Math-Net.Ru

Общероссийский математический портал

А. Д. Яшунский, О преобразованиях распределений вероятностей неповторными квазигрупповыми формулами, *Дискрет. матем.*, 2013, том 25, выпуск 2, 149–159

DOI: <https://doi.org/10.4213/dm1242>

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: 3.91.87.62

26 апреля 2023 г., 10:39:44

О преобразованиях распределений вероятностей бесповторными квазигрупповыми формулами*

© 2013 г. А. Д. Яшунский

Работа посвящена исследованию распределений значений бесповторных формул над квазигруппой при подстановке вместо переменных случайных независимых одинаково распределённых элементов квазигруппы. В работе устанавливаются условия сходимости распределений значений формул к равномерному распределению для произвольных бесповторных формул растущей сложности или глубины, а также показывается наличие сходимости «в среднем» в тех случаях, когда эти условия не выполнены.

1. Основные определения

Конечное множество Q с заданной на нём бинарной операцией умножения $(\cdot)$ называется *квазигруппой*, если уравнения $x \cdot b = a$ и $b \cdot y = a$ однозначно разрешимы относительно x и y для любых $a, b \in Q$ (см. [1]). Таким образом, в Q также определены операции правого и левого деления: a/b и $b \backslash a$. Таблица умножения квазигруппы из шести элементов, не являющейся группой, приведена ниже в качестве примера.

$\cdot$	1	2	3	4	5	6
1	1	3	2	4	6	5
2	3	2	5	1	4	6
3	2	4	6	5	1	3
4	4	1	3	6	5	2
5	5	6	1	2	3	4
6	6	5	4	3	2	1

Пусть далее Q — произвольная квазигруппа из q элементов.

Определим понятие *формулы* над квазигруппой: во-первых, переменные x_k являются формулами, во-вторых, если F_1 и F_2 — формулы, то $(F_1 \cdot F_2)$ — формула. Для формулы F введём *сложность* $L(F)$ и *глубину* $D(F)$. Положим $L(x_k) = D(x_k) = 0$, а для формулы $F = (F_1 \cdot F_2)$ определим $L(F) = L(F_1) + L(F_2) + 1$ и $D(F) = \max\{D(F_1), D(F_2)\} + 1$. Для любой формулы F выполнено $D(F) \leq L(F) \leq 2^{D(F)} - 1$.

Работа выполнена при финансовой поддержке РФФИ (проект № 11-01-00508) и Программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

Формула называется *бесповторной*, если каждый символ переменной встречается в ней не более одного раза. Бесповторные формулы, различающиеся лишь наименованием переменных, будем отождествлять. Обозначим множество бесповторных формул глубины n через D_n , а множество бесповторных формул сложности t через L_t .

Заменим переменные бесповторной формулы F независимыми одинаково распределёнными случайными элементами из Q . В этом случае значение формулы F будет случайной величиной со значениями в Q . Обозначим распределение вероятностей значений F через $P(F)$, понимая под $P_i(F)$ вероятность того, что формула F принимает значение $i \in Q$. Множество распределений на Q будем обозначать P^q .

Для формулы $F = (F_1 \cdot F_2)$ выполнено $P(F) = P(F_1) * P(F_2)$, где операция $u * v$ для $u, v \in P^q$ есть *квазигрупповая свёртка*, определяемая соотношениями

$$(u * v)_i = \sum_{j \in Q} u_j v_{j \setminus i} = \sum_{j \in Q} u_{i/j} v_j. \quad (1)$$

Распределение $P(F)$ для произвольной формулы F зависит только от распределения значений переменных $P(x_k) = \pi$, которое будем называть *начальным*. Носителем распределения $u \in P^q$ будем называть множество $N(u) = \{i \in Q : u_i > 0\}$.

2. Свойства свёртки

Для удобства будем считать, что элементами квазигруппы Q являются числа $\{1, 2, \dots, q\}$. Для распределения $u = (u_1, u_2, \dots, u_q)$, следуя [2], будем обозначать через $(u_{[1]}, u_{[2]}, \dots, u_{[q]})$ распределение, получающееся из u перестановкой компонент таким образом, что $u_{[1]} \geq u_{[2]} \geq \dots \geq u_{[q]}$.

Используя это обозначение, можно записать следующие неравенства для компонент свёртки $u * v$, непосредственно вытекающие из неравенств, приведённых в [3], с. 261:

$$u_{[1]}v_{[q]} + u_{[2]}v_{[q-1]} + \dots + u_{[q]}v_{[1]} \leq (u * v)_i \leq u_{[1]}v_{[1]} + u_{[2]}v_{[2]} + \dots + u_{[q]}v_{[q]}. \quad (2)$$

Из этих неравенств вытекают также соотношения:

$$\max\{u_{[q]}, v_{[q]}\} \leq (u * v)_{[q]} \leq (u * v)_{[1]} \leq \min\{u_{[1]}, v_{[1]}\}. \quad (3)$$

Для распределения u введём величину $\delta_u = u_{[1]} - u_{[q]}$. Малые значения δ_u свидетельствуют о близости распределения u к равномерному.

Утверждение 1. Если $u, v \in P^q$, то $\delta_{u*v} \leq \min\{(1 - v_{\lfloor q/2 \rfloor + 1})\delta_u, (1 - u_{\lfloor q/2 \rfloor + 1})\delta_v\}$.

Доказательство. По определению, $\delta_{u*v} = (u * v)_{[1]} - (u * v)_{[q]}$. Используя неравенства из (2), оцениваем:

$$\begin{aligned} \delta_{u*v} &\leq (u_{[1]}v_{[1]} + u_{[2]}v_{[2]} + \dots + u_{[q]}v_{[q]}) - (u_{[1]}v_{[q]} + u_{[2]}v_{[q-1]} + \dots + u_{[q]}v_{[1]}) = \\ &= u_{[1]}(v_{[1]} - v_{[q]}) + u_{[2]}(v_{[2]} - v_{[q-1]}) + \dots + u_{[q]}(v_{[q]} - v_{[1]}) = \\ &= (u_{[1]} - u_{[q]})(v_{[1]} - v_{[q]}) + (u_{[2]} - u_{[q-1]})(v_{[2]} - v_{[q-1]}) + \dots + \\ &\quad + (u_{\lfloor q/2 \rfloor} - u_{\lfloor q/2 \rfloor + 1})(v_{\lfloor q/2 \rfloor} - v_{\lfloor q/2 \rfloor + 1}). \end{aligned}$$

Очевидно, что $u_{[i]} - u_{[q-i+1]} \leq \delta_u$ для всех i , поэтому

$$\delta_{u*v} \leq (v_{[1]} + v_{[2]} + \dots + v_{\lfloor q/2 \rfloor} - v_{\lfloor q/2 \rfloor + 1} - \dots - v_{[q]})\delta_u \leq (1 - v_{\lfloor q/2 \rfloor + 1})\delta_u.$$

Аналогично $\delta_{u*v} \leq (1 - u_{\lfloor q/2 \rfloor + 1})\delta_v$, откуда вытекает доказываемое неравенство.

3. Сходимость к равномерному распределению

Утверждение 1 позволяет показать, что при дополнительных условиях распределения значений формул приближаются к равномерному распределению с ростом сложности или глубины формул.

Теорема 1. Пусть начальное распределение $\pi \in \mathbb{P}^q$ удовлетворяет условию $|N(\pi)| > q/2$. Тогда существует такое $\alpha \in [0, 1)$, что $\delta_{P(F)} \leq \alpha^{D(F)}$ для любой бесповторной формулы F .

Доказательство. Из условия $|N(\pi)| > q/2$ вытекает, что $|N(\pi * \pi)| = q$. Пусть $\alpha = \max\{1 - \pi_{\lfloor q/2 \rfloor + 1}, 1 - (\pi * \pi)_{[q]}\} \in [0, 1)$. Покажем индукцией по n , что для всех $F \in D_n$ имеет место $\delta_{P(F)} \leq \alpha^n$. При $n = 0$ утверждение тривиально. Пусть утверждение выполнено для всех формул из D_n , и пусть $F \in D_{n+1}$. Тогда $F = (F_1 \cdot F_2)$ и из формул F_1, F_2 хотя бы одна принадлежит D_n . Пусть для определённости $F_1 \in D_n$, тогда в силу предположения индукции $\delta_{P(F_1)} \leq \alpha^n$.

В силу утверждения 1, $\delta_{P(F)} \leq (1 - P_{\lfloor q/2 \rfloor + 1}(F_2))\delta_{P(F_1)}$. Если $F_2 \in D_0$, то $P(F_2) = \pi$, и в силу выбора α выполнено $1 - P_{\lfloor q/2 \rfloor + 1}(F_2) \leq \alpha$.

Если $F_2 \in D_k$, где $k \geq 1$, то, учитывая неравенства (3), получаем:

$$P_{\lfloor q/2 \rfloor + 1}(F_2) \geq P_{[q]}(F_2) \geq (\pi * \pi)_{[q]},$$

откуда вытекает, что $1 - P_{\lfloor q/2 \rfloor + 1}(F_2) \leq \alpha$. Таким образом $\delta_{P(F)} \leq \alpha \cdot \alpha^n = \alpha^{n+1}$. Теорема доказана.

Доказанная в теореме 1 экспоненциальная скорость сходимости величин $\delta_{P(F)}$ к нулю в общем случае неулучшаема. В частности, в группе $\mathbb{Z}_2$ с таким начальным распределением π , что $N(\pi) = \mathbb{Z}_2$, для формул-«цепочек» $F_n = (\dots((x_1 \cdot x_2) \cdot x_3) \dots x_{n+1})$ имеет место $\delta_{P(F_n)} = (\pi_{[1]} - \pi_{[2]})^n$.

Теорему 1 легко обобщить на бесповторные формулы, составленные из нескольких разных квазигрупповых операций.

Теорема 2. Пусть $Q_1, \dots, Q_k$ — квазигруппы порядка q с общим множеством элементов, и пусть для начального распределения $\pi \in \mathbb{P}^q$ выполнено условие $|N(\pi)| > q/2$. Тогда существует такое $\alpha \in [0, 1)$, что $\delta_{P(F)} \leq \alpha^{D(F)}$ для любой бесповторной формулы F над $Q_1, \dots, Q_k$.

Неравенство $L(F) \leq 2^{D(F)} - 1$, переписанное в виде $D(F) \geq \log_2(L(F) + 1)$, позволяет получить оценку для $\delta_{P(F)}$ и через $L(F)$.

Теорема 3. Пусть для начального распределения $\pi \in \mathbb{P}^q$ выполнено условие $|N(\pi)| > q/2$. Тогда существует такое $\beta > 0$, что $\delta_{P(F)} \leq (L(F) + 1)^{-\beta}$ для любой бесповторной формулы F .

4. Связь с группами и цепями Маркова

Пусть квазигруппа Q в действительности является группой (т.е. умножение в ней ассоциативно). Тогда все формулы $F \in L_m$ при фиксированном m имеют одно и то же распределение $P(F)$, зависящее только от начального распределения π :

$$P(F) = (\dots((\underbrace{(\pi * \pi) * \pi}_{m \text{ раз}}} \dots * \pi)),$$

обозначим его $\pi^{(m)}$. Распределения формул из D_n при фиксированном n образуют множество $\{\pi^{(n)}, \pi^{(n+1)}, \dots, \pi^{(2^n-1)}\}$. Распределения $\pi^{(n)}$ в точности совпадают с распределениями, получающимися при анализе случайных блужданий на группе Q (подробнее см. [4]) с начальным распределением π и вероятностями перехода $p_{ij} = \pi_{i \setminus j}$. Сходимость распределений $\pi^{(n)}$ к равномерному при $n \rightarrow \infty$, а также утверждения теорем 1, 3 в этом случае следуют из свойств соответствующей цепи Маркова. В подобных задачах для оценки близости распределений u и v традиционно используется метрика $\rho(u, v) = \frac{1}{2} \sum_{i \in Q} |u_i - v_i|$. Обозначая равномерное на Q распределение через e , несложно заметить, что $\rho(u, e) \leq q\delta_u$. С помощью этого неравенства теоремы 1 и 3 можно переформулировать в терминах величины $\rho(u, e)$.

Отметим, что операция квазигрупповой свёртки может быть записана в матричном виде: $u * v = u^T A$, где $A = \{a_{ij}\}$ — бистохастическая матрица с $a_{ij} = v_{i \setminus j}$, а u — вектор-столбец распределения. Таким образом, квазигрупповая свёртка распределений u и v эквивалентна одному шагу некоторой цепи Маркова, зависящей от распределения v . В групповом случае ассоциативность умножения позволяет в формулах, содержащих более одной операции умножения, использовать для всех умножений одну и ту же цепь Маркова, всегда полагая $v = \pi$.

Если же в квазигруппе Q нет ассоциативности умножения, то множество распределений формул из L_m при фиксированном m может содержать более одного элемента. Более того, в общем случае для формул $F \in L_m$ носители $N(P(F))$ могут зависеть от формулы F при сколь угодно больших m , в то время как в групповом случае для достаточно больших m носитель $N(\pi^{(m)})$ совпадает с подгруппой, порождённой $N(\pi)$. Проиллюстрируем это примером.

Рассмотрим квазигруппу $Q = \{1, 2, 3, 4, 5, 6\}$ с таблицей умножения, приведённой в начале статьи. Пусть $N(\pi) = \{1, 2\}$. Тогда носителем распределения $(\pi * \pi) * (\pi * \pi)$ является вся квазигруппа Q . Следовательно, любая формула F , содержащая подформулу $((x_1 \cdot x_2) \cdot (x_3 \cdot x_4))$, будет иметь носитель $N(P(F)) = Q$. Вместе с тем, распределения из последовательности $\pi^{(m)}$, соответствующие формулам-«цепочкам» $(\dots((x_1 \cdot x_2) \cdot x_3) \dots \cdot x_m)$, имеют носитель $\{1, 2, 3, 4\} \neq Q$. Таким образом, можно подобрать пару формул сколь угодно большой сложности, у которых носители распределений не совпадают.

Подобные эффекты не возникают, если π имеет носитель размера $|N(\pi)| > q/2$. Согласно теоремам 1 и 3 в этом случае распределения значений формул приближаются к равномерному распределению с ростом глубины или сложности. Аналогичные оценки можно получить, если хотя бы при каком-то m_0 для любой формулы $F \in L_{m_0}$ выполнено $N(P(F)) = Q$. Однако в случаях, подобных рассмотренному выше примеру, близость распределения значений формулы к равномерному нельзя оценить только через её сложность или глубину.

5. Объединённые носители

Для индивидуальной формулы F и начального распределения π значение $\delta_{P(F)}$ можно оценить с помощью неравенств из утверждения 1. Мы же будем рассматривать «осреднённое» поведение формул в множествах L_m и D_n . Введём *объединённые носители*:

$$N_n^D(\pi) = \bigcup_{F \in D_n} N(P(F)) \quad \text{и} \quad N_m^L(\pi) = \bigcup_{F \in L_m} N(P(F)).$$

Распространим операции квазигруппового умножения и правого деления на подмножества квазигруппы Q . Пусть $i \in Q$, $Q' \subseteq Q$, положим: $Q' \cdot i = \{j \cdot i : j \in Q'\}$, $Q'/i = \{j/i : j \in Q'\}$.

Используя введённые обозначения, запишем соотношения между объединёнными носителями. Для заданных $\pi \in P^q$ и $i \in N(\pi)$ выполнены включения $N_{n+1}^D(\pi) \supseteq N_n^D(\pi) \cdot i$ и $N_{m+1}^L(\pi) \supseteq N_m^L(\pi) \cdot i$, а следовательно, $|N_{n+1}^D(\pi)| \geq |N_n^D(\pi)|$ и $|N_{m+1}^L(\pi)| \geq |N_m^L(\pi)|$. Поскольку $|N_n^D(\pi)|$ и $|N_m^L(\pi)|$ ограничены сверху значением q , начиная с какого-то момента они будут постоянными.

Утверждение 2. Пусть задано $\pi \in P^q$. Тогда существуют такие n' и m' , что $|N_{n+1}^D(\pi)| = |N_n^D(\pi)|$ для любого $n \geq n'$ и $|N_{m+1}^L(\pi)| = |N_m^L(\pi)|$ для любого $m \geq m'$.

Укажем свойство последовательности множеств $N_n^D(\pi)$.

Утверждение 3. Для каждого $\pi \in P^q$ существуют такие число n' и множество $Q' \subseteq Q$, что $N_n^D(\pi) = Q'$ для любого $n > n'$.

Доказательство. Заметим, что в последовательности $\{N_n^D(\pi)\}$ имеется лишь конечное число различных множеств (не более 2^q). Следовательно, найдётся такой номер n' , что для любого $n > n'$ множество $N_n^D(\pi)$ встречается среди множеств $N_0^D(\pi), N_1^D(\pi), \dots, N_{n'}^D(\pi)$. Обозначим $Q' = N_0^D(\pi) \cup N_1^D(\pi) \cup \dots \cup N_{n'}^D(\pi)$. Тогда при $n > n'$ имеют место включения $N_n^D(\pi) \subseteq Q'$ и неравенство $|N_n^D(\pi)| \leq |Q'|$.

Пусть $i \in N_{n-1}^D(\pi)$. Тогда в силу определения множеств D_n имеет место включение:

$$(N_0^D(\pi) \cup N_1^D(\pi) \cup \dots \cup N_{n'}^D(\pi)) \cdot i = Q' \cdot i \subseteq N_n^D(\pi),$$

что влечёт $|N_n^D(\pi)| \geq |Q'|$. В объединении с ранее полученным неравенством это даёт $|N_n^D(\pi)| = |Q'|$. Поскольку $N_n^D(\pi) \subseteq Q'$, получаем, что $N_n^D(\pi) = Q'$ при всех $n > n'$. Утверждение доказано.

Отметим, что множество Q' является подквазигруппой в Q , получающейся замыканием множества $N(\pi)$ относительно операции квазигруппового умножения. Далее, не ограничивая общности, можно считать, что $Q' = Q$, так как на элементах, не входящих в Q' , все распределения, получаемые из π , заведомо равны нулю.

Структура последовательности множеств $N_m^L(\pi)$ несколько сложнее.

Утверждение 4. Для каждого $\pi \in P^q$ существуют такие числа r и l' , а также множества $Q_0, Q_1, \dots, Q_{r-1} \subseteq Q$, что $N_{l'+b}^L(\pi) = Q_b$ для любых $l \geq l'$ и $b = 0, 1, \dots, r-1$, причём множества Q_b попарно не пересекаются и $|Q_0| = |Q_1| = \dots = |Q_{r-1}|$.

Доказательство. По утверждению 2 существует такое число m' , что $|N_{m+1}^L(\pi)| = |N_m^L(\pi)|$ для любого $m \geq m'$. Тогда по определению множеств L_m для $m \geq m'$ и $j \in N_k^L(\pi)$, где k — произвольное, имеет место $N_m^L(\pi) \cdot j = N_{m+k+1}^L(\pi)$, откуда

$$N_m^L(\pi) = N_{m+k+1}^L(\pi)/j. \quad (4)$$

Пусть k'' и k' таковы, что $k'' > k' \geq m'$, $N_{k''}^L(\pi) \cap N_{k'}^L(\pi) \neq \emptyset$ и разность $k'' - k'$ минимальна. Такие k'' и k' обязательно найдутся, так как различных множеств $N_m^L(\pi)$ лишь конечное число.

Выберем $j \in N_{k''}^L(\pi) \cap N_{k'}^L(\pi)$ и произвольное $m \geq m'$. Тогда, с одной стороны $N_m^L(\pi) \cdot j = N_{m+k''+1}^L(\pi)$, а с другой стороны $N_m^L(\pi) \cdot j = N_{m+k'+1}^L(\pi)$, откуда получаем, что $N_{m+k''+1}^L(\pi) = N_{m+k'+1}^L(\pi)$ для произвольного $m \geq m'$.

Выбирая теперь $i \in N_m^L(\pi)$ и используя соотношение, аналогичное (4), преобразуем равенство $N_{m+k''+1}^L(\pi) = N_{m+k'+1}^L(\pi)$ в $N_{k''}^L(\pi) = N_{k'}^L(\pi)$. Таким образом, если объединённые носители пересекаются, то они обязательно совпадают. Аналогично показывается, что для произвольного $m \geq m'$ выполнено $N_{m+k''-k'}^L(\pi) = N_m^L(\pi)$.

Обозначим $r = k'' - k'$. Тогда $N_{m+r}^L(\pi) = N_m^L(\pi)$ при любом $m \geq m'$. Предположение о том, что $N_m^L(\pi) \cap N_{m+k}^L(\pi) \neq \emptyset$ при некотором $k < r$ противоречит выбору k'' и k' , следовательно, такие пересечения пусты. Выберем такое l' , что $l'r \geq m'$, и положим $Q_b = N_{l'r+b}^L(\pi)$ для $b = 0, 1, \dots, r-1$. Утверждение доказано.

Если Q является группой, то $N_m^L(\pi) = N(\pi^{(m)})$, и утверждение 4 можно рассматривать как описание последовательности множеств $N(\pi^{(m)})$. Тогда в утверждении фактически говорится о периодичности, которая может возникать в соответствующей цепи Маркова (о периодических цепях Маркова см. [5]). В свете этого замечания можно рассматривать утверждение 4 как обобщение марковской периодичности. Число r будем называть *периодом* системы множеств $N_m^L(\pi)$, и периодический случай имеет место, если $r > 1$. Если же $r = 1$, то, начиная с номера m' , все множества $N_m^L(\pi)$ совпадают и равны некоторому $Q_0 \subseteq Q$.

Как и в случае носителей $N_n^D(\pi)$, множество $Q' = Q_0 \cup Q_1 \cup \dots \cup Q_{r-1}$ является подквазигруппой в Q , порождённой элементами из $N(\pi)$; не ограничивая общности, далее будем считать, что $Q' = Q$.

Критерий периодичности системы множеств $N_m^L(\pi)$ можно сформулировать в терминах квазигруппы Q и носителя $N(\pi)$. Система имеет период r тогда и только тогда, когда r — наибольшее натуральное число, для которого существует такой гомоморфизм $\varphi : Q \rightarrow \mathbb{Z}_r$, что $N(\pi) \subseteq \varphi^{-1}(1)$. Отметим, что по множествам Q_b гомоморфизм строится явно: для $i \in Q_b$ полагаем $\varphi(i) = (b+1) \bmod r$.

6. Осреднённые распределения

Несмотря на то, что в общем случае близость распределения значений индивидуальной формулы к равномерному нельзя оценить только через глубину или сложность, оказывается, что такую оценку можно получить для распределений «в среднем». Введём обозначения для «средних» распределений по множествам D_n и L_m , рассматривая распределения $P(F)$ как векторы в $\mathbb{R}^q$:

$$d^{(n)} = \frac{1}{|D_n|} \sum_{F \in D_n} P(F), \quad \ell^{(m)} = \frac{1}{|L_m|} \sum_{F \in L_m} P(F).$$

Заметим, что $d^{(n)}, \ell^{(m)} \in \mathbb{R}^q$, а кроме того, $N(d^{(n)}) = N_n^D(\pi)$ и $N(\ell^{(m)}) = N_m^L(\pi)$. Полезно отметить, что в пространстве $\mathbb{R}^q$ квазигрупповая свёртка, задаваемая для векторов $u, v \in \mathbb{R}^q$ соотношениями (1), является билинейной, т.е. для $a, b \in \mathbb{R}$ и $u, v, w \in \mathbb{R}^q$ выполняются равенства

$$(au + bv) * w = a(u * w) + b(v * w), \quad w * (au + bv) = a(w * u) + b(w * v).$$

Кроме того, для векторов u, v с неотрицательными компонентами и $a, b \geq 0$ имеют место неравенства

$$au_{[q]} + bv_{[q]} \leq (au + bv)_{[q]} \leq (au + bv)_{[1]} \leq au_{[1]} + bv_{[1]}, \quad (5)$$

из которых вытекает:

$$\delta_{au+bv} \leq a\delta_u + b\delta_v. \quad (6)$$

Из определений $P(F)$ и множества D_{n+1} следует соотношение

$$\sum_{F \in D_{n+1}} P(F) = \sum_{\substack{F_1 \in D_n, \\ F_2 \in D_k, \\ k < n}} P(F_1) * P(F_2) + \sum_{\substack{F_1 \in D_k, \\ F_2 \in D_n, \\ k < n}} P(F_1) * P(F_2) + \sum_{\substack{F_1 \in D_n, \\ F_2 \in D_n}} P(F_1) * P(F_2),$$

которое с учётом определения $d^{(n)}$ и билинейности свёртки преобразуется к виду

$$d^{(n+1)} = \sum_{k=0}^{n-1} \frac{|D_n||D_k|}{|D_{n+1}|} \left((d^{(n)} * d^{(k)}) + (d^{(k)} * d^{(n)}) \right) + \frac{|D_n|^2}{|D_{n+1}|} (d^{(n)} * d^{(n)}). \quad (7)$$

Аналогичное соотношение для величин $\ell^{(m)}$ имеет вид

$$\ell^{(m+1)} = \frac{1}{|L_{m+1}|} \sum_{k=0}^m |L_k||L_{m-k}| (\ell^{(k)} * \ell^{(m-k)}). \quad (8)$$

Кроме того, мощности множеств D_n и L_m удовлетворяют рекуррентным соотношениям¹

$$|D_{n+1}| = 2|D_n| \sum_{k=0}^{n-1} |D_k| + |D_n|^2, \quad |L_{m+1}| = \sum_{k=0}^m |L_k||L_{m-k}|. \quad (9)$$

Покажем, что осреднённые распределения приближаются к равномерному даже без предположения о величине $|N(\pi)|$.

Теорема 4. Пусть $\pi \in P^q$ таково, что $N(\pi)$ порождает Q относительно квазигруппового умножения, и пусть $d^{(n)}$ — соответствующие осреднённые распределения. Тогда найдутся такие число $\alpha \in [0; 1)$ и номер n' , что для любого $n \geq n'$ имеет место неравенство $\delta_{d^{(n)}} \leq \alpha^{n-n'}$.

Доказательство. Из неравенств (3) вытекает, что $(d^{(n)} * d^{(k)})_{[q]} \geq d_{[q]}^{(n)}$, $(d^{(k)} * d^{(n)})_{[q]} \geq d_{[q]}^{(n)}$ и $(d^{(n)} * d^{(n)})_{[q]} \geq d_{[q]}^{(n)}$. Используя эти соотношения, из равенства (7) с учётом (5) и (9) получаем оценку $d_{[q]}^{(n+1)} \geq d_{[q]}^{(n)}$.

Согласно утверждению 3, найдётся такой номер n'' , что $N_n^D(\pi) = Q$ для $n \geq n''$. Следовательно, для таких n выполнено неравенство $d_{[q]}^{(n)} > 0$. Положим $\alpha' = d_{[q]}^{(n'')}$, тогда в силу полученной выше оценки $d_{[q]}^{(n+1)} \geq d_{[q]}^{(n)}$, при $n \geq n''$ выполнено $d_{[q]}^{(n)} \geq \alpha'$.

Рассмотрим теперь величины $\delta_{d^{(n)}}$. Из соотношения (7) с помощью (6) выводится неравенство

$$\delta_{d^{(n+1)}} \leq \sum_{k=0}^{n-1} \frac{|D_n||D_k|}{|D_{n+1}|} (\delta_{d^{(n)} * d^{(k)}} + \delta_{d^{(k)} * d^{(n)}}) + \frac{|D_n|^2}{|D_{n+1}|} \delta_{d^{(n)} * d^{(n)}}.$$

Воспользовавшись утверждением 1 и оценкой $d_{[q]}^{(n)} \geq \alpha'$ при $n \geq n''$, для достаточно больших n получим

$$\delta_{d^{(n+1)}} \leq \sum_{k=0}^{n''-1} \frac{|D_n||D_k|}{|D_{n+1}|} \cdot 2\delta_{d^{(n)}} + \sum_{k=n''}^{n-1} \frac{|D_n||D_k|}{|D_{n+1}|} \cdot 2(1 - \alpha')\delta_{d^{(n)}} + \frac{|D_n|^2}{|D_{n+1}|} (1 - \alpha')\delta_{d^{(n)}}.$$

¹Величины $|L_m|$ образуют последовательность, известную как числа Каталана.

С помощью соотношения (9) это неравенство преобразуется в

$$\delta_{d(n+1)} \leq (1 - \alpha')\delta_{d(n)} + 2\alpha' \frac{|D_n|}{|D_{n+1}|} \left(\sum_{k=0}^{n''-1} |D_k| \right) \delta_{d(n)}. \quad (10)$$

Из соотношения (9) и очевидного неравенства $|D_n| \geq n$ вытекает соотношение $|D_{n+1}|/|D_n| \geq |D_n| \geq n$, которое влечёт $|D_n|/|D_{n+1}| \leq 1/n$. Положим $\alpha'' = \sum_{k=0}^{n''-1} |D_k|$. Тогда соотношение (10) принимает вид

$$\delta_{d(n+1)} \leq (1 - \alpha')\delta_{d(n)} + \frac{2\alpha'}{n}\alpha''\delta_{d(n)} = \left(1 - \alpha' + \frac{2\alpha'\alpha''}{n}\right)\delta_{d(n)}.$$

Найдётся такое $n' > n''$, что при $n \geq n'$: $1 - \alpha' + \frac{2\alpha'\alpha''}{n} < 1$. Обозначим $\alpha = 1 - \alpha' + \frac{2\alpha'\alpha''}{n'}$. Тогда при всех $n \geq n'$ имеет место неравенство $\delta_{d(n+1)} \leq \alpha\delta_{d(n)}$, из которого легко вытекает утверждение теоремы.

Для доказательства сходимости осреднённых распределений $\ell^{(m)}$ введём величины $\Delta_n = \max_{m=2^n+1, \dots, 2^{n+1}} \delta_{\ell^{(m)}}$.

Теорема 5. Пусть $\pi \in P^q$, $\ell^{(m)}$ — соответствующие осреднённые распределения на квазигруппе Q , и пусть существует m' такое, что при $m \geq m'$ выполнено $N_m^L(\pi) = Q$. Тогда найдётся $\alpha \in [0; 1)$ и номер n' такой, что для любого $n \geq n'$ имеет место неравенство $\Delta_n \leq \alpha^{n-n'}$.

Доказательство. При $m \geq m'$ из условия $N_m^L(\pi) = Q$ следует, что $\ell_{[q]}^{(m)} > 0$. Положим: $\alpha' = \min_{m=m', \dots, 2m'} \ell_{[q]}^{(m)} > 0$. Из соотношения (8) с помощью (3), (5) и (9) при $m \geq 2m' + 1$ индукцией по m выводим, что $\ell_{[q]}^{(m)} \geq \alpha'$. Положим:

$$\alpha'' = \frac{1}{|L_{4m'+3}|} \sum_{k=0}^{2m'} |L_k| |L_{4m'+2-k}| = \frac{1}{|L_{4m'+3}|} \sum_{k=2m'+2}^{4m'+2} |L_k| |L_{4m'+2-k}| < \frac{1}{2}$$

и обозначим $\alpha = 1 - \alpha'(1 - 2\alpha'') < 1$.

Рассмотрим целое $n > \log_2(4m' + 3)$ и последовательно для каждого значения $s = 2^{n+1} + 1, \dots, 2^{n+2}$ покажем, что $\delta_{\ell^{(s)}} \leq \alpha\Delta_n$. Пусть неравенство уже доказано для $s = 2^{n+1} + 1, \dots, m - 1$, покажем, что оно верно при $s = m$.

Используя соотношения (6) и (8), получаем:

$$\delta_{\ell^{(m)}} \leq \frac{1}{|L_m|} \sum_{k=0}^{m-1} |L_k| |L_{m-1-k}| \delta_{\ell^{(k)} * \ell^{(m-1-k)}}.$$

В слагаемых с $k \leq 2m'$ воспользуемся оценкой $\delta_{\ell^{(k)} * \ell^{(m-1-k)}} \leq \delta_{\ell^{(m-1-k)}}$, а в слагаемых с $k \geq m - 2m' - 1$ оценкой $\delta_{\ell^{(k)} * \ell^{(m-1-k)}} \leq \delta_{\ell^{(k)}}$ (эти оценки являются простым следствием утверждения 1). При этом в правых частях неравенств фигурируют величины $\delta_{\ell^{(t)}}$ с $t \geq m - 2m' - 1$. Поскольку $m > 2^{n+1} > 2(4m' + 3)$, для указанных значений t выполнено $t > 3m/4 > m/2 > 2^n$. Следовательно, значения t попадают либо в интервал $2^n + 1, \dots, 2^{n+1}$, либо в $2^{n+1} + 1, \dots, 2^{n+2}$. В первом случае

$\delta_{\ell(t)} \leq \Delta_n$ по определению Δ_n . Во втором случае, по ранее доказанному имеет место $\delta_{\ell(t)} \leq \alpha \Delta_n < \Delta_n$.

В слагаемых с $2m' + 1 \leq k \leq m - 1 - 2m' - 1$ по утверждению 1 с учётом определения α' оцениваем:

$$\delta_{\ell(k) * \ell(m-1-k)} \leq (1 - \alpha') \min\{\delta_{\ell(k)}, \delta_{\ell(m-1-k)}\},$$

причём в силу того, что $m \geq 2^{n+1} + 1$, хотя бы один из номеров $k, m - 1 - k$ не меньше, чем 2^n . Используя рассуждения, аналогичные приведённым выше, получаем, что $\delta_{\ell(k) * \ell(m-1-k)} \leq (1 - \alpha') \Delta_n$. Таким образом получаем:

$$\begin{aligned} \delta_{\ell(m)} &\leq \left(\frac{1}{|L_m|} \sum_{k=0}^{2m'} |L_k| |L_{m-1-k}| + \frac{1 - \alpha'}{|L_m|} \sum_{k=2m'+1}^{m-1-2m'-1} |L_k| |L_{m-1-k}| + \right. \\ &\quad \left. + \frac{1}{|L_m|} \sum_{k=m-2m'-1}^{m-1} |L_k| |L_{m-1-k}| \right) \Delta_n = \left(1 - \alpha' + \frac{2\alpha'}{|L_m|} \sum_{k=0}^{2m'} |L_k| |L_{m-1-k}| \right) \Delta_n. \end{aligned}$$

Для дальнейших рассуждений воспользуемся одним свойством чисел Каталана, доказательство которого приведём для полноты изложения. Покажем, что при $t \leq m$ имеет место неравенство

$$\frac{1}{|L_{m+2}|} \sum_{k=0}^t |L_k| |L_{m+1-k}| < \frac{1}{|L_{m+1}|} \sum_{k=0}^t |L_k| |L_{m-k}|.$$

Пользуясь соотношением $\frac{|L_{m+1}|}{|L_m|} = \frac{2(2m+1)}{m+2}$, вытекающим из свойств чисел Каталана (см., например, [6]), преобразуем отношение:

$$\begin{aligned} \frac{\frac{1}{|L_{m+2}|} \sum_{k=0}^t |L_k| |L_{m+1-k}|}{\frac{1}{|L_{m+1}|} \sum_{k=0}^t |L_k| |L_{m-k}|} &= \frac{|L_{m+1}|}{|L_{m+2}|} \frac{\sum_{k=0}^t |L_k| |L_{m-k}| \frac{|L_{m+1-k}|}{|L_{m-k}|}}{\sum_{k=0}^t |L_k| |L_{m-k}|} \leq \\ &\leq \frac{m+3}{2(2m+3)} \max_{k=0, \dots, t} \frac{|L_{m-k+1}|}{|L_{m-k}|} = \frac{m+3}{2(2m+3)} \max_{k=0, \dots, t} \frac{2(2(m-k)+1)}{m-k+2} = \\ &= \frac{2m^2 + 7m + 3}{2m^2 + 7m + 6} < 1. \end{aligned}$$

Из доказанного неравенства и выбора α'' следует, что $\frac{1}{|L_m|} \sum_{k=0}^{2m'} |L_k| |L_{m-1-k}| \leq \alpha''$, откуда $\delta_{\ell(m)} \leq (1 - \alpha' + 2\alpha'\alpha'') \Delta_n$, т.е. $\delta_{\ell(m)} \leq \alpha \Delta_n$.

Из выполнения неравенств $\delta_{\ell(m)} \leq \alpha \Delta_n$ для всех $m = 2^{n+1} + 1, \dots, 2^{n+2}$ вытекает, что $\Delta_{n+1} \leq \alpha \Delta_n$. Выбирая целое $n' > \log_2(4m' + 3)$, получаем утверждение теоремы.

Теорема 5 позволяет оценить и сами величины $\delta_{\ell(m)}$.

Следствие 1. В условиях теоремы 5 найдутся числа $\beta, \gamma > 0$, а также номер $m'' > m'$ такие, что при $m \geq m''$ выполнено $\delta_{\ell(m)} \leq \gamma m^{-\beta}$.

Случай периодических носителей распределений ($r > 1$) в определённом смысле сводится к аperiodическому случаю ($r = 1$). Пусть $Q = Q_0 \cup Q_1 \cup \dots \cup Q_{r-1}$, где

$Q_b = N_m^L(\pi)$ при $m \bmod r = b$ (для заданного π и достаточно больших m). Пусть $\psi : Q \rightarrow Q_0$ — некоторое отображение, обладающее свойством: $\psi(Q_b) = Q_0$ для любого b . Для каждого множества Q_b определено обратное к ψ отображение $\psi_b^{-1} : Q_0 \rightarrow Q_b$. Используя отображение ψ , можно свести рассмотрение распределений на Q к распределениям на Q_0 .

Введём распределения $\tilde{\ell}^{(m)}$ на множестве Q_0 следующим образом:

$$\tilde{\ell}_i^{(m)} = \ell_{\psi_m^{-1} \bmod r(i)}^{(m)}.$$

Заметим, что квазигрупповое умножение элементов множества Q_b на элементы Q_c для произвольных b и c даёт в точности элементы из множества $Q_{(b+c) \bmod r}$. Определим на Q_0 квазигрупповые операции $x \cdot_{b,c} y = \psi(\psi_b^{-1}(x) \cdot \psi_c^{-1}(y))$ для всех пар b, c . Для каждой пары b и c операции $\cdot_{b,c}$, вообще говоря, различны; если все они совпадают, то соответствующая квазигруппа есть фактор-квазигруппа Q по $\mathbb{Z}_r$.

С каждой квазигрупповой операцией $\cdot_{b,c}$ свяжем свёртку распределений на множестве Q_0 , обозначив её $*_{b,c}$. Тогда распределения $\tilde{\ell}^{(m)}$ удовлетворяют соотношению

$$\tilde{\ell}^{(m+1)} = \frac{1}{|L_{m+1}|} \sum_{k=0}^m |L_k| |L_{m-k}| (\tilde{\ell}^{(k)} *_{k \bmod r, (m-k) \bmod r} \tilde{\ell}^{(m-k)}). \quad (11)$$

Остаётся заметить, что в доказательстве теоремы 5 используемые свойства квазигрупповой свёртки не зависят от устройства квазигруппы, а опираются только на то, что это какая-то квазигрупповая свёртка (аналогично теореме 2). Таким образом, утверждение теоремы 5 и её следствия можно распространить и на распределения $\tilde{\ell}^{(m)}$, задаваемые соотношением (11). Отсюда легко получить, что при $r > 1$ распределения $\ell^{(m)}$ с m вида $rl + b$ сходятся с ростом l к распределению, равному на Q_b .

7. Заключительные замечания

Существующие работы сходной тематики касаются преимущественно групп. Обычно рассматривается модель случайных блужданий на группе — подробный обзор этих работ приведён в [4]. Описание случайного блуждания на группе подходящей марковской цепью и её сходимость (при дополнительных условиях) к равномерному распределению относятся, фактически, к математическому фольклору, а основным объектом исследований является феномен, известный как *cut-off* («обрыв») — это «резкое» приближение распределений к пределу после некоторого числа шагов. Это явление, подробно описанное в [4], имеет место далеко не во всех группах.

Случайные вычисления в квазигруппах рассматривались в криптологических приложениях (см. обзор [7]), например при построении потоковых фильтров. Однако и в этих работах используемая модель сводилась к цепи Маркова, с помощью которой доказывалась сходимость распределений к равномерным.

Ранее автором была установлена асимптотика осреднённых распределений [8]. В данной работе оценки близости распределений к равномерному получены для индивидуальных квазигрупповых формул. Их можно рассматривать как аналоги «стандартной» экспоненциальной оценки для скорости сходимости цепи Маркова к предельному распределению. Дальнейшим направлением работы в этой области может быть, например, поиск квазигрупп, в которых имеет место «обрыв».

Автор выражает признательность О. М. Касим-Заде за полезные обсуждения и ценные замечания по содержанию работы.

Список литературы

1. Белоусов В. Д., *Основы теории квазигрупп и луп*. Наука, Москва, 1967.
2. Маршалл А., Олкин И., *Неравенства. Теория мажоризации и ее приложения*. Мир, Москва, 1983.
3. Hardy G. H., Littlewood J. E., Pólya G., *Inequalities*. Univ. Press, Cambridge, 1934.
4. Saloff-Coste L., Random walks on finite groups. In: *Probability on discrete structures. Encyclopaedia Math. Sci.*, **110**. Springer, Berlin, 2004, pp. 263–346.
5. Феллер В., *Введение в теорию вероятностей и ее приложения*. Мир, Москва, 1984.
6. Грэхем Р., Кнут Д., Паташник О., *Конкретная математика. Основание информатики*. Мир, Москва, 1998.
7. Şcerbacov V., Quasigroups in cryptology. *Comp. Sci. J. of Moldova* (2009) **17**, №2 (50), 193–228.
8. Яшунский А. Д., О предельных вероятностях значений случайных выражений в квазигруппах. *Материалы XVIII Международной школы-семинара «Синтез и сложность управляющих систем» имени академика О. Б. Лупанова (Пенза, 28 сентября – 3 октября, 2009 г.)* (2009) 128–132.

Статья поступила 23.10.2012.