Новые по порядку экспоненциальные темпы роста

С. А. Комков[1]

Для конечного множества A с заданным на нем множеством операций M определена функция $d_{(A,M)}(n)$, называемая темпом роста. Порядок роста этой функции характеризует силу и исчислимость множества операций. Известно, что темп роста принадлежит либо классу $O(n^k)$ для некоторого $k \in \mathbb{N}$, либо классу $2^{\Theta(n)}$. В работе исследуются классы экспоненциальных темпов роста, на которые разбиваются темпы роста из класса $2^{\Theta(n)}$ при выносе асимптотического ограничения из показателя. Показано, что для любых заранее заданных натуральных k и c существует такая пара (A, M), что $d_{(A,M)}(n) \in \Theta(n^k \cdot c^n)$. Если дополнительно $c \geqslant k+1$, то существует такая пара (A, M), что $d_{(A,M)}(n) \in \Theta(\log n \cdot n^k \cdot c^n)$.

Ключевые слова: темп роста, генерирующие множества, конечные множества, EGP.

1. Введение

Рассмотрим декартову степень $n \in \mathbb{N}$ конечного множества A с заданным на нём множеством операций M. Элементы A^n будем называть наборами. Применяя операции из M к уже имеющимся наборам покоординатно, мы можем получать новые наборы:

$$\begin{pmatrix} a_1^1 \\ \vdots \\ a_n^1 \end{pmatrix}, \ldots, \begin{pmatrix} a_1^k \\ \vdots \\ a_n^k \end{pmatrix} \to \begin{pmatrix} f(a_1^1,\ldots,a_1^k) \\ \vdots \\ f(a_n^1,\ldots,a_n^k) \end{pmatrix}, \ f \in M.$$

Темпом роста для пары (A, M) называют функцию $d_{(A,M)}(n),\ n \in \mathbb{N}$, равную для каждого n минимальному числу наборов, из которых можно получить всё A^n, применяя операции из M покоординатно. Таким образом, асимптотика темпа роста характеризует силу и исчислимость заданного множества операций.

Пример 1. Пусть $A = \{0, 1\}$, $M = \{\neg\}$. Тогда $d_{(A,M)}(n) = 2^{n-1}$.

Пример 2. Пусть $A = \{0, 1, 2\}$, $M = \{+_{\mathrm{mod}\ 3}\}$. Тогда $d_{(A,M)}(n) = n$.

[1] *Комков Степан Алексеевич* — аспирант каф. математической теории интеллектуальных систем мех.-мат. ф-та МГУ, e-mail: stepan.komkov@intsys.msu.ru.

Komkov Stepan Alekseevich — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Mathematical Theory of Intellectual Systems.

Множество наборов, из которых можно получить всё A^n, применяя операции из M, называют *генерирующим множеством для A^n по операциям из M*. Если при этом мощность этого множества равна $d_{(A,M)}(n)$, то это *минимальное генерирующее множество.*

Темп роста — не просто количественная характеристика. От темпа роста может зависеть тип решаемой задачи. Так, например, в [1] показано, что подкванторная задача удовлетворения ограничений (QSCP) сводится к обычной задаче удовлетворения ограничений (SCP) в случае если алгебра, задающая язык ограничений, имеет темп роста из класса $O(n^k)$ для некоторого $k \in \mathbb{N}$.

Изучение темпов роста началось с работ Джеймса Уиголда, посвящённых темпам роста конечных групп. В [9, 10, 11] он показал, что темп рост произвольной нетривиальной совершенной конечной группы принадлежит классу $\Theta(\log n)$, а темп роста произвольной несовершенной конечной группы — классу $\Theta(n)$.

Возможные темпы роста для конечных полугрупп [12] отличаются от темпов роста для конечных групп. Если конечная полугруппа содержит нейтральный элемент, то её темп роста принадлежит классу $\Theta(n)$. В противном случае её темп роста принадлежит классу $2^{\Theta(n)}$.

Полученные результаты для конечных групп были обобщены на другие классические конечные алгебраические структуры [8]. Оказалось, что темпы роста нетривиальных колец, модулей, алгебр и алгебра Ли также принадлежат одному из классов $\Theta(\log n)$ или $\Theta(n)$.

Возникает закономерный вопрос о существовании таких пар (A, M), что $d_{(A,M)}(n)$ не принадлежит ни одному из классов $\Theta(\log n)$, $\Theta(n)$ или $2^{\Theta(n)}$. Оказалось, что такие пары существуют. В [2] показано, что для любого $k \in \mathbb{N}$ существует такая пара (A, M), что $d_{(A,M)}(n) \in \Theta(n^k)$.

В [3, 4] обобщены результаты для классических алгебраических структур на случай конечных множеств с некоторыми ограничениями на множества заданных на них операций. Однако, полученные критерии вновь разбивают возможные темпы роста на классы $\Theta(\log n)$, $\Theta(n)$ или $2^{\Theta(n)}$.

В [14] показано, что темп роста принадлежит либо классу $O(n^k)$ для некоторого $k \in \mathbb{N}$, либо классу $2^{\Theta(n)}$. Актуален вопрос о существовании темпов роста, принадлежащих одновременно классам $\omega(\log n)$ и $o(n)$.

В [6] найдены все возможные темпы роста пар вида (E_2, M). В этом случае темпы роста асимптотически равны одной из функций: $\log n$, n, 2^n, 2^{n-1}.

Возникает вопрос о дальнейшем уточнении порядков и асимптотик возможных темпов роста. Так, например, среди пар (A, M), чей темп роста принадлежит классу $\Theta(\log n)$, можно выделить пары с *минимальным логарифмическим* темпом роста. Это такие пары, для которых

$d_{(A,M)}(n) - \log_{|A|} n \in O(1)$. Существуют критерии минимального логарифмического темпа роста [7, 5].

В данный момент все экспоненциальные темпы роста группируются в один класс, где асимптотически ограничен показатель экспоненты. Возникает вопрос о выносе асимптотического ограничения из показателя экспоненты. В настоящей работе показано, что для любых заранее заданных натуральных k и c существует такая пара (A, M), что $d_{(A,M)}(n) \in \Theta(n^k \cdot c^n)$. Если дополнительно $c \geqslant k+1$, то существует такая пара (A, M), что $d_{(A,M)}(n) \in \Theta(\log n \cdot n^k \cdot c^n)$.

Исследование выполнено при поддержке Междисциплинарной научно-образовательной школы Московского университета «Мозг, когнитивные системы, искусственный интеллект».

2. Формулировка и доказательство основных результатов

Приведем некоторые общеизвестные результаты, которые нам понадобятся:

Замечание 1. $d_{(A,M)} = d_{(A,[M])}$, где $[\cdot]$ — замыкание по операциям суперпозиции, A и M — произвольные.

Замечание 2. $d_{(A,M)} = d_{(A,M\cup\{x\})}$, где x — тождественная функция, A и M — произвольные.

Для биномиального распределения известна оценка вероятности того, что сумма превосходит математическое ожидание на заранее заданную величину x:

Теорема. *(Граница Чернова [13]) Пусть $B(n,p)$ — биномиальное распределение с вероятностью успеха p и числом испытаний n. Тогда $P(B(n,p) > n \cdot p + x) \leqslant \exp\left(\frac{-x^2}{2\cdot n\cdot p\cdot(1-p)}\right)$.*

Сформулируем и докажем вспомогательные леммы:

Лемма 1. *Пусть $f(n) > 0$, $f(0) = 1$ и $f(n) \in \Theta\left((\log n)^m \cdot n^k \cdot t^n\right)$, $n \to \infty$, где $m, k \in \mathbb{Z}_+$, $t \in \mathbb{N}$. Тогда для любого $c \in \mathbb{N}$ верно, что $\sum_{l=0}^{n} C_n^l \cdot c^{n-l} \cdot f(l) \in \Theta\left((\log n)^m \cdot n^k \cdot (c+t)^n\right)$, $n \to \infty$.*

Доказательство. Так как $f(n) > 0$ и $f(n) \in \Theta\left((\log n)^m \cdot n^k \cdot t^n\right)$, $n \to \infty$, то существуют такие p, $P > 0$, что $p\cdot(\log n)^m \cdot n^k \cdot t^n \leqslant f(n) \leqslant P\cdot(\log n)^m \cdot n^k \cdot t^n$. Тогда при достаточно большом n выполняется:

$$\sum_{l=0}^{n} C_n^l \cdot c^{n-l} \cdot f(l) \geqslant \sum_{l=0}^{n} \frac{n!}{l!\cdot(n-l)!} \cdot c^{n-l} \cdot p \cdot (\log l)^m \cdot l^k \cdot t^l \geqslant$$

$$\geqslant p \cdot \left(\log\left(\frac{t \cdot (n-k)}{2 \cdot (t+c)} + k\right)\right)^m \cdot \sum_{l=\lfloor \frac{t\cdot(n-k)}{2\cdot(t+c)}+k\rfloor+1}^{n} \frac{n!}{l! \cdot (n-l)!} \cdot c^{n-l} \cdot l^k \cdot t^l \geqslant$$

$$\geqslant p \cdot \left(\log \frac{t \cdot (n-k)}{2 \cdot (t+c)}\right)^m \cdot n \cdot (n-1) \cdot \ldots \cdot (n-k+1) \cdot t^k \cdot$$

$$\cdot \sum_{l=\lfloor \frac{t\cdot(n-k)}{2\cdot(t+c)}+k\rfloor+1}^{n} \frac{(n-k)!}{l! \cdot (n-l)!} \cdot c^{n-l} \cdot l^k \cdot t^{l-k} \geqslant$$

$$\geqslant p \cdot \left(\log \frac{t \cdot n}{4 \cdot (t+c)}\right)^m \cdot (n-k)^k \cdot$$

$$\cdot \sum_{l=\lfloor \frac{t\cdot(n-k)}{2\cdot(t+c)}+k\rfloor+1}^{n} \frac{(n-k)!}{(l-k)! \cdot (n-l)!} \cdot c^{n-l} \cdot t^{l-k} \geqslant$$

$$\geqslant p \cdot \left(\log n - \log \frac{4 \cdot (t+c)}{t}\right)^m \cdot (n-k)^k \cdot (c+t)^{n-k} \cdot$$

$$\cdot \sum_{l=\lfloor \frac{t\cdot(n-k)}{2\cdot(t+c)}+k\rfloor+1}^{n} C_{n-k}^{l-k} \cdot \left(\frac{c}{c+t}\right)^{n-l} \cdot \left(\frac{t}{c+t}\right)^{l-k} =$$

$$= p \cdot \left(\log n - \log \frac{4 \cdot (t+c)}{t}\right)^m \cdot (n-k)^k \cdot (c+t)^{n-k} \cdot$$

$$\cdot \sum_{l=\lfloor \frac{t\cdot(n-k)}{2\cdot(t+c)}\rfloor+1}^{n-k} C_{n-k}^{l} \cdot \left(\frac{c}{c+t}\right)^{n-k-l} \cdot \left(\frac{t}{c+t}\right)^{l} =$$

$$= p \cdot \left(\log n - \log \frac{4 \cdot (t+c)}{t}\right)^m \cdot (n-k)^k \cdot (c+t)^{n-k} \cdot$$

$$\cdot P\left(B(n-k, \frac{t}{c+t}) \geqslant \left\lfloor \frac{t \cdot (n-k)}{2 \cdot (t+c)} \right\rfloor + 1\right).$$

Оценим вероятность для достаточно больших n, используя границу Чернова:

$$P\left(B(n-k, \frac{t}{c+t}) \geqslant \left\lfloor \frac{t \cdot (n-k)}{2 \cdot (t+c)} \right\rfloor + 1\right) =$$

$$= P\left(B(n-k, \frac{t}{c+t}) > \left\lfloor \frac{t\cdot(n-k)}{2\cdot(t+c)} \right\rfloor\right) =$$

$$= \left(1 - P\left(B(n-k, \frac{t}{c+t}) \leqslant \left\lfloor \frac{t\cdot(n-k)}{2\cdot(t+c)} \right\rfloor\right)\right) =$$

$$= \left(1 - P\left(B(n-k, \frac{c}{c+t}) > n-k-\left\lceil \frac{t\cdot(n-k)}{2\cdot(t+c)} \right\rceil\right)\right) \geqslant$$

$$\geqslant \left(1 - P\left(B(n-k, \frac{c}{c+t}) > n-k-\frac{t\cdot(n-k)}{2\cdot(t+c)}\right)\right) =$$

$$= \left(1 - P\left(B(n-k, \frac{c}{c+t}) > \frac{c}{c+t}\cdot(n-k)+\frac{t\cdot(n-k)}{2\cdot(c+t)}\right)\right) \geqslant$$

$$\geqslant \left(1 - \exp\left(\frac{-t^2\cdot(n-k)^2\cdot(t+c)^2}{2\cdot 4\cdot(c+t)^2\cdot(n-k)\cdot t\cdot c}\right)\right) =$$

$$= \left(1 - \exp\left(\frac{-t\cdot(n-k)}{8\cdot c}\right)\right) \geqslant \frac{1}{2}.$$

Получаем:

$$\sum_{l=0}^{n} C_n^l \cdot c^{n-l}\cdot f(l) \geqslant \frac{p}{2}\cdot\left(\log n - \log\frac{4\cdot(t+c)}{t}\right)^m \cdot$$
$$\cdot (n-k)^k\cdot(c+t)^{n-k} \in \Omega\left((\log n)^m\cdot n^k\cdot(c+t)^n\right).$$

Оценим сумму сверху:

$$\sum_{l=0}^{n} C_n^l \cdot c^{n-l}\cdot f(l) \leqslant \sum_{l=0}^{n}\frac{n!}{l!\cdot(n-l)!}\cdot c^{n-l}\cdot P\cdot(\log l)^m\cdot l^k\cdot t^l \leqslant$$

$$\leqslant P\cdot(\log n)^m\cdot\left(\sum_{l=0}^{k-1} C_n^l\cdot c^{n-l}\cdot l^k\cdot t^l + \right.$$
$$\left. + \sum_{l=k}^{n}\frac{n!}{(l-k)!\cdot(n-l)!}\cdot c^{n-l}\cdot\frac{l^k}{l\cdot\ldots\cdot(l-k+1)}\cdot t^l\right) \leqslant$$

$$\leqslant P\cdot(\log n)^m\cdot\left(k\cdot n^{k-1}\cdot c^n\cdot(k-1)^k\cdot t^{k-1} + \right.$$
$$\left. + L\cdot n^k\cdot t^k\cdot\sum_{l=k}^{n}\frac{(n-k)!}{(l-k)!\cdot(n-l)!}\cdot c^{n-l}\cdot t^{l-k}\right) \leqslant$$

$$\leqslant P \cdot (\log n)^m \cdot \Big(n^{k-1} \cdot c^n \cdot k^{k+1} \cdot t^{k-1} + \\ + L \cdot n^k \cdot t^k \cdot \sum_{l=0}^{n-k} \frac{(n-k)!}{l! \cdot (n-k-l)!} \cdot c^{n-k-l} \cdot t^l \Big) =$$

$$= P \cdot (\log n)^m \cdot \Big(n^{k-1} \cdot c^n \cdot k^{k+1} \cdot t^{k-1} + \\ + L \cdot n^k \cdot t^k \cdot (c+t)^{n-k} \Big) \in O\left((\log n)^m \cdot n^k \cdot (c+t)^n \right).$$

Здесь L — некоторая константа, ограничивающая последовательность $\frac{l^k}{l \cdot (l-1) \cdot \ldots \cdot (l-k+1)}$. Так как последовательность $\frac{l^k}{l \cdot (l-1) \cdot \ldots \cdot (l-k+1)}$, $l \geqslant k$, сходится при $l \to \infty$, то такая константа существует.

Следовательно, $\sum_{l=0}^{n} C_n^l \cdot c^{n-l} \cdot f(l) \in \Theta\left((\log n)^m \cdot n^k \cdot (c+t)^n \right)$, $n \to \infty$. □

Лемма 2. *Пусть $d_{(A,M)}(n)$ принадлежит одному из следующих классов: $\Theta(\log n)$, $n \to \infty$, или $\Theta(n^k)$, $n \to \infty$, для некоторого натурального k. Тогда для любого натурального c существует такая пара (B, M'), что $d_{(B,M')}(n) \in \Theta\left(d_{(A,M)}(n) \cdot c^n \right)$, $n \to \infty$.*

Доказательство. Случай, когда $c = 1$ тривиален. Достаточно взять $B = A$ и $M' = M$. Рассмотрим случаи, когда $c > 1$.

Рассмотрим множество $B = A \cup \{b_1, \ldots, b_c\}$, где $\{b_1, \ldots, b_c\}$ — такое множество, что $\{b_1, \ldots, b_c\} \cap A = \emptyset$. Зададим на множестве B множество операций M', сопоставив каждой функций $f(x_1, \ldots, x_n) \in M$ функцию

$$f'(x_1, \ldots, x_n) = \begin{cases} b_1, \text{ если } x_1 = \ldots = x_n = b_1, \\ \ldots \\ b_{c-1}, \text{ если } x_1 = \ldots = x_n = b_{c-1}, \\ f(x_1, \ldots, x_n), \ x_1, \ldots, x_n \in A, \\ b_c, \text{ иначе.} \end{cases}$$

Заметим, что в частности $f'(x_1, \ldots, x_n) = b_c$, если хотя бы один из x_i, $1 \leqslant i \leqslant n$, равен b_c.

Покажем, что $d_{(B,M')}(n) \in \Theta\left(d_{(A,M)}(n) \cdot c^n \right)$. Рассмотрим множество наборов $\overline{B} = (B \setminus \{b_c\})^n$. Рассмотрим набор $t \in \overline{B}$ у которого некоторые координаты равны b_1. Без утери общности будем считать, что это первые l координат. Допустим, что мы можем получить набор t из наборов $a^1, \ldots, a^m$ применяя операцию из M' покоординатно:

$$\begin{pmatrix} a_1^1 \\ \vdots \\ a_n^1 \end{pmatrix}, \ldots, \begin{pmatrix} a_1^m \\ \vdots \\ a_n^m \end{pmatrix} \to \begin{pmatrix} b_1 \\ \vdots \\ b_1 \\ t_{l+1} \\ \vdots \\ t_n \end{pmatrix}.$$

Тогда никакая a_i^j, $l+1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$, не принадлежит множеству $\{b_1, b_c\}$, иначе t_i для некоторого $i \in \{l+1, \ldots, n\}$ принадлежало бы множеству $\{b_1, b_c\}$. Также все a_i^j, $1 \leqslant i \leqslant l$, $1 \leqslant j \leqslant m$, равны b_1, иначе в результате не получилось бы b_1.

Таким образом, набор t можно получить только из таких наборов $\overline{B}$, что их множество координат со значением b_1 совпадает с множеством координат набора t со значением b_1.

Проводя аналогичные рассуждения для каждого из значений $b_2, \ldots, b_{c-1}$, а так же множества A, мы получаем, что наборы из $\overline{B}$ можно получить только из наборов $\overline{B}$ таких, что значения $b_1, \ldots, b_{c-1}$, а также значения из множества A встречаются в одних и тех же координатах.

Разобьем множество $\overline{B}$ на c^n классов эквивалентности. Согласно этому разбиению будем считать эквивалентными те наборы, у которых значения $b_1, \ldots, b_{c-1}$, а также значения из множества A встречаются в одних и тех же координатах. По вышеприведенным рассуждениям наборы из каждого построенного класса эквивалентности можно получить только из других наборов этого класса эквивалентности.

Рассмотрим класс эквивалентности ϵ, у которого значения из множества A встречаются в $l \geqslant 1$ координатах. Без утери общности будем считать, что это первые l координат.

Пусть X — генерирующее множество для B^n по операциям из M'. Рассмотрим подмножество наборов генерирующего множества X из класса эквивалентности ϵ. Это подмножество непустое, так как наборы класса эквивалентности ϵ нельзя получить ни из чего другого. Все наборы этого подмножества, а также наборы, которые мы из них получаем, совпадают в последних $n-l$ координатах. То есть, чтобы получить все возможные наборы класса эквивалентности ϵ, достаточно получить все возможные комбинации значений в первых l координатах внутри этого класса эквивалентности. На значениях из A операции из M' ведут себя также как операции множества M, из которых они были получены. Из этого следует, что в X должно быть не менее $d_{(A,M)}(l)$ наборов из класса эквивалентности ϵ.

Положим, что $d_{(A,M)}(0) = 1$. Тогда полученный вывод становится верным для случая $l = 0$.

Итого мощность множества X не меньше чем $\sum_{l=0}^{n} C_n^l \cdot (c-1)^{n-l} \cdot d_{(A,M)}(l)$. Здесь суммирование ведет по числу координат со значениями из множества A в классе эквивалентности. Вычет C_n^l соответствует количеству способов выбрать эти координаты. Для каждого выбранного множества координат существует $(c-1)^{n-l}$ способов сопоставить каждой из оставшихся координат одно из значений $b_1, \ldots, b_{c-1}$. Наконец, для каждого полученного класса эквивалентности в генерирующем множестве должно быть не менее $d_{(A,M)}(l)$ наборов из этого класса эквивалентности.

Покажем, что существует генерирующее множество размера $\sum_{l=0}^{n} C_n^l \cdot (c-1)^{n-l} \cdot d_{(A,M)}(l)$. В качестве его примера возьмем множество X, состоящее только из некоторых наборов множества $\overline{B}$. А именно, из каждого класса эквивалентности, в котором значения из A встречаются на l координатах, в X возьмем $d_{(A,M)}(l)$ таких наборов, что если отбросить из них координаты не из A, то оставшиеся наборы будут генерирующим множеством для A^l по операциям из M.

По построению множества X и определению классов эквивалентности из множества X заведомо можно получить все наборы из $\overline{B}$. Покажем, как из этих наборов теперь получить все наборы, содержащие значение b_c.

Без утери общности согласно замечаниям можно считать, что M — замкнутое множество, содержащее все селекторы. Значит, в частности M содержит селектор $g_1^2(x_1, x_2) = x_1$.

Рассмотрим произвольный набор $u \in B^n \setminus \overline{B}$. Без утери общности будем считать, что только первые l координат этого набора равны b_c. Тогда набор u можно получить из наборов $\overline{B}$ следующим образом:

$$g_1^{2\prime}\left(\begin{pmatrix} b_1 \\ \vdots \\ b_1 \\ u_{l+1} \\ \vdots \\ u_n \end{pmatrix}, \begin{pmatrix} a \\ \vdots \\ a \\ u_{l+1} \\ \vdots \\ u_n \end{pmatrix}\right) \to \begin{pmatrix} g_1^{2\prime}(b_1, a) \\ \vdots \\ g_1^{2\prime}(b_1, a) \\ g_1^{2\prime}(u_{l+1}, u_{l+1}) \\ \vdots \\ g_1^{2\prime}(u_n, u_n) \end{pmatrix} = \begin{pmatrix} b_c \\ \vdots \\ b_c \\ u_{l+1} \\ \vdots \\ u_n \end{pmatrix}.$$

Здесь a — произвольный элемент из A.

Итак, $\sum_{l=0}^{n} C_n^l \cdot (c-1)^{n-l} \cdot d_{(A,M)}(l)$ наборов необходимо и достаточно. Так как $\sum_{l=0}^{n} C_n^l \cdot (c-1)^{n-l} \cdot d_{(A,M)}(l) = \sum_{l=0}^{n} C_n^l \cdot (c-1)^{n-l} \cdot d_{(A,M)}(l) \cdot 1^l$, то по лемме 1 получаем, что $\sum_{l=0}^{n} C_n^l \cdot (c-1)^{n-l} \cdot d_{(A,M)}(l) \in \Theta\left(d_{(A,M)}(n) \cdot c^n\right)$, $n \to \infty$. □

Лемма 3. *Пусть $d_{(A,M)}(n)$ принадлежит классу: $\Theta(\log n \cdot n^k \cdot c^n)$, $n \to \infty$, где $k \in \mathbb{Z}_+$, $c \in \mathbb{N}$. Тогда существует такая пара (B, M'), что $d_{(B,M')}(n) \in \Theta(\log n \cdot n^{k+1} \cdot (c+1)^n)$, $n \to \infty$.*

Доказательство. Рассмотрим множество $B = A \cup \{-1, 0, 1\}$, где $\{-1, 0, 1\} \cap A = \emptyset$. Этого всегда можно добиться за счет переобозначения элементов множества A. Зададим на множестве B множество операций M', сопоставив каждой функции $f(x_1, \ldots, x_n) \in M$ две функции на множестве B:

$$f'(x_1, \ldots, x_n) = \begin{cases} 0, \text{ если } x_1 = \ldots = x_n = 0, \\ 1, \text{ если } x_1 = \ldots = x_n = 1, \\ f(x_1, \ldots, x_n), \ x_1, \ldots, x_n \in A, \\ -1, \text{ иначе;} \end{cases}$$

$$f''(x_1, \ldots, x_n) = \begin{cases} \max(x_1, \ldots, x_n), \text{ если } x_1, \ldots, x_n \in \{0, 1\}, \\ a, \text{ если } x_1 = \ldots = x_n = a \in A, \\ -1, \text{ иначе.} \end{cases}$$

Заметим, что в частности $f'(x_1, \ldots, x_n) = -1$ и $f''(x_1, \ldots, x_n) = -1$, если хотя бы один из x_i, $1 \leqslant i \leqslant n$, равен -1.

Покажем, что $d_{(B,M')}(n) \in \Theta(\log n \cdot n^{k+1} \cdot (c+1)^n)$, $n \to \infty$. Рассмотрим набор t, у которого все координаты принадлежат множеству $A \cup \{0\}$. Без утери общности будем считать, что только первые l координат принадлежат множеству A. Допустим, что мы можем получить набор t из наборов $a^1, \ldots, a^m$ применяя операцию из M' покоординатно:

$$\begin{pmatrix} a_1^1 \\ \vdots \\ a_n^1 \end{pmatrix}, \ldots, \begin{pmatrix} a_1^m \\ \vdots \\ a_n^m \end{pmatrix} \to \begin{pmatrix} t_1 \\ \vdots \\ t_l \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Если набор получен с помощью операции вида f'', то $a_i^1 = \ldots = a_i^m = t_i$, $1 \leqslant i \leqslant l$, так как $t_i \in A$, $1 \leqslant i \leqslant l$. Также $a_i^1 = \ldots = a_i^m = 0$, $l+1 \leqslant i \leqslant n$, так как эти элементы должны принадлежать множеству $\{0, 1\}$, и их максимум должен быть равен нулю. Следовательно, с помощью операций операций вида f'' набор t из неравных ему наборов получен быть не может.

Если набор получен с помощью операции вида f', то $a_i^1 = \ldots = a_i^m \in A$, $1 \leqslant i \leqslant l$, так как $t_i \in A$, $1 \leqslant i \leqslant l$. Также $a_i^1 = \ldots = a_i^m = 0$, $l+1 \leqslant i \leqslant n$ по определению операций вида f'.

Итак, наборы, у которых все координаты принадлежат множеству $A \cup \{0\}$, могут быть получены только из таких неравных им наборов, у которых ровно те же координаты равны 0, а остальные координаты из множества A.

Рассмотрим набор t, у которого все координаты кроме одной принадлежат множеству $A \cup \{0\}$. Оставшаяся же координата равняется 1. Без утери общности будем считать, что только первые l координат принадлежат множеству A, а последняя координата равна 1. Допустим, что мы можем получить набор t из наборов $a^1, \ldots, a^m$ применяя операцию из M' покоординатно:

$$\begin{pmatrix} a_1^1 \\ \vdots \\ a_n^1 \end{pmatrix}, \ldots, \begin{pmatrix} a_1^m \\ \vdots \\ a_n^m \end{pmatrix} \to \begin{pmatrix} t_1 \\ \vdots \\ t_l \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

Если набор получен с помощью операции вида f'', то $a_i^1 = \ldots = a_i^m = t_i$, $1 \leqslant i \leqslant l$, так как $t_i \in A$, $1 \leqslant i \leqslant l$. Также $a_i^1 = \ldots = a_i^m = 0$, $l+1 \leqslant i \leqslant n-1$, так как эти элементы должны принадлежать множеству $\{0, 1\}$, и их максимум должен быть равен нулю. Наконец, хотя бы одна из $a_n^1, \ldots, a_n^m$ должна быть равна 1, чтобы их максимум равнялся 1. Следовательно, с помощью операций вида f'' набор t из неравных ему наборов получен быть не может.

Если набор получен с помощью операции вида f', то $a_i^1 = \ldots = a_i^m \in A$, $1 \leqslant i \leqslant l$, так как $t_i \in A$, $1 \leqslant i \leqslant l$. Также $a_i^1 = \ldots = a_i^m = 0$, $l + 1 \leqslant i \leqslant n - 1$, и $a_n^1 = \ldots = a_n^m = 1$ по определению операций вида f'.

Итак, наборы, у которых все координаты принадлежат множеству $A \cup \{0\}$ кроме одной единичной координаты, могут быть получены только из таких неравных им наборов, у которых ровно те же координаты равны 0, совпадает единичная координата, а остальные координаты из множества A.

Рассмотрим множество $K \subset B^n$, состоящее из наборов, где l фиксированных координат принадлежат множеству A, а все остальные координаты равны 0, за исключением, быть может, одной фиксированной координаты, равной 1. Без утери общности будем полагать, что первые l координат принадлежат множеству A.

Пусть X — генерирующее множество для B^n по операциям из M'. Множество $K \cap X$ — непустое, так как наборы множества K нельзя получить ни из чего другого. Все наборы множества K, а также наборы, которые мы из них получаем, совпадают в последних $n - l$ координатах. То есть, чтобы получить все возможные наборы множества K, достаточно получить все возможные комбинации значений в первых l координатах. На значениях из A операции вида f' из M' ведут себя также как операции множества M, из которых они были получены. С помощью операций вида f'' из M' получить новые наборы из A^n невозможно. Из этого следует, что в X должно быть не менее $d_{(A,M)}(l)$ наборов из множества K.

Положим, что $d_{(A,M)}(0) = 1$. Тогда полученный вывод становится верным для случая $l = 0$.

Просуммируем необходимое число наборов в генерирующем множестве X для каждого множества, состоящего из наборов, где l фиксированных координат принадлежат множеству A, а все остальные координаты равны 0, за исключением, быть может, одной фиксированной координаты, равной 1. Итого мощность множества X не меньше чем $\sum_{l=0}^{n} C_n^l \cdot (n-l+1) \cdot d_{(A,M)}(l)$. Здесь суммирование ведет по числу координат со значениями из множества A. Вычет C_n^l соответствует количеству способов выбрать эти координаты. Для каждого выбранного множества координат из множества A существует $(n-l)$ способ выбрать среди оставшихся координат единичную координату и один способ назначить все оставшиеся координаты нулевыми. Наконец, для каждого полученного разбиения координат на множества координат из A, нулевых координат и единичной координаты в генерирующем множестве должно быть не менее $d_{(A,M)}(l)$ наборов.

Покажем, что существует генерирующее множество размера $\sum_{l=0}^{n} C_n^l \cdot (n-l+1) \cdot d_{(A,M)}(l)$. Из каждого множества, состоящего из наборов, где l фиксированных координат принадлежат множеству A, а все остальные координаты равны 0, за исключением, быть может, одной фиксированной координаты, равной 1, возьмем $d_{(A,M)}(l)$ таких наборов, что если отбросить из них координаты не из A, то оставшиеся наборы будут генерирующим множеством для A^l по операциям из M. Покажем, что полученное множество X будет генерирующим множеством.

По построению множества X из множества X заведомо можно получить все наборы, где l фиксированных координат принадлежат множеству A, а все остальные координаты равны 0, за исключением, быть может, одной фиксированной координаты, равной 1. Покажем, как из этих наборов теперь получить все наборы множества B^n.

Сначала получим все наборы, чьи координаты принадлежат множеству $A \cup \{0, 1\}$, при этом 1 встречает более одного раза. Обозначим это множество B_1.

Рассмотрим произвольный набор $t \in B_1$ из описанного класса. Без утери общности будем считать, что только первые l координат этого набора принадлежат множеству A, и только последние p координат равны 1. Также без утери общности согласно замечаниям можно считать, что M — замкнутое множество, содержащее все селекторы. Значит, в частности M содержит селектор $g_1^p(x_1, \dots, x_p) = x_1$. Тогда, так как $t_i \in A$, $1 \leqslant i \leqslant l$, набор t можно получить с помощью операции $g_1^{p''}$ из следующих уже имеющихся наборов:

$$\begin{pmatrix} t_1 \\ \vdots \\ t_l \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} t_1 \\ \vdots \\ t_l \\ 0 \\ \vdots \\ 0 \\ 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} t_1 \\ \vdots \\ t_l \\ 0 \\ \vdots \\ 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \to \begin{pmatrix} t_1 \\ \vdots \\ t_l \\ 0 \\ \vdots \\ 0 \\ 1 \\ 1 \\ \vdots \\ 1 \\ 1 \end{pmatrix}.$$

Итак, из множества X можно получить все наборы без -1. Наборы, содержащие -1, можно получить аналогично получению наборов, содержащих b_c, в доказательстве леммы 2.

Получаем, что $\sum_{l=0}^{n} C_n^l \cdot (n-l+1) \cdot d_{(A,M)}(l)$ наборов необходимо и достаточно. С помощью леммы 1 получаем, что

$$\sum_{l=0}^{n} C_n^l \cdot (n-l+1) \cdot d_{(A,M)}(l) =$$

$$= \sum_{l=0}^{n} C_n^l \cdot (n-l) \cdot d_{(A,M)}(l) + \sum_{l=0}^{n} C_n^l \cdot d_{(A,M)}(l) =$$

$$= n \cdot \sum_{l=0}^{n-1} C_{n-1}^l \cdot 1^{n-l} \cdot d_{(A,M)}(l) +$$

$$+ \sum_{l=0}^{n} C_n^l \cdot 1^{n-l} \cdot d_{(A,M)}(l) \in n \cdot \Theta(\log n \cdot n^k \cdot (c+1)^n) =$$

$$= \Theta(\log n \cdot n^{k+1} \cdot (c+1)^n),\ n \to \infty.$$

□

Теорема 1. *Для любых $k, c \in \mathbb{N}$ существует такая пара (A, M), что $d_{(A,M)}(n) \in \Theta(n^k \cdot c^n)$, $n \to \infty$. Если дополнительно $c \geqslant k+1$, то существует такая пара (A, M), что $d_{(A,M)}(n) \in \Theta(\log n \cdot n^k \cdot c^n)$, $n \to \infty$.*

Доказательство. Как показано в [2], для любого $k \in \mathbb{N}$ существует такая пара (A, M), что $d_{(A,M)}(n) \in \Theta(n^k)$, $n \to \infty$. По лемме 2 для любого $c \in \mathbb{N}$ существует такая пара (B, M'), что $d_{(B,M')(n)} \in \Theta\left(d_{(A,M)}(n) \cdot c^n\right) = \Theta\left(n^k \cdot c^n\right)$, $n \to \infty$. Тем самым доказана первая часть теоремы.

Допустим, что $c \geqslant k+1$. По лемме 2 существует такая пара (A, M), что $d_{(A,M)}(n) \in \Theta(\log n \cdot (c-k)^n)$, $n \to \infty$. Применяя k раз лемму 3, получаем такую пару (B, M'), что $d_{(B,M')(n)} \in \Theta\left(\log n \cdot n^k \cdot (c-k+k)^n\right) = \Theta\left(\log n \cdot n^k \cdot c^n\right)$, $n \to \infty$. Тем самым доказана вторая часть теоремы. □

Список литературы

[1] С. А. Комков, “Мощности генерирующих множеств по операциям из классов решетки Поста”, *Дискрет. матем.*, **30**:1 (2018), 19–38; *Discrete Math. Appl.*, **29**:3 (2019), 159–173.

[2] С. А. Комков, “Новая формулировка критерия минимального логарифмического темпа роста”, *Вестн. Моск. ун-та. Сер. 1. Матем., мех.*, 2020, № 5, 60–62; *Moscow University Mathematics Bulletin, Moscow University Mechanics Bulletin*, **75**:5 (2020), 220–221.

[3] С. А. Комков, “О классах функций многозначной логики с минимальным логарифмическим темпом роста”, *Дискрет. матем.*, **31**:3 (2019), 47–57; *Discrete Math. Appl.*, **30**:4 (2020), 265–272.

[4] Chen H., “Quantified constraint satisfaction and the polynomially generated powers property”, International Colloquium on Automata, Languages, and Programming, 2008, 197–208.

[5] Kearnes K. A., Kiss E. W., Szendrei Á., “Growth rates of algebras, I: Pointed cube terms”, *Journal of the Australian Mathematical Society*, **101**:1 (2016), 56–94.

[6] Kearnes K. A., Kiss E. W., Szendrei Á., “Growth rates of algebras, II: Wiegold dichotomy”, *International Journal of Algebra and Computation*, **25**:4 (2015), 555–566.

[7] Kearnes K. A., Kiss E. W., Szendrei Á., “Growth rates of algebras, III: finite solvable algebras”, *Algebra universalis*, **76**:2 (2016), 199–222.

[8] Quick M., Ruškuc N., “Growth of generating sets for direct powers of classical algebraic structures”, *Journal of the Australian Mathematical Society*, **89**:1 (2010), 105–126.

[9] Wiegold J., “Growth sequences of finite groups”, *Journal of the Australian Mathematical Society*, **17**:2 (1974), 133–141.

[10] Wiegold J., “Growth sequences of finite groups II”, *Journal of the Australian Mathematical Society*, **20**:2 (1975), 225–229.

[11] Wiegold J., “Growth sequences of finite groups III”, *Journal of the Australian Mathematical Society*, **25**:2 (1978), 142–14.

[12] Wiegold J., Lausch H., “Growth sequences of finite semigroups”, *Journal of the Australian Mathematical Society*, **43**:1 (1987), 16–20.

[13] Wikipedia, *Chernoff bound* `https://en.wikipedia.org/wiki/Chernoff_bound`.

[14] Zhuk D., “The size of generating sets of powers”, *Journal of Combinatorial Theory, Series A*, **167** (2019), 91–103.

Undescribed exponential growth rates

Komkov S.A.

There is a function $d_{(A,M)}(n)$ called growth rate that is defined for an arbitrary finite set A with a set of operations M defined on it. It characterizes the strength of given operations. It has been proved that growth rate is either $O(n^k)$ for some $k \in \mathbb{N}$, either $2^{\Theta(n)}$. We research classes of exponential growth rates that appear after splitting the class with asymptotic bound in the exponent to classes with outward asymptotic bounds. We show that there exists a pair (A, M) with the growth rate $d_{(A,M)}(n) \in \Theta(n^k \cdot c^n)$ for arbitrary predefined natural numbers k and c. In addition, if $c \geqslant k+1$ then there exists a pair (A, M) with the growth rate $d_{(A,M)}(n) \in \Theta(\log n \cdot n^k \cdot c^n)$.

Keywords: growth rate, generating sets, finite sets, EGP.

References

[1] Chen H., "Quantified constraint satisfaction and the polynomially generated powers property", International Colloquium on Automata, Languages, and Programming, 2008, 197–208.

[2] Kearnes K. A., Kiss E. W., Szendrei Á., "Growth rates of algebras, I: Pointed cube terms", *Journal of the Australian Mathematical Society*, **101**:1 (2016), 56–94.

[3] Kearnes K. A., Kiss E. W., Szendrei Á., "Growth rates of algebras, II: Wiegold dichotomy", *International Journal of Algebra and Computation*, **25**:4 (2015), 555–566.

[4] Kearnes K. A., Kiss E. W., Szendrei Á., "Growth rates of algebras, III: finite solvable algebras", *Algebra universalis*, **76**:2 (2016), 199–222.

[5] Komkov S. A., "A new formulation of a criterion for the minimal logarithmic growth rate", *Moscow University Mathematics Bulletin*, **75**:5 (2020), 219–220.

[6] Komkov S. A., "Cardinality of generating sets for operations from the Post lattice classes", *Discrete Mathematics and Applications*, **29**:3 (2019), 159–173.

[7] Komkov S. A., "On classes of functions of many-valued logic with minimal logarithmic growth rate", *Discrete Mathematics and Applications*, **30**:4 (2020), 265–272.

[8] Quick M., Ruškuc N., "Growth of generating sets for direct powers of classical algebraic structures", *Journal of the Australian Mathematical Society*, **89**:1 (2010), 105–126.

[9] Wiegold J., "Growth sequences of finite groups", *Journal of the Australian Mathematical Society*, **17**:2 (1974), 133–141.

[10] Wiegold J., "Growth sequences of finite groups II", *Journal of the Australian Mathematical Society*, **20**:2 (1975), 225–229.

[11] Wiegold J., "Growth sequences of finite groups III", *Journal of the Australian Mathematical Society*, **25**:2 (1978), 142–14.

[12] Wiegold J., Lausch H., "Growth sequences of finite semigroups", *Journal of the Australian Mathematical Society*, **43**:1 (1987), 16–20.

[13] Wikipedia, *Chernoff bound* `https://en.wikipedia.org/wiki/Chernoff_bound`.

[14] Zhuk D., "The size of generating sets of powers", *Journal of Combinatorial Theory, Series A*, **167** (2019), 91–103.