Math-Net.Ru

Общероссийский математический портал

В. И. Шерстнев, Совместное распределение переносов при сложении целых чисел, *Теория вероятн. и ее примен.*, 1996, том 41, выпуск 2, 467–473

DOI: <https://doi.org/10.4213/tvp2962>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 35.173.137.237

26 апреля 2023 г., 13:40:54

СПИСОК ЛИТЕРАТУРЫ

1. Ибрагимов И. А., Розанов Ю. А. Гауссовские случайные процессы. М.: Наука, 1970, 384 с.
2. Розанов Ю. А., Козлов М. В. Об асимптотической эффективности оценок коэффициентов регрессии. — Докл. АН СССР, 1969, т. 188, № 1, с. 37–40.
3. Розанов Ю. А. Гауссовские бесконечномерные распределения. — Труды Математического института им. В. А. Стеклова, 1968, т. 108, с. 3–135.
4. Холево А. С. Об асимптотической эффективности псевдонаилучших оценок. — Теория вероятн. и ее примен., 1971, т. XVI, в. 3, с. 524–534.

Поступила в редакцию
14.XII.1995

© 1996 г.

ШЕРСТНЕВ В. И.*

СОВМЕСТНОЕ РАСПРЕДЕЛЕНИЕ ПЕРЕНОСОВ
ПРИ СЛОЖЕНИИ ЦЕЛЫХ ЧИСЕЛ¹⁾

В работе получены двусторонние асимптотически точные явные оценки совместного распределения переносов при сложении нескольких целых чисел. Отдельно рассмотрен случай сложения в двоичной системе счисления.

Ключевые слова и фразы: цепи Маркова, целочисленное сложение, поразрядное сложение.

1. Пусть V^n — множество целых чисел от 0 до $d^n - 1$ ($n, d \geq 2$ — некоторые натуральные числа). На этом множестве естественным образом вводятся две операции сложения. Одна из них — сложение чисел по модулю d^n , обозначаемое в дальнейшем $+$. (Обычное сложение действительных чисел будет обозначаться тем же знаком $+$, что не должно вызвать недоразумений.) С другой стороны, так как каждое число можно записать в d -ичной системе, множество $V^n = \{0, 1, \dots, d\}^n = V \times \dots \times V$ отождествляется с множеством d -ичных векторов размерности n . Разряды в d -ичном разложении числа будем нумеровать от младшего к старшему. Такие векторы складываются поразрядно, а внутри каждого разряда — по модулю d . Эта операция поразрядного сложения далее обозначается знаком $\oplus$ (соответствующее ей вычитание — знаком $\ominus$). Сложение отличается от поразрядного сложения наличием переноса из разряда в разряд. Перенос из разряда зависит от значений более младших разрядов слагаемых, поэтому алгебраическая связь между двумя рассматриваемыми операциями довольно сложна. В случае $d = 2$ поведение переноса из n -го разряда при $n \rightarrow \infty$ исследовалось в [1]. Мы изучаем вопрос о том, сколько существует наборов слагаемых, дающих фиксированную разность между результатами сложения и поразрядного сложения, например, насколько часто эти суммы совпадают.

Опишем вероятностную постановку задачи. Введем независимые случайные величины η_{lj} , $l = 1, \dots, k$, $j = 1, \dots, n$, равномерно распределенные на $\{0, 1, \dots, d - 1\}$.

*Математический ин-т им. В. А. Стеклова РАН, ул. Вавилова, 42, 117966 Москва, ГСП-1, Россия.

¹⁾Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект 93-011-1443.

Случайные величины $\xi_i = \eta_{i1} + \eta_{i2}d + \dots + \eta_{in}d^{n-1}$ при этом будут независимыми и равномерно распределенными на V^n . В данной работе будут построены оценки для распределения поразрядной разности случайных величин $\xi_1 + \dots + \xi_k$ и $\xi_1 \oplus \dots \oplus \xi_k$; будем называть эту разность вектором переносов. Вектор переносов — это вектор, в котором по порядку разрядов записаны все переносы в соответствующий разряд (приведенные по модулю d), возникшие при сложении «столбиком». Вектор переносов будем отождествлять с числом, имеющим такое d -ичное разложение.

Заметим, что младший разряд в каждой из двух сумм случайных величин равен $\eta_{11} \oplus \dots \oplus \eta_{k1}$, поскольку в него нет переноса. Поэтому первый (младший) разряд разности $(\xi_1 + \dots + \xi_k) \ominus (\xi_1 \oplus \dots \oplus \xi_k)$ всегда равен 0, и рассматривать его нет необходимости. Для того чтобы иметь возможность отбрасывать у n -мерного вектора младшие разряды, введем на V^n операцию правого сдвига: для $v = v_1 + v_2d + v_3d^2 + \dots + v_nd^{n-1}$ положим $\text{rs}(v) = [v/d] = v_2 + v_3d + \dots + v_nd^{n-2}$ (здесь $[v/d]$ означает целую часть v/d).

Итак, в дальнейшем будет исследоваться поведение вероятности

$$q_{nk}(M) = P\left\{\text{rs}\left((\xi_1 + \dots + \xi_k) \ominus (\xi_1 \oplus \dots \oplus \xi_k)\right) = M\right\}, \quad 0 \leq M \leq d^{n-1} - 1.$$

Вероятность совпадения результатов сложения и поразрядного сложения равна $q_{nk}(0)$.

Предельные значения $q_{nk}(M)$ при $k \rightarrow \infty$ и фиксированных n и d найти совсем просто. Нетрудно видеть, что перенос из первого разряда, равный $\text{rs}(\eta_{11} + \dots + \eta_{k1})$, в пределе при $k \rightarrow \infty$ имеет равномерное распределение на V^{n-1} , поскольку к равномерному распределению на V^n сходится при $k \rightarrow \infty$ распределение суммы $\eta_{11} + \dots + \eta_{k1}$. В то же время случайную величину $\text{rs}((\xi_1 + \dots + \xi_k) \ominus (\xi_1 \oplus \dots \oplus \xi_k))$ можно представить в виде суммы $\text{rs}(\eta_{11} + \dots + \eta_{k1})$ и некоторой не зависящей от нее случайной величины, зависящей лишь от разрядов, начиная со второго. Отсюда следует, что $q_{nk}(M) \rightarrow 1/d^{n-1}$ при $k \rightarrow \infty$ для любых M и n . Конечно, предельные значения содержат лишь качественную информацию о виде допредельных распределений.

Следующая теорема дает двусторонние оценки совместного распределения переносов.

Теорема 1. *Вероятность того, что для k независимых равномерно на V^n распределенных слагаемых вектор переносов принимает значение M , удовлетворяет двойному неравенству*

$$\left\{\frac{1}{d} - \frac{1}{d^{k-1}} \left(\frac{\sin(\pi/d)}{\sin(\pi/d^2)}\right)^k\right\}^{n-1} \leq q_{kn}(M) \leq \left\{\frac{1}{d} + \frac{1}{d^{k-1}} \left(\frac{\sin(\pi/d)}{\sin(\pi/d^2)}\right)^k\right\}^{n-1}.$$

Видно, что и верхняя, и нижняя оценки теоремы 1 при $k \rightarrow \infty$ стремятся к $1/d^{n-1}$, т.е. они являются асимптотически точными. Доказательство этой теоремы проводится в п. 2.

Теорема 1 дает возможность получить предельное распределение вектора переносов и в ситуации, когда число разрядов n зависит от числа слагаемых k . Действительно, перепишем верхнюю границу в виде

$$\frac{1}{d^{n-1}} \exp \left\{ (n-1) \ln \left(1 + \frac{1}{d^{k-2}} \left(\frac{\sin(\pi/d)}{\sin(\pi/d^2)} \right)^k \right) \right\}.$$

Отсюда видно, что если $k \rightarrow \infty$, а n меняется так, что

$$\frac{n}{dk} \left(\frac{\sin(\pi/d)}{\sin(\pi/d^2)} \right)^k \rightarrow 0,$$

то верхняя граница стремится к $1/d^{n-1}$ при любом M . Такое же утверждение для нижней границы доказывается аналогично, т.е. при данных условиях предельное поведение верхней и нижней границ одинаково, а по теореме 1 таким же должно быть и предельное поведение $q_{nk}(M)$. Сформулируем доказанный результат.

Следствие 1. Если $k \rightarrow \infty$, а n меняется так, что при этом $(n/d^k)(\sin(\pi/d)/\sin(\pi/d^2))^k \rightarrow 0$, то $q_{nk}(M) \sim 1/d^{n-1}$ при любом M .

Отметим, что условия следствия 1 допускают экспоненциально быстрый рост n как функции k .

Случай $d = 2$, представляющий наибольший интерес с точки зрения практики, рассматривается более подробно в п. 3. Там будет доказана теорема 2, уточняющая теорему 1 для этого случая, в частности, будет показано, что $q_{nk}(0) = 1/2^{n-1}$ при любых k , сравнимых с 3 по модулю 4.

2. Доказательство теоремы 1. Введем случайные величины ζ_j , $j = 1, \dots, n-1$, — суммарный перенос из j -го разряда в $j+1$ -й, и пусть $\zeta_0 = 0$. Эти случайные величины связаны между собой соотношением

$$\zeta_j = \text{rs} \left[\zeta_{j-1} + \sum_{l=1}^k \eta_{lj} \right]. \quad (1)$$

Последовательность ζ_j образует однородную цепь Маркова, так как слагаемые в правой части равенства (1) независимы, а $\sum_{l=1}^k \eta_{lj}$, $j = 1, 2, \dots$, одинаково распределены. Переходную матрицу этой цепи обозначим $P = (p_{it}) = (P\{\zeta_j = t \mid \zeta_{j-1} = i\})$. При суммировании k слагаемых перенос из разряда не превосходит $k-1$, поэтому можно считать, что матрица P имеет размер k . Для удобства вычислений занумеруем ее строки и столбцы числами от 0 до $k-1$.

Если M имеет d -ичное разложение $m_1, \dots, m_{n-1}$, то

$$q_{kn}(M) = P\{\zeta_1 \equiv m_1 \pmod{d}, \dots, \zeta_{n-1} \equiv m_{n-1} \pmod{d}\}, \quad (2)$$

потому что, как уже отмечалось, вектор переносов состоит из младших разрядов всех переносов. Обозначим P_{ab} подматрицу матрицы P , получающуюся выбором строк, номера которых сравнимы с a по модулю d , и столбцов, номера которых сравнимы с b по модулю d . Матрица P_{ab} содержит вероятности перехода от переносов, имеющих a в первом разряде, к переносам, имеющим в нем b . Тогда по свойству марковской цепи равенство (2) переписывается в виде

$$q_{kn}(M) = \mathbf{e}_1 P_{0m_1} P_{m_1 m_2} \cdots P_{m_{n-2} m_{n-1}} \mathbf{1}, \quad (3)$$

где $\mathbf{e}_1 = (1, 0, \dots, 0)$ — вектор-строка, дающая начальное распределение цепи, $\mathbf{1} = (1, \dots, 1)$ — вектор-столбец.

Согласно (3) исследуемая вероятность равна сумме элементов нулевой строки произведения указанных матриц. Эта сумма ограничена сверху (и снизу) произведением максимумов (соответственно, минимумов) сумм по строкам матриц-сомножителей. Пусть $S(A)$ обозначает для произвольной матрицы A максимум сумм по строкам ее элементов, $s(A)$ — минимум таких сумм для матрицы A . Используя эти обозначения, можно выписать двусторонние оценки

$$\begin{aligned} & s(P_{0m_1}) s(P_{m_1 m_2}) \cdots s(P_{m_{n-2} m_{n-1}}) \\ & \leq q_{kn}(M) \leq S(P_{0m_1}) S(P_{m_1 m_2}) \cdots S(P_{m_{n-2} m_{n-1}}). \end{aligned} \quad (4)$$

Рассмотрим структуру матрицы P . Пусть α — случайная величина, имеющая то же распределение, что и $\sum_{l=1}^k \eta_{lj}$ (от j это распределение не зависит вследствие

независимости и одинаковой распределенности случайных величин η_{ij}). Тогда из равенства (1) следует, что элементы матрицы P представимы в виде

$$p_{il} = P\{ld - t \leq \alpha < (l+1)d - t\}. \quad (5)$$

Отсюда видно, что $p_{il} = p_{i+d, l+1}$, поэтому строки матрицы P , номера которых отличаются на d , состоят из одних и тех же элементов, отличаясь лишь сдвигом на одну позицию. Следовательно, с точностью до сдвига существует только d чередующихся вариантов строк данной матрицы P . В матрицу $P_{m_1 m_2}$ строки выбираются так, чтобы их номера в матрице P шли как раз с шагом d , те же строки берутся и в матрицу $P_{m_1 m_2+1}$. Хотя матрицы $P_{m_1 m_2}$ и $P_{m_1 m_2+1}$ могут состоять из разного числа столбцов, ненулевые элементы любой строки первой матрицы совпадают с ненулевыми элементами следующей по номеру строки матрицы $P_{m_1 m_2+1}$. Отсюда немедленно получаем, что $S(P_{m_1 m_2})$ и $s(P_{m_1 m_2})$ не зависят от m_2 , если в матрице $P_{m_1 m_2}$ не менее d строк, поскольку для любой ее строки в матрице $P_{m_1 m_1}$ имеется по крайней мере одна строка с такой же суммой элементов. Поэтому $S(P_{m_1 m_2}) = S(P_{m_1 m_1})$ и $s(P_{m_1 m_2}) = s(P_{m_1 m_1})$, что позволяет переписать (4) в следующем виде:

$$\begin{aligned} & s(P_{00}) s(P_{m_1 m_1}) \cdots s(P_{m_{n-2} m_{n-2}}) \\ & \leq q_{kn}(M) \leq S(P_{00}) S(P_{m_1 m_1}) \cdots S(P_{m_{n-2} m_{n-2}}). \end{aligned} \quad (6)$$

Теперь оценим величины $S(P_{mm})$ и $s(P_{mm})$ для некоторого m между 0 и $d-1$. Элемент матрицы P_{mm} , стоящий на пересечении t -й строки и l -го столбца обозначим $p_{il}(m)$. Этот элемент в матрице P стоит на пересечении строки $m + td$ и столбца $m + ld$. Поэтому, используя (5), можно написать

$$\begin{aligned} p_{il}(m) &= P\left\{m + ld \leq \frac{m + td + \alpha}{d} < m + ld + 1\right\} \\ &= \sum_{j=0}^{d-1} P\{\alpha = (ld + m - t)d - m + j\}. \end{aligned} \quad (7)$$

Отсюда получаем, что сумма всех элементов в строке t матрицы P равна

$$\begin{aligned} \sum_{l=0}^{[k/d]} p_{il}(m) &= \sum_{j=0}^{d-1} \sum_{l=0}^{[k/d]} P\{\alpha = (ld + m - t)d - m + j\} \\ &= \sum_{j=0}^{d-1} P\{\alpha \equiv (m - t)d + j - m \pmod{d^2}\}. \end{aligned} \quad (8)$$

Второе равенство в (8) имеет место, поскольку сумма по j берется по всем возможным значениям.

Вероятность $P\{\alpha \equiv m \pmod{d^2}\}$, очевидно, равна числу решений уравнения $x_1 + \cdots + x_k \equiv m \pmod{d^2}$ в целых числах $0 \leq x_1, \dots, x_k < d-1$, деленному на d^k , т.е.

$$\begin{aligned} P\{\alpha \equiv m \pmod{d^2}\} &= \frac{1}{d^{k+2}} \sum_{x=0}^{d^2-1} \sum_{x_1, \dots, x_k=0}^{d-1} \exp\left\{\frac{2\pi i x}{d^2} (x_1 + \cdots + x_k - m)\right\} \\ &= \frac{1}{d^2} + \frac{1}{d^{k+2}} \sum_{x=1}^{d^2-1} \exp\left\{-\frac{2\pi i x m}{d^2}\right\} \left(\sum_{y=0}^{d-1} \exp\left\{-\frac{2\pi i x y}{d^2}\right\}\right)^k. \end{aligned} \quad (9)$$

По формуле для суммы геометрической прогрессии

$$\sum_{y=0}^{d-1} \exp \left\{ \frac{2\pi i x y}{d^2} \right\} = \exp \left\{ \frac{\pi i x (d-1)}{d^2} \right\} \frac{\sin(\pi x/d)}{\sin(\pi x/d^2)}.$$

Модуль правой части этого равенства достигает при $x = 1$ своего максимального значения на множестве $\{1, \dots, d^2 - 1\}$. Поэтому из равенства (9) следует, что

$$\begin{aligned} \left| P \left\{ \alpha \equiv m \pmod{d^2} \right\} - \frac{1}{d^2} \right| &\leq \frac{1}{d^{k+2}} \sum_{x=1}^{d^2-1} \left| \frac{\sin(\pi x/d)}{\sin(\pi x/d^2)} \right|^k \\ &\leq \frac{1}{d^k} \left(\frac{\sin(\pi/d)}{\sin(\pi/d^2)} \right)^k. \end{aligned} \quad (10)$$

Таким образом, для суммы элементов одной строки матрицы P_{mm} из (8) и (10) вводится оценка

$$\left| \sum_{l=0}^{[k/d]} p_{tl}(m) - \frac{1}{d} \right| \leq \frac{1}{d^{k-1}} \left(\frac{\sin(\pi/d)}{\sin(\pi/d^2)} \right)^k.$$

Правая часть этого неравенства не зависит от номера строки t , следовательно, она может быть использована для оценивания максимума и минимума сумм по строкам:

$$\begin{aligned} S(P_{mm}) &\leq \frac{1}{d} + \frac{1}{d^{k-1}} \left(\frac{\sin(\pi/d)}{\sin(\pi/d^2)} \right)^k, \\ s(P_{mm}) &\geq \frac{1}{d} - \frac{1}{d^{k-1}} \left(\frac{\sin(\pi/d)}{\sin(\pi/d^2)} \right)^k. \end{aligned} \quad (11)$$

Отметим, что эти оценки не зависят от m , поэтому, подставляя их в (5), окончательно получаем

$$\left\{ \frac{1}{d} - \frac{1}{d^{k-1}} \left(\frac{\sin(\pi/d)}{\sin(\pi/d^2)} \right)^k \right\}^{n-1} \leq q_{kn}(M) \leq \left\{ \frac{1}{d} + \frac{1}{d^{k-1}} \left(\frac{\sin(\pi/d)}{\sin(\pi/d^2)} \right)^k \right\}^{n-1}.$$

З а м е ч а н и е. При доказательстве теоремы можно было обойтись без двойного неравенства (6), полностью аналогично оценив сомножители оценок (4). Однако, так как сомножители в правой и левой частях (6) могут быть только d типов, это двойное неравенство можно переписать в виде

$$\begin{aligned} s(P_{00})^{v_0(M)+1} s(P_{11})^{v_1(M)} \dots s(P_{d-1,d-1})^{v_{d-1}(M)} &\leq q_{kn}(M) \\ &\leq S(P_{00})^{v_0(M)+1} S(P_{11})^{v_1(M)} \dots S(P_{d-1,d-1})^{v_{d-1}(M)}, \end{aligned}$$

где $v_j(M)$ равно числу разрядов, не считая $(n-1)$ -й, которые в d -ичном разложении M равны j (очевидно, что $v_0 + \dots + v_{d-1} = n-2$). Эти оценки понадобятся в следующем пункте.

3. Особый интерес представляет случай $d = 2$. Использование оценок из теоремы 1 дает для этого случая

$$(2^{-1} - 2^{1-k/2})^{n-1} \leq q_{kn}(M) \leq (2^{-1} + 2^{1-k/2})^{n-1}.$$

Однако данные оценки можно улучшить. Из (8) и (9) следует, что

$$\begin{aligned} \sum_{l=0}^{[k/2]} p_{ll}(m) &= P\{\alpha \equiv m - 2t \pmod{4}\} + P\{\alpha \equiv m - 2t + 1 \pmod{4}\} \\ &= 2^{-1} + 2^{-k-2} \sum_{x=1}^3 e^{-\pi i x m / 2} e^{\pi i x t} (1 + e^{\pi i x / 2})^k (1 + e^{-\pi i x / 2}). \end{aligned}$$

Отсюда получаем, что

$$\begin{aligned} S(P_{mm}) &= 2^{-1} + 2^{-k-2} \left| e^{-\pi i m / 2} (1 + i)^k (1 - i) + e^{\pi i m / 2} (1 - i)^k (1 + i) \right| \\ &= 2^{-1} + 2^{-1-(k+1)/2} \left| e^{-\pi i m / 2} e^{\pi i (k-1)/4} + e^{\pi i m / 2} e^{-\pi i (k-1)/4} \right|, \end{aligned}$$

аналогично

$$s(P_{mm}) = 2^{-1} - 2^{-1-(k+1)/2} \left| e^{-\pi i m / 2} e^{\pi i (k-1)/4} + e^{\pi i m / 2} e^{-\pi i (k-1)/4} \right|.$$

В рассматриваемом случае m может принимать два значения. При $m = 0$

$$\begin{aligned} S(P_{00}) &= 2^{-1} + 2^{-(k+1)/2} \left| \cos \frac{\pi(k-1)}{4} \right|, \\ s(P_{00}) &= 2^{-1} - 2^{-(k+1)/2} \left| \cos \frac{\pi(k-1)}{4} \right|, \end{aligned}$$

а при $m = 1$

$$\begin{aligned} S(P_{11}) &= 2^{-1} + 2^{-(k+1)/2} \left| \sin \frac{\pi(k-1)}{4} \right|, \\ s(P_{11}) &= 2^{-1} - 2^{-(k+1)/2} \left| \sin \frac{\pi(k-1)}{4} \right|. \end{aligned}$$

Теперь двусторонние оценки для $q_{kn}(M)$ можно построить, исходя из оценок замечания пункта 2. Если обозначить $v(M) = v_0(M) = m_1 + \dots + m_{n-2}$, то можно написать

$$\begin{aligned} \left(\frac{1}{2} - \frac{|\sin(\pi(k-1)/4)|}{2^{(k+1)/2}} \right)^{v(M)} \left(\frac{1}{2} - \frac{|\cos(\pi(k-1)/4)|}{2^{(k+1)/2}} \right)^{n-v(M)-1} &\leq q_{kn}(M) \\ &\leq \left(\frac{1}{2} + \frac{|\sin(\pi(k-1)/4)|}{2^{(k+1)/2}} \right)^{v(M)} \left(\frac{1}{2} + \frac{|\cos(\pi(k-1)/4)|}{2^{(k+1)/2}} \right)^{n-v(M)-1} \end{aligned} \quad (12)$$

Таким образом, доказано следующее утверждение.

Теорема 2. В двоичной системе счисления суммарный перенос при сложении k штук n -разрядных слагаемых равен M с вероятностью, удовлетворяющей двойному неравенству (12).

Заметим, что $\cos(\pi(k-1)/4) = 0$ при $k \equiv 3 \pmod{4}$, а $\sin(\pi(k-1)/4) = 0$ при $k \equiv 1 \pmod{4}$. Это дает возможность упрощать в некоторых случаях оценки (12). В частности, при $v(M) = 0$ из теоремы 2 получаем следующее следствие.

Следствие 2. $q_{kn}(0) = 1/2^{n-1}$, если $k \equiv 3 \pmod{4}$.

Приведенное следствие отмечает интересный факт: вероятность совпадения результатов сложения и поразрядного сложения совпадает со своим предельным значением уже при $k = 3$ и возвращается к этому значению, если количество слагаемых увеличивается на число, кратное 4.

Попробуем объяснить этот факт с вероятностной точки зрения. Сумма и поразрядная сумма совпадают в том и только том случае, когда все переносы — четные. При $k = 3$ перенос из первого разряда может быть четным только, если он нулевой, и вероятность этого события, как нетрудно подсчитать, равна $\frac{1}{2}$. Но если перенос из

первого разряда нулевой, то второй разряд тоже должен давать нулевой перенос (вероятность этого $\frac{1}{2}$) и т.д. Следовательно, $q_{3n}(0) = 1/2^{n-1}$. Добавление 4 слагаемых ситуацию не меняет. Перенос из первого разряда при любом $k \equiv 3 \pmod{4}$ четен с вероятностью $\frac{1}{2}$, так как сумма первых разрядов имеет биномиальное распределение с параметрами k и $\frac{1}{2}$. Вероятность того, что перенос из второго разряда четен, не зависит от значения первого переноса и равна $\frac{1}{2}$, и т.д. Значит,

$$q_{kn}(0) = \frac{1}{2^{n-1}} \quad \text{при } k \equiv 3 \pmod{4}.$$

СПИСОК ЛИТЕРАТУРЫ

1. *Staffelbach O., Meier W.* Cryptographic significance of the carry for cipher based on integer addition. — *Lect. Notes Comput. Sci.*, 1991, v. 537, p. 601–614.

Поступила в редакцию
10.XII.1993

© 1996 г.

ШОЛОМИЦКИЙ А. Г.*

**ТЕОРЕМА В. ФЕЛЛЕРА
ДЛЯ СУММ ЗАВИСИМЫХ ВЕЛИЧИН¹⁾**

Работа посвящена доказательству необходимости условия Линдеберга для нормальной сходимости для некоторых классов зависимых случайных величин (обобщению известной теоремы В. Феллера). Условия теоремы формулируются в терминах условных (относительно некоторых сигма-алгебр) распределений слагаемых.

Ключевые слова и фразы: условие предельной малости, нормальная сходимость, условие Линдеберга, условное распределение, сигма-алгебра.

1. Достаточность условия Линдеберга для нормальной сходимости зависимых случайных величин (в дальнейшем с.в.) рассматривалась А. Дворецким [7], Р. Ш. Липцером и А. Н. Ширяевым (см. [1], [2]). Здесь будет решаться обратная задача — нахождения необходимых условий нормальной сходимости, т.е. обобщения теоремы, известной как теорема В. Феллера. В работе использованы некоторые идеи метода стохастических экспонент, развитого в [1], [2].

Пусть $\{X_{j,n}\}_{j=1}^{\infty}$ — схема серий некоторых случайных величин, заданных на вероятностном пространстве $(\Omega, \mathcal{F}, P)$, $S_n^k = \sum_{j=k}^{\infty} X_{j,n}$, $S_n := S_n^{\infty}$.

Основная задача состоит в определении таких σ -алгебр $\mathcal{K}_{j,n}$, для которых

$$E \prod_j E \left(\exp(itX_{j,n}) \mid \mathcal{K}_{j,n} \right) = E \exp(itS_n), \quad (1.1)$$

*Центральный экономико-математический институт РАН, ул. Красикова, 32, 117418 Москва, Россия.

¹⁾Осуществление настоящей работы стало возможным частично благодаря гранту Международного научного фонда № 1NX000.