Math-Net.Ru

Общероссийский математический портал

Б. В. Рязанов, Г. П. Шанкин, Критерий равномерности распределения суммы независимых случайных величин на примарной циклической группе, *Дискрет. матем.*, 1997, том 9, выпуск 1, 95–102

DOI: <https://doi.org/10.4213/dm458>

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: 54.237.59.107

26 апреля 2023 г., 16:08:50

Критерий равномерности распределения суммы независимых случайных величин на примарной циклической группе

© 1997 г. Б. В. Рязанов, Г. П. Шанкин

Исследуется распределение суммы независимых случайных величин, принимающих значения в примарной циклической группе и имеющих равномерное распределение на множествах одинаковой мощности.

1. Формулировка результатов

Пусть G — произвольная конечная абелева группа и $\xi_1, \dots, \xi_n$ — независимые случайные элементы этой группы с равномерными распределениями на некоторых подмножествах $A_1, \dots, A_n$:

$$p_t(g) = \mathbf{P}\{\xi_t = g\} = |A_t|^{-1}, \quad g \in A_t, \quad t = 1, \dots, n, \quad (1)$$

где $|A|$ — мощность множества A . Рассматривается задача: найти необходимые и достаточные условия (на множества $A_1, \dots, A_n$), при которых сумма

$$\xi = \sum_{t=1}^n \xi_t \quad (2)$$

имеет равномерное распределение на группе G .

В общем виде эта задача не решена. В [1] найден критерий равномерности распределения суммы (2) в предположении, что

$$|G| = |A_1| \dots |A_n|. \quad (3)$$

В настоящей работе находится критерий равномерности распределения суммы (2) без предположения (3) (теорема 1), но при этом рассматривается лишь примарная циклическая группа $\mathbf{Z}_M$ порядка $M = q^m$ (q — простое число) и на множества A_t вводится достаточно жесткое ограничение

$$|A_t| = q, \quad t = 1, \dots, n. \quad (4)$$

В этой связи отметим, что в работах [2] и [3] исследовался вопрос о критериях равномерности распределения суммы независимых случайных элементов на аддитивной группе вычетов по произвольному модулю M . В [2] в качестве

основного результата приведено утверждение о том, что для равномерности распределения исходной суммы необходимо и достаточно, чтобы (хотя бы) одно из ее слагаемых имело равномерное распределение. В [3] построен пример, опровергающий это утверждение. Близкие к [3] контрпримеры известны авторам от А. С. Амбросимова и Н. Н. Шарова. Примеры, опровергающие [2], дают также теоремы 1 и 2 настоящей работы.

Перейдем к формулировке результатов.

Теорема 1. Пусть Z_M — примарная циклическая группа порядка $M = q^m$ и носители A_t случайных элементов ξ_t , $t = 1, \dots, n$, удовлетворяют условию (4).

Если среди множеств $A_1, \dots, A_n$ содержатся множества вида

$$A_{t_k} = \{\mu_k + q^{k-1}(a_{k\nu}q + \nu) : \nu = 0, \dots, q-1\}, \quad k = 1, \dots, m, \quad (5)$$

где μ_k и $a_{k\nu}$ — произвольные целые числа, $0 \leq \mu_k \leq q^{k-1} - 1$, $0 \leq a_{k\nu} \leq q^{m-k} - 1$, и при этом

$$P\{\xi_{t_k} = g\} = q^{-1}, \quad g \in A_{t_k}, \quad k = 1, \dots, m, \quad (6)$$

то сумма (2) имеет равномерное на Z_M распределение.

Обратно, если сумма (2) равномерно распределена на Z_M и $q = 2$, или $q \geq 3$ и все вероятности $p_t(g)$, $g \in A_t$, $t = 1, \dots, n$, рациональны, то выполняются условия (5) и (6).

Отметим, что условия (5) и (6) конструктивны, то есть они, по сути дела, дают алгоритм построения равновероятных на Z_M сумм (2) из достаточно простых слагаемых. Это представляет практический интерес, например, при построении высокоскоростных датчиков случайных чисел по большому модулю на основе (одного или нескольких) датчиков чисел по небольшому модулю.

Необходимость условий (5) и (6) в теореме 1 мы получаем как следствие более общего утверждения для группы вычетов Z_M по произвольному модулю

$$M = q_1^{m_1} \dots q_r^{m_r}, \quad (7)$$

где m_s — натуральные числа, а q_s — простые попарно различные числа, $s = 1, \dots, r$.

Теорема 2. Пусть Z_M — группа вычетов по модулю (7) и сумма (2) равномерно распределена на Z_M . Если при этом носители A_t слагаемых ξ_t удовлетворяют условию (4), а

$$q \leq \min\{q_1, \dots, q_r\}, \quad (8)$$

и все вероятности $p_t(g)$, $g \in A_t$, $t = 1, \dots, n$, рациональны при $q \geq 3$, то

$$M = q^m \quad (9)$$

и выполняются условия (5) и (6).

Пусть выполнены условия (4) и (9) и при этом $n = m$ и сумма (2) распределена равномерно на $\mathbf{Z}_M$. Тогда, очевидным образом, имеет место соотношение (8) и

$$\mathbf{P}\{\xi_t = g\} = q^{-1}, \quad g \in A_t, \quad t = 1, \dots, n, \quad (10)$$

то есть все вероятности $p_t(g)$, $g \in A_t$, $t = 1, \dots, n$, рациональны. В таком случае, согласно теореме 1, множества A_t при соответствующей перенумерации имеют вид

$$A_t = \{\mu_t + q^{t-1}(a_{t\nu}q + \nu) : \nu = 0, \dots, q-1\}, \quad (11)$$

где μ_t и $a_{t\nu}$ — произвольные целые числа, $0 \leq \mu_t \leq q^{t-1} - 1$, $0 \leq a_{t\nu} \leq q^{m-t} - 1$. Это утверждение является частным случаем основной теоремы упоминавшейся выше работы [3] для группы $\mathbf{Z}_{q^n}$.

Замечание. В теоремах 1 и 2 случаи $q = 2$ и $q \geq 3$ разделены, и во втором случае для обеспечения необходимости условий (9), (5) и (6) введено дополнительное условие рациональности вероятностей $p_t(g)$, $g \in A_t$, $t = 1, \dots, n$. Это требование (в рассматриваемой нами ситуации $M = q^m$, $m \leq n$, в отличие от исследованной в [3] ситуации $m = n$, где оно выполняется автоматически) существенно. В следующем параграфе мы приведем примеры случайных величин $\xi_1, \dots, \xi_n$, для которых выполнены условия (4), (8), (9), сумма (2) распределена равномерно на $\mathbf{Z}_M$ с $M = q^m$ (q — произвольное простое число, $q \geq 3$, $m \geq 2$), но при этом не выполнены условия (5) и (6).

2. Доказательства

В основе дальнейших рассуждений лежит следующее утверждение ([4], стр. 102).

Лемма 1. *Произвольная случайная величина η имеет равномерное распределение на $\mathbf{Z}_M$ тогда и только тогда, когда*

$$\mathbf{E}e^{2\pi i g^* \eta / M} = \sum_{g \in \mathbf{Z}_M} \mathbf{P}\{\eta = y\} e^{2\pi i g^* y / M} = 0, \quad g^* \in \mathbf{Z}_M \setminus \{0\}. \quad (12)$$

Пусть выполнены условия (9), (5) и (6), в которых, чтобы не загромождать обозначения, положим $t_k = k$, $k = 1, \dots, m$. Отметим, что в условии (5), не ограничивая общности, можно положить $\mu_k = 0$, ибо наличие ненулевых μ_k будет привносить лишь постоянный сдвиг $\mu_1 + \dots + \mu_m$ в сумму (2), что не влияет на равномерность ее распределения. Возьмем произвольное g^* из $\mathbf{Z}_M \setminus \{0\}$ и представим его в виде $g^* = q^{m-k}l$, где l не делится на q , $1 \leq l \leq q^{m-k} - 1$, $1 \leq k \leq m$. Тогда

$$q \mathbf{E}e^{2\pi i g^* \xi_k / M} = \sum_{g \in A_k} e^{2\pi i g^* g / M} = \sum_{\nu=0}^{q-1} e^{2\pi i l \nu / q} = \sum_{\nu=0}^{q-1} e^{2\pi i \nu / q} = 0,$$

и, ввиду независимости слагаемых $\xi_1, \dots, \xi_n$,

$$\mathbf{E}e^{2\pi i g^* \xi / M} = \prod_{t=1}^n \mathbf{E}e^{2\pi i g^* \xi_t / M} = 0, \quad (13)$$

что, согласно лемме 1, и доказывает первую часть теоремы 1.

Перейдем к доказательству теоремы 2. Так как сумма ξ распределена равномерно, а $\xi_1, \dots, \xi_n$ независимы, то, согласно лемме 1, справедливо соотношение (13), которое при произвольно выбранном целом s , $1 \leq s \leq r$, и $g^* = Mq_s^{-m_s+1}$ принимает вид

$$\mathbf{E}e^{2\pi i g^* \xi / M} = \mathbf{E}e^{2\pi i \xi / q_s} = \prod_{t=1}^n \mathbf{E}e^{2\pi i \xi_t / q_s} = 0. \quad (14)$$

Из (14) следует, что

$$\sum_{g \in A_{t_s}} \mathbf{P}\{\xi_{t_s} = g\} e^{2\pi i g / q_s} = \sum_{\nu=0}^{q_s-1} \mathbf{P}\{\xi_{t_s} \equiv \nu \pmod{q_s}\} e^{2\pi i \nu / q_s} = 0 \quad (15)$$

для некоторого t_s , $1 \leq t_s \leq n$. Последнее равенство имеет вид

$$f(\varepsilon) = \sum_{\nu=0}^{q_s-1} f_\nu \varepsilon^\nu = 0,$$

где $\varepsilon = \exp\{2\pi i / q_s\}$, а

$$f(x) = \sum_{\nu=0}^{q_s-1} f_\nu x^\nu \quad (16)$$

— многочлен с коэффициентами

$$f_\nu = \mathbf{P}\{\xi_{t_s} \equiv \nu \pmod{q_s}\}, \quad \nu = 0, \dots, q_s - 1. \quad (17)$$

Коэффициенты (17) рациональны. Для $q \geq 3$ это определено условием теоремы 2, а для $q = 2$, то есть когда носитель A_{t_s} состоит из некоторых двух элементов g_1 и g_2 , это с очевидностью вытекает из (15):

$$\mathbf{P}\{\xi_{t_s} = g_1\} = \mathbf{P}\{\xi_{t_s} = g_2\} = 1/2.$$

Далее, заметим, что многочлен (16) имеет общий корень $x = \varepsilon$ с многочленом

$$\varphi(x) = \sum_{\nu=0}^{q_s-1} x^\nu,$$

который, как известно ([5], стр. 157, 209), неразложим над полем рациональных чисел $\mathbf{Q}$, и поэтому, согласно [5, стр. 141], $f = c\varphi$, где c — некоторая константа. Но в таком случае, ввиду условия $q \leq q_s$, из (16) и (17) следует, что $q_s = q$, $s = 1, \dots, r$, и $M = q^m$, где $m = m_1 + \dots + m_r$.

Для завершения доказательства необходимости условия (9) остается отметить, что, с одной стороны, сумма ξ из-за ограничения (4) не может принимать более q^n значений, а с другой стороны, ввиду равномерности своего распределения на $\mathbf{Z}_M$, она должна принимать с положительной вероятностью каждое из $M = q^m$ значений. Поэтому $m \leq n$.

Докажем необходимость условий (5) и (6), для чего возьмем произвольное k , $1 \leq k \leq m$, и $g^* = g^{m-k}$. В этом случае (13) принимает вид

$$\prod_{t=1}^n \mathbf{E} e^{2\pi i g^* \xi_t / M} = \prod_{t=1}^n \mathbf{E} e^{2\pi i \xi_t / q^k} = 0,$$

откуда следует, что для некоторого t_k , $1 \leq t_k \leq n$, имеет место соотношение

$$\mathbf{E} e^{2\pi i \xi_{t_k} / q^k} = \sum_{l=0}^{q^k-1} \mathbf{P}\{\xi_{t_k} \equiv l \pmod{q^k}\} e^{2\pi i l / q^k} = 0,$$

которое мы представим, по аналогии с (15) и (16), в виде

$$f_k(\varepsilon_k) = \sum_{l=0}^{q^k-1} f_{kl} \varepsilon_k^l = 0,$$

где $\varepsilon_k = \exp\{2\pi i q^{-k}\}$, а

$$f_k(x) = \sum_{l=0}^{q^k-1} f_{kl} x^l = 0 \quad (18)$$

— многочлен с коэффициентами

$$f_{kl} = \mathbf{P}\{\xi_{t_k} \equiv l \pmod{q^k}\}, \quad l = 0, \dots, q^k - 1. \quad (19)$$

Коэффициенты (19) рациональны, а многочлен (18) имеет общий корень ε_k с неразложимым над полем $\mathbf{Q}$ многочленом ([5], стр. 157)

$$\varphi_k(x) = \sum_{\nu=0}^{q-1} x^{\nu q^{k-1}}.$$

Поэтому f_k делится на φ_k :

$$f_k(x) = \varphi_k(x) \tilde{f}_k(x), \quad (20)$$

где

$$\tilde{f}_k(x) = \sum_{\mu=0}^{q^{k-1}-1} \tilde{f}_{k\mu} x^\mu.$$

Из (20) вытекает, что

$$f_{kl} = \tilde{f}_{k\mu}, \quad l = \mu + \nu q^{k-1}, \quad \mu = 0, \dots, q^{k-1} - 1, \quad \nu = 0, \dots, q - 1.$$

Таким образом, мы получаем, что вероятности (19) с номерами $l = \mu + \nu q^{k-1}$ при любом фиксированном μ не зависят от ν :

$$\mathbf{P}\{\xi_{t_k} \equiv \mu + \nu q^{k-1} \pmod{q^k}\} = \tilde{f}_{k\mu}, \quad \nu = 0, \dots, q - 1. \quad (21)$$

Из этого факта и условия (4) вытекает, что вероятности (21) строго положительны только при некотором одном значении $\mu = \mu_k$ и при этом

$$\mathbf{P}\{\xi_{t_k} \equiv \mu_k + \nu q^{k-1} \pmod{q^k}\} = q^{-1}, \quad \nu = 0, \dots, q-1,$$

или

$$\mathbf{P}\{\xi_{t_k} = \mu_k + q^{k-1}(a_{k\nu}q + \nu)\} = q^{-1}, \quad \nu = 0, \dots, q-1,$$

где $a_{k\nu}$ — некоторые произвольные целые числа, $0 \leq a_{k\nu} \leq q^{m-k} - 1$.

Перейдем к построению примеров, анонсированных в замечании. Мы приведем лишь схему построения таких примеров, не останавливаясь на легко воспроизводимых деталях. В основе предлагаемой схемы лежат лемма 1 и следующее утверждение из [6].

Лемма 2. Пусть точки единичной окружности $e^{2\pi i \alpha_\nu}$, $\nu = 1, \dots, q-1$, $0 \leq \alpha_0 < \dots < \alpha_{q-1} < 1$, являются вершинами выпуклого многоугольника, который содержит внутри себя точку 0. Тогда существует набор чисел $p_0, \dots, p_{q-1}$ такой, что

$$\sum_{\nu=0}^{q-1} p_\nu e^{2\pi i \alpha_\nu} = 0, \quad \sum_{\nu=0}^{q-1} p_\nu = 1, \quad p_\nu > 0, \quad \nu = 0, \dots, q-1. \quad (22)$$

Пусть $M = n = q^m$, $q \geq 3$, $m \geq 2$. Возьмем произвольное t , $1 \leq t \leq n$, и построим ξ_t следующим образом. Положим $g^* = t - 1$ и представим g^* в виде $g^* = q^{m-l}s$, где s не делится на q , $1 \leq s \leq q^l - 1$. Далее выберем целые числа $\tilde{g}_1, \dots, \tilde{g}_{q-1}$ из области $0 \leq \tilde{g}_0 < \dots < \tilde{g}_{q-1} \leq q^l - 1$ таким образом, чтобы многоугольник с вершинами $\exp\{2\pi i \tilde{g}_\nu q^{-l}\}$ содержал внутри себя точку 0. Для таких чисел по лемме 2 существует такой набор чисел $p_0, \dots, p_{q-1}$, что

$$\sum_{\nu=0}^{q-1} p_\nu e^{2\pi i \tilde{g}_\nu / q^l} = 0, \quad \sum_{\nu=0}^{q-1} p_\nu = 1, \quad p_\nu > 0, \quad \nu = 0, \dots, q-1. \quad (23)$$

Теперь заметим, что преобразование $x \rightarrow sx \pmod{q^l}$ образует подстановку на множестве $\{0, 1, \dots, q^l - 1\}$ и у элементов $\tilde{g}_0, \dots, \tilde{g}_{q-1}$ существуют попарно различные преобразы g_ν :

$$sg_\nu \equiv \tilde{g}_\nu \pmod{q^l}, \quad \nu = 0, \dots, q-1. \quad (24)$$

Определим ξ_t условием

$$\mathbf{P}\{\xi_t = g_\nu\} = p_\nu, \quad \nu = 0, \dots, q-1.$$

В соответствии с (23)

$$\mathbf{E} e^{2\pi i g^* \xi_t / M} = \sum_{\nu=0}^{q-1} p_\nu e^{2\pi i \tilde{g}_\nu / q^l} = 0$$

и случайные величины $\xi_1, \dots, \xi_n$ по определению независимы, поэтому, согласно лемме 1, их сумма распределена равномерно на $\mathbf{Z}_M$.

Покажем, что в предложенной конструкции элементы $\tilde{g}_0, \dots, \tilde{g}_{q-1}$ можно брать таким образом, чтобы свойство (5) не выполнялось ни при каком $k \geq 2$.

Пусть $t = s + 1$, где s не делится на q , и допустим, что множество

$$A_t = \{g: p_t(g) > 0\} = \{g_0, \dots, g_{q-1}\}$$

состоит из элементов вида $g_\nu = h_\nu q^{k-1}$, $\nu = 0, \dots, q-1$. В этом случае первая сумма в (23) (в которой при рассматриваемом t , очевидным образом, нужно положить $l = 1$) будет иметь вид

$$\sum_{\nu=0}^{q-1} p_\nu e^{2\pi i h_\nu q^{k-2}} = \sum_{\nu=0}^{q-1} p_\nu = 1,$$

что противоречит свойству (23).

Пусть теперь $t = q^{l-1}s + 1$, где $l \geq 2$, а s не делится на q . Положим

$$\tilde{g}_1 = q^{l-1} + 1, \quad \tilde{g}_\nu = \nu q^{l-1}, \quad \nu \neq 1, \quad 0 \leq \nu \leq q-1. \quad (25)$$

Ясно, что многоугольник с вершинами в точках $\exp\{2\pi i \tilde{g}_\nu q^{-l}\}$, $\nu = 0, \dots, q-1$, содержит внутри себя точку 0, и поэтому для данных $\tilde{g}_\nu$ найдутся $p_0, \dots, p_{q-1}$ со свойствами (23). Рассмотрим элементы g_ν , порождаемые элементами (25) и соотношением (24). Легко видеть, что g_ν при $\nu \neq 1$ имеют вид $g_\nu = q^{l-1}(a_{l\nu}q + b_\nu)$, где $1 \leq b_\nu \leq q-1$, а g_1 не делится на q^{l-1} . Таким образом, мы приходим к выводу, что ни одно из множеств A_t , $t = 1, \dots, n$, не обладает свойством (5) ни при каком $k \geq 2$.

Перейдем к обсуждению условия (6). Покажем, что при $t = q^{l-1}s$ с $l \geq 2$ (s не делится на q) каждая из построенных случайных величин ξ_t распределена на своем носителе A_t неравномерно. Допустим, что это не так, и какая-то ξ_t распределена на A_t равномерно. В этом случае из (23) и (25) вытекает, что

$$1 + e^{2\pi i(q^l+1)/q^l} + \sum_{\nu=2}^{q-1} e^{2\pi i \nu/q} = 0,$$

откуда с помощью очевидного равенства

$$\sum_{\nu=0}^{q-1} e^{2\pi i \nu/q} = 0$$

мы приходим к противоречию: $e^{2\pi i/q^l} = 1$.

В заключение отметим, что в рассмотренной выше конструкции в случае $n = M = q^m$ при $q \geq 5$ и $m \geq 2$ можно подобрать $\tilde{g}_0, \dots, \tilde{g}_{q-1}$ и $p_0, \dots, p_{q-1}$ таким образом, что множества A_t будут иметь вид

$$A_t = \{\nu q^{t-1} : \nu = 0, \dots, q-1\}, \quad t = 1, \dots, n,$$

а

$$\mathbf{P}\{\xi_t = g\} \neq q^{-1}, \quad g \in A_t, \quad t = 1, \dots, n.$$

Это означает, что сумма таких $\xi_1, \dots, \xi_n$ распределена равномерно на $\mathbf{Z}_{q^n}$ и при этом выполняются все упомянутые в теореме 2 условия кроме условия (6) (и, естественным образом, кроме условия рациональности вероятностей $p_t(g)$, $g \in A_t$, $t = 1, \dots, n$).

Список литературы

1. Redei L. Die neue Theorie der endlichen Abelschen Gruppen und Verallgemeinerung des Hauptsatzes von Hajos. *Acta Math. Acad. Sci. Hung.* (1965) **16**, №3–4, 329–373.
2. Rizzi A. On the sum (modulo m) of two statistical variables. *Boll. Unione Math. Ital.* (1976) **A13**, №5, 163–167.
3. Arnold B. C. Non-uniform decompositions of uniform random variables under summation modulo m . *Boll. Unione Math. Ital.* (1979) **A16**, №1, 100–102.
4. Воробьев Н. Н. Сложение независимых случайных величин на конечных абелевых группах. *Матем. сборник* (1954) **34 (76)**, №1, 89–126.
5. Ван дер Варден Б. Л. *Алгебра*. Наука, Москва, 1976.
6. Емеличев В. А., Ковалев М. М., Кравцов М. К. *Многогранники, графы, оптимизация*. Наука, Москва, 1981.

Статья поступила 27.02.96.