СРАВНЕНИЕ СУММ ПО МОДУЛЮ 2^n И МОДУЛЮ 2

В.А. Галинский

Белгосуниверситет, НИИ прикладных проблем математики и информатики, Минск, Беларусь
GalinskijVA@bsu.by

Операции сложения по модулю 2^n и модулю 2 являются базовыми операциями криптографических алгоритмов. Поэтому исследование свойств указанных операций является актуальной задачей.

В докладе рассматривается задача сравнения результатов применения операций сложения по модулю 2^n и модулю 2 к малому числу независимых случайных булевых

векторов $X_i = (x_{in}, \ldots, x_{i1})^\top$, $i = \overline{1,m}$, координаты которых являются независимыми дискретными случайными величинами с распределниями вероятностей:

$$P\{x_{ij} = 1\} = p_j, \quad P\{x_{ij} = 0\} = 1 - p_j, \quad 0 < p_j < 1, \quad j = \overline{1,n}.$$

При сложении по модулю 2^n вектор X_i будем отождествлять с числом $x_i = \sum_{j=1}^{n} x_{ij} \times$ $\times 2^{j-1}$. Пусть $z = (x_1 + \ldots + x_m) \bmod 2^n$. Используя двоичное представление числа z, определим булев вектор $Z = (z_n, \ldots, z_1)^\top$. Координаты вектора Z удовлетворяют следующим соотношениям:

$$z_1 = I_1 \bmod 2, \quad z_j = (I_j + \sigma_{j-1}) \bmod 2, \quad j = \overline{2,n}, \tag{1}$$

где $I_j = \sum_{i=1}^{m} x_{ij}$, $j = \overline{1,n}$, $\sigma_1 = [I_1/2]$, $\sigma_j = [(I_j + \sigma_{j-1})/2]$, $j = \overline{2,n}$, $[a]$ — целая часть числа a.

Определим булев вектор $Y = (y_n, \ldots, y_1)^\top = X_1 \oplus \ldots + \oplus X_m$, где $y_j = I_j \bmod 2$, $j = \overline{1,n}$. Требуется найти вероятности $\delta_j(m) = P\{z_j = y_j\}$, $j = \overline{1,n}$.

Из (1) следует, что $\delta_1(m) = 1$, а

$$\delta_j(m) = P\{\sigma_{j-1} \bmod 2 = 0\}, \quad j = \overline{2,n}. \tag{2}$$

В [1] построена рекуррентная процедура для вычисления вероятностей (2).

В настоящей работе рассматривается случай $p_j = p$, $j = \overline{1,n}$. Известно [2], что в этом случае последовательность переносов образует однородную цепь Маркова. На основе стационарного распределения вероятностей переносов $(\sigma_j,\ j = \overline{1,n-1})$ получены приближенные явные формулы для вероятностей (2) при $m = 2, 3, 4$.

В случае $m = 2$ для $j = \overline{2,n}$ имеем:

$$\delta_j(2) = P\{\sigma_{j-1} \bmod 2 = 0\} = P\{\sigma_{j-1} = 0\} \approx (1-p)^2/(p^2 + (1-p)^2).$$

Литература

1. Галинский В. А. *Сравнение операций сложения по модулю 2^n и по модулю 2* // XI Белорусская матем. конф.: Тез. докл. Междунар. науч. конф. (Минск, 5–9 ноября 2012 г.) Ч. 4. Мн.: Институт математики НАН Беларуси, 2012. С. 55–56.

2. Галинский В. А. *Вероятностные свойства переносов при сложении по модулю 2^n* // Обозрение прикладной и промышленной математики. 2003. Т. 10, вып. 1. С. 129–130.