

УДК 519.21

ОЦЕНКА СКОРОСТИ СХОДИМОСТИ В МНОГОМЕРНОЙ ЦЕНТРАЛЬНОЙ ПРЕДЕЛЬНОЙ ТЕОРЕМЕ

А. В. Волгин

Известна оценка скорости многомерной нормальной аппроксимации для сумм локально зависимых случайных векторов, которая неявным образом зависит от размерности суммируемых векторов. Приводится явный вид зависимости оценки от размерности.

Ключевые слова: многомерная центральная предельная теорема, скорость сходимости, локально зависимые случайные векторы.

В [1] рассматривается оценка скорости нормальной аппроксимации суммы локально независимых случайных векторов $W = \sum_{i=1}^n X_i$, $X_i \in \mathbb{R}^d$. Предполагается, что слагаемые ограничены так, что $|X_i| \leq B$, $i = 1, \dots, n$, где через $|\cdot|$ обозначается сумма абсолютных значений координат вектора (или элементов матрицы), B — некоторая константа. Под локальной зависимостью подразумевается существование декомпозиций

$$W = U_i + V_i, \quad W = R_i + T_i, \quad i = 1, \dots, n, \quad (1)$$

таких, что $|U_i| \leq A_1$, $|R_i| \leq A_2$, $i = 1, \dots, n$, для некоторых констант $A_1 \leq A_2$. В качестве меры аппроксимации нормальным распределением рассматривается величина

$$\Delta = \sup_{A \in \mathcal{A}} |\mathbb{P}(W \in A) - \mathbb{P}(Z \in A)|,$$

где Z — случайный вектор, имеющий d -мерное стандартное нормальное распределение; $\mathcal{A}$ — класс всех измеримых выпуклых подмножеств $\mathbb{R}^d$.

Теорема 1 [1]. Пусть $W = \sum_{i=1}^n X_i$ представляется в виде декомпозиций (1), I — единичная матрица размера $d \times d$ над полем $\mathbb{R}$,

$$\chi_1 = \sum_{i=1}^n \mathbb{E}|\mathbb{E}(X_i|V_i)|, \quad \chi_2 = \sum_{i=1}^n \mathbb{E}|\mathbb{E}(X_i U_i^T) - \mathbb{E}(X_i U_i^T | T_i)|, \quad \chi_3 = \left| I - \sum_{i=1}^n \mathbb{E}(X_i U_i^T) \right|.$$

Тогда существует константа c , зависящая от размерности векторов d , такая, что

$$\Delta \leq c [aA_2 + naA_1A_2B (|\ln A_2B| + \ln n) + \chi_1 + (|\ln A_1B| + \ln n) (\chi_2 + \chi_3)], \text{ где } a \leq \sqrt{2d}.$$

Оценка величины Δ в теореме 1 приводится в условиях фиксированной размерности векторов $d \equiv \text{const} \in \mathbb{N}$ и роста числа слагаемых $n \rightarrow \infty$. В данном случае явный вид зависимости величины c от размерности d не имеет значения.

Рассматривается задача оценки величины Δ при условии одновременного роста размерности векторов и числа слагаемых $d, n \rightarrow \infty$. Предлагается подход, который основан на уточнении явного вида зависимости величины Δ от размерности d .

Теорема 2. В условиях теоремы 1

$$\Delta \leq 3(2\pi)^{d/2} aA_2 + d(2\pi)^{d/2} naA_1A_2B (\ln |17(2\pi)^{d/2} A_1A_2B| + \ln n) + 2d\chi_1 + \\ + d(d+1) (\ln |17(2\pi)^{d/2} A_1A_2B| + \ln n) (\chi_2 + \chi_3), \quad a \leq \sqrt{2d}.$$

ЛИТЕРАТУРА

1. Rinott Y. and Rotar V. A multivariate CLT for local dependence with $n^{-1/2} \log n$ rate and applications to multivariate graph related statistics // J. Multivariate Analysis. 1996. V. 56. P. 333–350.

УДК 512.62

О ПОЛИКВАДРАТИЧНОМ РАСШИРЕНИИ БИНАРНЫХ ПОЛЕЙ

Кр. Л. Геут, С. С. Титов

Работа посвящена генерации неприводимых многочленов степени 2^n посредством поликватратичного расширения поля над $\text{GF}(2)$. Построено полное бинарное дерево неприводимых многочленов, рассмотрены свойства этого расширения.

Ключевые слова: неприводимый многочлен, поликватратичное расширение, след многочлена.

Неприводимые многочлены активно применяются при передаче информации по каналам связи в виде битовых строк, помехоустойчивом кодировании, работе конечных автоматов, стандартах защиты информации [1]. Использование свойств неприводимых многочленов позволяет максимизировать эффективность компьютерной реализации арифметики в конечных полях.

Рассмотрим уравнение $x^2 + x = z$ в поле $\text{GF}(2^m)$, где z — корень неприводимого многочлена f над $\text{GF}(2)$ степени m . Если x не лежит в этом же поле $\text{GF}(2^m)$, а лежит в расширении $\text{GF}(2^{2m})$ этого поля, то след $\text{Tr}(f) = 1$ [2] и x — корень неприводимого многочлена F степени $2m$ [3–5]. Многочлен F получается из f посредством так называемой операции A [6]: $F(X) = f(X^2 + X)$. Многочлен F неприводимый и периодический (с периодом равным единице), т. е. $F(X + 1) = F(X)$.

Если же x лежит в том же поле $\text{GF}(2^m)$, то многочлен, полученный с помощью операции A из многочлена f , приводим, $F(X) = p(X)q(X)$, $\text{Tr}(f) = 0$, $\deg p = \deg q = m$, и x — корень одного из этих двух неприводимых многочленов p, q , связанных соотношением сдвига: $p(X + 1) = q(X)$ [6].

Если $m = 2^k$ и $\text{Tr}(x) = 1$, то после поэтапного применения операции A можно построить полное бинарное дерево, ветви которого символизируют применение операции A , а вершины — многочлены, полученные с помощью этой операции [6]. Если представить шаг (т. е. применение операции A) как уровень, то можно заметить, что вершина с неприводимым многочленом степени 2^{n+1} появляется только после прохождения всех уровней с неприводимыми многочленами степени 2^n , причём число этих уровней-шагов равно 2^{n-1} . Приводимость многочлена, полученного с помощью операции A , зависит от следа многочлена, к которому была применена эта операция.

Многочлены степени 2^n со значением следа $\text{Tr} = 1$ всегда лежат на нижнем уровне, так как после применения операции A они дают неприводимый периодический многочлен степени 2^{n+1} , а на остальных уровнях лежат многочлены с нулевым значением следа $\text{Tr} = 0$.

Симметричные (самовозвратные) многочлены (т. е. многочлены, у которых коэффициенты симметричны относительно центрального бита) степени 2^{n+1} с нулевыми значениями следа и антиследа ($\text{Tr} = \text{Tr}^{-1} = 0$) получаются из многочленов степени 2^n со значениями $\text{Tr} = 0$, $\text{Tr}^{-1} = 1$, а многочлены степени 2^{n+1} со значениями $\text{Tr} = \text{Tr}^{-1} = 1$ — из аналогичных многочленов степени 2^n со значениями $\text{Tr} = \text{Tr}^{-1} = 1$,