Math-Net.Ru

Общероссийский математический портал

И. В. Кучеренко, О числе обратимых однородных структур, *Дискрет. матем.*, 2003, том 15, выпуск 2, 123–127

DOI: <https://doi.org/10.4213/dm199>

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., 15:22:13

О числе обратимых однородных структур

© 2003 г. И. В. Кучеренко

В статье оценивается число $r(n, m)$ функций n -значной логики от $m + 1$ переменного, которые являются локальными функциями переходов обратимых однородных структур с произвольным фиксированным шаблоном соседства, состоящим из m векторов. Из полученных результатов следует, что при $n \rightarrow \infty$

$$\ln r(n, m) \sim n^{m+1} \ln n$$

равномерно по m .

Работа выполнена при поддержке Российского фонда фундаментальных исследований, проект 02-01-00162.

1. Введение

Важный класс однородных структур образуют обратимые однородные структуры, то есть такие, в которых предыстория возникновения конфигурации определяется однозначно. Такие однородные структуры играют в теории однородных структур роль, аналогичную роли групп перестановок в k -значной логике. Эти объекты имеют много приложений, в том числе в вопросах защиты информации.

В статье исследуется число обратимых однородных структур. Приводятся верхняя и нижняя оценки, из которых извлекается асимптотика поведения логарифма этой величины.

2. Основные понятия и результаты

В статье используются следующие определения из монографии [1]. Однородная структура σ есть четверка $(\mathbf{Z}^k, E_n, V, \varphi)$, где $\mathbf{Z}^k$ — совокупность всех k -мерных векторов с целочисленными координатами, $E_n = \{0, 1, \dots, n-1\}$, $V = \{v_1, \dots, v_m\}$ — упорядоченный набор различных ненулевых векторов из $\mathbf{Z}^k$, $\varphi: (E_n)^{m+1} \rightarrow E_n$, $\varphi(0, \dots, 0) = 0$. Элементы множества $\mathbf{Z}^k$ называются ячейками, элементы множества E_n — состояниями ячеек, 0 — состоянием покоя. При помощи шаблона соседства V каждой ячейке α ставится в соответствие набор

$$V(\alpha) = \{\alpha, \alpha + v_1, \alpha + v_2, \dots, \alpha + v_m\},$$

который называется ее окрестностью. Функция φ называется локальной функцией переходов однородной структуры σ . Функции $g: \mathbf{Z}^k \rightarrow E_n$ называются состояниями однородной структуры. Основная функция переходов Φ задается как отображение множества

всех состояний однородной структуры σ в себя, причем, если $g = \Phi(g')$, то для всех α

$$g(\alpha) = \varphi(g'(\alpha), g'(\alpha + v_1), g'(\alpha + v_2), \dots, g'(\alpha + v_m)).$$

Функционирование однородной структуры определяется как последовательность ее состояний $g_0, g_1, g_2, \dots$, получающаяся в результате применения основной функции переходов к некоторому ее состоянию g_0 , то есть

$$g_{t+1} = \Phi(g_t), \quad t = 0, 1, \dots$$

Состояние однородной структуры, у которого лишь конечное число ячеек находится в нулевом состоянии, называется конфигурацией.

Для исследования локальных свойств однородных структур вместо всего множества Z^k рассматриваются некоторые его подмножества. Конечные непустые множества ячеек однородной структуры σ называются ее блоками. Конфигурацией блока B называется ограничение некоторого состояния однородной структуры на этот блок, то есть функция

$$f: B \rightarrow E_n.$$

Окрестностью блока B называется блок

$$V(B) = \bigcup_{\alpha \in B} V(\alpha).$$

Введем ограничение основной функции переходов на блок B , получим функцию

$$\Phi|_B: V(B) \rightarrow B,$$

которая соответствует изменению конфигурации f блока B в результате функционирования однородной структуры, а именно, для всех $\alpha \in B$

$$\Phi|_B(f)(\alpha) = \varphi(f(\alpha), f(\alpha + v_1), f(\alpha + v_2), \dots, f(\alpha + v_m)).$$

Однородная структура называется обратимой, если для любой ее конфигурации g существует не более одной конфигурации g' такой, что $\Phi(g') = g$. Другими словами, каждая конфигурация как элемент области действия отображения Φ имеет не более одного прообраза, который также является конфигурацией.

Зафиксируем параметр k . Пусть V — некоторый шаблон соседства, число векторов в котором равно m . Обозначим через $r(n, m)$ число функций n -значной логики от $m + 1$ переменных, которые являются локальными функциями переходов обратимых однородных структур с данными размерностью множества ячеек и шаблоном соседства.

Теорема 1. *Справедлива оценка*

$$\frac{1}{n} (n!)^{n^m} \leq r(n, m) \leq \frac{n^{m+1}!}{(n^m!)^n}.$$

После преобразования к экспоненциальному виду этих оценок получаем следующее утверждение.

Следствие 1. *При $n \rightarrow \infty$*

$$\ln r(n, m) \sim n^{m+1} \ln n$$

равномерно по m .

3. Доказательства утверждений

Получим верхнюю оценку для $r(n, m)$. Воспользуемся теоремой 1.1.3 из [1], которая, как нетрудно убедиться, допускает следующую переформулировку в терминах обратимых однородных структур.

Теорема 2. Однородная структура σ является обратимой тогда и только тогда, когда для любой конфигурации f любого блока B число конфигураций g блока $V(B)$, удовлетворяющих соотношению

$$\Phi|_B(g) = f,$$

равно $n^{|V(B) \setminus B|}$, где $|V(B) \setminus B|$ — число ячеек блока $V(B) \setminus B$.

Рассмотрим блок, состоящий из одной ячейки. Тогда локальная функция переходов должна принимать каждое свое значение на одинаковом числе значений аргумента. Найдем число $|\{\varphi\}|$ таких функций. Нетрудно видеть, что

$$\begin{aligned} |\{\varphi\}| &= \binom{n^{m+1}}{n^m} \binom{n^{m+1} - n^m}{n^m} \cdots \binom{n^{m+1} - (n-1)n^m}{n^m} \\ &= \frac{n^{m+1}!}{n^m!(n^{m+1} - n^m)!} \frac{(n^{m+1} - n^m)!}{n^m!(n^{m+1} - 2n^m)!} \cdots \frac{(n^{m+1} - (n-1)n^m)!}{n^m!0!}, \end{aligned}$$

откуда

$$r(n, m) \leq \frac{n^{m+1}!}{(n^m!)^n}.$$

Найдем верхнюю оценку в экспоненциальной форме. Применяя формулу Стирлинга, находим, что

$$\begin{aligned} \ln r(n, m) &\leq \ln \frac{n^{m+1}!}{(n^m!)^n} = \ln(n^{m+1}!) - n \ln n^m \\ &= n^{m+1} \ln n^{m+1} - n^{m+1} + \frac{1}{2} \ln(2\pi n^{m+1}) + O\left(\frac{1}{n^{m+1}}\right) \\ &\quad - \left(n^m \ln n^m - n^m + \frac{1}{2} \ln(2\pi n^m) + O\left(\frac{1}{n^m}\right)\right), \end{aligned}$$

откуда получаем, что

$$\ln r(n, m) \leq \left(n^{m+1} - \frac{nm}{2} + \frac{m}{2} + \frac{1}{2}\right) \ln n - \frac{n-1}{2} \ln(2\pi) + O\left(\frac{1}{n^{m-1}}\right). \quad (1)$$

Найдем нижнюю оценку. Рассмотрим однородную структуру $\sigma = (\mathbf{Z}^k, E_n, V, \varphi)$, где шаблон соседства V состоит из векторов $v_i = (v_i^1, \dots, v_i^k)$, $i = 1, \dots, m$. Без ограничения общности будем считать, что

$$|v_m| = \sqrt{(v_m^1)^2 + \dots + (v_m^k)^2} \geq |v_i|, \quad i < m.$$

Определим φ так, чтобы для каждого набора $(a_0, a_1, \dots, a_{m-1})$ функция

$$\varphi(a_0, a_1, \dots, a_{m-1}, x)$$

аргумента x являлась перестановкой. Это можно сделать $n!$ способами для ненулевых наборов и $(n - 1)!$ способами для нулевого наборов (так как $\varphi(0, \dots, 0) = 0$). Число таких функций φ равно

$$(n!)^{n^m-1} (n - 1)! = \frac{1}{n} (n!)^{n^m} \leq r(n, m).$$

Возьмем произвольную конфигурацию K однородной структуры σ . Предположим, что она имеет прообраз K_1 , являющийся конфигурацией.

Рассмотрим некоторую ячейку $\theta \in \mathbb{Z}^k$. Проведем через нее прямую l в направлении v_m . Выберем на прямой аффинную систему координат с началом в точке θ с базисным вектором v_m . Введем отношение эквивалентности на множестве всех ячеек: будем считать, что $\alpha_1 \sim \alpha_2$, если координаты ортогональных проекций α_1 и α_2 на прямую l совпадают. Множество $\mathbb{Z}^k$ распадается на классы эквивалентности, причем их число будет счетным, так как множество $\mathbb{Z}^k$ счетно. Построим соответствие между полученным множеством классов и множеством целых чисел, причем классу, содержащему ячейку θ , присвоим номер 0, а остальные классы пронумеруем в порядке возрастания координаты проекций их элементов на l . Далее номером ячейки будем называть номер класса, к которому она принадлежит.

Возьмем число $D \in \mathbb{Z}$ так, чтобы номер любой ячейки, имеющей ненулевое состояние в конфигурации K , был не меньше D . Предположим, что существует ячейка с ненулевым состоянием в конфигурации K_1 и номером, меньшим D . Выберем из множества таких ячеек одну, имеющую наименьший номер. Обозначим эту ячейку через β . Ячейка $\beta - v_m$ имеет номер, меньший номера β . Ее состояние в конфигурации K , равное

$$K(\beta - v_m) = \varphi(0, \dots, K_1(\beta)),$$

отлично от нулевого, что невозможно в силу выбора числа D . Следовательно, прообраз K не может иметь ячеек с ненулевыми состояниями и номером, меньшим D .

Далее, пусть известны состояния всех ячеек K_1 с номером, меньшим заданного $h \in \mathbb{Z}$. Рассмотрим ячейку γ с номером h . В силу того, что

$$|v_m| \geq |v_i|, \quad i < m,$$

и шаблон соседства не может содержать одинаковых векторов, номера ячеек

$$\gamma - v_m, \gamma - v_m + v_1, \gamma - v_m + v_2, \dots, \gamma - v_m + v_{m-1}$$

меньше h . Для значения состояния ячейки γ в конфигурации K_1 получаем соотношение

$$K_1(\gamma) = \varphi|_{(K_1(\gamma-v_m), K_1(\gamma-v_m+v_1), \dots, K_1(\gamma-v_m+v_{m-1}))}^{-1}(K(\gamma - v_m)),$$

из которого K_1 определяется однозначно. Заметим, что K_1 может оказаться не конфигурацией, в таком случае K не имеет прообразов-конфигураций.

Предположим, что конфигурации K_1 и K_2 являются прообразами K . Пусть β — ячейка с наименьшим номером, для которой $K_1(\beta) \neq K_2(\beta)$. Тогда

$$\begin{aligned} & \varphi(K_1(\beta), K_1(\beta + v_1), \dots, K_1(\beta + v_{m-1}), K_1(\beta + v_n)) \\ &= \varphi(K_2(\beta), K_2(\beta + v_1), \dots, K_2(\beta + v_{m-1}), K_1(\beta + v_n)) \\ &\neq \varphi(K_2(\beta), K_2(\beta + v_1), \dots, K_2(\beta + v_{m-1}), K_2(\beta + v_n)), \end{aligned}$$

что противоречит выбору β . Следовательно, $K_1 \equiv K_2$.

Найдем нижнюю оценку в экспоненциальной форме. Справедливы соотношения

$$\begin{aligned} \ln r(n, m) &\geq \ln((n!)^{n^m} / n) = n^m \ln(n!) - \ln n \\ &= n^m \left(n \ln n - n + \frac{1}{2} \ln(2\pi n) + O\left(\frac{1}{n}\right) \right), \end{aligned}$$

откуда следует, что

$$\ln r(n, m) \geq (n^{m+1} + n^m/2) \ln n = \frac{n^m}{2} \ln(2\pi) - n^{m+1} + O(n^{m-1}). \quad (2)$$

Из неравенств (1) и (2) следуют соотношения

$$n^{n^{m+1}} e^{-n^{m+1}} \lesssim r(n, m) \lesssim n^{n^{m+1}} n^{n(m-1)/2}.$$

При $n \rightarrow \infty$ из (1) и (2) получаем, что

$$\ln r(n, m) \sim n^{m+1} \ln n.$$

Нетрудно видеть, что это соотношение выполняется равномерно по m .

Список литературы

1. Кудрявцев В. Б., Подколзин А. С., Болотов А. А., *Основы теории однородных структур*. Наука, Москва, 1990.
2. Кудрявцев В. Б., Алешин С. В., Подколзин А. С., *Введение в теорию автоматов*. Наука, Москва, 1985.

Статья поступила 10.10.2002.