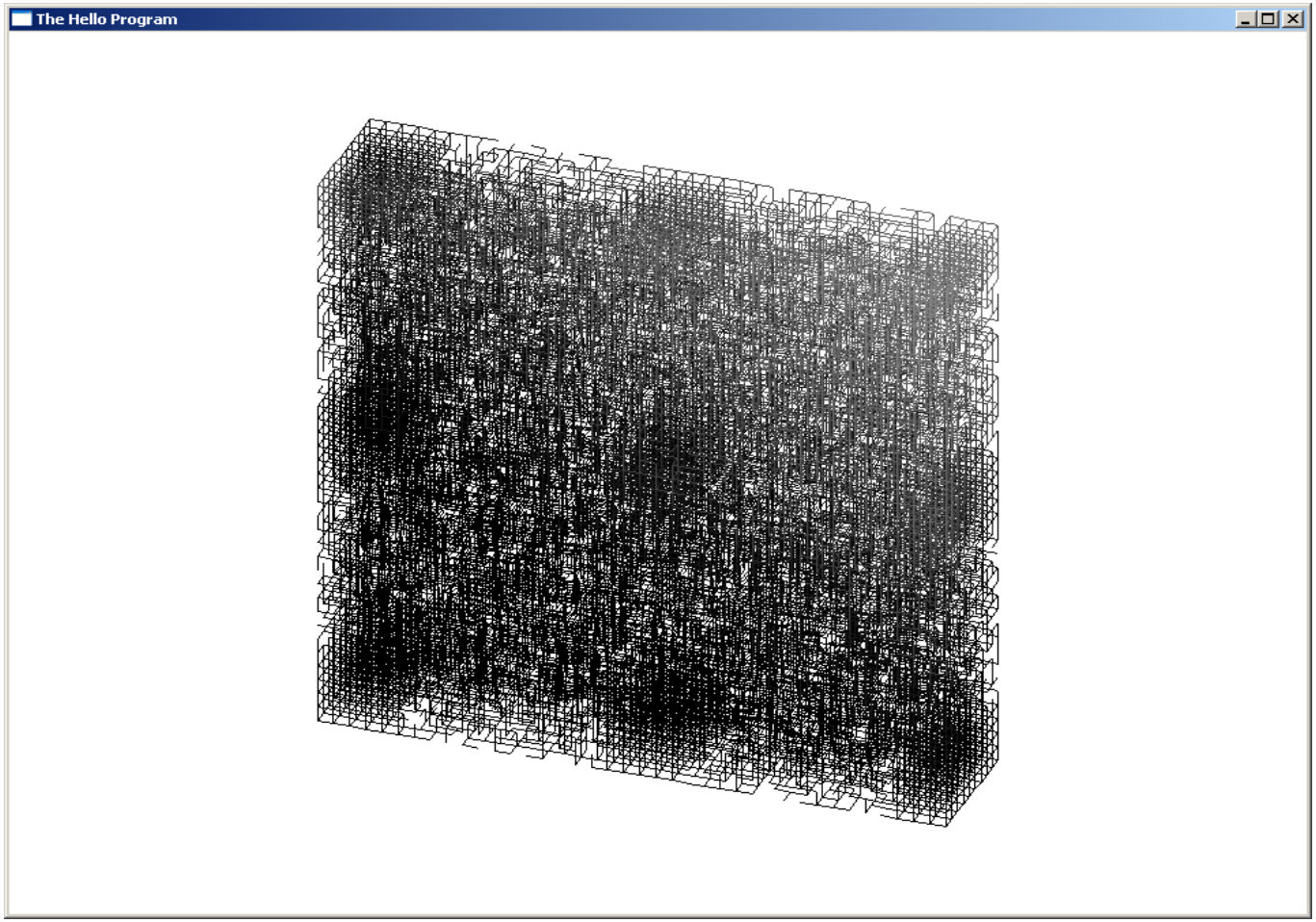
Перколяционная решетка p=80%



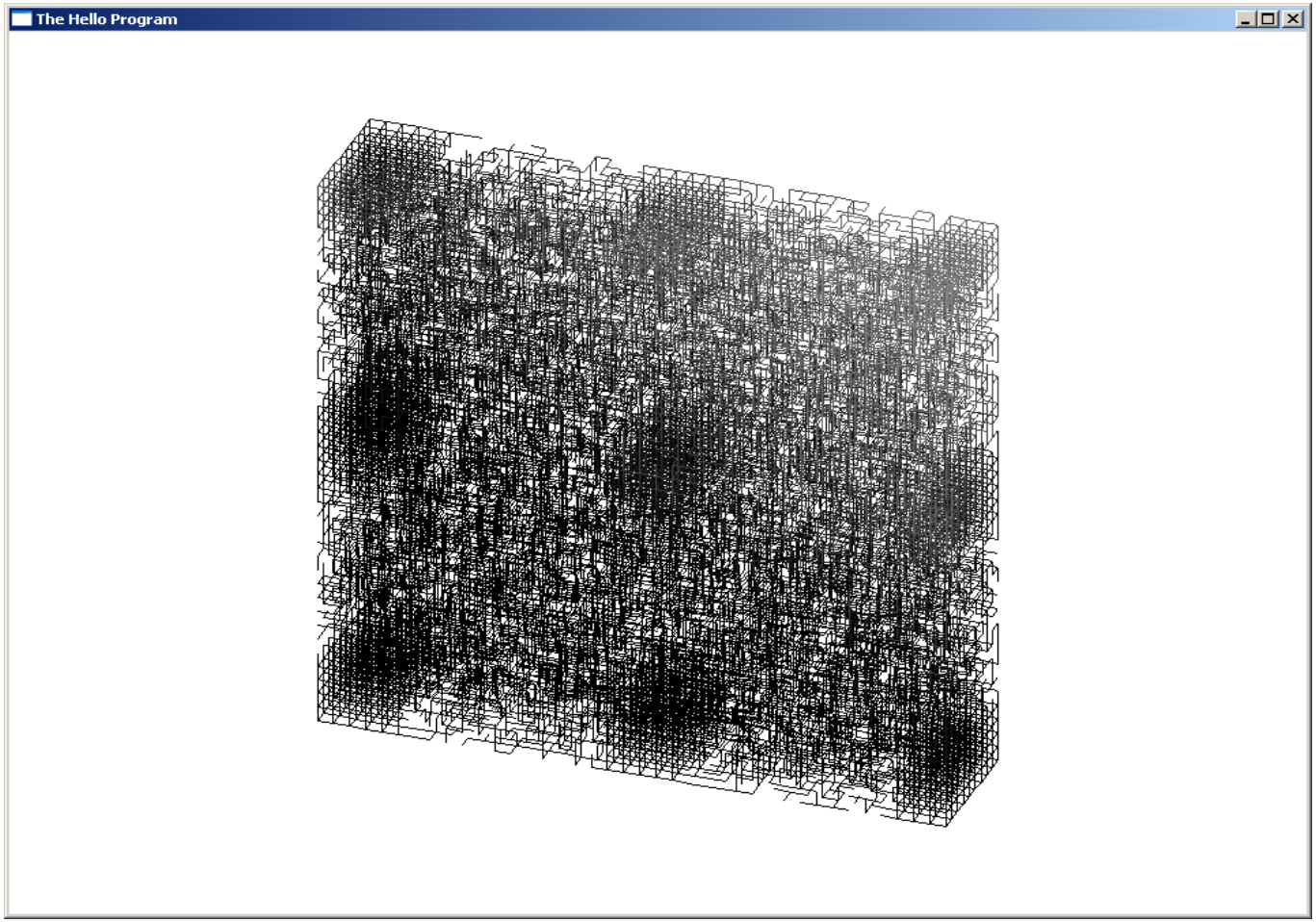
Перколяционная решетка p=70%



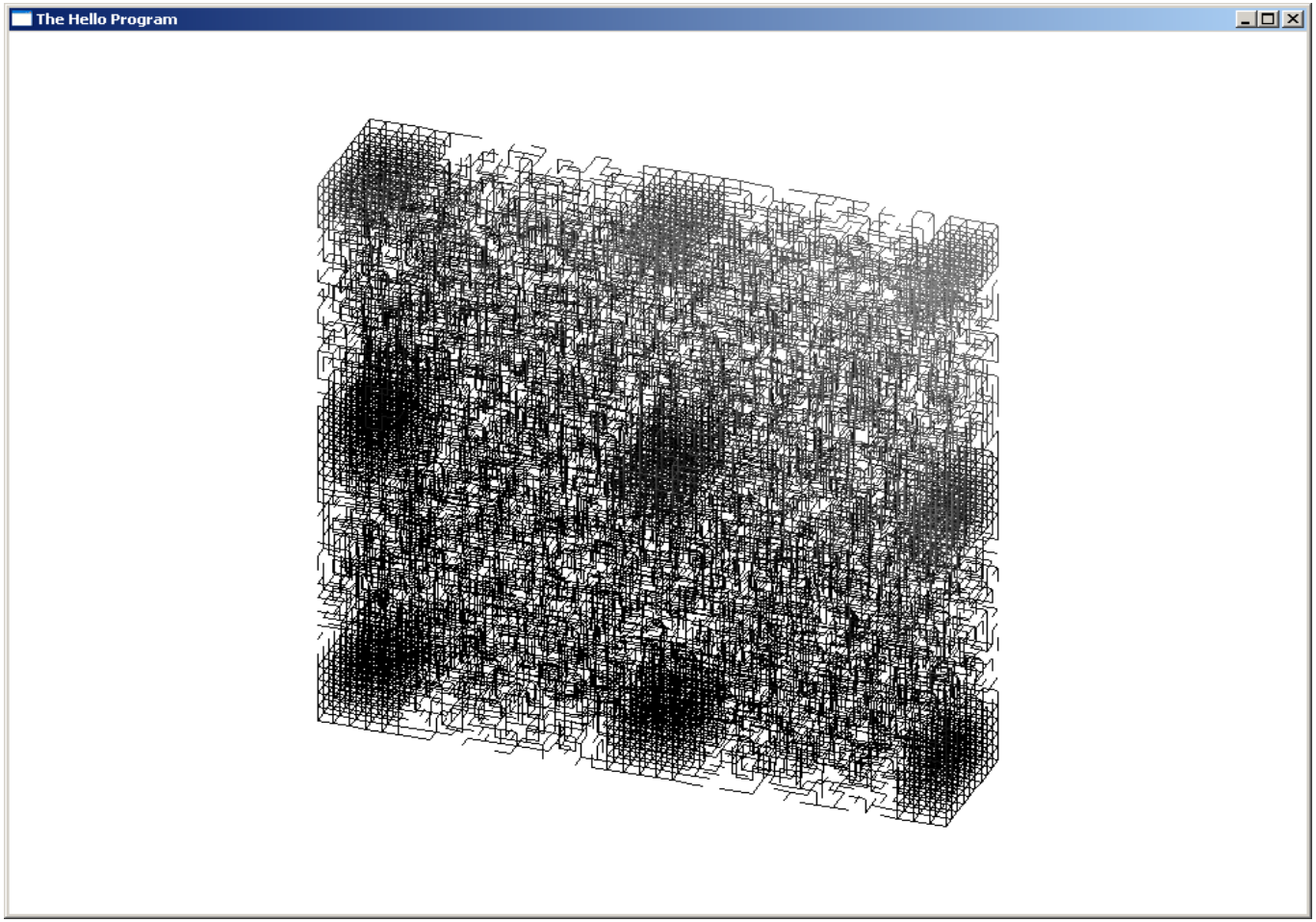
Перколяционная решетка p=60%



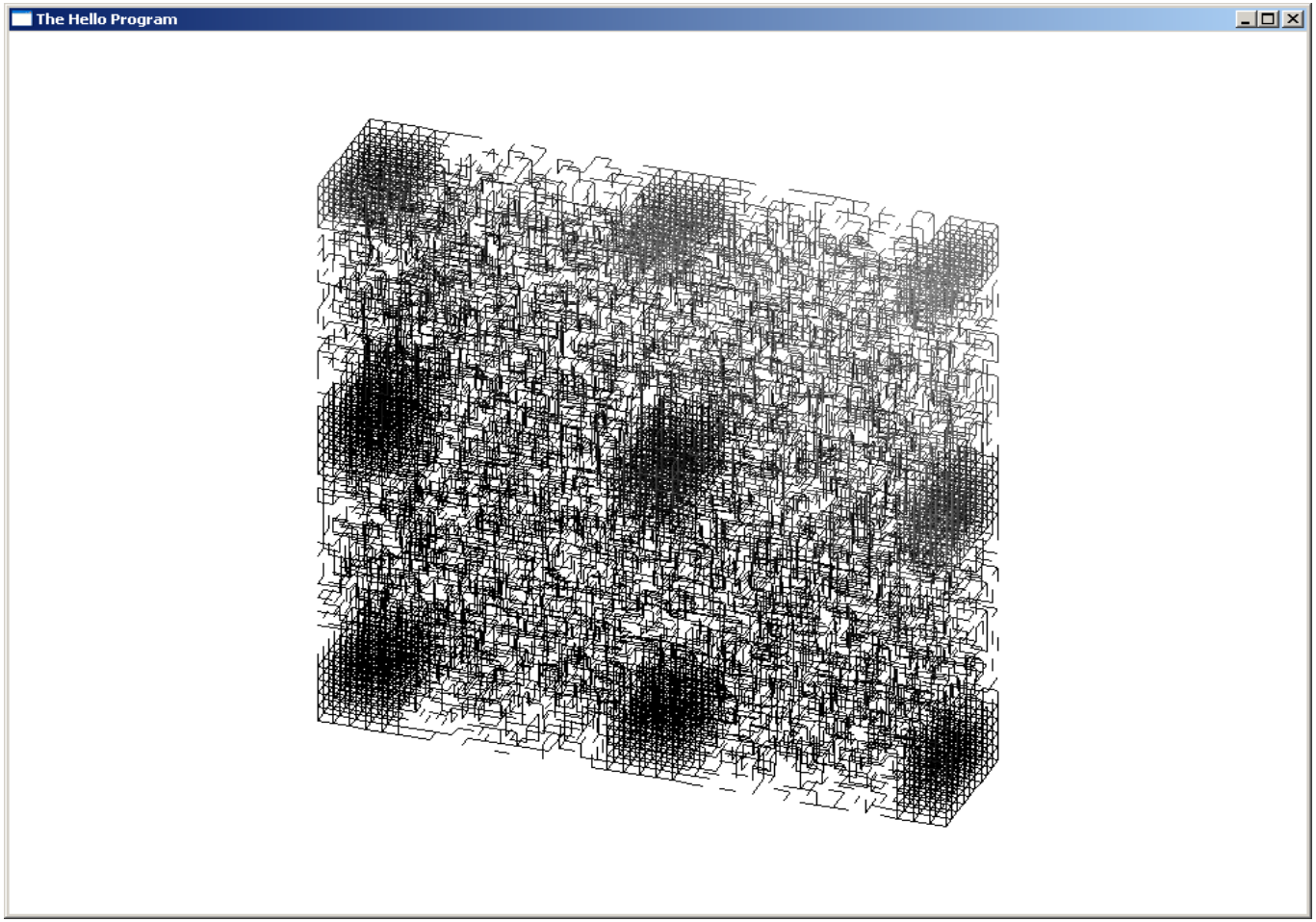
Перколяционная решетка p=50%



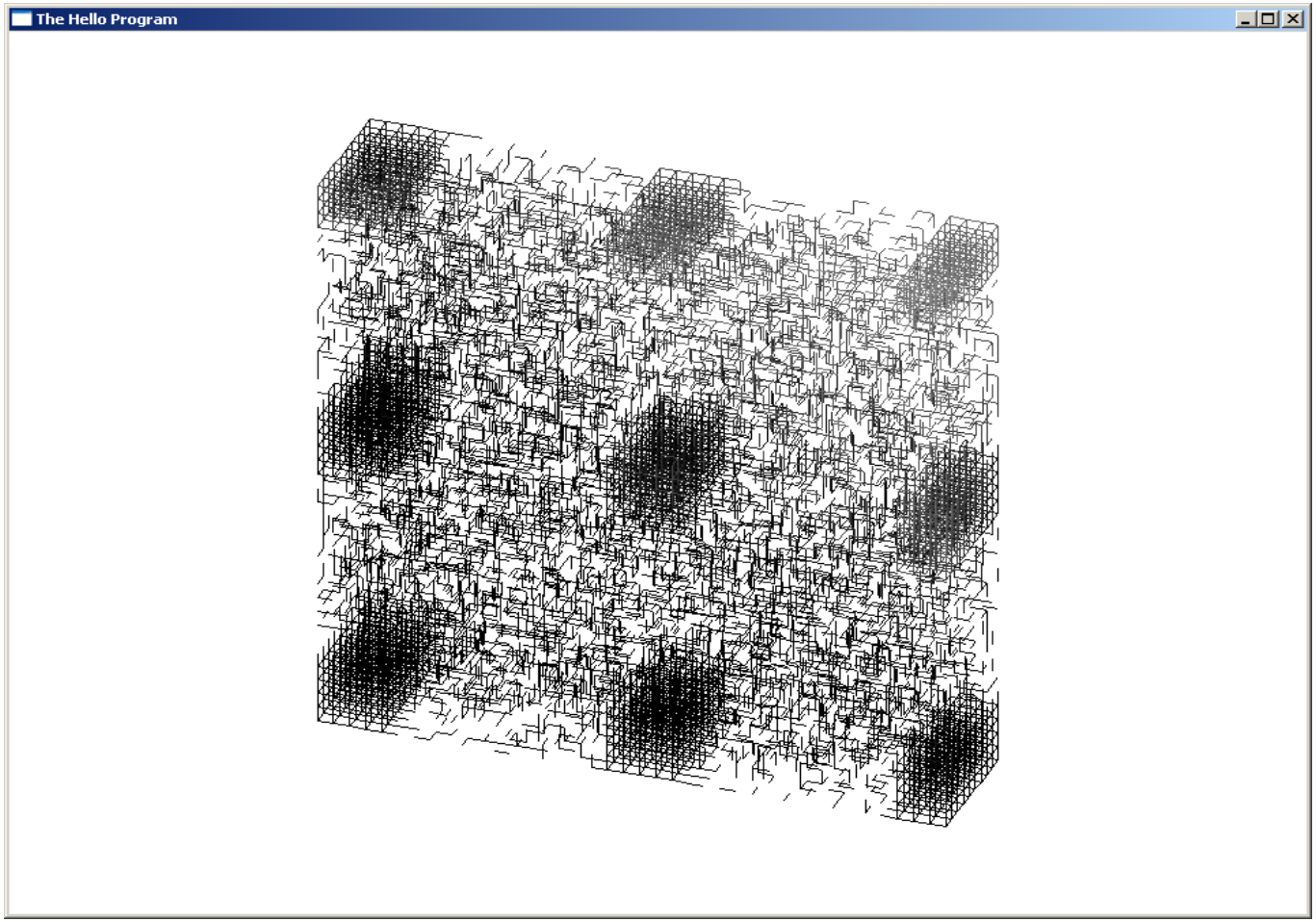
Перколяционная решетка p=40%



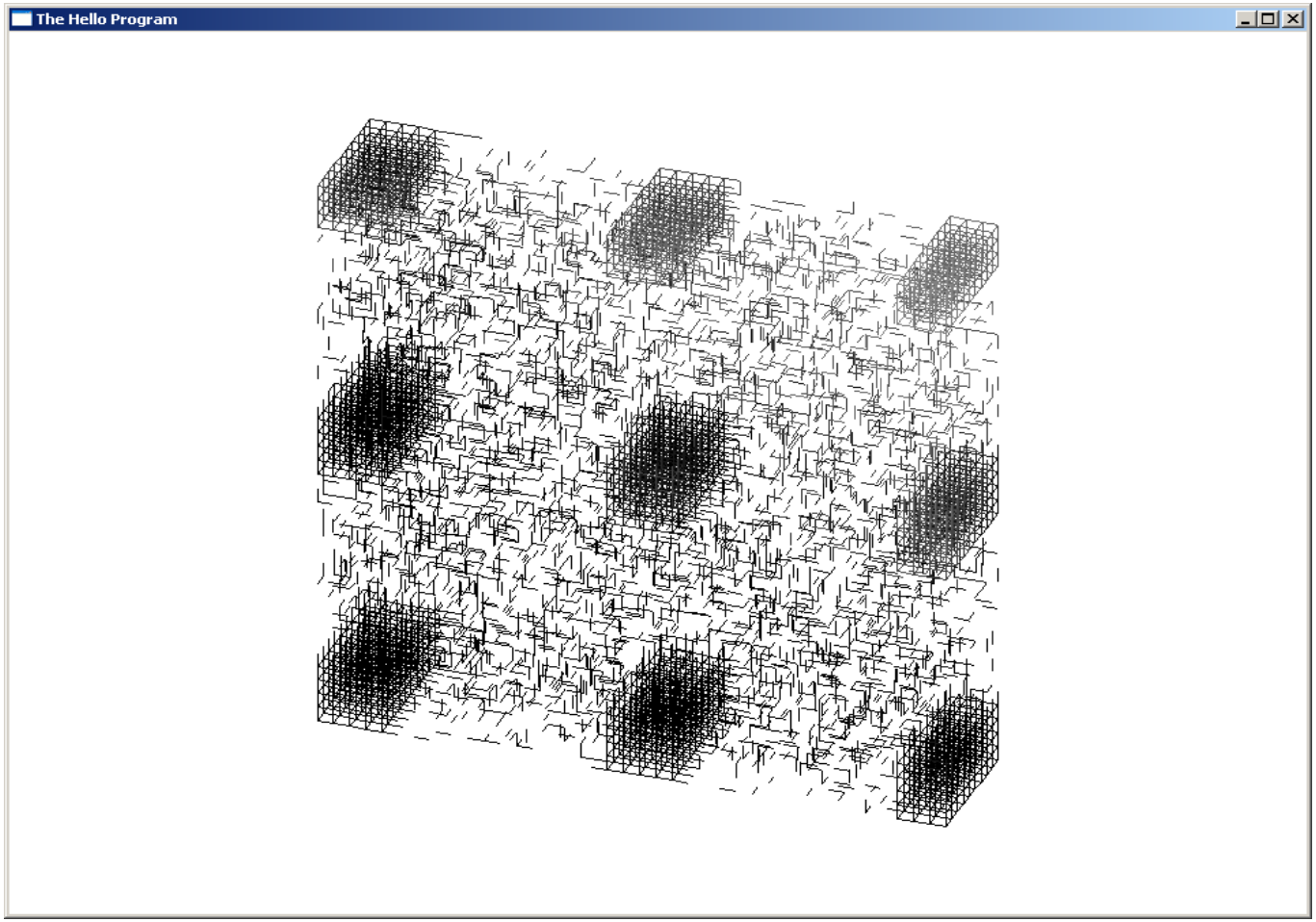
Перколяционная решетка p=30%



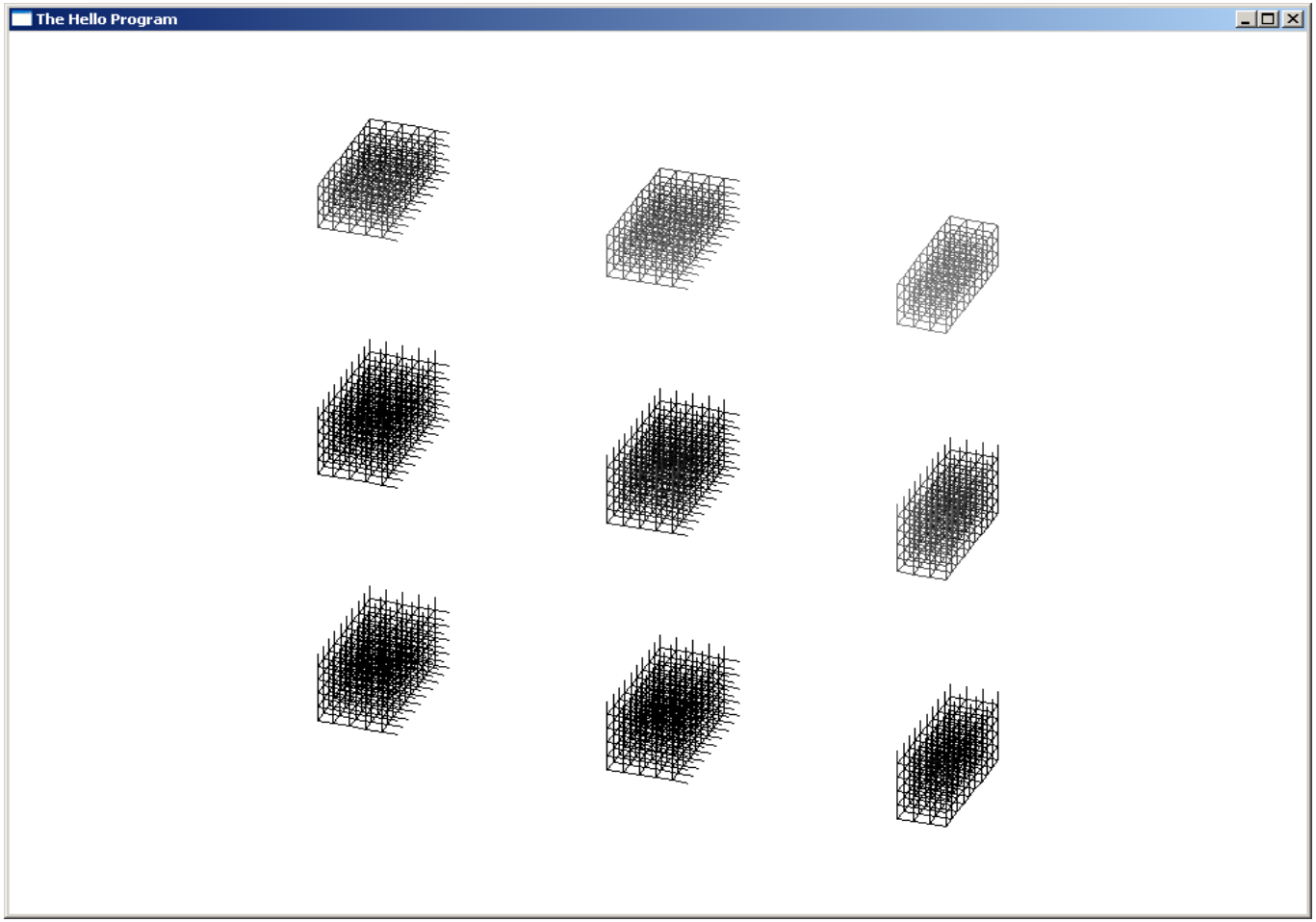
Перколяционная решетка p=20%



Перколяционная решетка p=10%



Перколяционная решетка p=0%

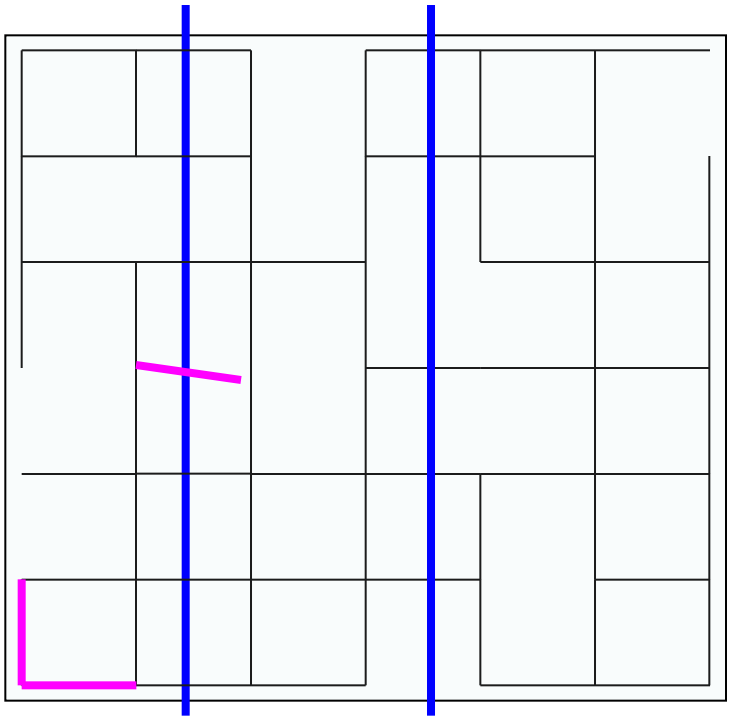


Генерация псевдослучайных чисел

- Достаточная длина периода последовательности псевдослучайных чисел

- Согласованность определения множества открытых ребер при **параллельной** обработке

  - Возможность определения любого элемента последовательности за короткое, не зависящее от номера элемента, время



Генерация псевдослучайных чисел

- линейные конгруэнтные генераторы
  [Деррик Генри Леммер (Derrick Henry Lehmer), 1948]

$$U_{n+1} = (aU_n + c) \bmod m$$

- c=1mod2, a=1mod4, $m=2^k$ -> $T=m$

Вычисление элемента с номером *n*

$$U_n = a^n U_0 + \left(\frac{a^n - 1}{a - 1} \right) c \bmod m$$

Использование для векторных компьютеров leapfrog

Номер шага

0	1	2	3	.	.	.	.
0+P	0+2P	0+3P	0+4P				
1+P	1+2P	1+3P	1+4P				
2+P	2+2P	2+3P	2+4P				
3+P	3+2P	3+3P	3+4P				
4+P	4+2P	4+3P	4+4P				

.

.

.

$$U_n = \left[a^n U_0 + \left(\frac{a^n - 1}{a - 1} \right) c \right] \bmod m$$

$$A = a^n \bmod m \quad C = \left(\frac{a^n - 1}{a - 1} \right) c \bmod m$$

$$U_n = [AU_0 + C] \bmod m$$

$$U_{P+i} = [AU_i + C] \bmod m$$

$$U_{P+i+1} = [AU_{i+1} + C] \bmod m$$

Как быстро вычислить?

$$U_n = a^n U_0 + \left(\frac{a^n - 1}{a - 1} \right) c \bmod m$$

$$(a + b) \bmod m = (a \bmod m + b \bmod m) \bmod m$$

$$(km + r) + (tm + q) = (k + t)m + r + q$$

$$(ab) \bmod m = [(a \bmod m)(b \bmod m)] \bmod m$$

$$(km + r)(tm + q) = (ktm + kq + rt)m + rq$$

Вычислить a^n

- За log(n) шагов

$$a^n \bmod m =$$

$$a^{\left\lceil \frac{n}{2} \right\rceil + \left(n - \left\lceil \frac{n}{2} \right\rceil \right)} \bmod m =$$

$$\left(a^{\left\lceil \frac{n}{2} \right\rceil} \bmod m \cdot a^{n - \left\lceil \frac{n}{2} \right\rceil} \bmod m \right) \bmod m$$

$$a^{13} = a^{7+6} = a^{4+3} a^{3+3} = \left(a^{2+2} a^{2+1} \right) \left(a^{2+1} a^{2+1} \right)$$

Бинарное умножение

$$13 = 8 + 4 + 1$$

$$13 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

$$13_{10} = 1101_2$$

$$a^{13} = a^{8+4+1} = a^8 a^4 a^1$$

Вычислить *a*^*n* за *O*(log*n*) операций

*2**log(*n*) операций

$$a^{153} = aa^{2*76} = a\left(a^{2*38}\right)^2 = a\left(\left(a^{2*19}\right)^2\right)^2 =$$

$$= a\left(\left(a\left[aa^{2*9}\right]^2\right)^2\right)^2 = a\left(\left(\left[a\left(aa^{8}\right)^2\right]^2\right)^2\right)^2$$

Как вычислить быстро?

$$U_n = a^n U_0 + \left(\frac{a^n - 1}{a - 1} \right) c \bmod m$$

Разложение дроби

$$U_n = a^n U_0 + \left(\frac{a^n - 1}{a - 1} \right) c \bmod m$$

$$a^n - 1 = a^t \left(a^k - 1 \right) + a^t - 1$$

$$n = k + t \quad k = \lfloor n/2 \rfloor$$

Понижение степени разложением дроби

$$\left(\frac{a^n-1}{a-1}\right)c \bmod m = \left[\left(a^t\,\frac{a^k-1}{a-1}+\frac{a^t-1}{a-1}\right)c\right] \bmod m =$$

$$\left\{\left(\left(a^t\right)_m\left(\frac{a^k-1}{a-1}\right)_m+\left(\frac{a^t-1}{a-1}\right)_m\right)c\right\} \bmod m$$

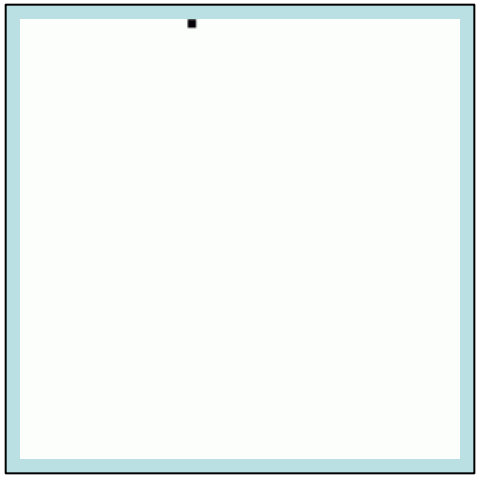
$$k=\lfloor n/2 \rfloor \qquad t=n-k$$

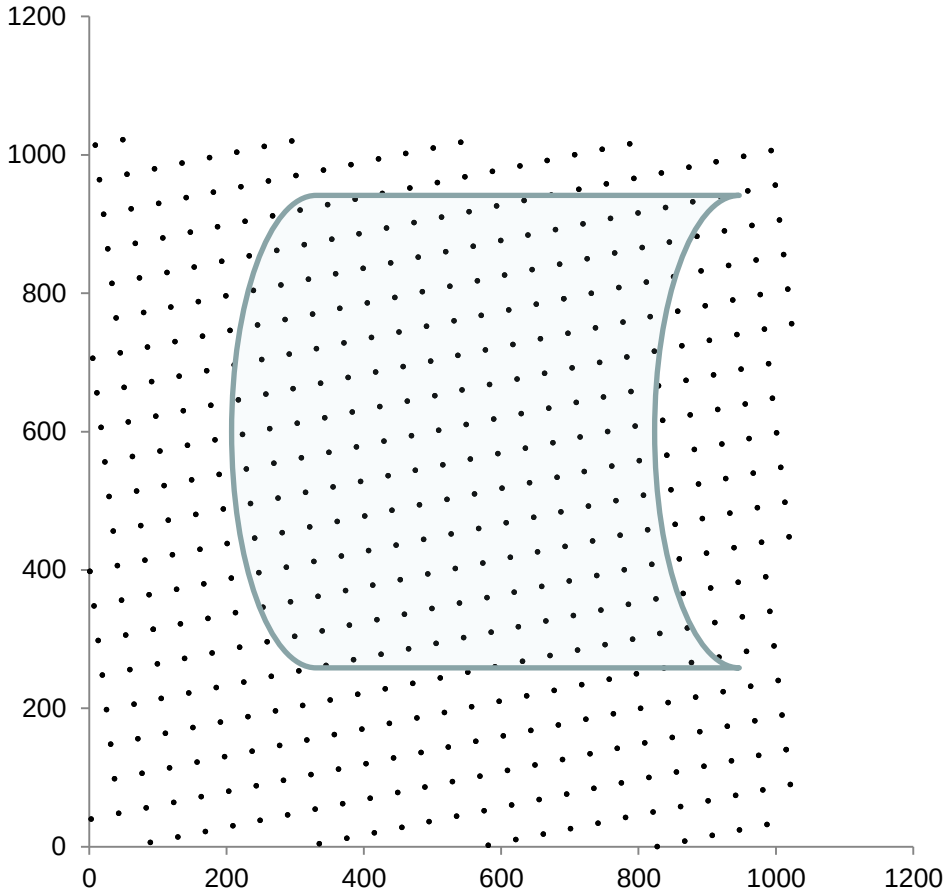
Случайные точки

Последовательность

$$x_{n+1} = (845x_n + 2625) \bmod 1024$$

512 точек вида (x_{2i}, x_{2i+1}) лежат на нескольких прямых





Линейные конгруэнтные генераторы [Лемер, 1948]

- При c=0 d-мерные точки расположены не более чем в $\sqrt[d]{d!m}$ гиперплоскостях

[G. Marsaglia 1968]

- Для RANDU(IBM 360/370) $a=2^{16}+3$, $m=2^{31}$, $c=0$

$$(a-3)^2 = 0 \bmod m$$

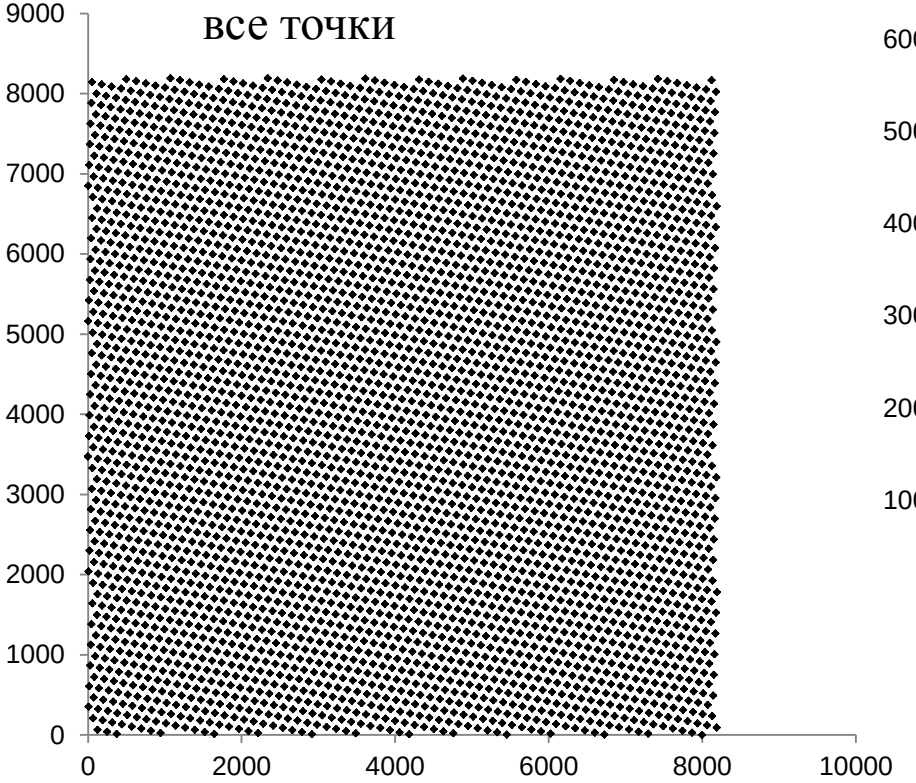
- Не более 16-ти плоскостей [Richard P.Brent, 1992]

$$U_{n+2} - 6U_{n+1} + 9U_n = 0 \bmod m$$

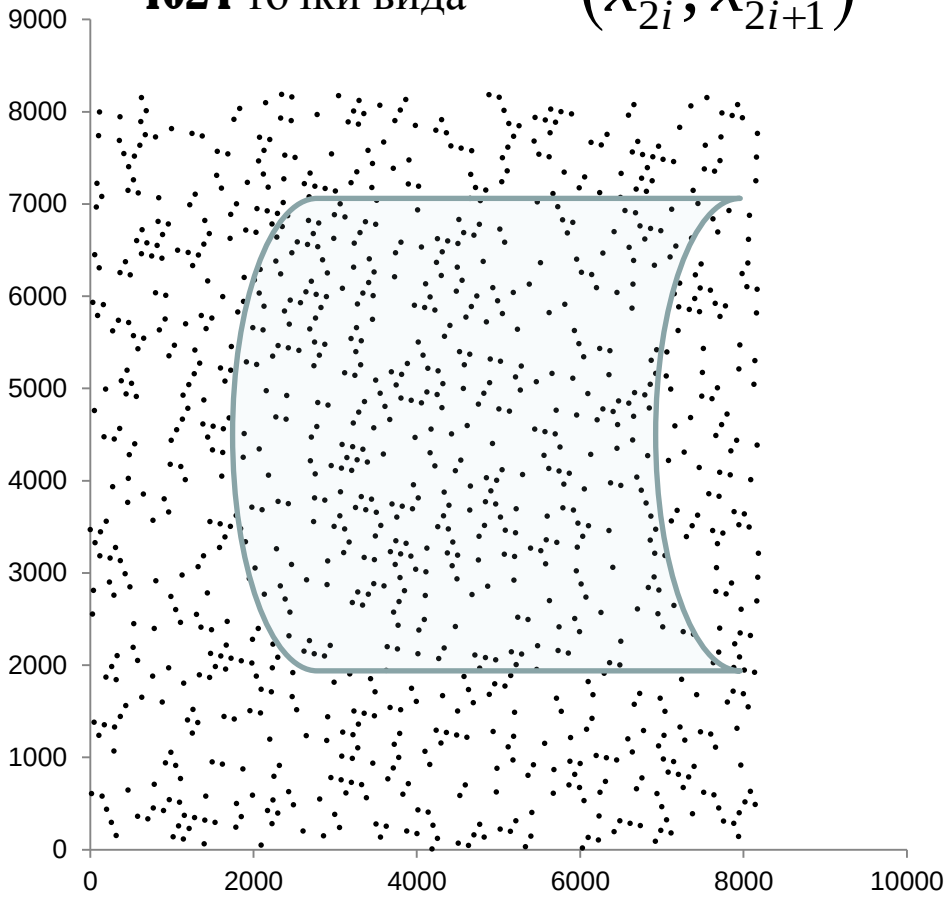
Случайные точки

Последовательность

$$x_{n+1} = (845x_n + 2625) \bmod 8192$$



1024 точки вида (x_{2i}, x_{2i+1})

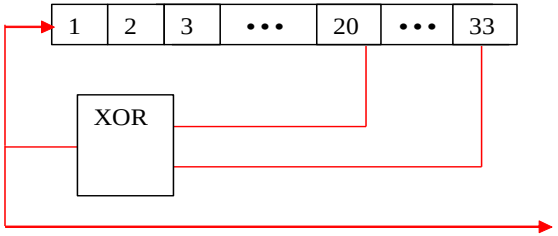


Разумная альтернатива

M – последовательности

М-последовательности

- Генератор на сдвиговом регистре [П.Хоровиц,У.Хилл, 1983]



- М-последовательности [И.М. Соболь, 1973]

$$\gamma_i \oplus \gamma_{i+20} \oplus \gamma_{i+33} = 0$$

$$\gamma_{n+r} = \left(\sum_{k=0}^{r-1} e_k \gamma_{n+k} \right) \bmod 2$$

Генерация псевдослучайных чисел

ABCD

F=(A+D)mod2

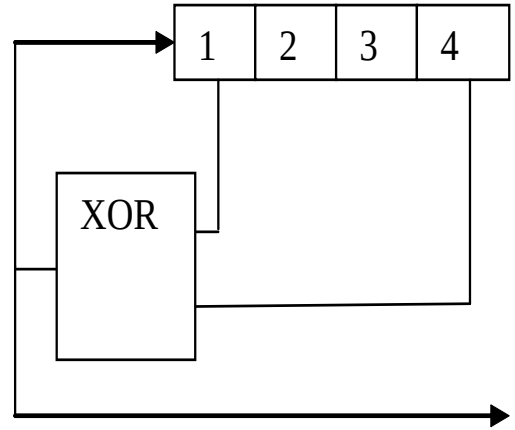
D=C

C=B

B=A

A=F

		A	B	C	D	(A+D)mod2
1	15	1	1	1	1	0
2	14	0	1	1	1	1
3	13	1	0	1	1	0
4	10	0	1	0	1	1
5	5	1	0	1	0	1
6	11	1	1	0	1	0
7	6	0	1	1	0	0
8	12	0	0	1	1	1
9	9	1	0	0	1	0
10	2	0	1	0	0	0
11	4	0	0	1	0	0
12	8	0	0	0	1	1
13	1	1	0	0	0	1
14	3	1	1	0	0	1
15	7	1	1	1	0	1
16	15	1	1	1	1	0



Генерация псевдослучайных чисел

ABCD

F=(A+D)mod2

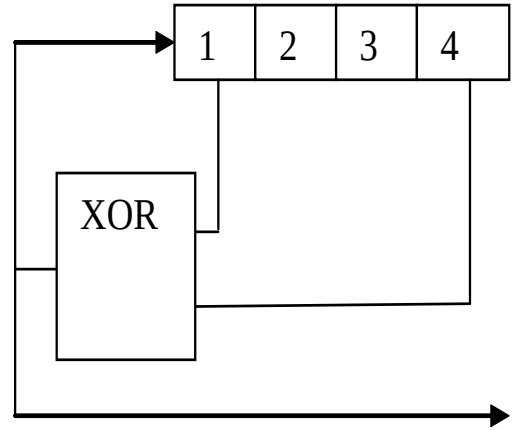
D=C

C=B

B=A

A=F

		A	B	C	D	(A+D)mod2
1	15	1	1	1	1	0
2	14	0	1	1	1	1
3	13	1	0	1	1	0
4	10	0	1	0	1	1
5	5	1	0	1	0	1
6	11	1	1	0	1	0
7	6	0	1	1	0	0
8	12	0	0	1	1	1
9	9	1	0	0	1	0
10	2	0	1	0	0	0
11	4	0	0	1	0	0
12	8	0	0	0	1	1
13	1	1	0	0	0	1
14	3	1	1	0	0	1
15	7	1	1	1	0	1
16	15	1	1	1	1	0



Генерация псевдослучайных чисел

ABCD

F=(A+D)mod2

D=C

C=B

B=A

A=F

		A	B	C	D	(A+D)mod2	
1	15	1	1	1	1	0	
2	14	0	1	1	1	1	010 = 2
3	13	1	0	1	1	0	
4	10	0	1	0	1	1	
5	5	1	0	1	0	1	110 = 6
6	11	1	1	0	1	0	
7	6	0	1	1	0	0	
8	12	0	0	1	1	1	010 = 2
9	9	1	0	0	1	0	
10	2	0	1	0	0	0	
11	4	0	0	1	0	0	001 = 1
12	8	0	0	0	1	1	
13	1	1	0	0	0	1	
14	3	1	1	0	0	1	111 = 7
15	7	1	1	1	0	1	
16	15	1	1	1	1	0	

Связь между $t^n \bmod G(t)$ и фрагментом M последовательности

Если

$$t^n = \sum_{j=0}^{r-1} a_{n,j} t^j \bmod (2, G(t))$$

то

$$x_n = \sum_{j=0}^{r-1} a_{n,j} x_j \bmod 2$$

Richard P. Brent
On the period of generalized Fibonacci recurrences, 1992

Генерация элемента с произвольным номером *k*

$$f_k = x^k \bmod G$$

$$k = \sum_{i=0}^{n-1} \alpha_i 2^i, \quad \alpha_i \in \{0,1\}$$

$$x^k = \prod_{i=0}^{n-1} \left(x^{2^i}\right)^{\alpha_i} \bmod G$$

$$f_k = x^k \bmod \left(x^4 + x^1 + 1\right)$$

Проверка примитивности полинома

$$x^{2^r} = x \bmod G(x)$$

$$x^{\frac{(2^r-1)}{h_i}} \neq 1 \bmod G(x)$$

h_i – простые делители

$$2^r - 1 = \prod_i h_i$$

Определение. Полином $P(x)$ степени $r > 1$ называется примитивным, если $P(x)$ неприводим и $x^j \not\equiv 1 (\bmod P(x))\ \forall j \in \{1,2,\ldots,2^r - 2\}$.

Вычислить *x*^*n* за *O*(log*n*) операций перемножения полиномов

*2**log(*n*) операций

$$x^{153} = xx^{2*76} = x\left(x^{2*38}\right)^2 = x\left(\left(x^{2*19}\right)^2\right)^2 =$$

$$= x\left(\left(x\left[xx^{2*9}\right]^2\right)^2\right)^2 = x\left(\left(\left[x\left(xx^{8}\right)^2\right]^2\right)^2\right)^2$$

$$x^0 \bmod \left(x^4 + x^3 + 1\right) = 1$$

$$x^1 \bmod \left(x^4 + x^3 + 1\right) = x$$

$$x^2 \bmod \left(x^4 + x^3 + 1\right) = x^2$$

$$x^3 \bmod \left(x^4 + x^3 + 1\right) = x^3$$

$$x^4 \bmod \left(x^4 + x^3 + 1\right) = x^4 + \quad x^4 + x^3 + 1 = x^3 + 1$$

$$x^5 = (x^3 + 1)x = x^4 + x = x^4 + x + x^4 + x^3 + 1 = x^3 + x + 1$$

$$x^6 = x^4 + x^2 + x + \quad x^4 + x^3 + 1 = x^3 + x^2 + x + 1$$

$$x^7 = x^4 + x^3 + x^2 + x + \quad x^4 + x^3 + 1 = x^2 + x + 1$$

$$x^8 = x^3 + x^2 + x$$

$$x^9 = x^4 + x^3 + x^2 + \quad x^4 + x^3 + 1 = x^2 + 1$$

$$x^{10} = x^3 + x$$

$$x^5 = (x^3+1)x = x^4 + x = x^4 + x + x^4 + x^3 + 1 = x^3 + x + 1$$

$$x^6 = x^4 + x^2 + x + \quad x^4 + x^3 + 1 = x^3 + x^2 + x + 1$$

$$x^7 = x^4 + x^3 + x^2 + x + \quad x^4 + x^3 + 1 = x^2 + x + 1$$

$$x^8 = x^3 + x^2 + x$$

$$x^9 = x^4 + x^3 + x^2 + \quad x^4 + x^3 + 1 = x^2 + 1$$

$$x^{10} = x^3 + x$$

$$x^{11} = x^4 + x^2 + \quad x^4 + x^3 + 1 = x^3 + x^2 + 1$$

$$x^{12} = x^4 + x^3 + x + \quad x^4 + x^3 + 1 = x + 1$$

$$x^{13} = x^2 + x$$

$$x^{14} = x^3 + x^2$$

$$x^{15} = x^4 + x^3 + \quad x^4 + x^3 + 1 = 1$$

$$x^{16} = x$$

$$x^0 \bmod \left(x^4+x^3+1\right)=1$$
$$x^1 \bmod \left(x^4+x^3+1\right)=x$$
$$x^2 \bmod \left(x^4+x^3+1\right)=x^2$$
$$x^3 \bmod \left(x^4+x^3+1\right)=x^3$$
$$x^4 \bmod \left(x^4+x^3+1\right)=x^4+\quad x^4+x^3+1=x^3+1$$
$$x^5=(x^3+1)x=x^4+x=x^4+x+x^4+x^3+1=x^3+x+1$$
$$x^6=x^4+x^2+x+\quad x^4+x^3+1=x^3+x^2+x+1$$
$$x^7=x^4+x^3+x^2+x+\quad x^4+x^3+1=x^2+x+1$$
$$x^8=x^3+x^2+x$$
$$x^9=x^4+x^3+x^2+\quad x^4+x^3+1=x^2+1$$
$$x^{10}=x^3+x$$
$$x^{11}=x^4+x^2+\quad x^4+x^3+1=x^3+x^2+1$$
$$x^{12}=x^4+x^3+x+\quad x^4+x^3+1=x+1$$
$$x^{13}=x^2+x$$
$$x^{14}=x^3+x^2$$

$$x^0 \bmod \left(x^4+x^3+1\right) \bmod x=1$$
$$x^1 \bmod \left(x^4+x^3+1\right) \bmod x=0$$
$$x^2 \bmod \left(x^4+x^3+1\right) \bmod x=0$$
$$x^3 \bmod \left(x^4+x^3+1\right) \bmod x=0$$
$$x^4 \bmod \left(x^4+x^3+1\right) \bmod x=1$$
$$x^5 \bmod \left(x^4+x^3+1\right) \bmod x=1$$
$$x^6 \bmod \left(x^4+x^3+1\right) \bmod x=1$$
$$x^7 \bmod \left(x^4+x^3+1\right) \bmod x=1$$
$$x^8 \bmod \left(x^4+x^3+1\right) \bmod x=0$$
$$x^9 \bmod \left(x^4+x^3+1\right) \bmod x=1$$
$$x^{10} \bmod \left(x^4+x^3+1\right) \bmod x=0$$
$$x^{11} \bmod \left(x^4+x^3+1\right) \bmod x=1$$
$$x^{12} \bmod \left(x^4+x^3+1\right) \bmod x=1$$
$$x^{13} \bmod \left(x^4+x^3+1\right) \bmod x=0$$
$$x^{14} \bmod \left(x^4+x^3+1\right) \bmod x=0$$

Генерация псевдослучайных чисел

ABCD

F=(A+D)mod2

D=C

C=B

B=A

A=F

		A	B	C	D	(A+D)mod2
1	15	1	1	1	1	0
2	14	0	1	1	1	1
3	13	1	0	1	1	0
4	10	0	1	0	1	1
5	5	1	0	1	0	1
6	11	1	1	0	1	0
7	6	0	1	1	0	0
8	12	0	0	1	1	1
9	9	1	0	0	1	0
10	2	0	1	0	0	0
11	4	0	0	1	0	0
12	8	0	0	0	1	1
13	1	1	0	0	0	1
14	3	1	1	0	0	1
15	7	1	1	1	0	1

Генерация псевдослучайных чисел

ABCD

F=(A+D)mod2

D=C

C=B

B=A

A=F

		A	B	C	D	(A+D)mod2
1	15	1	1	1	1	0
2	14	0	1	1	1	1
3	13	1	0	1	1	0
4	10	0	1	0	1	1
5	5	1	0	1	0	1
6	11	1	1	0	1	0
7	6	0	1	1	0	0
8	12	0	0	1	1	1
9	9	1	0	0	1	0
10	2	0	1	0	0	0
11	4	0	0	1	0	0
12	8	0	0	0	1	1
13	1	1	0	0	0	1
14	3	1	1	0	0	1
15	7	1	1	1	0	1

$$x^0 \bmod (x^4 + x^3 + 1) \bmod x = 1$$
$$x^1 \bmod (x^4 + x^3 + 1) \bmod x = 0$$
$$x^2 \bmod (x^4 + x^3 + 1) \bmod x = 0$$
$$x^3 \bmod (x^4 + x^3 + 1) \bmod x = 0$$
$$x^4 \bmod (x^4 + x^3 + 1) \bmod x = 1$$
$$x^5 \bmod (x^4 + x^3 + 1) \bmod x = 1$$
$$x^6 \bmod (x^4 + x^3 + 1) \bmod x = 1$$
$$x^7 \bmod (x^4 + x^3 + 1) \bmod x = 1$$
$$x^8 \bmod (x^4 + x^3 + 1) \bmod x = 0$$
$$x^9 \bmod (x^4 + x^3 + 1) \bmod x = 1$$
$$x^{10} \bmod (x^4 + x^3 + 1) \bmod x = 0$$
$$x^{11} \bmod (x^4 + x^3 + 1) \bmod x = 1$$
$$x^{12} \bmod (x^4 + x^3 + 1) \bmod x = 1$$
$$x^{13} \bmod (x^4 + x^3 + 1) \bmod x = 0$$
$$x^{14} \bmod (x^4 + x^3 + 1) \bmod x = 0$$

$x^0 \bmod (x^4 + x^2 + 1) = 1$

$x^1 \bmod (x^4 + x^2 + 1) = x$

$x^2 \bmod (x^4 + x^2 + 1) = x^2$

$x^3 \bmod (x^4 + x^2 + 1) = x^3$

$x^4 \bmod (x^4 + x^2 + 1) = x^4 + \quad x^4 + x^2 + 1 = x^2 + 1$

$x^5 = (x^2 + 1)x = x^3 + x$

$x^6 = x^4 + x^2 + \quad x^4 + x^2 + 1 = 1$

$x^7 = x$

$x^8 = x^2$

$x^9 = x^3$

$x^{10} = x^3 + x$

$x^{11} = 1$

$x^{12} = x$

$x^{13} = x^2$

$x^{14} = x^3$

$x^{15} = x^3 + x$

$x^{16} = 1$

$$x^{2^r} = x \bmod G(x)$$

$$x^{\frac{(2^r - 1)}{h_i}} \neq 1 \bmod G(x)$$

h_i – простые делители

$$2^r - 1 = \prod_i h_i$$

Вычислить *x*^*n* за *O*(log*n*) операций перемножения полиномов

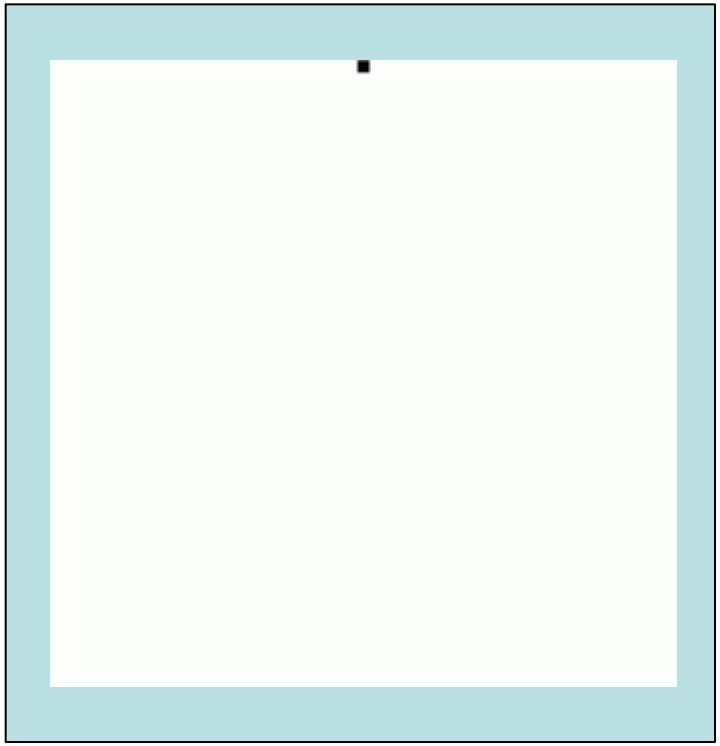
*2**log(*n*) операций

$$x^{153} \bmod \left(x^4 + x^3 + 1\right) = x\left(\left(\left[x\left(xx^8\right)^2\right]^2\right)^2\right)^2 \bmod \left(x^4 + x^3 + 1\right)$$

$$x^8 \bmod \left(x^4 + x^3 + 1\right) = x^3 + x^2 + x$$

$$x^{153} \bmod \left(x^4 + x^3 + 1\right) = x^3$$

$$f_k = x^k \bmod x^{19} + x^{15} + x^7 + x + 1$$



512 десятиразрядных двоичных чисел

$$x^k = x^{k-1}x \bmod G \qquad f_k = x^k = \prod_{i=0}^{r-1}\left(x^{2^i}\right)^{\alpha_i} \bmod G, \quad k = \sum_{j=0}^{r-1}\alpha_j 2^j, \quad \alpha_j \in \{0,1\}$$

i	$x^{2^i} \bmod\left(x^{31}+x^3+1\right)$	$x^{2^i} \bmod\left(x^{31}+x^{28}+1\right)$
0	x	x
1	x^2	x^2
2	x^4	x^4
3	x^8	x^8
4	x^16	x^16
5	x^4+x	x^29+x
6	x^8+x^2	x^28+x^27+x^24+x^21+x^18+x^15+x^12+x^9+x^6+x^3+x^2+1
7	x^16+x^4	x^30+x^29+x^25+x^24+x^23+x^22+x^20+x^19+x^18+x^16+x^13+x^12x^11+x^10+x^8+x^7+x^6+x+1
8	x^8+x^4+x	x^30+x^29+x^28+x^27+x^23+x^22+x^21+x^19+x^18+x^14+x^12+x^9+x^7+x^6+x^5+x^4+x^3
9	x^16+x^8+x^2	x^28+x^27+x^26+x^25+x^22+x^21+x^19+x^16+x^14+x^12+x^11+x^10+x^7+x^6+x^4+x
10	x^16+x	x^29+x^25+x^24+x^23+x^21+x^18+x^17+x^15+x^13+x^10+x^9+x^8+x^6+x^3+x^2+x+1
11	x^4+x^2+x	x^29+x^28+x^27+x^26+x^24+x^21+x^20+x^19+x^17+x^14+x^13+x^12+x^10+x^7+x^6+x^5+x^3+x
12	x^8+x^4+x^2	x^30+x^28+x^27+x^26+x^25+x^23+x^22+x^19+x^16+x^14+x^13+x^12+x^11+x^9+x^8+x^5
13	x^16+x^8+x^4	x^28+x^25+x^24+x^21+x^16+x^13+x
14	x^16+x^8+x^4+x	x^29+x^26+x^25+x^22+x^17+x^14+x^2+x
15	x^16+x^8+x^4+x^2+x	x^27+x^24+x^19+x^16+x^4+x^3+x^2+1
16	x^16+x^8+x^2+x	x^23+x^20+x^8+x^7+x^6+1
17	x^16+x^2+x	x^16+x^15+x^14+1
18	x^2+x	x^30+x^29+x^28+x+1
19	x^4+x^2	x^30+x^28+x^27+x^26+x^25+x^24+x^23+x^22+x^21+x^20+x^19+x^18+x^17+x^16+x^15+ x^14+x^13+x^12+x^11+x^10+x^9+x^8+x^7+x^6+x^5+x^4+x^3+x
20	x^8+x^4	x^28+x^25+x^24+x^21+x^20+x^17+x^16+x^13+x^12+x^9+x^8+x^5+x
21	x^16+x^8	x^29+x^26+x^25+x^24+x^22+x^18+x^17+x^16+x^14+x^10+x^9+x^6+x^2+x
22	x^16+x^4+x	x^29+x^27+x^24+x^20+x^19+x^18+x^17+x^16+x^14+x^12+x^11+x^8+x^4+x^3+x^2+x+1
23	x^8+x^4+x^2+x	x^30+x^27+x^23+x^22+x^21+x^20+x^18+x^16+x^15+x^12+x^8+x^7+x^6+x^5+x^3
24	x^16+x^8+x^4+x^2	x^30+x^29+x^26+x^24+x^16+x^15+x^14+x^13+x^11+x^8+x^7+x^6+x^4
25	x^16+x^8+x	x^30+x^28+x^27+x^24+x^23+x^22+x^20+x^16+x^14+x^12+x^8+x
26	x^16+x^4+x^2+x	x^30+x^28+x^26+x^25+x^24+x^22+x^19+x^17+x^15+x^14+x^12+x^11+x^8+x^5+x
27	x^8+x^2+x	x^30+x^29+x^28+x^26+x^25+x^24+x^23+x^21+x^20+x^18+x^16+x^15+x^13+x^12+x^9+x^6+x^2
28	x^16+x^4+x^2	x^30+x^27+x^25+x^23+x^22+x^20+x^18+x^15+x^11+x^8+x^4+x
29	x^8+x	x^29+x^26+x^22+x^19+x^15+x^12+x^8+x^5
30	x^16+x^2	x^30+x^27+x^16+x^13
31	x	x

$$G(x) = \sum_{i=0}^{r-1}\beta_i x^{2^i-1}, \ \beta_j \in \{0,1\}$$

$x^{2^i} \bmod G(x)$ - разреженные полиномы

- x^31+x^3+1
- x^31+x^7+1

- x^31+x^7+x^3+x+1
- x^31+x^15+x^3+x+1

- x^127+x^1+1
- x^127+x^63+1

- x^127+x^7+x^3+x+1
- x^127+x^63+x^15+x+1

- x^255+x^15+x^7+x^3+1

- x^255+x^31+x^7+x+1
- x^255+x^31+x^7+x^3+1

- x^255+x^63+x^7+x^3+1
- x^255+x^63+x^31+x^15+1

- x^255+x^127+x^7+x^3+1
- x^255+x^127+x^3+x+1
- x^255+x^127+x^31+x^7+1

$$G(x) = x^{511} + x^{15} + 1 \qquad G(x) = x^{1023} + x^7 + 1$$

$$2^{255} - 1 = 7 \cdot 31 \cdot 103 \cdot 151 \cdot 2143 \cdot 11119 \cdot 106591 \cdot 131071 \cdot 949111 \cdot$$
$$95209728063337584 31 \cdot 57024515776397755458386431 51$$

$$2^{511} - 1 = 127 \cdot 439 \cdot 2298041 \cdot 9361973132609 \cdot 15212471 \cdot$$
$$144780974187086260903935034761413745643657829092415 0417 \cdot$$
$$2537599745025519134156761164267591913521835535529224725592538658153$$

Проверка примитивности полинома

$$x^{2^r} = x \bmod G(x)$$

$$x^{\frac{(2^r-1)}{h_i}} \neq 1 \bmod G(x)$$

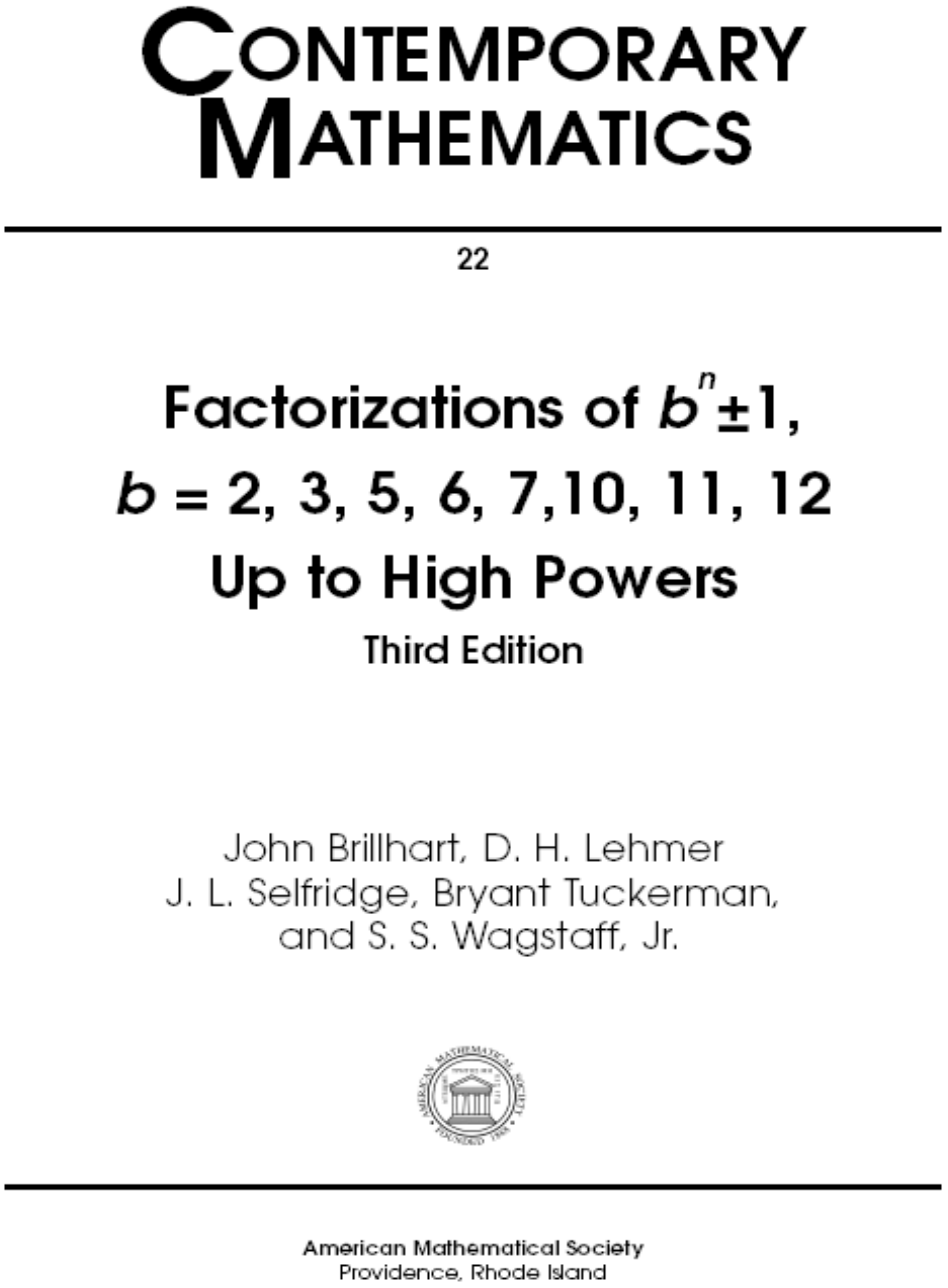
h_i – простые делители

$$2^r - 1 = \prod_i h_i$$

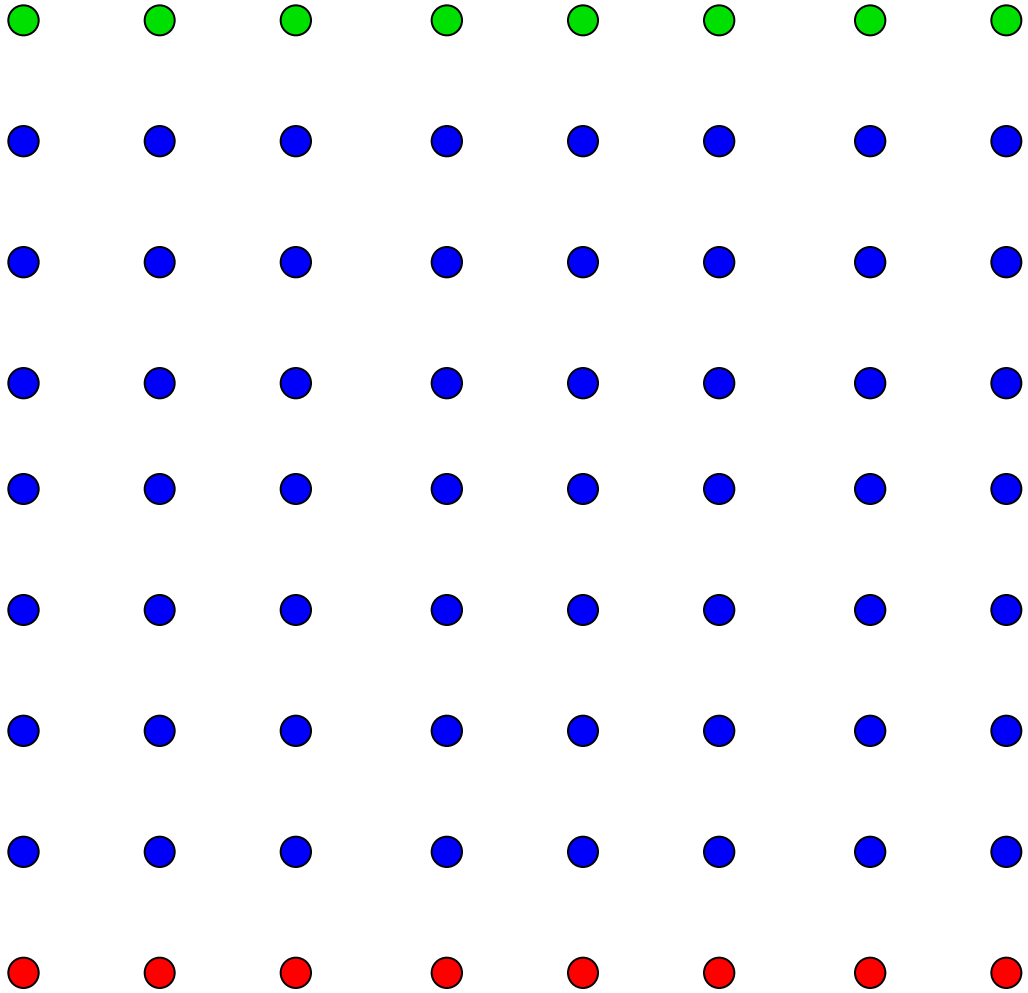
Определение. Полином $P(x)$ степени $r > 1$ называется примитивным, если $P(x)$ неприводим и $x^j \not\equiv 1 (\bmod P(x))\ \forall j \in \{1,2,\ldots,2^r - 2\}$.

Publication Date: 2002
Number of Pages: 236pp.
Publisher: AMS

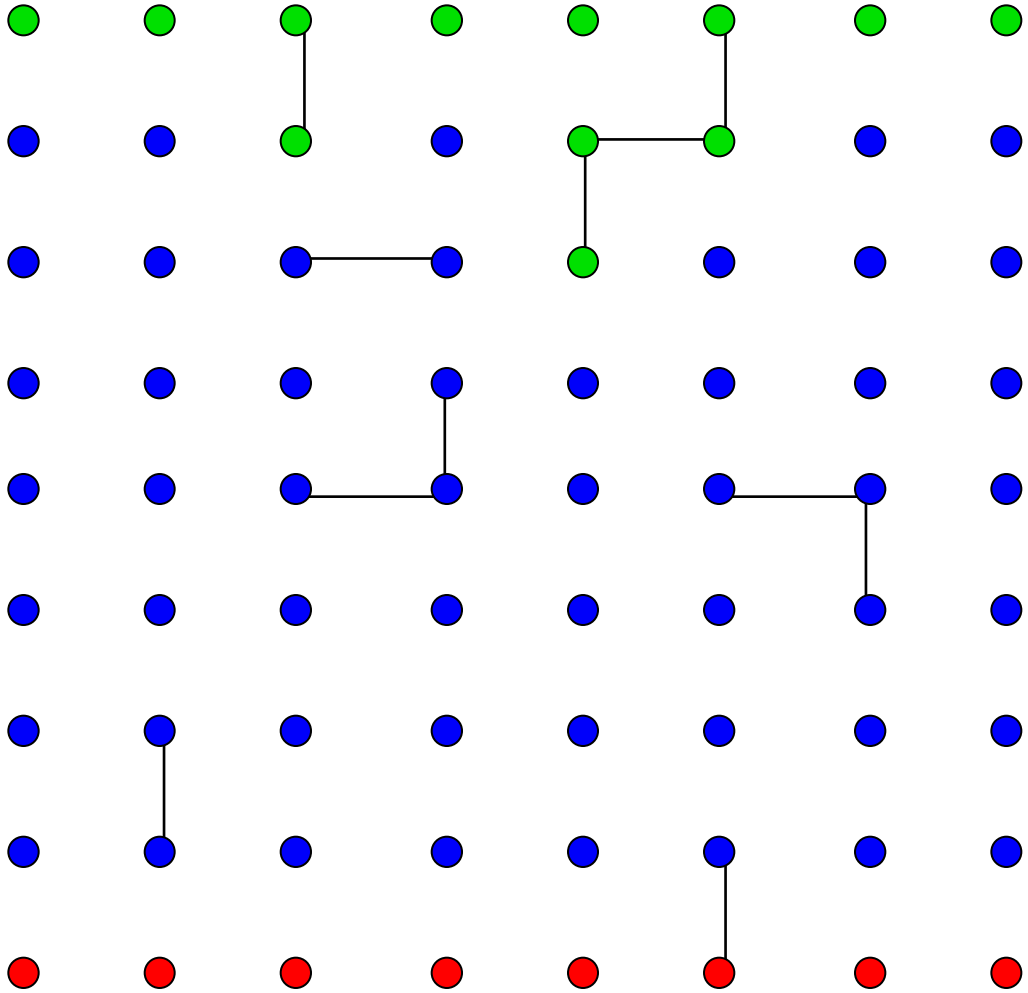
http://www.mersenneforum.org/attachment.php?attachmentid=7727&d=1330555980



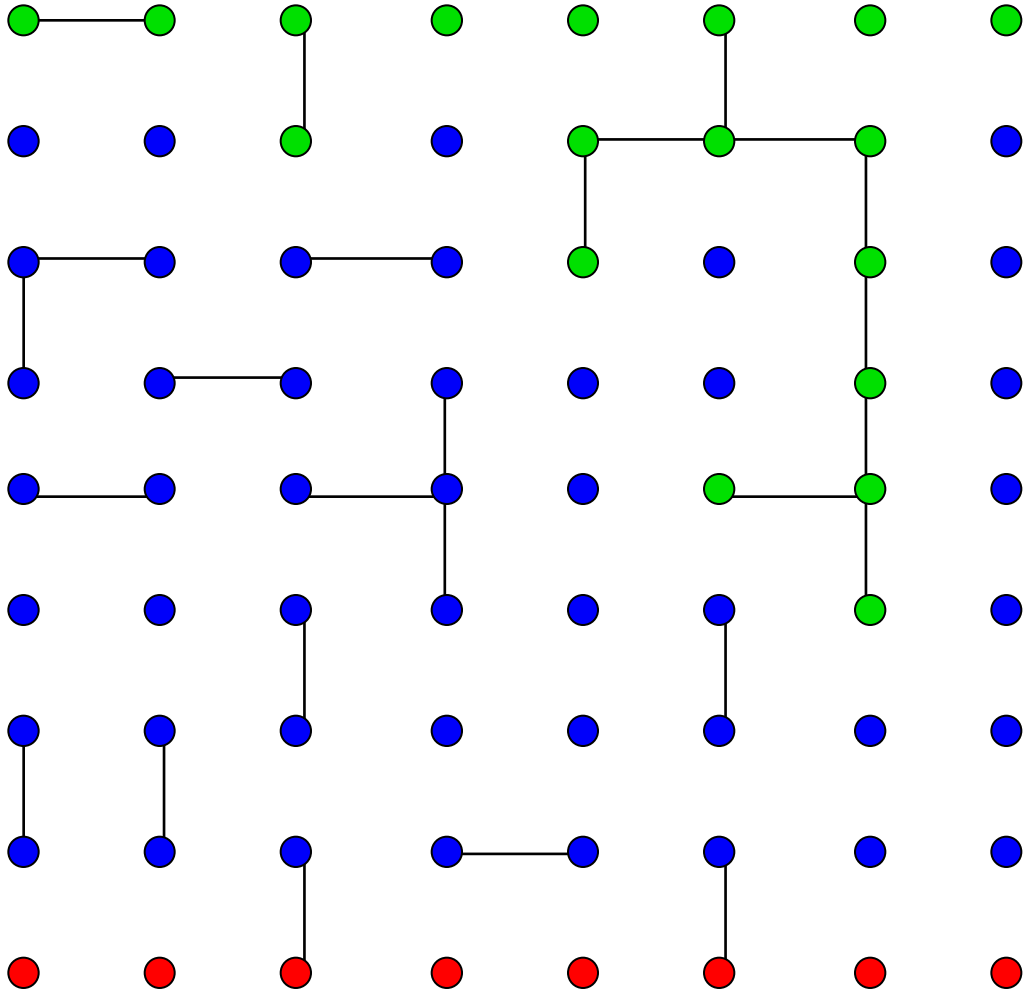
Перколяционный кластер



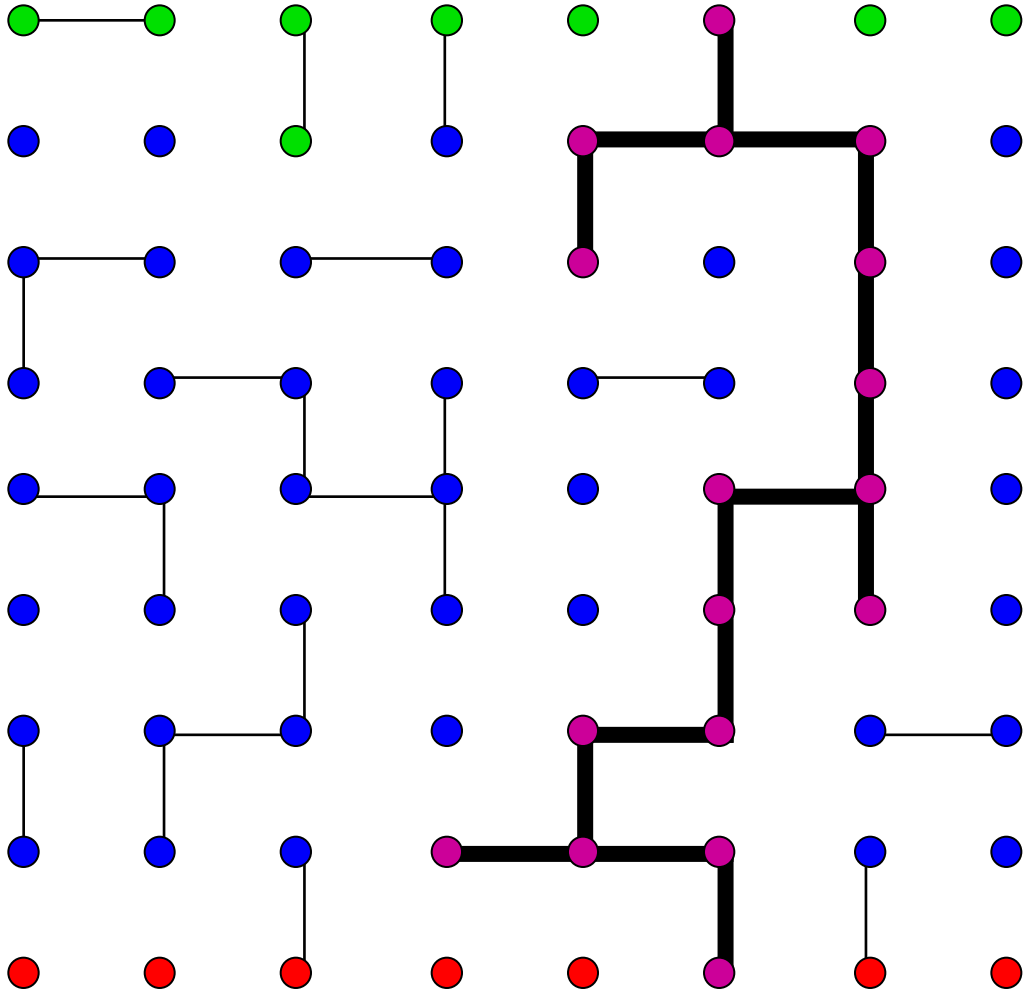
Перколяционный кластер



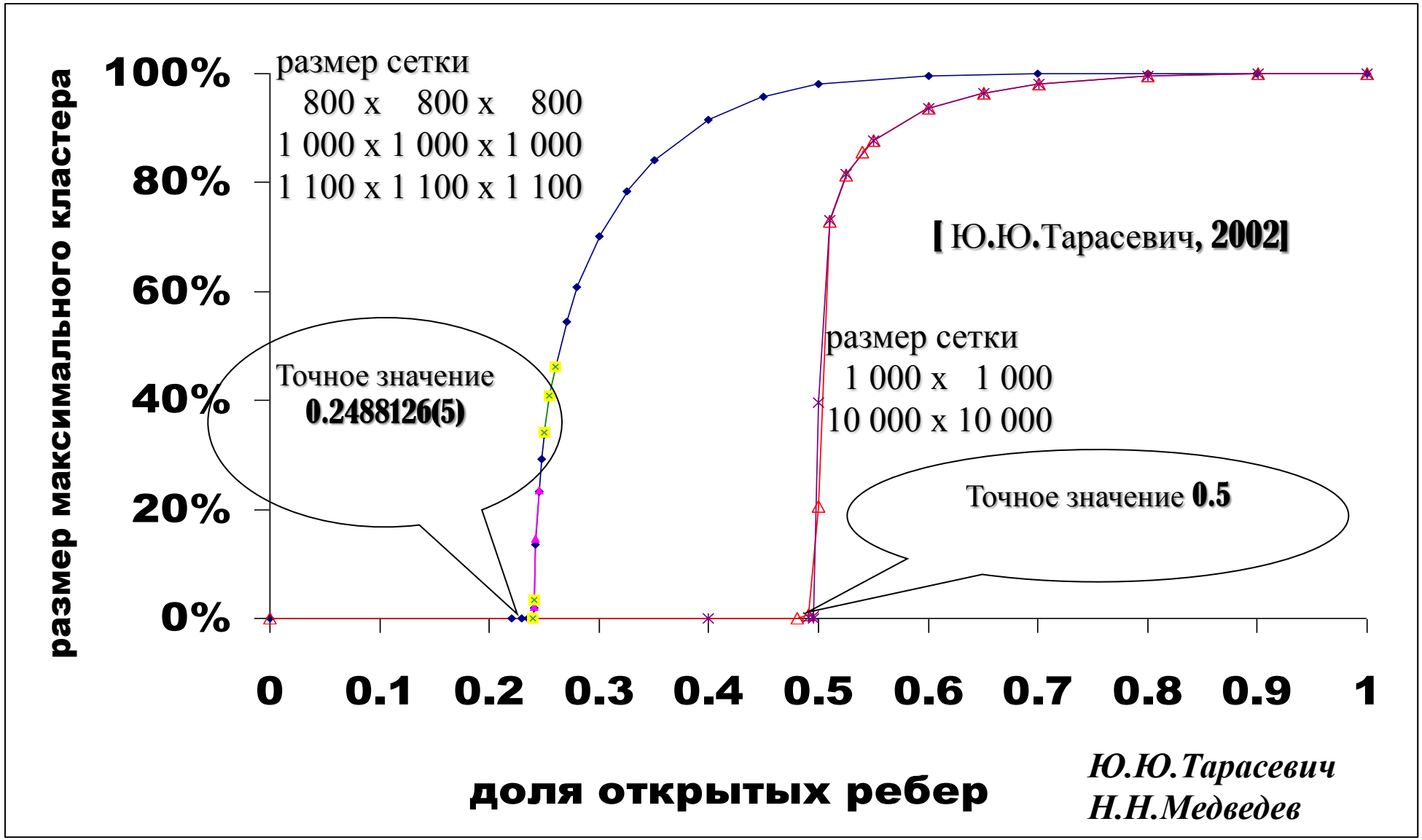
Перколяционный кластер



Перколяционный кластер



Порог перколяции

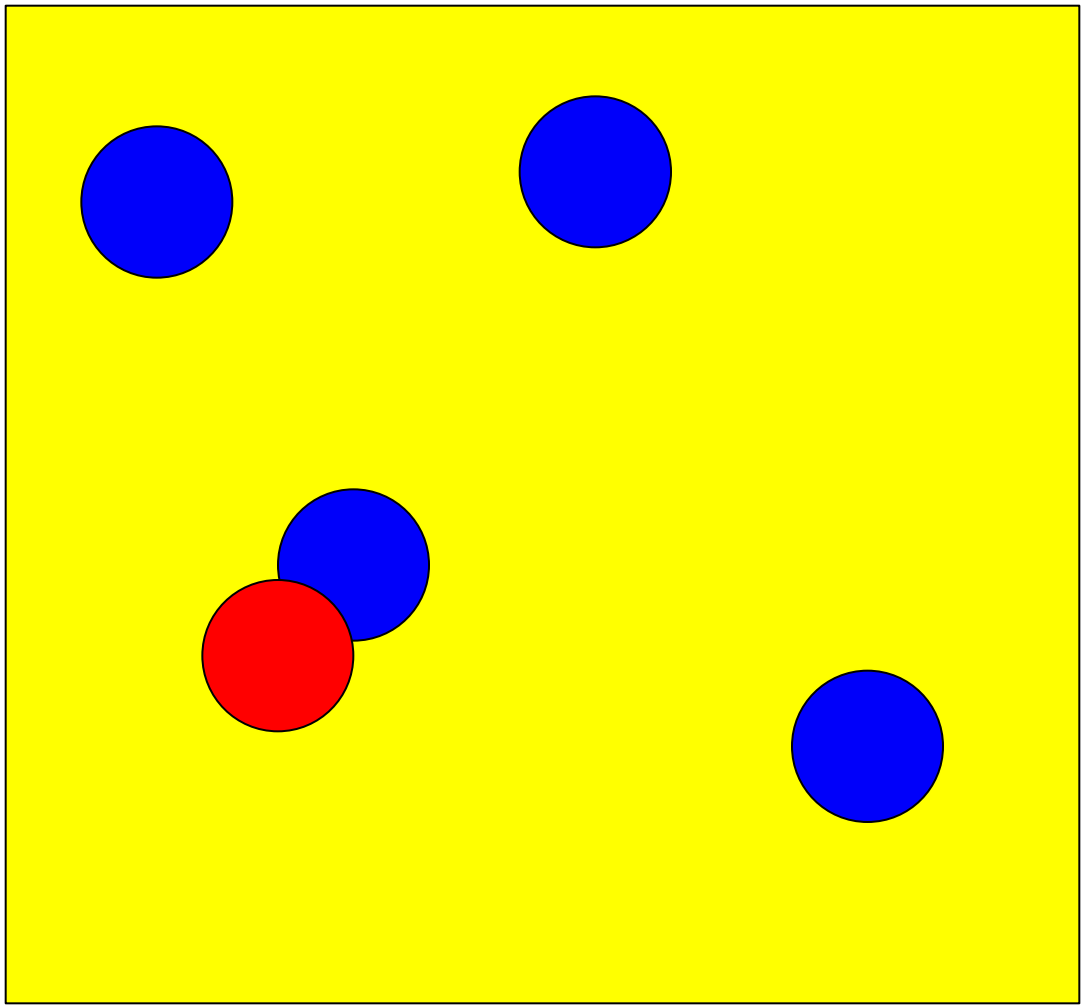


Батарея тестов Diehard

$$G(x) = x^{255} + x^{31} + x^7 + x^3 + 1$$

	P=0	P < 0.00001	P < 0.001	P < 0.01	0.01 ≤ P ≤ 0.99	P > 0.99	P > 0.999	P > 0.99999	P=1
	a	b	c	d		D	C	B	A
LRND32 0	0	0	1	3	309	5	1	0	0
123456	0	0	1	4	312	2	0	0	0
1234567	0	0	0	6	309	4	0	0	0
12345678	0	0	1	5	312	1	0	0	0
123456789	0	0	0	2	311	6	0	0	0
SWBMWC	0	0	0	4	312	3	0	0	0
MWC	0	1	0	5	307	6	0	0	0
MIXRNDX	12	8	8	5	263	3	9	11	0
MIXRNDXY	12	10	5	5	262	4	7	14	0
BRND	74	5	2	13	187	2	11	18	7
RAND	146	117	0	0	32	2	2	2	18

Парковочный тест



Тестируемые последовательности

- BRND $x_{n+1} = 3141592653 x_n + 2718281829 \bmod 2^{35}, \; x_0 = 0$
- MIXRND рандомизация перемешиванием
- MWC генератор на основе метода умножения с переносом MWC, период 4*10^18
- SWBMWC комбинированный генератор на основе методов умножения с переносом MWC и Фибоначчи с запаздыванием SWBG, период 4*10^364

Батарея тестов Diehard

$$G(x) = x^{255} + x^{31} + x^7 + x^3 + 1$$

	P=0	P < 0.00001	P < 0.001	P < 0.01	0.01 ≤ P ≤ 0.99	P > 0.99	P > 0.999	P > 0.99999	P=1
	a	b	c	d		D	C	B	A
LRND32 0	0	0	1	3	309	5	1	0	0
123456	0	0	1	4	312	2	0	0	0
1234567	0	0	0	6	309	4	0	0	0
12345678	0	0	1	5	312	1	0	0	0
123456789	0	0	0	2	311	6	0	0	0
SWBMWC	0	0	0	4	312	3	0	0	0
MWC	0	1	0	5	307	6	0	0	0
MIXRNDX	12	8	8	5	263	3	9	11	0
MIXRNDXY	12	10	5	5	262	4	7	14	0
BRND	74	5	2	13	187	2	11	18	7
RAND	146	117	0	0	32	2	2	2	18

Резюме

$$G(x) = x^{255} + x^{31} + x^7 + x^3 + 1$$

- Есть возможность вычисления за время O(log(*k*)) числа с произвольным номером *k* с помощью бинарного возведения в степень

$$f_k = x^k \bmod G$$

- При наличии числа с номером *k* есть возможность быстрого вычисления числа с номером *k*+1 с помощью

$$f_{k+1} = x f_k \bmod G$$

Сравнение различных библиотек генерации ПСЧ

Библио-тека/ Генератор	Тип	Пери-од	Возм.пе-рехода(skip-ahead)	V, 10^6 ПСЧ/с	V пере-хода, 10^3 шт/с
PRAND					
G(x) r 255	М-посл-ть	2^{255}-1	+	20,4	38,5
G(x) r 1023	М-посл-ть	2^{1023}-1	+	18,5	12,3
ANSI					
rand	ЛКГ m=31	2^{31}-1	–	204,1	--
Intel MKL					
MCG31m1	ЛКГ m=31	2^{31}- 1	+		
R250	М-посл-ть	2^{250}	–		
MRG32k3a	2 ген-ра Фибоначчи	2^{191}	+	105,3	21,3
MCG59	ЛКГ m=59	2^{57}	+		
WH	273 ЛКГ	2^{80}	+		
MT19937	Mersenne-Twister (MT)	2^{19937}-1	–		
MT2203	1024 MT	2^{2203}-1	–		

Доступные реализации генераторов ПСЧ для GPU

- CURAND (Nvidia)
- Библиотека для генерации псевдослучайных и квазислучайных чисел на GPU / CPU
- Генераторы случайных чисел (СЧ)
  - XORWOW
  - MRG32k3a
  - MTGP32 (Mersenne Twister)
  - Генераторы квазислучайных чисел Соболя (Sobol’)
- Распределения:

  равномерное, нормальное, логнормальное, Пуассона

Библиотека LRND32-GPU

Генератор

$$\varphi_{j+1023} = \varphi_{j+511} + \varphi_{j+127} + \varphi_{j+7} + \varphi_j$$

То же для 32-битных слов

$$w_{j+8} = (w_j << 1) \oplus (w_{j+1} >> 31) \oplus (w_j << 8) \oplus (w_{j+1} >> 24) \oplus w_{j+4} \oplus w_{j+16}$$

Период: $2^{1023}-1$

Скорость: $2{,}6 \cdot 10^7$ ПСЧ/с на NVidia Tesla C2050

Исходные коды библиотеки LRND32-GPU:
http://apos.imamod.ru/Programms/GK_07_514_11_4002_rng.tar.gz

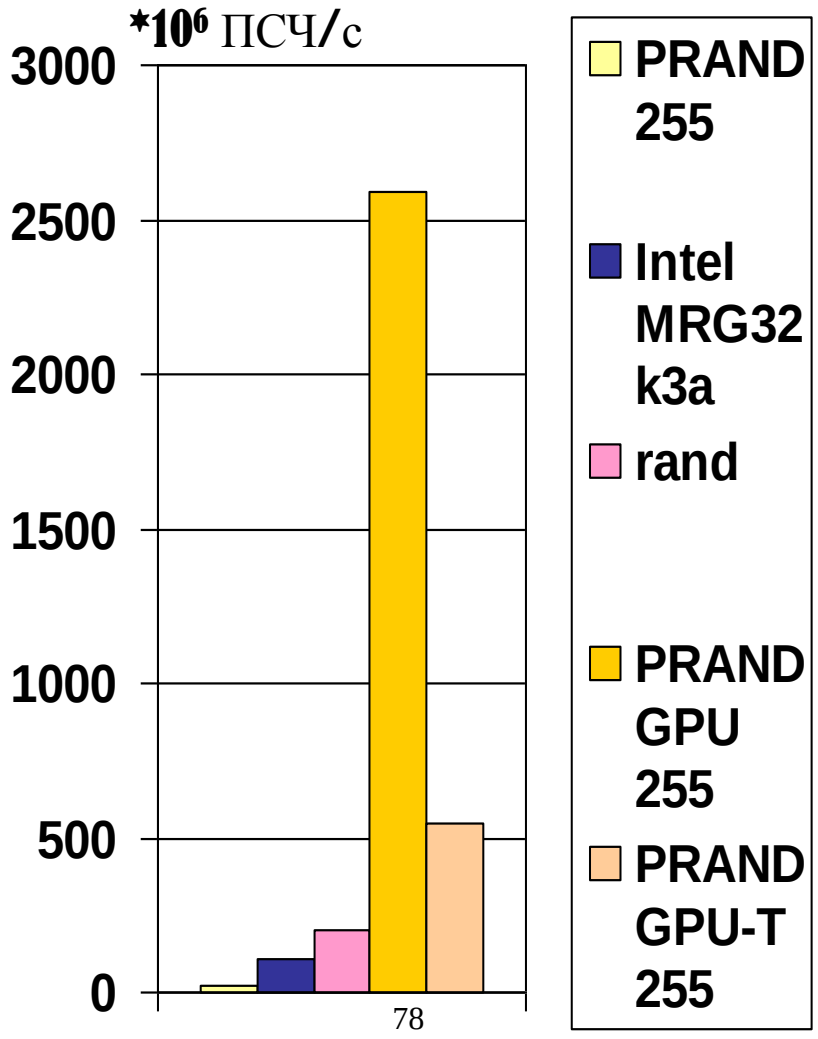
М.Н. Воронюк, М.В. Якобовский. 2012

Сравнение LRND32-GPU и CURAND (NVidia)

Библио-тека/ Генератор	**Тип**	**Пери-од**	**Возм.пе-рехода (skip-ahead)**	**ϑ пере-хода, 10^3 шт/с**
PRAND				
G(x) r 255	М-посл-ть	2^{255}-1	+	149,5
G(x) r 1023	М-посл-ть	2^{1023}-1	+	42,1
Nvidia CUDAND				
XORWOW	xor-shift	2^{31}- 1	+	19,1
MRG32k3a	2 рекуррентных ген-ра	2^{191}	+	38,2
MTGP32	Mersenne-Twister (MT)	2^{11213}-1	–	

Результат работы алгоритма для GPU

Библио-тека/ Генератор	V, 10^6 ПСЧ/с	Уск. к PRAND	Уск. к ANSI rand
PRAND GPU-T			
G(x) r 255	549,2	26,9	2,7
G(x) r 1023	539,3	29,2	2,6
PRAND GPU			
G(x) r 255	2 591,0	127,0	12,7
G(x) r 1023	2 382,0	128,8	11,7
PRAND			
G(x) r 255	20,4	1	0,1
G(x) r 1023	18,5	1	0,1
ANSI			
rand	204,1	--	1
Intel MKL			
MRG32k3a	105,3	--	0,5



Отличия генерации ПСЧ на GPU от генерации на CPU

- Генерация ПСЧ возможна только порциями.
  При blockDim=128 и r=255 порция составляет 512 ПСЧ.
  - На практике для полноценной загрузки GPU требуется выбирать размер порции гораздо больше, например 10^6 ПСЧ.
- Время на генерацию ПСЧ в ~3-4 раза меньше времени передачи их с графической карты в оперативную память при использовании page-locked-выделения памяти, и в ~8-9 раз меньше без использования.
  - Использовать ПСЧ на GPU без передачи
  - Латентность передачи можно частично покрыть, если совмещать передачу с генерацией следующей порции
- Скорость генерации сильнее зависит от шаблона доступа к глобальной памяти, чем от вычислительной сложности алгоритма (возрастающей к ростом r)

Заключение

- Сформулированы требования к генераторам псевдослучайных чисел для многопроцессорных систем
- Рассмотрены параллельные алгоритмы генерации псевдослучайных чисел обеспечивающие возможность использования произвольного числа процессоров

Литература

- Якобовский М.В. Введение в параллельные методы решения задач: Учебное пособие / Предисл.: В. А. Садовничий. – М.: Издательство Московского университета, 2013. – 328 с., илл. – (Серия «Суперкомпьютерное образование») ISBN 978-5-211-06382-2
- *И.М.Соболь.* Численные методы Монте-Карло. – М.: Наука, 1973.
- *Richard P. Brent*, Uniform Random Number Generators for Supercomputers, Computer Sciences Laboratory; Australian National University Appeared in Proceedings Fifth Australian Supercomputer Conference (Melbourne, December 1992), 95-104. c 1992, 5ASC Organising Committee.
- *Кнут Дональд Эрвин*, искусство программирования, том.2. Получисленные алгоритмы, 3-е издание.: Пер с англ., : Уч пос - М.: Издательский дом <Вильямс>, 2001. - 832 с., ил.
- *G. Marsaglia*, "Random numbers fall mainly on the planes", Proc. Nat. Acad. Sci. USA 61, 1 (1968), 25-28.
- *П.Хоровиц, У.Хилл.* Искусство схемотехники: В 2-х томах. Пер. с англ. – М.: Мир, 1983. - Т.2 590с.
- *Тарасевич Ю.Ю.* Перколяция: теория, приложения, алгоритмы. 2002. 112 с.
- *Л.Ю. Бараш*. Алгоритм AKS проверки чисел на простоту и поиск констант генераторов псевдослучайных чисел, Безопасность информационных технологий, 2 (2005) 27-38.
- *В.Жельников.* Криптография от папируса до компьютера – М., ABF, 1996, ил., 336 с.
- *Якобовский М.В.* Библиотека генерации псевдослучайных чисел lrnd32. Дистрибутив. 2007, http://www.imamod.ru/projects/FondProgramm/RndLib/lrnd32_v02

Контакты

Якобовский М.В.

проф., д.ф.-м.н.,

зав. сектором

«Программного обеспечения многопроцессорных систем и вычислительных сетей»

Института прикладной математики им. М.В.Келдыша Российской академии наук

mail: lira@imamod.ru

web: http://lira.imamod.ru