О сложности перехода от перечислимого задания конечной структуры к её явному заданию

Андрей Мучник*

Пусть фиксирован оптимальный в смысле [1] язык программирования. Под *энтропией* конструктивного объекта мы будем понимать длину кратчайшей программы, выдающей этот объект на пустом входе. Рассмотрим множество S конструктивных объектов мощности k перечисляемое программой длины $\alpha \ll \log k$ (здесь и далее логарифмы берутся по основанию 2). Как известно, в некоторых случаях энтропия списка элементов множества S как конструктивного объекта может быть больше $\log k$. (То есть, сложность явного задания конечного множества может быть гораздо больше сложности его перечисления.) Тем не менее, просто строится другой список L мощности $O(k \cdot 4^{\alpha})$ и энтропии не больше $\log\log k + O(1)$, в котором для каждого элемента S есть *двойник*. Это значит, что

$$\forall x \in S\, \exists y \in L \quad [K(x|y) \leqslant O(1)] \wedge [K(y|x) \leqslant \alpha + O(1)]\,,$$

где $K(x|y)$ — условная энтропия x при известном y, введённая в [1]. Список L, обладающий указанными свойствами, мы будем называть *напарником* S.

А. Ромащенко выдвинул гипотезу, что если некоторое отношение R на множестве S перечисляется короткой программой, то у полученной структуры тоже есть напарник (при естественном обобщении понятия напарника). Более точно, предположение состояло в том, что существует список L и отношение T на его элементах, такие что

---

*Институт новых технологий, 109004, Москва, ул. Нижняя Радищевская, 10. E-mail: muchnik@lpcs.math.msu.ru, fax: (095)9156963. Работа выполнена при поддержке Российского Фонда Фундаментальных Исследований, гранты N 01-01-00505, N 02-01-22001.

1) мощность L не во много раз больше мощности S, мощность T не во много раз больше мощности R;

2) энтропия $\langle L, T\rangle$ не намного больше длины α программы, перечисляющей множества S, R;

3) $\forall x_1, \ldots, x_i \in S\, \exists y_1, \ldots, y_i \in L$
$[R(x_1, \ldots, x_i) \Rightarrow T(y_1, \ldots, y_i)] \wedge [\forall j\ x_j$ — двойник $y_j]$.

Приводимая ниже теорема опровергает сформулированную гипотезу уже для $i = 2$.

Выражение $x \sim y$ будет сокращением для

$$[K(x|y) < C \log n] \wedge [K(y|x) < C \log n]\,.$$

Теорема. *Пусть число n достаточно велико по сравнению с числом C. Рассмотрим S — множество двоичных слов длины $3n$ — и двуместное отношение R, содержащее те пары $\langle x, u\rangle$ элементов S, для которых $K(\langle x, u\rangle) < 5n$. (Заметим, что $|R| = 2^{5n-O(1)}$.) Тогда не существует списка L и двуместного отношения T на его элементах, таких что*

1) $|L| < |S| \cdot n^C$, $|T| < 2^{5n} \cdot n^C$;

2) $K(\langle L, T\rangle) < C \log n$;

3) $\forall x, u \in S\, \exists y, v \in L\ \ [R(x, u) \Rightarrow T(y, v)] \wedge [x \sim y] \wedge [u \sim v]$.

Доказательство. По n и C мы определим алгоритм перечисления некоторого множества A пар двоичных слов длины $3n$. Мощность A будет не больше $2^{4n}n^C$, поэтому энтропия каждого элемента A будет не больше $4n+O(\log n) < 5n$. Следовательно, $A \subseteq R$. Нам удобно интерпретировать множество A как двудольный граф $\mathbf{A}$.

Рассмотрим перечисление всех пар $\langle L, T\rangle$, удовлетворяющих пунктам 1 и 2 из условия теоремы. За счёт пункта 2 количество таких пар меньше n^C. При появлении очередной пары мы построим соответствующий ей двудольный граф $\mathbf{B}$. В качестве долей $\mathbf{B}$ используются две копии множества S. Степень ветвления каждой вершины левой доли $\mathbf{B}$ будет не больше 2^n. Множество рёбер графа $\mathbf{A}$ будет объединением множеств рёбер всех графов $\mathbf{B}$. Для каждой пары $\langle L, T\rangle$ в соответствующем графе $\mathbf{B}$ найдётся такое ребро $\langle x, u\rangle$, что $\forall y \sim x\ \ \forall v \sim u\ \ \ \neg T(y, v)$. Поэтому $\langle L, T\rangle$ заведомо не будет напарником $\langle S, R\rangle$.

Теперь определим как паре $\langle L, T\rangle$ (которую мы будем интерпретировать как двудольный граф $\mathbf{L}$) сопоставляется граф $\mathbf{B}$. Рассмотрим подмножество L' левой доли $\mathbf{L}$, состоящее из вершин со степенью ветвления больше $2^{2n}n^{3C}$. Понятно, что $|L'| < |T|/2^{2n}n^{3C} < 2^{3n}/n^{2C}$. *Отношением сходства* будем называть произвольное множество $D \subseteq S \times L$, для которого выполнено $\forall x \quad \bigl|\{y|D(x,y)\}\bigr| < n^C$ и $\forall y \quad \bigl|\{x|D(x,y)\}\bigr| < n^C$. Введённое ранее отношение $\sim$, ограниченное на $S \times L$, является отношением сходства. Количество всех отношений сходства не превышает

$$|L|^{2^{3n}\cdot n^C} \leqslant 2^{2^{3n+O(\log n)}}.$$

Пусть E — множество всех двоичных слов длины n. Рассмотрим равномерное вероятностное распределение на множестве всех функций из $S \times E$ в S. Мы хотим показать, что существует функция $F\colon S \times E \to S$, для которой выполнено событие

$$\forall D \text{ — отношения сходства } \exists z \in E\, \exists x, u \in S$$
$$F(x,z) = u \,\wedge\, \forall y, v \in L\, [D(x,y) \wedge D(u,v) \Rightarrow \neg T(y,v)]\,.$$

Для этого мы докажем, что вероятность противоположного события (обозначим его $\mathfrak{B}$) строго меньше 1. Так как рассматриваемое событие разрешимо равномерно по $\mathbf{L}$, то функцию F можно будет найти перебором. Ясно, что в качестве множества рёбер графа $\mathbf{B}$ можно будет взять

$$\{\langle x, u\rangle \mid \exists z \in E\, F(x,z) = u\}\,.$$

Фиксируем отношение сходства D. Обозначим через S' множество элементов S, которые D-сходны с элементами L'. Очевидно, что $|S'| \leqslant |L'|\cdot n^c < |S|/2$. Пусть $z \in E$ и x — вершина левой доли $\mathbf{B}$, не принадлежащая S'. Оценим сверху вероятность следующего события $\mathfrak{D}$:

$$\forall y, v \in L \quad [D(x,y) \wedge D(F(x,z),v) \Rightarrow \neg T(y,v)]\,.$$

Для этого рассмотрим в правой доле $\mathbf{B}$ следующее подмножество

$$\{u \mid \exists y, v \in L\;\, D(x,y) \wedge T(y,v) \wedge D(u,v)\}\,.$$

Его мощность меньше $n^C \cdot 2^{2n}n^{3C} \cdot n^C < |S|/2$. Отсюда следует, что вероятность $\mathfrak{D}$ меньше $1/2$.

Вероятность события $\mathfrak{B}$ не превышает количества отношений сходства, умноженного на вероятность события $\mathfrak{D}$ в степени $|E \times (S \setminus S')|$. То есть, интересующая нас вероятность меньше

$$2^{2^{3n+O(\log n)}} \cdot 2^{-2^n \cdot 2^{3n-1}},$$

что при больших n строго меньше 1.

Теорема доказана. $\square$

Автор признателен Андрею Евгеньевичу Ромащенко за постановку вопроса и полезные обсуждения. Большую помощь оказал Алексей Вячеславович Чернов при подготовке текста к публикации, за что автор ему очень благодарен.

Литература

[1] А. Н. Колмогоров. Три подхода к определению понятия „количество информации“. *Проблемы передачи информации*, т. 1 (1965), N 1, с. 3–11.