Несколько задач, связанных с генерацией псевдослучайных чисел

Суровикина Тамара Олеговна, гр. 422

Санкт-Петербургский государственный университет
Математико-механический факультет
Кафедра статистического моделирования

Научный руководитель: к.ф.-м.н., доцент Некруткин В.В.
Рецензент: к.ф.-м.н., доцент Коробейников А.И.

Санкт-Петербург
2017 г.

Решетка чисел с плавающей точкой: множество $X_{L,S}$

Результат работы генератора: $u_1, \ldots, u_n \in [0, 1]$.

u_i в памяти компьютера — числа с плавающей точкой.
IEEE 754-2008:

$$X_{L,S} = \{x_{jk} = 2^{-j}(1 + k2^{-S})\} \cup \{0, 1\} \subset [0, 1], \text{ где}$$

- S отвечает за мантиссу: $k \in \{0, \ldots, 2^S - 1\}$;
- L — максимальный порядок: $1 \leq j \leq L = 2^{2^{B-1}-1}$.

Для double: $B = 11, S = 52$.

Обозначение: $X_S = X_{L,S}$ при $L = \infty$.

Моделирование на решётке IEEE 754-2008

Как можно получать псевдослучайные числа, согласованные с double?

Способы получения чисел с двойной точностью:

- Деление целых чисел, нормировка происходит автоматически (LCG, Mersenne Twister, SFMT, etc).
- Непосредственное получение чисел из $X_{L,52}$.
  Алгоритмы: Agner Fog (1997), Morgenstern (2007), Saito и Matsumoto (2009).
- Другие (например, Wichmann и Hill (1982) — осреднение 3-х вещественных чисел).

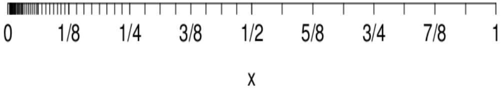
Распределение $\mathrm{U}(S)$ (V. Nekrutkin, 2016).

$$\mathrm{U}(S): \begin{pmatrix} x_{jk} \\ p_{jk} \end{pmatrix}, \text{ где}$$

- $j \geq 1, 1 \leq k < 2^S$;
- $x_{jk} = 2^{-j}\left(1 + k2^{-S}\right)$;
- $p_{jk} = 2^{-S-j}$.

$\mathrm{U}(S)$ соответствует максимальному порядку $L = \infty$.

Решётка значений $\mathrm{U}(S)$, $S = 3$.



Вероятности 2^{-j-S} в точках, принадлежащих $[2^{-j}, 2^{-j+1})$.

Постановка задачи

Задачи

- Изучить распределение $\mathrm{U}(S)$ и его варианты, а именно:
    - распределения мантисс и порядков,
    - распределения двоичных бит,
    - их зависимость/независимость.
- Рассмотреть модель метода нормировки.
- Сравнить модель $\mathrm{U}(S)$ с реальными генераторами.
- Изучить образ распределения $\mathrm{U}(S)$ при отображении $x \mapsto 1 - x$. Особенность: согласование с решёткой X_S.

Распределение $\mathrm{U}(S)$ как результат проектирования

В (V. Nekrutkin, 2016): вид $\mathrm{U}(S)$ постулировался.

На самом деле (результат):

Предложение

Пусть $\alpha \in \mathrm{U}(0,1)$, $\lfloor \alpha_S \rfloor$ — проекция α на решётку X_S (при округлении «вниз»). Тогда $\mathcal{L}(\lfloor \alpha_S \rfloor) = \mathrm{U}(S)$.

Проекция x на решетку X_S:

- $\lfloor x_S \rfloor$ — при округлении x «вниз»;
- $\lceil x_S \rceil$ — при округлении «вверх»;
- $\lfloor x_S \rceil$ — при округлении до ближайшей точки из X_S.

А что происходит при других вариантах округления?

Варианты округления $\alpha \in \mathrm{U}(0,1)$

Пусть $\alpha \in \mathrm{U}(0,1)$ и $x_{jk} = 2^{-j}\left(1 + k2^{-S}\right)$. Тогда

Предложение

1. $\mathrm{P}(\lceil \alpha_S \rceil = x_{jk}) = 2^{-S-j}$ *при* $j \geq 1, k \in \{1, \ldots, 2^S\}$.
2. $\mathrm{P}(\lfloor \alpha_S \rceil = x_{jk}) = q_{jk}$ *при* $j \geq 1, k \in \{0, \ldots, 2^S - 1\}$, *где*

$$q_{jk} = \begin{cases} 2^{-S-j} & \text{при } j \geq 1 \text{ и } k \neq 0, \\ 3 \cdot 2^{-S-j-2} & \text{иначе.} \end{cases}$$

Кроме того, $\mathrm{P}(\lfloor \alpha_S \rceil = 1) = 2^{-S-2}$ *и* $\mathrm{P}(\lceil \alpha_S \rceil = 1) = 2^{-S-1}$.

Порядок γ и мантисса η результатов всех видов проектирования независимы, причем $\gamma \in \mathrm{Geom}(1/2)$.

Модель метода нормировки. Постановка задачи

Дано: $Y_d = \{0, \dots, 2^d - 1\}$, $\Upsilon_d \in \mathrm{U}(Y_d)$.

Задача: найти распределение проекции $\Upsilon_d / 2^d$ на решетку X_S.

Возможные ситуации (на примере double):

- при $d = 32$ — все значения принадлежат X_{52};
- при $d = 64$ — происходит округление.

Результаты

- Получено, что округление значений $\Upsilon_d/2^d$ при $d \leq S+1$ не происходит.
- Выписан явный вид распределения $\mathcal{L}(\Upsilon_d/2^d)$ при $d \leq S+1$ и распределений $\mathcal{L}(\lfloor \Upsilon_d/2^d \rfloor)$, $\mathcal{L}(\lfloor \Upsilon_d/2^d \rceil)$ и $\mathcal{L}(\lceil \Upsilon_d/2^d \rceil)$ при $d > S+1$.
- Получены распределения мантисс и порядков.
- Мантисса и порядок для всех вариантов распределений $\Upsilon_d/2^d$ зависимы, причем порядки описываются урезанными геометрическими распределениями.

$$\mathrm{U}(S) \ni \xi_S = \sum_{i \geq 1} \beta_i 2^{-i}.$$

Результаты

- При $i < j$ случайные биты β_i и β_j оказываются независимыми тогда и только тогда, когда $i \leq S$ и $j \leq i + S$.
- Биты $\beta_1, \ldots, \beta_{S+1}$ независимы в совокупности и соответствуют симметричным испытаниям Бернулли.
- $P(\beta_j = 1) = 2^{-(j-S)}$ при $j > S + 1$.

Для остальных вариантов округления: все биты имеют несимметричные распределения Бернулли. Кроме того, они зависимы.

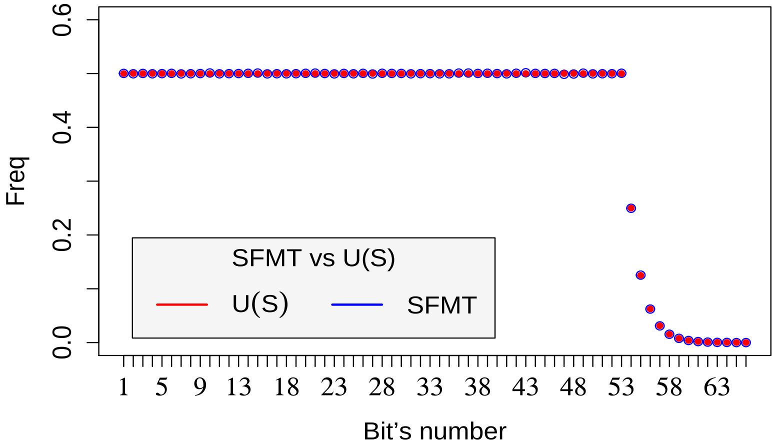
Вычислительный эксперимент: генераторы

- генератор SFMT (Matsumoto, Saito, 2008): нормировка на единицу целых чисел;
- генератор dSFMT (Saito, Matsumoto, 2009): равномерная решетка, согласованная с double;
- специальный генератор WH (Wichmann–Hill, 1982).

Побитовое сравнение методов с $\mathrm{U}(S)$.

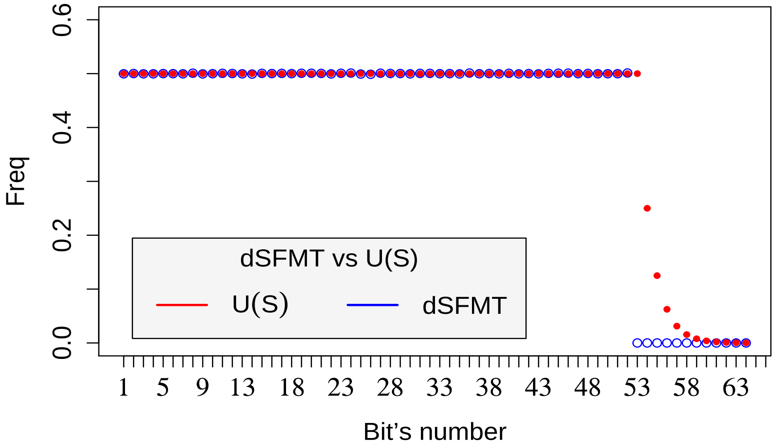
Моделирование:

$$\text{SFMT19937, seed} = 1,\ N = 10^6.$$



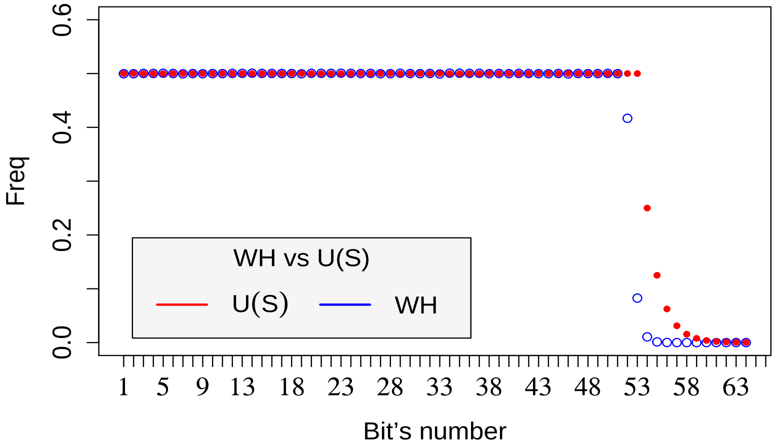
Моделирование:

$$\text{dSFMT19937, seed} = 1,\ N = 10^6.$$



Моделирование:

WH, seed1 $=$ 12345, seed2 $=$ 34567, seed3 $=$ 56789, $N = 10^6$.



Об особенностях $\mathrm{U}(S)$: вычитание из 1

Известно: $\alpha \in \mathrm{U}(0,1) \Rightarrow 1-\alpha \in \mathrm{U}(0,1)$.

Вопрос: а как для $\xi_S \in \mathrm{U}(S)$?

Проблема: $1-\xi_S$ не всегда попадает на решётку

$$x_{jk} = 2^{-j}(k2^{-S}+1), k \in \{0,\ldots,2^S-1\}, j = 1,2,\ldots.$$

Таким образом, снова возникает задача округления.

Вычитание из 1: округление «вверх»

Обозначим $\xi_S^{(1)} = 1 - \xi_S$, $\lceil \xi_S^{(1)} \rceil$ — при округлении «вверх».
Положим $q_{ik} = \mathrm{P}(\lceil \xi_S^{(1)} \rceil = x_{ik})$.

Предложение

Имеют место равенства:

- $q_{1k} = 2^{-S-1}$ *при* $k = 0, \dots, 2^S - 1$;
- *если* $x_{ik} = 1 - 2^{-1}(m2^{-S} + 1)$ *для некоторого* $m \in \{1, \dots, 2^S - 1\}$, *то* $q_{ik} = 2^{-S-1}$;
- *остальные* x_{ik} *реализуются с нулевой вероятностью;*
- *кроме того, значение 1 принимается с вероятностью* 2^{-S-1}.

Для других вариантов округления аналогично, но более громоздко.

Кроме того,

Результаты

- Исследована мера близости распределений $\mathcal{L}(\lfloor \xi_S^{(1)} \rceil)$, $\mathcal{L}(\lfloor \xi_S^{(1)} \rfloor)$ и $\mathcal{L}(\lceil \xi_S^{(1)} \rceil)$ в смысле расстояния по вариации. Оказалось, что это расстояние стремится к нулю при $S \to \infty$.
- В то же время расстояние по вариации между $\mathrm{U}(S)$ и вариантами распределений $\xi_S^{(1)}$ не обладает этим свойством.

Заключение

Основные результаты (кратко)

- Получена новая интерпретация распределения $\mathrm{U}(S)$. Рассмотрены близкие к нему распределения.
- Построена теоретическая модель метода нормировки.
- Исследованы битовые свойства $\mathrm{U}(S)$ и его вариантов.
- Проведено сравнение битовых структур $\mathrm{U}(S)$ и некоторых реальных генераторов.
- Рассмотрены варианты округления $1 - \xi_S$, где $\xi_S \in \mathrm{U}(S)$. Изучена мера близости между распределениями $\mathrm{U}(S)$, $\mathcal{L}(\lfloor \xi_S^{(1)} \rceil)$, $\mathcal{L}(\lfloor \xi_S^{(1)} \rfloor)$ и $\mathcal{L}(\lceil \xi_S^{(1)} \rceil)$.