Об асимптотических оценках сложности управляющих систем

О. Б. Лупанов

Этот доклад содержит обзор некоторых результатов в области асимптотической теории сложности управляющих систем. Здесь, с одной стороны, будет кратко охарактеризовано общее состояние теории и, с другой стороны, несколько более подробно будут изложены некоторые результаты последних лет.

Асимптотическая теория синтеза управляющих систем фактически началась с работ Шеннона [1, 2]. С. В. Яблонским было введено весьма общее понятие управляющей системы (УС) и были сформулированы основные задачи теории управляющих систем [3]. Полностью привести здесь определение УС не представляется возможным. Укажем лишь некоторые примеры УС. Управляющими системами являются релейно-контактные схемы, цифровые вычислительные машины, программы (для ЭВМ), арифметические формулы и т. д. Все эти объекты характеризуются тем, что они обладают некоторой структурой, схемой S, и реализуют определенную функцию f. С каждым множеством УС естественным образом связывается множество $\mathfrak{S}$ их схем и множество $\mathfrak{F}$ их функций.

Одной из основных задач теории УС является задача синтеза: по функции f из $\mathfrak{F}$ требуется найти УС, схема которой реализует f. В настоящее время для исследования разных вопросов, связанных с задачей синтеза УС (как и для других задач теории УС) характерно рассмотрение конкретных классов УС (модельных объектов). К таким классам можно отнести следующие.

1. Вентильные схемы.
2. Дизъюнктивные нормальные формы.
3. Формулы, являющиеся суперпозициями базисных формул.

В частности, формулы в базисе $\&$, $\vee$, $\neg$.

4. Схемы из функциональных элементов.
5. Контактные схемы.
6. Автоматы (логические сети).
7. Алгоритмы.

Всюду в дальнейшем речь будет идти о сложности задания, а не о сложности вычисления.

Задача синтеза решается, как правило, неоднозначно. Для уточнения постановки задачи вводится мера сложности схем $L(S)$ функционал, удовлетворяющий некоторым естественным условиям. Например, $L(S)$ в случае формул можно определить как число вхождений символов переменных, а в случае схем из функциональных элементов как число элементов схемы; или несколько более общим образом: функциональным элементам (базисным формулам) приписываются веса, $L(S)$ определяется как сумма весов всех элементов схемы (всех вхождений символов базисных формул соответственно). После этого задача о синтезе уточняется так: для любой функции f из $\mathfrak{F}$ требуется найти схему S из $\mathfrak{S}$, реализующую f и такую, что $L(S)$ минимально («минимальную схему»). Это минимальное значение будем обозначать через $L(f)$.

В большинстве случаев существует алгоритм для построения минимальных схем, основанный на переборе всех схем определенной сложности. Однако трудоемкость этого алгоритма весьма велика, и он практически нереализуем при использовании ЭВМ даже в случае функций от сравнительно небольшого числа переменных (5—10). Все попытки найти более эффективные алгоритмы пока не привели к цели. Более того, С. В. Яблонским была высказана гипотеза (и получены первые результаты в направлении обоснования этой гипотезы), что «полный перебор» в этих задачах необходим [4]. Поэтому задачу синтеза приходится уточнять дальше. Один из подходов к этому принадлежит К. Шеннону [2]. При этом подходе отказываются от нахождения минимальной схемы для каждой функции. Вместо этого рассматривают задачу синтеза для целого класса функций (например, для класса $\mathfrak{F}^{(n)}$ булевых функций от n переменных); кроме того, требование минимальности заменяется требованием «почти минимальности». Более точная постановка задачи состоит в следующем. Пусть $L(n)=\max L(f)$, где максимум берется по всем функциям $f(x_1, \ldots \ldots, x_n)$ из $\mathfrak{F}^{(n)}$. Функция $L(n)$ получила название функции Шеннона. Требуется найти алгоритм, который для каждой функции $f(x_1, \ldots, x_n)$ строит схему S такую, что $L(S) \lesssim L(n)$; трудоемкость этого алгоритма должна быть существенно меньше трудоемкости полного перебора.

Первые результаты в этом направлении были получены К. Шенноном [2]. Им был предложен оптимальный по порядку алгоритм синтеза контактных схем и получены оценки

$$\frac{2^n}{n} \lesssim L(n) \lesssim \frac{2^{n+2}}{n}.$$

Асимптотически наилучший алгоритм был построен автором, и тем самым установлена асимптотика функции Шеннона: $L(n) \sim \frac{2^n}{n}$ [5, 6]. Автором были построены также асимптотически наилучшие алгоритмы синтеза формул и схем из функциональных элементов в произвольном конечном базисе [7, 8]. Асимптотики функций Шеннона для этих случаев имеют соответственно вид

$$L(n) \sim \varrho \frac{2^n}{\log_2 n}, \quad L(n) \sim \varrho \frac{2^n}{n},$$

где ϱ — константа, простым способом определяемая по базису.

На основе этих методов позже появились аналогичные асимптотические результаты для других классов управляющих систем. Среди них отметим работу В. А. Кузьмина, установившего асимптотику функции Шеннона для сложности реализации булевых функций некоторыми типами алгоритмов (нормальные алгорифмы, машины Тьюринга) и выяснившего зависимость этой асимптотики от числа букв используемого алфавита [9].

Исследовался также вопрос о влиянии на сложность реализации различных дополнительных требований, предъявляемых к схемам. Здесь в первую очередь следует отметить результаты Э. И. Нечипорука о реализации функций в базисах, некоторые элементы которых имеют нулевые веса [10], и о синтезе самокорректирующихся контактных схем [11]. Сюда же можно отнести результат автора об асимптотике функции Шеннона для схем из пороговых элементов:

$$L(n) \sim 2\left(\frac{2^n}{n}\right)^{1/2};$$

в случае реализации систем m функций асимптотика имеет вид (при условии $\left.\frac{m}{2^n}\to 0\right)$

$$L(n, m) \sim 2\left(\frac{m\,2^n}{n-\log_2 m}\right)^{1/2} \text{[12].}$$

Здесь $L(S)$ — число элементов в схеме S; для случая, когда $L(S)$ равно сумме модулей весов входов элементов, асимптотика была получена ранее Е. Ю. Захаровой [13].

В случае схем в автоматных базисах положение оказалось более сложным. Для некоторых частных случаев удалось получить асимптотические формулы для функции Шеннона (Б. А. Трахтенброт [14], То Суан Зунг [15]). В общем же случае задача об асимптотическом поведении функции Шеннона для произвольного автоматного базиса оказалась алгоритмически неразрешимой (В. А. Орлов [16]). Для частного случая (реализация булевых функций схемами в автоматных базисах) результат В. А. Орлова может быть сформулирован следующим образом. Существует бесконечное множество автоматных базисов $\{\mathfrak{B}\}$, такое что для базиса $\mathfrak{B}$ функция Шеннона имеет асимптотику вида

$$L(n) \sim C_{\mathfrak{B}} \frac{2^n}{n}$$

($C_{\mathfrak{B}}$ константа, зависящая от базиса $\mathfrak{B}$), но не существует алгоритма, определяющего по любому базису из $\{\mathfrak{B}\}$ значение константы $C_{\mathfrak{B}}$.

Результаты асимптотической теории показывают, что поведение функции Шеннона слабо зависит от класса УС. Кроме того, оказывается, что почти все функции из $\mathfrak{F}^{(n)}$ имеют почти одинаковую сложность, асимптотически равную сложности самой сложной функции.

Из приведенных выше оценок видно, что почти все функции допускают лишь очень сложную реализацию и поэтому практически недоступны. Поэтому возникает вопрос о выделении классов функций, реализуемых более просто. Примеры таких классов известны давно, со времени первых работ по синтезу.

Затем С. В. Яблонским [4] было построено и изучено континуальное семейство функций, допускающих более простую схемную реализацию, чем большинство функций. Это классы функций, замкнутые относительно операции подстановки констант вместо (некоторых) переменных. Каждый класс характеризуется некоторым числовым параметром σ, отражающим «мощность» класса ($0 \leqq \sigma \leqq 1$). Для этих классов при $\sigma \neq 0$ С. В. Яблонским были построены асимптотически наилучшие методы синтеза и получены асимптотики функции Шеннона.

Впоследствии автором был предложен один общий подход к синтезу схем — принцип локального кодирования [17]. Этот подход позволяет по описанию класса функций (с соблюдением некоторых специальных требований) строить асимптотически наилучший метод синтеза для функций из этого класса. С помощью этого принципа оказалось возможным единым способом получить методы синтеза для известных классов функций, а также для многих новых классов. Асимптотика сложности схем в конечных базисах для функций из этих классов определяется числом M_n функций $f(x_1, \ldots, x_n)$ в этом классе и имеет вид $\varrho \dfrac{\log M_n}{\log_2 \log_2 M_n}$. Эта функция может принимать значения от величин, близких к n, до $\dfrac{2^n}{n}$. Принцип локального кодирования особенно удобен при применении к достаточно богатым классам УС (схемы из функциональных элементов, автоматы, алгоритмы). Интересный вариант принципа локального кодирования описан в работе Е. П. Липатова [18].

Как уже отмечалось, большинство булевых функций допускает лишь очень сложную схемную реализацию. Однако доказательство этого факта является неэффективным. Первая «эффективная» нелинейная нижняя оценка была получена Б. А. Субботовской для сложности реализации линейной функции от n переменных формулами в базисе &, $\vee$, $\neg$; эта оценка имеет вид $Cn^{3/2}$ [19]. В. М. Храпченко усилил эту оценку до n^2; тем самым установлен порядок сложности [20]. Им же предложен общий метод установления квадратичных нижних оценок для сложности формул в базисе &, $\vee$, $\neg$ [21]. Близкие к квадратичным нижние оценки в «более сильных» классах УС (формулы в произвольном базисе; контактные схемы) были получены Э. И. Нечипоруком [22]. Общий метод получения нелинейных нижних оценок для формул в произвольном базисе предложен Л. Ходесом и Е. Шпекером [23]. В «более слабых» классах УС (формулы в функционально неполных базисах) удается получать нижние оценки порядка n^c, где C — произвольная константа (Э. И. Нечипорук [24], М. М. Рохлина [25]). До сих пор не удалось получить ни одной нелинейной нижней оценки для схем из функциональных элементов (в полном базисе булевых функций). Для неполных базисов в k-значной логике удается получать экспоненциальные оценки в случае схем из функциональных элементов (Г. А. Ткачев [26]).

В связи с установлением некоторых общих закономерностей сложности особый интерес сейчас, по-видимому, представляет изучение различных мер сложности и связи между ними, выявление различных нетривиальных ситуаций, а также установление более общих закономерностей.

Важной мерой сложности, связанной с числом элементов схемы, является ее глубина, т. е. максимальная длина цепочки элементов, соединяющей вход схемы с ее выходом. Соответствующую функцию Шеннона будем обозначать через $T(n)$. Из анализа известных методов синтеза и из нижней оценки для $L(n)$ легко получается асимптотическая формула для $T(n)$. Например, для базиса &, $\vee$, $\neg$ справедливо соотношение $T(n) \sim n$. Более точная формула была получена лишь совсем недавно С. Б. Гашковым [27]

$$T(n) = n - \log_2 \log_2 n + O(1)$$

(нижняя оценка непосредственно следует из нижней оценки для $L(n)$ в случае формул; ранее известные верхние оценки для $T(n)$ таковы:

$$T(n) \leqq n + \log^* n \quad [28], \qquad T(n) \leqq n + O(1) \quad [29]).$$

Глубину схемы можно трактовать как ее задержку; однако, как показал В. М. Храпченко, эти характеристики не всегда совпадают [30]. Полный анализ возможных функций $T(n)$ в случае, когда некоторые базисные элементы имеют нулевую задержку, провел С. А. Ложкин. Оказалось, что возможны лишь три типа поведения функции $T(n)$:

$$T(n) \sim \tau n; \quad T(n) \sim \alpha \log n; \quad T(n) = c \quad (n \geqq n_0) \quad [31].$$

Кроме того, оказалось, что во многих случаях возможно одновременное (т. е. в одной схеме) достижение асимптотики сложности и задержки [32, 33].

Из работ последних лет по исследованию других мер сложности следует отметить результаты О. М. Касим-Заде [34]. Он продолжил начатые М. Н. Вайнцвайгом [38] исследования так называемой мощности схем из функциональных элементов (мощность схемы — это максимальное число ее элементов, имеющих на выходе единицу). Пусть $E_{\mathfrak{A}}(n)$ соответствующая функция Шеннона для базиса $\mathfrak{A}$. Основные результаты О. М. Касим-Заде состоят в следующем

1. Для почти всех (в некотором естественном смысле) базисов $\mathfrak{A}$

$$E_{\mathfrak{A}}(n) \asymp n.$$

2. Существует бесконечно много различных по порядку функций $E_{\mathfrak{A}}(n)$. Например, для любого целого положительного m существует базис $\mathfrak{A}_m$, для которого

$$E_{\mathfrak{A}_m}(n) \asymp \left(\frac{2^n}{n}\right)^{1/m}.$$

3. Для любого конечного базиса $\mathfrak{A}$ имеет место лишь одна из возможностей: либо $\log E_{\mathfrak{A}}(n) \asymp n$, либо $\log E_{\mathfrak{A}}(n) \asymp \log n$; при этом по базису эффективно устанавливается, какая из возможностей имеет место.

4. Для базиса &, $\vee$, $\neg$ возможно одновременное достижение (в одной схеме) асимптотики сложности и порядка мощности.

В заключение отметим, что обзоры такого рода (а также по более широкому кругу вопросов) делались раньше [35—37].

Литература

[1] Shannon, C. E., A symbolic analysis of relay and switching circuits, *Trans. Amer. Electr. Eng.*, v. 57, 1938, pp. 713—722.

[2] Shannon, C. E., The synthesis of two-terminal switching circuits, *Bell System Tech. J.*, v. 28, 1949, No. 1, pp. 59—98.

[3] Яблонский, С. В., Основные понятия кибернетики, *Проблемы кибернетики*, вып. 2, 1959, стр. 7—38.

[4] Яблонский, С. В., Об алгоритмических трудностях синтеза минимальных контактных схем, *Проблемы кибернетики*, вып. 2, 1959, стр. 75—121.

[5] Лупанов, О. Б., О синтезе контактных схем, *ДАН СССР*, т. 119, № 1, 1958, стр. 23—26.

[6] Лупанов, О. Б., О синтезе некоторых классов управляющих систем, *Проблемы кибернетики*, вып. 10, 1963, стр. 63—97.

[7] Лупанов, О. Б., О сложности реализации функций алгебры логики формулами, *Проблемы кибернетики*, вып. 3, 1960, стр. 61—80.

[8] Лупанов, О. Б., Об одном методе синтеза схем, Известия вузов, *Радиофизика*, т. 1, № 1, 1958, стр. 120—140.

[9] Кузьмин, В. А., Реализация функций алгебры логики автоматами, нормальными алгорифмами и машинами Тьюринга, *Проблемы кибернетики*, вып. 13, 1965, стр. 75—96.

[10] Нечипорук, Э. И., О сложности схем в некоторых базисах, содержащих нетривиальные элементы с нулевыми весами, *Проблемы кибернетики*, вып. 8, 1962, стр. 123—160.

[11] Нечипорук, Э. И., О топологических принципах самокорректирования, *Проблемы кибернетики*, вып. 21, 1969, стр. 5—102.

[12] Лупанов, О. Б., О синтезе схем из пороговых элементов, *Проблемы кибернетики*, вып. 26, 1973, стр. 109—140.

[13] Захарова, Е. Ю., О синтезе схем из пороговых элементов, *Проблемы кибернетики*, вып. 9, 1963, стр. 317—319.

[14] Трахтенброт, Б. А., Асимптотическая оценка сложности логических сетей с памятью, *ДАН СССР*, т. 127, № 2, 1959, стр. 281—284.

[15] То Суан Зунг, Об асимптотических закономерностях сложности автоматов из некоторых классов, *Проблемы кибернетики*, вып. 22, 1970, стр. 5—43.

[16] Орлов, В. А., О сложности реализации ограниченно-детерминированных операторов схемами в автоматных базисах, *Проблемы кибернетики*, вып. 26, 1973, стр. 141—182.

[17] Лупанов, О. Б., Об одном подходе к синтезу управляющих систем—принципе локального кодирования, *Проблемы кибернетики*, вып. 14, 1965, стр. 31—110.

[18] Липатов, Е. П., Об одном случае неравномерного локального кодирования, *Проблемы кибернетики*, вып. 26, 1973, стр. 95—107.

[19] Субботовская, Б. А., О реализации линейных функций формулами в базисе $\vee$, &, —, *ДАН СССР*, т. 136, № 3, 1961, стр. 553—555.

[20] Храпченко, В. М., О сложности реализации линейной функции в классе п-схем, *Мат. заметки*, т. 9, № 1, 1971, стр. 35—40.

[21] Храпченко, В. М., Об одном методе получения нижних оценок сложности п-схем, *Мат. заметки*, т. 10, № 1, 1971, стр. 83—92.

[22] Нечипорук, Э. И., Об одной булевской функции, *ДАН СССР*, т. 169, № 4, 1966, стр. 765—767.

[23] Hodes, L., E. Specker, Lengths of formulas and elimination of quantifiers I. Proc. Logic Colloquium, Hannover 1966, *Contributions to mathematical logic*, North-Holland, Amsterdam, 1968, pp. 175—188.

[24] Нечипорук, Э. И., О реализации дизъюнкции и конъюнкции в некоторых монотонных базисах, *Проблемы кибернетики*, вып. 23, 1970, стр. 291—293.

[25] Рохлина, М. М., О схемах, повышающих надежность, *Проблемы кибернетики*, вып. 23, 1970, стр. 295—301.

[26] Ткачев, Г. А., О сложности реализации одной последовательности функций k-значной логики, Вестник Московского университета, Вычислительная математика и кибернетика, № 1, 1977, стр. 45—57.

[27] Гашков, С. Б., О глубине булевых функций, *Проблемы кибернетики*, вып. 34, 1978, стр. 265—268.

[28] Spiza, P. M., On the time necessary to compute switching functions, *IEEE Trans. Comput.*, C—20, No. 1, 1977, pp. 104—105.

[29] McColl, W. F., M. S. Paterson, The depth of all Boolean functions, *SIAM J. Comput.*, v. 6, No. 2, 1977, pp. 373—380.
[30] Храпченко, В. М., Различие и сходство между задержкой и глубиной, *Проблемы кибернетики*, вып. 35, 1979, стр. 141—168.
[31] Ложкин, С. А., Асимптотическое поведение функций Шеннона для задержек схем из функциональных элементов, *Мат. заметки*, т. 19, № 6, 1976, стр. 939—951.
[32] Лупанов, О. Б., О схемах из функциональных элементов с задержками, *Проблемы кибернетики*, вып. 23, 1970, стр. 43—81.
[33] Loshkan, S. A., Über die Synthese von Schemata aus Funktional-elementen mit Verzögerung, *Wiss. Z. Humboldt-Univ. Berlin Math.-Natur. Reihe*, v. 24, 1975, No. 6, pp. 730—732.
[34] Касим-Заде, О. М., Об одной мере сложности схем из функциональных элементов, *ДАН СССР*, т. 250, № 4, 1980, стр. 797—801.
[35] Yablonski, S. V., A survey of some results in the field of discrete mathematics, *Proc. IFIP Congress 1968, Edinburgh*, North-Holland, Amsterdam, 1969, pp. 266—270.
[36] Лупанов, О. Б., Об асимптотических оценках сложности управляющих систем, Международный конгресс математиков в Ницце 1970, Доклады советских математиков, М., 1972, стр. 162—167.
[37] Лупанов, О. Б. О методах получения оценок сложности и вычисления индивидуальных функции, *Дискретный анализ*, Новосибирск, вып. 25, 1974, стр. 3—18.
[38] Вайнцвайг, М. Н., О мощности схем из функциональных элементов, *ДАН СССР*, т. 139, № 2, 1961, стр. 320—323.

(Поступило 2-ого августа 1979 г.)