Оценка погрешности ГПЧ при выборе НОД эскорта.

noise@sumus.team

22 июня 2019 г.

Аннотация

...

ГПЧ – генератор псевдослучайной (последовательности) чисел.

1 *черновик-1*

Дано подмножество натуральных чисел, взятых последовательно: $1, 2, \ldots, n$. Пусть x – случайная величина, принимающая значение этих чисел. Если x имеет равномерное распределение, то каждое её значение $x_i = i, i = 1, \ldots, n$, появляется с вероятностью (теоретической) $p_i = \frac{1}{n}$ в каждом опыте.

Если в эксперименте получено, что x_i появляется с частотой $\omega_i \neq \frac{1}{n}$, то имеется погрешность плотности равномерного распределения реального генератора псевдослучайных чисел, которую можно вычислить так:

$$\Delta = \sum_{i=1}^{n} |p_i - \omega_i| = \sum_{i=1}^{n} \left| \frac{1}{n} - \omega_i \right| \tag{1}$$

где ω_i равна отношению числа появлений значения $x_i = i$ в k опытах, $K \gg n$; $i = 1, \ldots, n$.

Формула (1) даёт абсолютную погрешность реального ГПЧ (невязку). Относительная погрешность может быть, вообще говоря, вычислена как отношение Δ к $\sum\limits_{i=1}^{n} \lim p_i$, но поскольку $\sum\limits_{i=1}^{n} \lim p_i = 1$, то формула (1) численно равна как абсолютной так и относительной погрешности.

2 *замечание-1*

Если вычислять погрешность, учитывая что $1 = \sum\limits_{i=1}^{n} \frac{1}{n}$, по принципу $\varepsilon = \frac{\left| \frac{1}{n} - \frac{1}{n} \sum\limits_{i=1}^{n} \omega_i \right|}{\frac{1}{n}}$, то получим

$$\varepsilon = \left| 1 - \sum_{i=1}^{n} \omega_i \right| = \left| \frac{1}{n} - \omega_1 + \frac{1}{n} - \omega_2 + \cdots + \frac{1}{n} - \omega_n \right| \neq \sum_{i=1}^{n} \left| \frac{1}{n} - \omega_i \right| \tag{2}$$

более того

$$\left| \sum_{i=1}^{n} \left(\frac{1}{n} - \omega_i \right) \right| \leq \sum_{i=1}^{n} \left| \frac{1}{n} - \omega_i \right| \tag{3}$$

То есть если $\frac{1}{n} - \omega_i$ имеет разные знаки для разных i, то формула (2) не даёт полной погрешности так как погрешности разных знаков в сумме уменьшают значение погрешности, что и видно из примера

$$\begin{aligned} \Delta = |0{,}25 - 0{,}23| + |0{,}25 - 0{,}26| + |0{,}25 - 0{,}24| + |0{,}25 - 0{,}21| \\ = 0{,}02 + 0{,}01 + 0{,}01 + 0{,}04 = 0{,}08 \end{aligned}$$

$$\langle \omega \rangle = \frac{1}{4} (0{,}23 + 0{,}26 + 0{,}24 + 0{,}21) = 0{,}235$$

$$\frac{1}{n} - \langle \omega \rangle = |0{,}25 - 0{,}235| = 0{,}015$$

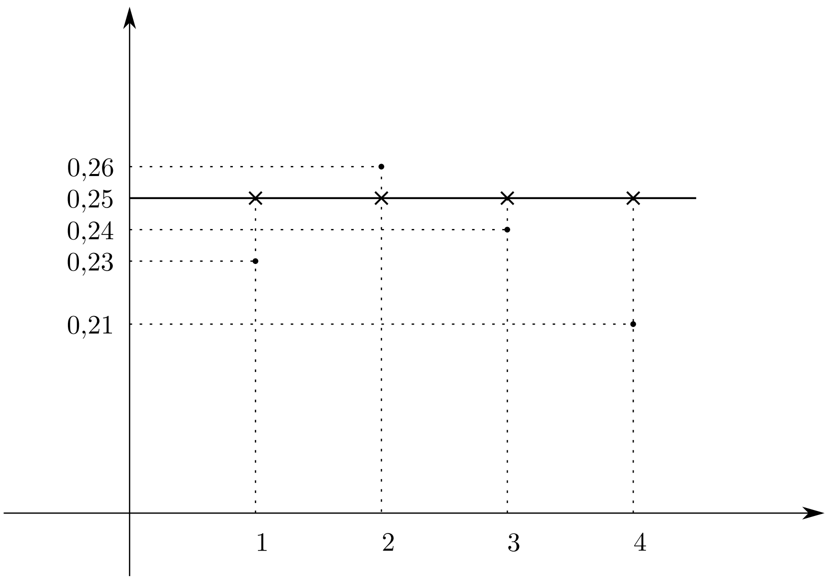

Рис. 1: *Пример-1.*

$$\frac{\frac{1}{n} - \langle\omega\rangle}{\frac{1}{n}} = \frac{0{,}15}{0{,}25} = 0{,}06\,;$$

показано, что неравенство (3) выполняется.

3 *черновик-2*

$B_{n'}$ – множество *нод*, участвующих в выработке консенсуса. Пусть из $B_n \supset B_{n'}$ $(n \gg n')$ уже выбран *мастер-узел*. Какова (теоретическая) вероятность того, что один из оставшихся $n-1$ узлов попадёт в $B_{n'}$ при $n'-1$ попытках? Распределение при выборе номера узла (номеров узлов) – равномерное. Вероятность того, что конкретный узел будет выбран в первом из $n'-1$ опытов равна $\frac{1}{n-1}$. Со второй попытки – $\frac{1}{n-2}$, ..., с m-той попытки – $\frac{1}{n-m-1}$, если $m = n'-1$, то $\frac{1}{n-1-(n'-1)} = \frac{1}{n-n'}$. Вероятность того, что конкретный узел с номером i будет выбран есть сумма этих вероятностей :

$$p_i = \sum_{k=1}^{n'} \frac{1}{n-k}\,;\;\; i = 1, \ldots, n-1 \qquad (4)$$

Пусть в результате M экспериментов по определению множества $B_{n'}$ узел с номером i попадал в эскорт M_i раз. Тогда $\omega_i = \frac{M_i}{M}$; $\omega_i \longrightarrow p_i$ при $M \longrightarrow +\infty$

Замечание $\sum\limits_{i=1}^{n} p_i \neq 1$, а значит p_i должны быть нормированы.

Абсолютная погрешность ГПЧ в данной задаче:

$$\Delta^* = \sum_{i=1}^{n-1} |p_i - \omega_i| = \sum_{i=1}^{n-1} \left| \sum_{k=1}^{n'} \frac{1}{n-k} - \omega_i \right| \qquad (5)$$

Поскольку все p_i одинаковы, то $\sum\limits_{i=1}^{n-1} p_i = (n-1)\sum\limits_{k=1}^{n'} \frac{1}{n-k}$ и тогда относительная погрешность ГПЧ в данной задаче

$$\varepsilon^* = \frac{\Delta^*}{\sum\limits_{i=1}^{n-1} p_i} = \frac{\sum\limits_{i=1}^{n-1} \left| \sum\limits_{k=1}^{n'} \frac{1}{n-k} - \omega_i \right|}{(n-1)\sum\limits_{k=1}^{n'} \frac{1}{n-k}} \tag{6}$$