С.С. Марченков

КЛАССЫ ЭЛЕМЕНТАРНЫХ РЕКУРСИВНЫХ ФУНКЦИЙ

МОСКВА
ФИЗМАТЛИТ®
2017

УДК 519.7
ББК 22.176
М 30

Марченков С.С. **Классы элементарных рекурсивных функций.** — М.: ФИЗМАТЛИТ, 2017. — 136 с. — ISBN 978-5-9221-1714-2.

В книге представлены основные классы элементарных рекурсивных функций, изучаемых в теории рекурсивных функций. Приведены различные определения исследуемых классов, установлены соотношения включения между ними. В терминах сложности вычислений получено описание большого числа классов элементарных функций. Для ряда классов дано решение проблемы существования конечных базисов по суперпозиции.

Для студентов и аспирантов математических факультетов, изучающих теорию алгоритмов, а также научных сотрудников и преподавателей высшей школы.

Научное издание

МАРЧЕНКОВ Сергей Серафимович

КЛАССЫ ЭЛЕМЕНТАРНЫХ РЕКУРСИВНЫХ ФУНКЦИЙ

Редактор *В.С. Аролович*
Оригинал-макет: *Е.В. Сабаева*
Оформление переплета: *Д.Б. Белуха*

Подписано в печать 15.09.2016. Формат 60×90/16. Бумага офсетная. Печать офсетная.
Усл. печ. л. 8,5. Уч.-изд. л. 9,4. Тираж 300 экз. Заказ №

Издательская фирма «Физико-математическая литература»
МАИК «Наука/Интерпериодика»
117342, Москва, ул. Бутлерова, 17 Б
E-mail: porsova@fml.ru, sale@fml.ru
Сайт: http://www.fml.ru
Интернет-магазин: http://www.fmllib.ru

ISBN 978-5-9221-1714-2

9 785922 117142

Отпечатано с электронных носителей издательства
в АО «ИПК «Чувашия»,
428019, г. Чебоксары, пр-т И. Яковлева, 13

ISBN 978-5-9221-1714-2

ОГЛАВЛЕНИЕ

Предисловие

Исследования, проводимые в теории рекурсивных функций, можно условно разделить на две части. К первой части относятся исследования, в которых потенциально допускаются произвольные частично рекурсивные либо общерекурсивные функции. Исследования, входящие во вторую часть, напротив, имеют дело с рекурсивными функциями, которые подчиняются ограничениям различного типа. Как правило, эти ограничения носят сложностной характер.

Ограничения, налагаемые на рекурсивные функции, служат для достижения различных целей: построение иерархий рекурсивных функций, моделирование вычислений на абстрактных вычислительных устройствах, определение классов сложности, получение канонических представлений рекурсивных функций и др. Обычно класс функций, который удовлетворяет формулируемым ограничениям, сравнительно невелик, рекурсивно перечислим и состоит только из примитивно рекурсивных функций. Во многих случаях этот класс к тому же содержит «почти все» функции, используемые в наиболее распространенных конструкциях из математической логики и теории алгоритмов. Поэтому подобные классы функций часто называют классами «элементарных» функций.

В настоящее время известно довольно много классов элементарных функций. Некоторые из них определены более 60 лет назад и заняли прочное положение в теории рекурсивных функций. Другие классы появились сравнительно недавно, их введение в научный оборот связано с определенными тенденциями в развитии теории рекурсивных функций. Все эти классы объединяет то, что они имеют индуктивные определения, где в качестве порождающих операций выступают операция суперпозиции и ряд других эффективных операций.

В предлагаемой читателю книге изучаются следующие классы элементарных функций: класс функций, элементарных по Сколему; класс функций, элементарных по Кальмару; начальные классы иерархии Гжегорчика; обобщения классов Гжегорчика. Некоторые классы элементарных функций, появившиеся в последние годы, еще не имеют устоявшихся названий. В книге они представлены как в основном тексте, так и в задачах. Кроме того, подробно исследован класс ограниченно арифметических предикатов (он же класс рудиментарных предикатов), который представляет собой фундамент для большинства классов элементарных функций.

Исторически сложился круг вопросов, рассматриваемых при изучении классов элементарных функций. Это сравнение классов элементарных функций между собой и с другими известными классами функций, возможность порождения классов с помощью тех или иных операций, канонические представления функций из рассматриваемых классов и сложность вычисления функций.

Книга состоит из пяти глав. Глава I посвящена в основном классу **BA** ограниченно арифметических предикатов. Эти предикаты предложены А.В. Кузнецовым [11] в 1961 г. и представляют собой ограниченный вариант известных арифметических предикатов. Класс **BA** определен также независимо Р. Смальяном [34] в виде класса конструктивно арифметических предикатов. Класс **BA** достаточно широк: ему принадлежат многие хорошо известные предикаты из теории чисел и теории рекурсивных функций. Так же, как для класса арифметических предикатов [41, 22], класс **BA** можно определить чисто синтаксическим образом на базе предиката конкатенации. Соответствующее определение приводит к классу **R** рудиментарных предикатов [34]. Совпадение классов **BA** и **R** — далеко не очевидный факт — является одним из основных результатов главы I. Необходимо также отметить канонические представления ограниченно арифметических предикатов (теорема 1.1) и рудиментарных предикатов (теорема 1.2). На базе класса ограниченно арифметических предикатов в главе I определен первый класс элементарных функций — класс **FBA**.

В главе II вводится и исследуется целая серия классов элементарных функций. Это класс **Sk** функций, элементарных по Сколему [43], классы $\mathcal{E}^0$ – $\mathcal{E}^3$ иерархии Гжегорчика [6], классы $\mathcal{E}f$ — обобщения классов Гжегорчика [3], а также класс **K** функций, элементарных по Кальмару [38], совпадающий с классом $\mathcal{E}^3$ Гжегорчика. Приводится целый ряд эквивалентных определений классов **Sk**, $\mathcal{E}^i$, $\mathcal{E}f$, **K** и устанавливаются соотношения включения между ними. Доказываются некоторые важные представления функций из перечисленных классов, и исследуется возможность порождения множеств всех одноместных функций класса из конечного числа функций с помощью известных эффективных операций. В классе **K** определяется конечная система функций, порождающая класс **K** относительно операции суперпозиции.

В главе III вводится понятие стековой регистровой машины (машины SRM) [3]. В терминах вычислений на машинах SRM для достаточно широкого множества монотонных функций f определяются классы $\mathcal{E}f$, во многом схожие с классами Гжегорчика. С использованием машин SRM доказываются важные теоремы о существовании универсальных функций для классов $\mathcal{E}f$ и о существовании конечных базисов по суперпозиции в этих классах. Устанавливается ряд общих фактов о конечных базисах по суперпозиции в классах одноместных и многоместных функций.

Глава IV посвящена решению одной задачи — построению «простого» конечного базиса по суперпозиции в классе $\mathcal{E}^2$ Гжегорчика. Этот результат получен С.А. Волковым [5] сравнительно недавно, результат базируется на новом подходе к получению конечных базисов по суперпозиции в «малых» классах элементарных функций.

Глава V содержит результат, к достижению которого специалисты шли более 50 лет. Речь идет о построении в классе **K** функций, элементарных по Кальмару, конечного базиса по суперпозиции, состоящего только из «самых известных» арифметических функций. При получении этого результата были использованы разнообразные технические средства: некоторые теоретико-числовые и комбинаторные соотношения, экспоненциально диофантовы представления рекурсивно перечислимых предикатов, некоторые приемы из математической логики, а также специальные представления функций из класса **K**.

В конце большинства глав приводятся задачи и темы для дальнейших исследований. Часть из них предлагалась автором на факультете вычислительной математики и кибернетики МГУ в качестве тем для курсовых и дипломных работ.

В основу книги положены специальные курсы «Рекурсивные функции», «Элементарные рекурсивные функции», «Основы теории алгоритмов», «Суперпозиции элементарных арифметических функций» и «Вычисления на машинах Минского», которые автор на протяжении ряда лет читал на факультете вычислительной математики и кибернетики МГУ.

Книга адресована прежде всего студентам и аспирантам математических факультетов, изучающим вычислимые (рекурсивные) функции и желающим поближе познакомиться с идеями и методами, которые существуют в данном разделе теории алгоритмов. Она также может быть полезна преподавателям вузов и научным сотрудникам, интересующимся вопросами классификации и сложности вычисления рекурсивных функций.

Глава I

ОГРАНИЧЕННО АРИФМЕТИЧЕСКИЕ И РУДИМЕНТАРНЫЕ ПРЕДИКАТЫ

§ 1.1. Ограниченно арифметические предикаты

1. Пусть $\mathbb{N} = \{0, 1, 2, \ldots\}$. *Предикатом на множестве* $\mathbb{N}$ называется отображение ρ декартовой степени множества $\mathbb{N}$ в множество $\{\text{И}, \text{Л}\}$ истинностных значений. Если предикат $\rho(x_1, \ldots, x_n)$ принимает на наборе $(a_1, \ldots, a_n)$ значение И (значение Л), то говорят, что набор $(a_1, \ldots, a_n)$ удовлетворяет (не удовлетворяет) предикату ρ. Часто предикат отождествляют с множеством всех наборов, которые удовлетворяют предикату. Предикаты ρ, σ называются *эквивалентными*, если они совпадают как отображения. Для обозначения эквивалентности предикатов будем использовать знак $\equiv$.

На множестве предикатов определим нелогические операции, операции логики высказываний и операции ограниченной квантификации. Нелогические операции будем называть также *явными преобразованиями*. Они включают в себя операции введения фиктивных переменных, перестановки и отождествления переменных и подстановки констант (из множества $\mathbb{N}$) вместо переменных.

Операцию *введения фиктивных переменных* определим только в частном случае введения одной (последней) фиктивной переменной; общий случай получается последовательным применением частного случая с последующей перестановкой переменных. Итак, предикат $\sigma(x_1, \ldots, x_n, x_{n+1})$ получен из предиката $\rho(x_1, \ldots, x_n)$ введением фиктивной переменной x_{n+1}, если для любого набора $(a_1, \ldots, a_n, a_{n+1})$ из $\mathbb{N}^{n+1}$ значение $\sigma(a_1, \ldots, a_n, a_{n+1})$ истинно тогда и только тогда, когда истинно значение $\rho(a_1, \ldots, a_n)$.

Предикат σ получен из предиката ρ с помощью операции *перестановки переменных*, если

$$\sigma(x_1, \ldots, x_n) \equiv \rho(x_{i_1}, \ldots, x_{i_n}),$$

где $(i_1, \ldots, i_n)$ — перестановка элементов множества $\{1, \ldots, n\}$.

Операцию *отождествления переменных* продемонстрируем в частном случае отождествления двух переменных; общий случай получается последовательным выполнением операции для частных случаев.

Пусть $n \geqslant 2$ и $1 \leqslant i < j \leqslant n$. Отождествить в предикате $\rho(x_1, \ldots, x_n)$ переменные x_i, x_j — значит образовать предикат σ, где

$$\sigma(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n) \equiv \rho(x_1, \ldots, x_{j-1}, x_i, x_{j+1}, \ldots, x_n).$$

Операцию *подстановки констант* вместо переменных оставим без дополнительных разъяснений.

Из логических операций будем рассматривать только четыре: дизъюнкцию $\vee$, конъюнкцию $\&$, отрицание $\neg$ и импликацию $\Rightarrow$. Имея в виду возможность введения фиктивных переменых, операции $\vee$, $\&$, $\Rightarrow$ будем применять к предикатам, зависящим, вообще говоря, от различных переменных.

Предполагая, что читатель знаком с определением квантора $\exists$, будем говорить, что предикат $\sigma(x_1, \ldots, x_n, y)$ получен из предиката $\rho(x_1, \ldots, x_n, z)$ с помощью операции *навешивания ограниченного квантора существования*, и писать

$$\sigma(x_1, \ldots, x_n, y) \equiv (\exists z)_{z \leqslant y} \rho(x_1, \ldots, x_n, z),$$

если

$$\sigma(x_1, \ldots, x_n, y) \equiv (\exists z)\big((z \leqslant y) \mathbin{\&} \rho(x_1, \ldots, x_n, z)\big).$$

Аналогично определяется операция *навешивания ограниченного квантора общности*:

$$\sigma(x_1, \ldots, x_n, y) \equiv (\forall z)_{z \leqslant y} \rho(x_1, \ldots, x_n, z),$$

где

$$\sigma(x_1, \ldots, x_n, y) \equiv (\forall z)\big((z \leqslant y) \Rightarrow \rho(x_1, \ldots, x_n, z)\big).$$

2. Класс **BA** *ограниченно арифметических предикатов* определим индуктивно: исходными предикатами класса **BA** будем считать арифметические предикаты сложения $x + y = z$ и умножения $x \cdot y = z$, а порождающими операциями — явные преобразования, операции логики высказываний и операции ограниченной квантификации.

Установим принадлежность некоторых хорошо известных предикатов классу **BA**. Имеем:

$$\begin{aligned}
&(x = y) \equiv (x + 0 = y),\\
&(x \leqslant y) \equiv (\exists z)_{z \leqslant y}(x = z),\\
&(x < y) \equiv (\exists z)_{z \leqslant y}(x + 1 = z),\\
&(|x - y| = z) \equiv (x + z = y) \vee (y + z = x),\\
&(\max(x, y) = z) \equiv (x \geqslant y) \mathbin{\&} (x = z) \vee (x < y) \mathbin{\&} (y = z),\\
&(\min(x, y) = z) \equiv (x \leqslant y) \mathbin{\&} (x = z) \vee (x > y) \mathbin{\&} (y = z).
\end{aligned}$$

Предикат $x = c$, где $c \in \mathbb{N}$, получается из предиката $x = y$ подстановкой константы c.

Из принадлежности предиката $x < y$ классу **BA** нетрудно вывести, что класс **BA** замкнут относительно операций навешивания ограниченных кванторов вида $(\exists x)_{x<y}$ и $(\forall x)_{x<y}$. В самом деле, имеем:

$$(\exists x)_{x<y}\rho \equiv (\exists x)_{x\leqslant y}\big((x<y)\,\&\,\rho\big), \quad (\forall x)_{x<y}\rho \equiv (\forall x)_{x\leqslant y}\big((x<y)\Rightarrow\rho\big).$$

Пусть:

$$x \dot{-} y = \max(0, x-y),$$

$$[x/y] = \begin{cases}\text{целой части от деления } x \text{ на } y, \text{ если } y \neq 0,\\ 0 \text{ в противном случае;}\end{cases}$$

$$\mathrm{rm}\,(x,y) = \begin{cases}\text{остатку от деления } x \text{ на } y, \text{ если } y \neq 0,\\ 0 \text{ в противном случае;}\end{cases}$$

$$[\sqrt{x}\,] = \text{целой части корня квадратного из } x;$$

$$(x|y) \equiv (x \text{ делит нацело } y);$$

$$\mathrm{Pr}\,(x) \equiv (x \text{ есть простое число});$$

$$\mathrm{Dp}\,(x,y) \equiv (x \text{ есть степень простого числа } y).$$

Следующая серия предикатов также принадлежит классу **BA**:

$$(x \dot{-} y = z) \equiv (y+z=x) \vee (x<y)\,\&\,(z=0),$$

$$([x/y]=z) \equiv (\exists v)_{v\leqslant x}(\exists w)_{w\leqslant x}\big((yz=v)\,\&\,(w<y)\,\&\,(v+w=x)\big) \\ \vee(y=0)\,\&\,(z=0),$$

$$(\mathrm{rm}\,(x,y)=z) \equiv (\exists v)_{v\leqslant x}(\exists w)_{w\leqslant x}\big((yv=w)\,\&\,(z+w=x)\,\&\,(z<y)\big) \\ \vee(y=0)\,\&\,(z=0),$$

$$([\sqrt{x}\,]=y) \equiv (\exists z_1)_{z_1\leqslant x}(\exists z_2)_{z_2\leqslant x}(\exists z_3)_{z_3\leqslant x}\big((yy=z_1)\,\&\,(z_1+z_2=x) \\ \&(z_2 \dot{-} y = z_3)\,\&\,(z_3\leqslant y)\big),$$

$$(x|y) \equiv (\mathrm{rm}\,(y,x)=0),$$

$$\mathrm{Pr}\,(x) \equiv (x\geqslant 2)\,\&\,(\forall y)_{y\leqslant x}\big((y|x)\Rightarrow(y=1\vee y=x)\big),$$

$$\mathrm{Dp}\,(x,y) \equiv (x\geqslant 1)\,\&\,\mathrm{Pr}\,(y)\,\&\,(\forall z)_{z\leqslant x}((z|x)\,\&\,(z\geqslant 2)\Rightarrow(y|z)).$$

3. При построении некоторых из перечисленных выше предикатов из операций логики высказываний применялись лишь «позитивные» операции $\vee$ и $\&$. Назовем формулу, представляющую предикат класса **BA**, *позитивной*, если она не содержит логических связок $\neg$ и $\Rightarrow$.

Утверждение 1.1. *Любой предикат класса* **BA** *можно представить позитивной формулой.*

Доказательство. Согласно известным логическим правилам имеем:

$$(\rho\Rightarrow\sigma)\equiv(\neg\rho\vee\sigma), \quad \neg(\rho\vee\sigma)\equiv\neg\rho\&\neg\sigma,$$

$$\neg(\rho\&\sigma)\equiv\neg\rho\vee\neg\sigma, \quad \neg(\exists x)_{x\leqslant y}\rho\equiv(\forall x)_{x\leqslant y}\neg\rho,$$

$$\neg(\forall x)_{x\leqslant y}\rho\equiv(\exists x)_{x\leqslant y}\neg\rho.$$

Поэтому для доказательства утверждения достаточно установить, что с помощью позитивных формул можно представить предикаты $\neg(x + y = z)$ и $\neg(xy = z)$ (как это общепринято, данные предикаты далее будем обозначать $x + y \neq z$ и $xy \neq z$). Убеждаемся, что справедливы эквивалентности:

$$(x + y \neq z) \equiv (\exists v)_{v<z}(x + y = v)\vee \\ \vee(\exists v)_{v\leqslant x}(\exists w)_{w\leqslant y}\big(((v < x) \vee (w < y))\ \&\ (v + w = z)\big),$$

$$(xy \neq z) \equiv (x = 0)\ \&\ (z > 0) \vee (x > 0)\ \&\ (\exists v)_{v\leqslant z}(\exists w)_{w\leqslant z} \\ \big(([z/x] = v)\ \&\ (\mathrm{rm}\,(z, x) = w)\ \&\ ((y < v) \vee (v < y) \vee (w > 0))\big).$$

Кроме того, все предикаты, стоящие в правых частях приведенных эквивалентностей, представимы с помощью позитивных формул. Утверждение доказано.

Утверждение 1.2. *Любой предикат класса* **BA** *можно представить в форме*

$$(Q_1x_1)_{x_1\leqslant y_1} \dots (Q_mx_m)_{x_m\leqslant y_m}(R_1 = R_2),$$

где $Q_1, \dots, Q_m$ — кванторы $\exists$ или $\forall$, а R_1, R_2 — полиномы с натуральными коэффициентами.

Доказательство. Согласно утверждению 1.1 произвольный предикат класса **BA** можно представить позитивной формулой. Приведем эту формулу к предваренной нормальной форме и обозначим через Φ бескванторную часть полученной формулы. Предикаты вида $x + y = z$, $xy = z$ (вместо некоторых переменных здесь могут стоять константы), входящие в формулу Φ, заменим эквивалентными предикатами $(x + y - z)^2 = 0$ и $(xy - z)^2 = 0$. Далее замечаем, что если $P_1, \dots, P_k$ — полиномы с целыми коэффициентами, принимающие лишь значения из $\mathbb{N}$, то предикат $P_1 = 0 \vee \dots \vee P_k = 0$ эквивалентен предикату $P_1 \cdot \ldots \cdot P_k = 0$, а предикат $(P_1 = 0)\ \&\ \dots\ \&\ (P_k = 0)$ — предикату $P_1 + \ldots + P_k = 0$. Таким образом, формулу Φ можно преобразовать к эквивалентному виду $P = 0$, где P — полином с целыми коэффициентами, принимающий лишь значения из $\mathbb{N}$. Остается выделить в полиноме P «положительную» часть R_1 (т. е. слагаемые с положительными коэффициентами), «отрицательную» часть R_2 (аналогично) и записать предикат $P = 0$ в эквивалентной форме $R_1 = R_2$. Утверждение доказано.

Утверждение 1.3. *При любом $n \geqslant 2$ предикаты*

$$y \leqslant \max(x_1, \dots, x_n), \quad y = \max(x_1, \dots, x_n)$$

принадлежат классу **BA**. *Класс* **BA** *замкнут относительно операций навешивания ограниченных кванторов вида*

$$(\exists y)_{y\leqslant \max(x_1,\dots,x_n)}, \quad (\forall y)_{y\leqslant \max(x_1,\dots,x_n)}.$$

Доказательство. Имеем:

$$(y \leqslant \max(x_1, \ldots, x_n)) \equiv (y \leqslant x_1) \vee \ldots \vee (y \leqslant x_n),$$

$$(y = \max(x_1, \ldots, x_n)) \equiv \\ \equiv \bigvee_{1 \leqslant i \leqslant n} (y = x_i) \,\&(x_1 \leqslant x_i) \,\& \ldots \& \,(x_{i-1} \leqslant x_i) \,\& \\ \& \,(x_{i+1} \leqslant x_i) \,\& \ldots \& \,(x_n \leqslant x_i),$$

$$(\exists y)_{y \leqslant \max(x_1, \ldots, x_n)} \rho \equiv \bigvee_{1 \leqslant i \leqslant n} (\exists y)_{y \leqslant x_i} \rho,$$

$$(\forall y)_{y \leqslant \max(x_1, \ldots, x_n)} \rho \equiv \mathop{\&}_{1 \leqslant i \leqslant n} (\forall y)_{y \leqslant x_i} \rho.$$

Утверждение 1.4. *Классу* **BA** *принадлежат предикаты вида*

$$P_1(x_1, \ldots, x_n) = P_2(x_1, \ldots, x_n), \tag{1.1}$$

где P_1, P_2 — полиномы с натуральными коэффициентами.

Доказательство. Мы воспользуемся хорошо известной китайской теоремой об остатках:

пусть $q_1, \ldots, q_m$ — попарно взаимно простые натуральные числа и $0 \leqslant r_1 < q_1, \ldots, 0 \leqslant r_m < q_m$; тогда на отрезке $[0, q_1 \cdot \ldots \cdot q_m - 1]$ существует единственное число q такое, что

$$\mathrm{rm}(q, q_1) = r_1, \quad \ldots, \quad \mathrm{rm}(q, q_m) = r_m.$$

В качестве взаимно простых чисел $q_1, \ldots, q_m$ будем рассматривать последовательные простые числа $p_0, \ldots, p_{m-1}$ ($p_0 = 2$). Чтобы оценить величину $p_0 \cdot \ldots \cdot p_{m-1}$, воспользуемся известным в теории чисел фактом, что количество простых чисел, не превосходящих x, асимптотически равно $x/\ln x$. Поэтому при достаточно больших x выполняется неравенство

$$\prod_{p_i \leqslant x} p_i > [x/\ln x]!.$$

Выберем теперь число x_0 так, чтобы при любом $x \geqslant x_0$ выполнялось неравенство

$$[x'/\ln x']! > \max_{x_1, \ldots, x_n \leqslant x} \bigl\{P_1(x_1, \ldots, x_n), P_2(x_1, \ldots, x_n)\bigr\},$$

где $x' = [\sqrt{x}\,]$. Если при этом $x = \max(x_1, \ldots, x_n)$ и $x \geqslant x_0$, то равенство (1.1) выполняется в том и только том случае, когда для всех простых чисел p_i, не превосходящих $[\sqrt{x}\,]$, справедливо равенство

$$\mathrm{rm}\bigl(P_1(x_1, \ldots, x_n), p_i\bigr) = \mathrm{rm}\bigl(P_2(x_1, \ldots, x_n), p_i\bigr).$$

Иными словами, при $x \geqslant x_0$ предикат (1.1) эквивалентен предикату

$$(\forall p)_{p \leqslant x}\big((\mathrm{Pr}\,(p) \,\&\, (p \leqslant [\sqrt{x}\,])) \Rightarrow \\ \Rightarrow (\mathrm{rm}\,(P_1(x_1, \ldots, x_n), p) = \mathrm{rm}\,(P_2(x_1, \ldots, x_n), p))\big).$$

Предикат $p \leqslant [\sqrt{x}\,]$ представ́им в виде

$$(\exists x)_{x \leqslant \max\,(x_1,\ldots,x_n)}(\exists x')_{x' \leqslant \max\,(x_1,\ldots,x_n)}\big((x = \max\,(x_1, \ldots, x_n)) \,\& \\ \& \,(x' = [\sqrt{x}\,]) \,\&\, (p \leqslant x')\big).$$

С использованием утверждения 1.3 получаем, что предикат $p \leqslant [\sqrt{x}\,]$ принадлежит классу **BA**.

Предикат

$$\mathrm{rm}\,\big(P_1(x_1, \ldots, x_n), p\big) = \mathrm{rm}\,\big(P_2(x_1, \ldots, x_n), p\big)$$

разобьем на две части:

$$(\exists y)_{y \leqslant p}\big((\mathrm{rm}\,(P_1(x_1, \ldots, x_n), p) = y) \,\&\, (\mathrm{rm}\,(P_2(x_1, \ldots, x_n), p) = y)\big).$$

Чтобы выразить в классе **BA** предикат

$$\mathrm{rm}\,\big(P_1(x_1, \ldots, x_n), p\big) = y,$$

проведем индукцию по построению полинома P_1. Если, например, $P_1 = R_1 + R_2$, где R_1, R_2 — полиномы с натуральными коэффициентами, и $x = \max\,(x_1, \ldots, x_n)$, то

$$(\mathrm{rm}\,(P_1, p) = y) \equiv (\exists z_1)_{z_1 \leqslant x}(\exists z_2)_{z_2 \leqslant x}(\exists z_3)_{z_3 \leqslant x}\big((\mathrm{rm}\,(R_1, p) = z_1) \,\& \\ \&\, (\mathrm{rm}\,(R_2, p) = z_2) \,\&\, (z_1 + z_2 = z_3) \,\&\, (\mathrm{rm}\,(z_3, p) = y)\big).$$

При этом, выписывая ограничение $z_3 \leqslant x$ для квантора $\exists z_3$, мы пользуемся тем, что $p^2 \leqslant x$. Аналогичное представление имеет место в случае, когда $P_1 = R_1 \cdot R_2$.

Наконец, следует отметить, что при $\max\,(x_1, \ldots, x_n) < x_0$ предикат (1.1) можно задать «табличным» способом, т. е. в виде

$$\bigvee_{(i_1,\ldots,i_n)} (x_1 = i_1) \,\&\, \ldots \,\&\, (x_n = i_n),$$

где дизъюнкция проводится по всем наборам $(i_1, \ldots, i_n)$, удовлетворяющим условиям $i_1 < x_0, \ldots, i_n < x_0$ и $P_1(i_1, \ldots, i_n) = P_2(i_1, \ldots, i_n)$. Утверждение доказано.

Утверждение 1.5. *Класс* **BA** *замкнут относительно операций навешивания ограниченных кванторов вида*

$$(\exists x)_{x \leqslant P}, \quad (\forall x)_{x \leqslant P},$$

где P — полином с натуральными коэффициентами.

Доказательство. Пусть σ — предикат класса **BA**, который определяется формулой Φ, а предикат ρ задается формулой $(Qx)_{x\leqslant P}\Phi$, где Q — квантор $\exists$ или $\forall$, P — полином, отличный от переменной и константы. Согласно утверждению 1.1 можно считать, что формула Φ позитивна. Покажем, как преобразовать формулу $(Qx)_{x\leqslant P}\Phi$ в эквивалентную формулу, заменив квантор $(Qx)_{x\leqslant P}$ кванторами вида $(Qx)_{x\leqslant y}$.

Поскольку полином P отличен от переменной и константы, его можно представить в одной из форм P_1+P_2 или $P_1\cdot P_2$, где P_1, P_2 — полиномы с натуральными коэффициентами. Дальнейший процесс преобразования формулы $(Qx)_{x\leqslant P}\Phi$ носит индуктивный характер, в котором конкретный вид полиномов P_1, P_2 роли не играет.

Заметим, что при $P=P_1+P_2$ область $x\leqslant P$ можно получить в качестве множества значений функции x_1+x_2 при $x_1\leqslant P_1$ и $x_2\leqslant P_2$. Если же $P=P_1\cdot P_2$, то при $P_2\neq 0$ область $x\leqslant P$ представима в виде множества значений функции $x_1x_3+x_2$, где $x_1,x_2\leqslant P_1$ и $x_3<P_2$.

В связи с этим формула $(Qx)_{x\leqslant P}\Phi$ при $P=P_1+P_2$ будет преобразована в формулу вида

$$(\exists x_1)_{x_1\leqslant P_1}(\exists x_2)_{x_2\leqslant P_2}\Phi_1 \quad \text{или} \quad (\forall x_1)_{x_1\leqslant P_1}(\forall x_2)_{x_2\leqslant P_2}\Phi_1,$$

а при $P=P_1\cdot P_2$ — в формулу вида

$$\Phi(0)\vee(\exists x_1)_{x_1\leqslant P_1}(\exists x_2)_{x_2\leqslant P_1}(\exists x_3)_{x_3<P_2}\Phi_2$$

или

$$\Phi(0)\&(\forall x_1)_{x_1\leqslant P_1}(\forall x_2)_{x_2\leqslant P_1}(\forall x_3)_{x_3<P_2}\Phi_2,$$

где переменные x_1, x_2, x_3 не встречаются в формуле Φ.

Формулы Φ_1, Φ_2 определяются следующим образом. При $P=$ $=P_1+P_2$ переменная x в формуле Φ всюду (включая кванторы типа $(Qz)_{z\leqslant x}$) заменяется выражением x_1+x_2, при $P=P_1\cdot P_2$ — выражением $x_1x_3+x_2$. Образующиеся при этом в формулах Φ_1, Φ_2 предикаты вида

$$x_1+x_2+z=w, \quad z+w=x_1+x_2, \quad (x_1+x_2)z=w, \quad zw=x_1+x_2,$$

$$x_1x_3+x_2+z=w,\ z+w=x_1x_3+x_2,\ (x_1x_3+x_2)z=w,\ zw=x_1x_3+x_2$$

принадлежат классу **BA** согласно утверждению 1.4. С кванторами типа $(Qz)_{z\leqslant x_1+x_2}$ или $(Qz)_{z\leqslant x_1x_3+x_2}$, которые, возможно, появляются в формулах Φ_1, Φ_2, поступаем так же, как с квантором $(Qx)_{x\leqslant P}$ (отметим, что описанная выше процедура не увеличивает числа кванторов в формулах Φ_1 и Φ_2). Утверждение доказано.

Теорема 1.1. *Предикаты класса* **BA** *и только они представимы в форме*

$$(Q_1x_1)_{x_1\leqslant P_1}\ldots(Q_mx_m)_{x_m\leqslant P_m}(R_1=R_2), \tag{1.2}$$

где $Q_1,\ldots,Q_m$ — кванторы $\exists$ или $\forall$, а $P_1,\ldots,P_m,R_1,R_2$ — полиномы с натуральными коэффициентами.

Доказательство. Из утверждения 1.2 вытекает, что каждый предикат класса **BA** можно представить в форме (1.2). Обратно, если предикат ρ представи́м в форме (1.2), то принадлежность ρ классу **BA** следует из утверждений 1.4 и 1.5.

Следствие. *Класс* **BA** *замкнут относительно операции подстановки полиномов с натуральными коэффициентами.*

Доказательство. Пусть $\rho(y_1, \ldots, y_m) \in \mathbf{BA}$, $P_1(x_1, \ldots, x_n), \ldots, P_m(x_1, \ldots, x_n)$ — полиномы с натуральными коэффициентами и

$$\sigma(x_1, \ldots, x_n) \equiv \rho\big(P_1(x_1, \ldots, x_n), \ldots, P_m(x_1, \ldots, x_n)\big).$$

Тогда

$$\sigma(x_1, \ldots, x_n) \equiv (\exists y_1)_{y_1 \leqslant P_1(x_1, \ldots, x_n)} \ldots (\exists y_m)_{y_m \leqslant P_m(x_1, \ldots, x_n)} \big((y_1 = P_1(x_1, \ldots, x_n)) \;\&\; \ldots \;\&\; (y_m = P_m(x_1, \ldots, x_n)) \;\&\; \rho(y_1, \ldots, y_m)\big).$$

Далее используем утверждение 1.4 и доказанную теорему.

§ 1.2. Рудиментарные предикаты

1. Определим взаимно однозначное соответствие между множеством $\mathbb{N}$ и множеством всех слов в алфавите $\{1, 2\}$ (включая пустое слово Λ). Произвольному непустому слову $a_k \ldots a_0$, составленному из символов 1 и 2, сопоставим натуральное число

$$\nu(a_k \ldots a_0) = \sum_{i=0}^{k} a_i \cdot 2^i.$$

Пустому слову Λ сопоставим число 0. Слово $a_k \ldots a_0$ будем называть *диадическим представлением* числа $\nu(a_k \ldots a_0)$.

Отображение ν позволяет говорить о словарных предикатах в алфавите $\{1, 2\}$ как о числовых предикатах на множестве $\mathbb{N}$. Поэтому в дальнейшем мы будем часто определять словарные предикаты в алфавите $\{1, 2\}$, имея в виду, что одноименные им числовые предикаты на множестве $\mathbb{N}$ получаются с помощью отображения ν.

На множестве всех слов в алфавите $\{1, 2\}$ определим предикат $x * y = z$ *конкатенации* (сцепления): $(x * y = z) \equiv$ (слово z получается из слова x приписыванием слова y справа). Там, где это не вызывает недоразумения, предикат $x * y = z$ записываем в виде $xy = z$.

На основе предиката конкатенации дадим индуктивное определение класса **R** *рудиментарных* предикатов (которые будем рассматривать и как словарные предикаты в алфавите $\{1, 2\}$, и как числовые предикаты на множестве $\mathbb{N}$). Исходным предикатом класса **R** является предикат конкатенации $x * y = z$. В качестве порождающих операций класса **R** рассматриваются операции логики высказываний, операции навешивания ограниченных кванторов $(\exists x)_{x \leqslant y}$ и $(\forall x)_{x \leqslant y}$, а также явные преобразования. При этом для слов x, y неравенство $x \leqslant y$ в ограниченных кванторах понимается как $\nu(x) \leqslant \nu(y)$.

2. Установим, прежде всего, что все рудиментарные предикаты являются ограниченно арифметическими.

Обозначим через $l(x)$ длину диадического представления числа x (полагаем $l(0) = 0$). Очевидно, что наименьшим числом, имеющим длину диадического представления n, является число $2^n - 1$ (при $n > 0$ его диадическое представление состоит из n символов 1), а наибольшим — число $2(2^n - 1)$ (при $n > 0$ его диадическое представление состоит из n символов 2). Поэтому равенство $l(x) = l(y)$ выполняется в том и только в том случае, когда для некоторого n из $\mathbb{N}$ каждое из чисел x, y не менее числа $2^n - 1$ и не более числа $2(2^n - 1)$. Исходя из этого строим формулу, устанавливающую принадлежность предиката $l(x) = l(y)$ классу $\mathbf{BA}$:

$$\begin{aligned}(l(x) = l(y)) \equiv (\exists z)_{z \leqslant x} (\exists v)_{v \leqslant x+1} (\exists w)_{w \leqslant 2x} \big((z \leqslant y) \mathbin{\&} \\ \mathbin{\&} (z + 1 = v) \mathbin{\&} \mathrm{Dp}\,(v, 2) \mathbin{\&} (z + z = w) \mathbin{\&} (x \leqslant w) \mathbin{\&} (y \leqslant w)\big)\end{aligned}$$

(содержательно здесь $z = 2^n - 1$, $v = 2^n$ и $w = 2(2^n - 1)$). Если теперь $x * y = z$ и $n = l(y)$, то $z = x \cdot 2^n + y$. Поэтому

$$\begin{aligned}(x * y = z) \equiv (\exists s)_{s \leqslant z} (\exists t)_{t \leqslant z} (\exists v)_{v \leqslant z} \big((s + 1 = t) \mathbin{\&} \\ \mathbin{\&} \mathrm{Dp}\,(t, 2) \mathbin{\&} (l(s) = l(y)) \mathbin{\&} (x \cdot t = v) \mathbin{\&} (v + y = z)\big).\end{aligned}$$

Таким образом, предикат конкатенации принадлежит классу $\mathbf{BA}$. Сравнивая далее определения классов $\mathbf{BA}$ и $\mathbf{R}$, приходим к следующему утверждению.

Утверждение 1.6. *Имеет место соотношение* $\mathbf{R} \subseteq \mathbf{BA}$.

Докажем принадлежность классу $\mathbf{R}$ некоторых словарных предикатов. Имеем

$$(x = y) \equiv (x * \Lambda = y).$$

Пусть далее

$$\begin{aligned}&\mathrm{B}(x, y) \equiv (\text{слово } x \text{ есть начало слова } y),\\ &\mathrm{E}(x, y) \equiv (\text{слово } x \text{ есть конец слова } y),\\ &\mathrm{C}(x, y) \equiv (\text{слово } x \text{ входит в слово } y)\end{aligned}$$

(предикаты $\mathrm{B}(x, y)$, $\mathrm{E}(x, y)$, $\mathrm{C}(x, y)$ считаем истинными при $x = \Lambda$ и $x = y$). Тогда

$$\begin{aligned}&\mathrm{B}(x, y) \equiv (\exists z)_{z \leqslant y} (x * z = y),\\ &\mathrm{E}(x, y) \equiv (\exists z)_{z \leqslant y} (z * x = y),\\ &\mathrm{C}(x, y) \equiv (\exists z)_{z \leqslant y} \big(\mathrm{B}(z, y) \mathbin{\&} \mathrm{E}(x, z)\big).\end{aligned}$$

Следующее утверждение представляет собой аналог утверждения 1.1.

Утверждение 1.7. *Любой предикат класса* $\mathbf{R}$ *можно представить подходящей позитивной* (*словарной*) *формулой.*

Доказательство. Покажем сначала, что предикат $\neg\mathrm{B}(x,y)$ можно представить позитивной формулой. Для этого заметим, прежде всего, что неравенство $x \neq y$ (x и y считаем словами в алфавите $\{1,2\}$) выполняется в том и только в том случае, когда либо x есть начало y, отличное от y, либо y есть начало x, отличное от x, либо существует такое начало z слов x и y, что слово za есть начало x, слово zb есть начало y и символы a, b различны. В соответствии с этим имеем

$$\begin{aligned}(x \neq y) \equiv (\exists z)_{z\leqslant y}\big((x*1 = z \vee x*2 = z) \mathbin{\&} \mathrm{B}(z,y)\big) \vee \\ \vee (\exists z)_{z\leqslant x}\big((y*1 = z \vee y*2 = z) \mathbin{\&} \mathrm{B}(z,x)\big) \vee \\ \vee (\exists z)_{z\leqslant x}(\exists v)_{v\leqslant x}(\exists w)_{w\leqslant y}\big(\mathrm{B}(z,x) \mathbin{\&} \mathrm{B}(z,y) \mathbin{\&} \mathrm{B}(v,x) \mathbin{\&} \mathrm{B}(w,y) \mathbin{\&} \\ \mathbin{\&} ((z*1 = v) \mathbin{\&} (z*2 = w) \vee (z*2 = v) \mathbin{\&} (z*1 = w))\big).\end{aligned}$$

Теперь получаем

$$\begin{aligned}\neg\mathrm{B}(x,y) \equiv \mathrm{B}(y,x) \mathbin{\&} (x \neq y) \vee (\exists z)_{z\leqslant x}(\exists v)_{v\leqslant x}(\exists w)_{w\leqslant y} \\ \big(((z*1 = v) \mathbin{\&} (z*2 = w) \vee (z*2 = v) \mathbin{\&} (z*1 = w)) \mathbin{\&} \\ \mathbin{\&} \mathrm{B}(v,x) \mathbin{\&} \mathrm{B}(w,y)\big).\end{aligned}$$

Для завершения доказательства утверждения остается показать, что позитивной формулой можно представить предикат $\neg(x*y = z)$. Действительно,

$$\neg(x*y = z) \equiv \neg\mathrm{B}(x,z) \vee (\exists v)_{v\leqslant z}\big((x*v = z) \mathbin{\&} (v \neq y)\big).$$

3. В этом разделе мы хотим установить для класса $\mathbf{R}$ аналог теоремы 1.1. Для этого введем понятие словарного терма — аналог понятия полинома с натуральными коэффициентами: *словарным термом* будем называть любое слово, составленное из символов любых переменных и символов 1, 2.

При записи словарных термов будем пользоваться следующим соглашением: если T — словарный терм, а n — натуральное число, то T^n есть словарный терм

$$\underbrace{TT\ldots T}_{n}$$

(знак $*$ опускаем). В частности,

$$x^n = \underbrace{xx\ldots x}_{n}, \quad 1^n = \underbrace{11\ldots 1}_{n}.$$

Установим принадлежность ряда предикатов классу $\mathbf{R}$. Имеем:

$$(x \leqslant y) \equiv (\exists z)_{z\leqslant y}(x = z), \quad (x < y) \equiv (x \leqslant y) \mathbin{\&} (x \neq y).$$

Пусть предикат $1(x)$ истинен только на словах вида $11\ldots1$. Тогда

$$1(x) \equiv (\exists y)_{y\leqslant x}((1y = x) \mathbin{\&} (y1 = x)).$$

Далее,

$$(l(x) = l(y)) \equiv (x = \Lambda) \mathbin{\&} (y = \Lambda) \vee (\exists z)_{z \leqslant x} (\forall v)_{v \leqslant x} (\forall w)_{w \leqslant y} \\ \big(1(z) \mathbin{\&} (z \leqslant y) \mathbin{\&} (1(v) \Rightarrow \mathrm{B}(v, z)) \mathbin{\&} (1(w) \Rightarrow \mathrm{B}(w, z))\big),$$

$$(l(x) + l(y) = l(z)) \equiv (l(x) = l(\Lambda)) \mathbin{\&} (l(y) = l(z)) \vee (l(y) = l(\Lambda)) \mathbin{\&} \\ \mathbin{\&} (l(x) = l(z)) \vee (\exists x_1)_{x_1 \leqslant x} (\exists y_1)_{y_1 \leqslant y} (\exists z_1)_{z_1 \leqslant z} \big(1(x_1) \mathbin{\&} 1(y_1) \mathbin{\&} 1(z_1) \mathbin{\&} \\ \mathbin{\&} (l(x_1) = l(x)) \mathbin{\&} (l(y_1) = l(y)) \mathbin{\&} (l(z_1) = l(z)) \mathbin{\&} (x_1 y_1 = z_1)\big).$$

Аналогично доказывается рудиментарность предиката $l(x) + l(y) \leqslant l(z)$.

Утверждение 1.8. *Предикаты вида $T_1 = T_2$, где T_1, T_2 — словарные термы, рудиментарны.*

Доказательство. Если один из термов T_1, T_2 является словарной константой, то предикат $T_1 = T_2$ истинен только для конечного числа наборов значений переменных. Следовательно, в этом случае его можно задать табличным способом.

Пусть терм T_1 есть переменная x, а терм T_2 представим в виде

$$T_2 = y_1 y_2 \ldots y_m,$$

где $y_1, \ldots, y_m$ — либо переменные (не обязательно различные), либо словарные константы и $m \geqslant 3$. Тогда получаем

$$(T_1 = T_2) \equiv (x = y_1 y_2 \ldots y_m) \equiv (\exists z_1)_{z_1 \leqslant x} \ldots (\exists z_{m-2})_{z_{m-2} \leqslant x} \\ \big((y_1 y_2 = z_1) \mathbin{\&} (z_1 y_3 = z_2) \mathbin{\&} \ldots \mathbin{\&} (z_{m-3} y_{m-1} = z_{m-2}) \mathbin{\&} (z_{m-2} y_m = x)\big).$$

Предположим теперь, что каждый из термов T_1, T_2 отличен от переменной и от словарной константы. Представим их в виде

$$T_1 = x_1 T_1', \quad T_2 = x_2 T_2',$$

где x_1, x_2 — переменные либо словарные константы. Если (при подстановке словарных констант вместо всех переменных термов T_1, T_2) выполняется равенство $T_1 = T_2$, то либо x_1 является началом x_2, либо наоборот. В соответствии с этим

$$(T_1 = T_2) \equiv (x_1 T_1' = x_2 T_2') \equiv (\exists y)_{y \leqslant x_2} \big((x_1 y = x_2) \mathbin{\&} (T_1' = y T_2')\big) \vee \\ \vee (\exists y)_{y \leqslant x_1} \big((x_2 y = x_1) \mathbin{\&} (y T_1' = T_2')\big).$$

Таким образом, вопрос о рудиментарности предиката $x_1 T_1' = x_2 T_2'$ сводится к аналогичному вопросу для $T_1' = y T_2'$ и $y T_1' = T_2'$. Однако длины термов $y T_1'$ и $y T_2'$ равны соответственно длинам термов T_1 и T_2, а длины термов T_1', T_2' меньше длин термов T_1, T_2. Поэтому обращением к принципу индукции завершается доказательство утверждения.

Утверждение 1.9. *Класс* $\mathbf{R}$ *замкнут относительно операций навешивания ограниченных кванторов вида*

$$(\exists x)_{x \leqslant T}, \quad (\forall x)_{x \leqslant T},$$

где T *— словарный терм.*

Доказательство. Пусть рудиментарный предикат σ определяется формулой Φ и $\rho \equiv (Qx)_{x \leqslant T}\Phi$, где Q — квантор $\exists$ или $\forall$, а T — словарный терм, отличный от переменной и константы. Согласно утверждению 1.7 можно предполагать, что формула Φ позитивна.

Предположим, что $T = T_1T_2$, где T_1, T_2 — непустые словарные термы. Покажем, как преобразовать формулу $(Qx)_{x \leqslant T}\Phi$ в эквивалентную формулу Φ', в которой квантор $(Qx)_{x \leqslant T}$ заменен кванторами вида $(Qx_1)_{x_1 \leqslant T_1}$, $(Qx_2)_{x_2 \leqslant T_2}$.

Заметим, прежде всего, что область $x \leqslant T$ можно представить в виде объединения двух (вообще говоря, пересекающихся) множеств значений терма x_1x_2: одного для $x_1 \leqslant T_1$, $x_2 \leqslant T_2$ и другого для $x_1 < T_1$, $l(x_2) \leqslant l(T_2)$. При равенстве значений $l(x_2)$, $l(T_2)$ переменная x_2 может принимать значения, которые больше значений, принимаемых термом T_2. Поэтому область значений переменной x_2, подчиненной условию $l(x_2) \leqslant l(T_2)$, в свою очередь представим в виде множества значений терма $x_2'x_2''$, где $x_2' \leqslant T_2$, $x_2'' \leqslant T_2$ и $l(x_2') + l(x_2'') \leqslant l(T_2)$.

В соответствии с этим формула $(\exists x)_{x \leqslant T}\Phi$ будет заменена формулой вида

$$(\exists x_1)_{x_1 \leqslant T_1}(\exists x_2)_{x_2 \leqslant T_2}\Phi_1 \vee (\exists x_1)_{x_1 \leqslant T_1}(\exists x_2')_{x_2' \leqslant T_2}(\exists x_2'')_{x_2'' \leqslant T_2} \\ \big((x_1 < T_1) \,\&\, (l(x_2') + l(x_2'') \leqslant l(T_2)) \,\&\, \Phi_2\big),$$

а формула $(\forall x)_{x \leqslant T}\Phi$ — формулой вида

$$(\forall x_1)_{x_1 \leqslant T_1}(\forall x_2)_{x_2 \leqslant T_2}\Phi_1 \,\&\, (\forall x_1)_{x_1 \leqslant T_1}(\forall x_2')_{x_2' \leqslant T_2}(\forall x_2'')_{x_2'' \leqslant T_2} \\ \big((x_1 < T_1) \,\&\, (l(x_2') + l(x_2'') \leqslant l(T_2)) \Rightarrow \Phi_2\big),$$

где $x_1 < T_1$ и $l(x_2') + l(x_2'') \leqslant l(T_2)$ суть сокращения для формул

$$(\exists v)_{v \leqslant T_1}(x_1 < v), \quad (\exists v)_{v \leqslant T_2}(l(x_1') + l(x_2'') \leqslant l(v)).$$

Формулы Φ_1, Φ_2 получаются из формулы Φ следующими преобразованиями. Кванторы вида $(Qy)_{y \leqslant x}$ в формуле Φ_1 заменяем кванторами $(Qy)_{y \leqslant x_1x_2}$, а в формуле Φ_2 — кванторами $(Qy)_{y \leqslant x_1x_2'x_2''}$. Предикаты вида

$$xz = w, \quad zx = w, \quad zw = x,$$

входящие в формулу Φ, в формуле Φ_1 заменяем соответственно предикатами

$$x_1x_2z = w, \quad zx_1x_2 = w, \quad zw = x_1x_2,$$

а в формуле Φ_2 — предикатами

$$x_1x_2'x_2''z = w, \quad zx_1x_2'x_2'' = w, \quad zw = x_1x_2'x_2''.$$

Согласно утверждению 1.8 все выписанные предикаты принадлежат классу $\mathbf{R}$. В результате проведенных преобразований получим формулу Φ', которая, как нетрудно видеть, эквивалентна формуле $(Qx)_{x\leqslant T}\Phi$ и не содержит квантора $(Qx)_{x\leqslant T}$. Однако в ней помимо кванторов вида

$$(Qx_1)_{x_1\leqslant T_1},\quad (Qx_2')_{x_2'\leqslant T_2},\quad (Qx_2'')_{x_2''\leqslant T_2}\tag{1.3}$$

могут появиться кванторы вида $(Qy)_{y\leqslant x_1x_2}$ или $(Qy)_{y\leqslant x_1x_2'x_2''}$. Отметим, что последние кванторы «произошли» из квантора вида $(Qy)_{y\leqslant x}$, входившего в формулу Φ. Таким образом, мы имеем индуктивный процесс: квантор $(Qx)_{x\leqslant T}$ исходной формулы заменяется кванторами (1.3), а кванторы вида $(Qy)_{y\leqslant x}$, стоящие, быть может, в формуле Φ после квантора $(Qx)_{x\leqslant T}$, — кванторами $(Qy)_{y\leqslant x_1x_2}$ и $(Qy)_{y\leqslant x_1x_2'x_2''}$. Утверждение доказано.

Основная цель этого раздела — доказать для класса $\mathbf{R}$ аналог теоремы 1.1. Для этого нам понадобится установить несколько лемм. В этих леммах через $|A|$ обозначается длина слова A в алфавите $\{1,2\}$, причем $|\Lambda|=0$.

Лемма 1.1. *Для любых слов A_1, A_2, B_1, B_2 в алфавите $\{1,2\}$ равенства*

$$A_1=B_1,\quad A_2=B_2\tag{1.4}$$

выполняются одновременно тогда и только тогда, когда выполняется равенство

$$A_11B_1A_12B_1A_21B_2A_22B_2=B_11A_1B_12A_1B_21A_2B_22A_2.\tag{1.5}$$

Доказательство. Легко убедиться в том, что из равенств (1.4) следует равенство (1.5). Обратно, пусть выполняется равенство (1.5). Поскольку

$$|A_11B_1|=|B_11A_1|,\quad |A_12B_1|=|B_12A_1|,$$
$$|A_21B_2|=|B_21A_2|,\quad |A_22B_2|=|B_22A_2|,$$

из (1.5) следует, что

$$A_11B_1=B_11A_1,\ A_12B_1=B_12A_1,\ A_21B_2=B_21A_2,\ A_22B_2=B_22A_2.$$

Покажем, что из соотношений

$$A_11B_1=B_11A_1,\quad A_12B_1=B_12A_1\tag{1.6}$$

вытекает, что $A_1=B_1$. В самом деле, предположим, что, напротив, $A_1\neq B_1$. Равенства (1.6) показывают, что либо A_1 есть собственное начало слова B_1, либо B_1 есть собственное начало слова A_1. Пусть, например, A_1 есть собственное начало слова B_1. Если $m=|A_11|$, то первое из равенств (1.6) говорит о том, что m-я буква слова B_1 есть 1, а второе из равенств (1.6) — что та же самая буква есть 2. Противоречие показывает, что $A_1=B_1$. Аналогично устанавливается, что $A_2=B_2$. Лемма доказана.

Лемма 1.2. *Пусть A, B, C, D — слова в алфавите $\{1,2\}$. Тогда по крайней мере одно из равенств $A = B$, $C = D$ выполняется в том и только в том случае, когда выполняется хотя бы одно из равенств $AC = AD$ или $AC = BC$.*

Доказательство. Если $A = B$, то, очевидно, $AC = BC$, а если $C = D$, то $AC = AD$. Обратно, если $AC = AD$, то $C = D$, а если $AC = BC$, то $A = B$. Лемма доказана.

Пусть A, B, C — слова в алфавите $\{1,2\}$. Обозначим через L следующую систему словарных уравнений:

$$1A1B1 = x_1 1C1x_2, \tag{1.7}$$

$$2A2B2 = x_3 2C2x_4, \tag{1.8}$$

$$x_1x_2 = x_2x_1, \tag{1.9}$$

$$x_1x_4 = x_4x_1, \tag{1.10}$$

$$x_2x_3 = x_3x_2, \tag{1.11}$$

$$x_3x_4 = x_4x_3. \tag{1.12}$$

Лемма 1.3. *Если система уравнений L имеет решение x_1', x_2', x_3', x_4', то одно из слов x_1', x_2', x_3', x_4' является непустым, а два других (из оставшихся) — пустыми.*

Доказательство. Если бы все слова x_1', x_2', x_3', x_4' были пустыми, то из уравнения (1.7) после сокращения слева и справа на 1 получили бы $A1B = C$, а от уравнения (1.8) после аналогичного сокращения слева и справа на 2 осталось бы $A2B = C$. Равенство $A1B = A2B$, очевидно, невозможно.

Предположим, что не более чем одно из слов x_1', x_2', x_3', x_4' является пустым. Тогда либо $x_1' \neq \Lambda$, $x_3' \neq \Lambda$ и $x_{2\delta+2}' \neq \Lambda$ для некоторого δ из $\{0,1\}$, либо $x_2' \neq \Lambda$, $x_4' \neq \Lambda$ и $x_{2\delta+1}' \neq \Lambda$ для некоторого δ из $\{0,1\}$.

Рассмотрим первую возможность. Из уравнений (1.9)–(1.12) следует, что

$$x_1'x_{2\delta+2}' = x_{2\delta+2}'x_1', \quad x_{2\delta+2}'x_3' = x_3'x_{2\delta+2}'.$$

Поскольку все слова x_1', x_3', $x_{2\delta+2}'$ непустые, из этих равенств следует далее, что все слова x_1', x_3', $x_{2\delta+2}'$ начинаются с одного и того же символа. Однако уравнения (1.7), (1.8) показывают, что слова x_1', x_3' должны начинаться с различных символов.

Аналогично получаем противоречие при рассмотрении второй возможности, но здесь в словах x_2', x_4', $x_{2\delta+1}'$ необходимо рассматривать последний символ. Лемма доказана.

Лемма 1.4. *Если система уравнений L имеет решение x_1', x_2', x_3', x_4', то либо $x_1' = x_3' = \Lambda$, либо $x_2' = x_4' = \Lambda$.*

Доказательство. Из леммы 1.3 вытекает, что имеет место хотя бы одна из следующих возможностей:

$$x_1' = x_2' = \Lambda, \quad x_1' = x_3' = \Lambda, \quad x_1' = x_4' = \Lambda,$$
$$x_2' = x_3' = \Lambda, \quad x_2' = x_4' = \Lambda, \quad x_3' = x_4' = \Lambda.$$

Поскольку $|1A1B1| = |2A2B2|$ и хотя бы одно из слов x_1', x_2', x_3', x_4' непусто, из уравнений (1.7), (1.8) выводим, что случаи $x_1' = x_2' = \Lambda$ и $x_3' = x_4' = \Lambda$ невозможны.

Предположим, что $x_1' = x_4' = \Lambda$. Вновь рассматривая уравнения (1.7), (1.8) и пользуясь соотношениями

$$|1A1B1| = |2A2B2|, \quad |1C1| = |2C2|,$$

получаем, что $|x_2'| = |x_3'|$. Из уравнения (1.11) теперь следует, что $x_2' = x_3'$. Далее, уравнение (1.7) показывает, что число символов 1 в слове Cx_2' равно числу символов 1 в слове $A1B$, а уравнение (1.8) — что аналогичное число для слова $x_3'C$ будет равно числу символов 1 в слове $A2B$. Так как слова $A1B, A2B$ содержат различное число символов 1, приходим к противоречию.

Аналогичным образом приходим к противоречию в случае $x_2' = x_3' = \Lambda$. Лемма доказана.

Лемма 1.5. *Пусть A, B, C — слова в алфавите $\{1,2\}$. Тогда хотя бы одно из равенств $A = C$ или $B = C$ выполняется в том и только том случае, когда система уравнений L имеет решение x_1, x_2, x_3, x_4, где $x_1 \leqslant 1A$, $x_2 \leqslant B1$, $x_3 \leqslant 2A$, $x_4 \leqslant B2$.*

Доказательство. *Необходимость.* Если выполняется равенство $A = C$, то в качестве значений переменных x_1, x_2, x_3, x_4, удовлетворяющих системе L, следует взять слова Λ, $B1$, Λ, $B2$. Если же выполняется равенство $B = C$, то соответствующие слова суть $1A$, Λ, $2A$, Λ.

Достаточность. Пусть система L имеет решение x_1', x_2', x_3', x_4'. Согласно лемме 1.4 имеются две возможности: $x_1' = x_3' = \Lambda$ и $x_2' = x_4' = \Lambda$. В первом случае, сокращая обе части равенства (1.7) слева на 1 и обе части равенства (1.8) слева на 2, приходим к равенствам

$$A1B1 = C1x_2', \quad A2B2 = C2x_4'. \tag{1.13}$$

Из них следует, что $A = C$. В самом деле, если $|A| < |C|$, то слова $A1$ и $A2$ суть начала слова C, что невозможно. Если же $|A| > |C|$, то аналогичным образом получаем, что слова $C1$ и $C2$ суть начала слова A. Значит, $|A| = |C|$. А тогда равенства (1.13) показывают, что $A = C$.

Случай $x_2' = x_4' = \Lambda$ рассматривается аналогично. Лемма доказана.

Теорема 1.2. *Предикаты класса* $\mathbf{R}$ *и только они представимы в форме*

$$(Q_1x_1)_{x_1 \leqslant T_1} \ldots (Q_mx_m)_{x_m \leqslant T_m}(R_1 = R_2), \tag{1.14}$$

где $Q_1, \ldots, Q_m$ — кванторы $\exists$ или $\forall$, а $T_1, \ldots, T_m$, R_1, R_2 — словарные термы.

Доказательство. Пусть предикат ρ рудиментарен. Тогда в силу утверждения 1.6 его можно представить позитивной формулой Φ. Будем предполагать, что она находится в предваренной нормальной форме. Используя леммы 1.1, 1.2 и 1.5, будем последовательно заменять в формуле Φ конъюнкции и дизъюнкции равенств словарных термов формулами вида (1.14), вынося затем ограниченные кванторы существования в начало формулы. В результате придем к представлению (1.14) для предиката ρ.

Обратно, если предикат ρ представим в форме (1.14), то рудиментарность ρ следует из утверждений 1.8 и 1.9. Теорема доказана.

4. В заключение параграфа докажем рудиментарность двух более сложных предикатов.

Начнем с арифметического предиката $x + y = z$. Если w — непустое слово и $1 \leqslant i \leqslant |w|$, то через $w(i)$ будем обозначать i-й справа символ слова w. Для проверки выполнения равенства $x + y = z$ средствами класса $\mathbf{R}$ введем два вспомогательных слова u, v длины $l(z)$ в алфавите $\{1, 2\}$. Для любого i $(1 \leqslant i \leqslant l(z))$ пусть $u(i) = 1$ тогда и только тогда, когда при сложении чисел x, y, заданных диадическими представлениями, имеется перенос из $(i-1)$-го разряда в i-й разряд. Если $u(i) = 1$, то $v(i)$ есть величина переноса из $(i-1)$-го разряда в i-й разряд (при $u(i) = 2$ значение $v(i)$, равное 1 или 2, можно выбрать произвольно). Очевидно, что $u, v \leqslant 1z$.

Если длины диадических представлений чисел x, y не менее i, то

$$z(i) = \begin{cases} \text{первому справа разряду диадического представления числа} \\ x(i) + y(i) + v(i), \ \text{если } u(i) = 1; \\ \text{первому справа разряду диадического представления числа} \\ x(i) + y(i), \ \text{если } u(i) = 2 \end{cases}$$

(x, y, z одновременно рассматриваются и как числа из $\mathbb{N}$, и как соответствующие диадические представления).

Подобным образом определяется значение $z(i)$ в тех случаях, когда длина диадического представления хотя бы одного из чисел x, y меньше i.

Аналогично, если для данного i величины $x(i-1)$, $y(i-1)$, $u(i-1)$, $v(i-1)$ имеют смысл, то

$$u(i) = \begin{cases} 1, & \text{если } u(i-1) = 1 \text{ и длина диадического представления} \\ & \text{числа } x(i-1) + y(i-1) + v(i-1) \text{ равна 2, либо} \\ & u(i-1) = 2 \text{ и длина диадического представления числа} \\ & x(i-1) + y(i-1) \text{ равна 2;} \\ 2 & \text{в остальных случаях;} \end{cases}$$

$$v(i) = \begin{cases} \text{второму справа разряду диадического представления числа} \\ x(i-1) + y(i-1) + v(i-1), \ \text{если } u(i-1) = 1; \\ \text{второму справа разряду диадического представления числа} \\ x(i-1) + y(i-1), \ \text{если } u(i-1) = 2. \end{cases}$$

Опираясь на приведенные соотношения, нетрудно построить рудиментарное представление предиката $x+y=z$. Для упрощения дальнейших построений отбросим сразу тривиальные случаи, когда $x=0$ или $y=0$. Далее предполагаем, что $x \neq 0$, $y \neq 0$ и, следовательно, $z \neq 0$.

Искомая формула, выражающая в этом случае предикат $x+y=z$, будет иметь вид

$$(\exists u)_{u \leqslant 1z}(\exists v)_{v \leqslant 1z}\Phi(x,y,z,u,v).$$

В свою очередь формула $\Phi(x,y,z,u,v)$ будет представлять собой конъюнкцию формул

$$\Phi_1(x,y,z,u,v), \quad \Phi_2(x,y,z,u,v), \quad \Phi_3(x,y,z,u,v),$$

где содержательно формулы Φ_1, Φ_2, Φ_3 обеспечивают правильность вычисления разрядов $z(i)$, $u(i)$, $v(i)$.

Рассмотрим более подробно формулу Φ_1. Чтобы иметь возможность оперировать с i-ми разрядами слов x, y, z, u, v, введем переменные x_1, y_1, z_1, u_1, v_1. Содержательно они представляют собой концы слов x, y, z, u, v длины i. Таким образом, первые символы слов x_1, y_1, z_1, u_1, v_1 суть i-е разряды слов x, y, z, u, v. В соответствии с этим формула Φ_1 будет иметь вид

$$(\forall x_1)_{x_1 \leqslant x}(\forall y_1)_{y_1 \leqslant y}(\forall z_1)_{z_1 \leqslant z}(\forall u_1)_{u_1 \leqslant u}(\forall v_1)_{v_1 \leqslant v}\big(\mathrm{E}(x_1,x) \mathbin{\&} \mathrm{E}(y_1,y) \mathbin{\&} \\ \mathbin{\&} \mathrm{E}(z_1,z) \mathbin{\&} \mathrm{E}(u_1,u) \mathbin{\&} \mathrm{E}(v_1,v) \Rightarrow \Phi_{11}(x,y,x_1,y_1,z_1,u_1,v_1)\big).$$

Формула Φ_{11} осуществляет «разбор» всевозможных случаев:

$$\begin{aligned}
&l(x_1)=l(y_1)=l(z_1)=l(u_1)=l(v_1), \quad B(1,u_1);\\
&l(x_1)=l(y_1)=l(z_1)=l(u_1)=l(v_1), \quad B(2,u_1);\\
&l(x_1)=l(z_1)=l(u_1)=l(v_1)>l(y), \quad B(1,u_1);\\
&l(x_1)=l(z_1)=l(u_1)=l(v_1)>l(y), \quad B(2,u_1);\\
&l(y_1)=l(z_1)=l(u_1)=l(v_1)>l(x), \quad B(1,u_1);\\
&l(y_1)=l(z_1)=l(u_1)=l(v_1)>l(x), \quad B(2,u_1);\\
&l(z_1)=l(u_1)=l(v_1)=\max\left(l(x),l(y)\right)+1, \quad B(1,u_1).
\end{aligned}$$

Каждому из этих семи случаев в формуле Φ_{11} отвечает конъюнктивно входящая в нее подформула. Структура этих подформул по существу одинакова. Мы приведем лишь подформулу, которая отвечает первому случаю:

$$\begin{aligned}
(l(x_1)=l(y_1)=l(z_1)=l(u_1)=l(v_1)) \mathbin{\&} \mathrm{B}(1,u_1) \;\Rightarrow&\\
\Rightarrow\; (\mathrm{B}(1,x_1) \mathbin{\&} \mathrm{B}(1,y_1) \mathbin{\&} \mathrm{B}(1,v_1) &\vee\\
\vee\; \mathrm{B}(2,x_1) \mathbin{\&} \mathrm{B}(2,y_1) \mathbin{\&} \mathrm{B}(1,v_1) &\vee\\
\vee\; \mathrm{B}(2,x_1) \mathbin{\&} \mathrm{B}(1,y_1) \mathbin{\&} \mathrm{B}(2,v_1) &\vee
\end{aligned}$$

$$
\begin{aligned}
&\vee\ \mathrm{B}(1,x_1)\,\&\,\mathrm{B}(2,y_1)\,\&\,\mathrm{B}(2,v_1))\,\&\,\mathrm{B}(1,z_1) \vee \\
&\qquad \vee\ \mathrm{B}(1,x_1)\,\&\,\mathrm{B}(1,y_1)\,\&\,\mathrm{B}(2,v_1) \vee \\
&\qquad \vee\ \mathrm{B}(1,x_1)\,\&\,\mathrm{B}(2,y_1)\,\&\,\mathrm{B}(1,v_1) \vee \\
&\qquad \vee\ \mathrm{B}(2,x_1)\,\&\,\mathrm{B}(1,y_1)\,\&\,\mathrm{B}(1,v_1) \vee \\
&\qquad\qquad\qquad \vee\ \mathrm{B}(2,x_1)\,\&\,\mathrm{B}(2,y_1)\,\&\,\mathrm{B}(2,v_1)\,\&\,\mathrm{B}(2,z_1).
\end{aligned}
$$

Аналогично определяются формулы Φ_2 и Φ_3.

Рассмотрим теперь предикат $y = 2^x$. Очевидно, что его принадлежность классу $\mathbf{R}$ следует из принадлежности классу $\mathbf{R}$ предиката $y = 2^x - 1$. Заметим, что при $x > 0$ диадическое представление числа $2^x - 1$ имеет вид 1^x. В связи с этим предикат $y = 2^x - 1$ будем рассматривать в эквивалентной форме «диадическое представление y есть слово, составленное из x символов 1».

Пусть $a_n a_{n-1} \ldots a_1$ — диадическое представление x. Чтобы проверить выполнимость равенства $y = 2^x - 1$, достаточно образовать последовательность пар вида

$$(a_n, 1^{a_n}), (a_n a_{n-1}, 1^{a_n a_{n-1}}), \ldots, (a_n a_{n-1} \ldots a_1, 1^{a_n a_{n-1} \ldots a_1}) \tag{1.15}$$

и убедиться в том, что $y = 1^{a_n a_{n-1} \ldots a_1}$ (т. е. диадическое представление y имеет вид $1^{a_n a_{n-1} \ldots a_1}$). Переход от пары к паре в последовательности (1.15) подчиняется довольно простому правилу, которое ниже формализуется средствами класса $\mathbf{R}$. Поскольку в классе $\mathbf{R}$ невозможно непосредственно изобразить последовательность (1.15), мы определим вспомогательное слово u, которое будет кодировать эту последовательность. Слово u имеет вид

$$
\begin{aligned}
&2a_n 2 1^n 1^{a_n} \bullet 2a_n a_{n-1} 2 1^n 1^{a_n a_{n-1}} \bullet \ldots \bullet 2a_n \ldots a_2 2 1^n 1^{a_n \ldots a_2} \bullet \\
&\qquad\qquad\qquad 2a_n \ldots a_1 2 1^n 1^{a_n \ldots a_1},
\end{aligned}
\tag{1.16}
$$

где для большей наглядности жирными точками отделены подслова, которые отвечают парам последовательности (1.15). Нетрудно видеть, что при условии $l(y) = a_n a_{n-1} \ldots a_1$ справедлива оценка

$$|u| \leqslant 2l(y) + c \cdot (\log_2 l(y))^2 + d,$$

где c, d — некоторые положительные константы. Следовательно, если выбрать достаточно большое y_0, то при $y > y_0$ будет выполняться неравенство $u \leqslant yyy$.

Обозначим через $\sigma(u, x)$ предикат «диадическое представление u имеет вид (1.16)». Тогда при $y > y_0$ справедлива эквивалентность

$$(y = 2^x - 1) \equiv (\exists u)_{u \leqslant yyy} \big(\sigma(u, x)\,\&\,\varphi(u, x, y)\big), \tag{1.17}$$

где предикат $\varphi(u, x, y)$, используя особенности строения слова u, проверяет равенство $y = 2^x - 1$. Из представления (1.16) видно, что предикат φ можно выразить следующим образом:

$$
\begin{aligned}
\varphi(u, x, y) \equiv 1(y)\,\&\,(\exists v)_{v \leqslant u} (\exists w)_{w \leqslant u} \big(1(w)\,\&\,(v2w = u)\,\& \\
\&\ (l(x) + l(y) = l(w))\big).
\end{aligned}
$$

Приведенная эквивалентность показывает, что $\varphi \in \mathbf{R}$. Поскольку при $y \leqslant y_0$ предикат $y = 2^x - 1$ можно задать табличным способом, из формулы (1.17) заключаем, что предикат $y = 2^x - 1$ принадлежит классу $\mathbf{R}$, если только классу $\mathbf{R}$ принадлежит предикат σ. Поэтому наши дальнейшие усилия будут направлены на доказательство рудиментарности предиката σ.

Предикат σ будет определен формулой, состоящей из конъюнкции подформул, которые содержатся в нижеследующих пп. 1–5. Еще раз напомним, что предикат σ рассматривается при достаточно больших y и, следовательно, при достаточно больших x. В частности, будем предполагать, что $x > 2$.

1. Началом слова u служит слово вида $2a21^n1^a2$, где $n = l(x)$ и a — первый символ диадического представления числа x:

$$(\exists v)_{v \leqslant u}\big(1(v) \mathbin{\&} (l(v) = l(x)) \mathbin{\&} (\mathrm{B}(1, x) \Rightarrow \mathrm{B}(212v12, u)) \mathbin{\&} \\ \mathbin{\&} (\mathrm{B}(2, x) \Rightarrow \mathrm{B}(222v112, u))\big)$$

(здесь и далее мы используем выражение вида $\mathrm{B}(212v12, u)$ в качестве сокращения для формулы

$$(\exists v_1)_{v_1 \leqslant u}(\exists v_2)_{v_2 \leqslant u}\big((212v = v_1) \mathbin{\&} (v_1 12 = v_2) \mathbin{\&} \mathrm{B}(v_2, u)\big)).$$

2. Концом слова u является слово вида 1^k2x21^m, где $k, m > l(x)$:

$$(\exists v)_{v \leqslant u}(\exists w)_{w \leqslant u}\big(1(v) \mathbin{\&} 1(w) \mathbin{\&} \\ \mathbin{\&} (l(v) > l(x)) \mathbin{\&} (l(w) > l(x)) \mathbin{\&} \mathrm{E}(v2x2w, u)\big).$$

3. Если в слово u входит слово вида $1^{n+1}2w21^{n+1}$, где $n = l(x)$, и слово w не содержит подслова 1^{n+1}, то w есть начало x:

$$(\forall w)_{w \leqslant u}(\forall z)_{z \leqslant u}\big(1(z) \mathbin{\&} (l(z) = l(x) + 1) \mathbin{\&} \mathrm{C}(z2w2z, u) \mathbin{\&} \\ \mathbin{\&} \neg\mathrm{C}(z, w) \Rightarrow \mathrm{B}(w, x)\big).$$

4а. Если началом слова u является слово вида $2w_121^m2w_221^{n+1}$, где $|w_1| \leqslant l(x)$, $|w_2| \leqslant l(x)$, $m > l(x)$, $n = l(x)$, то $|w_2| = |w_1| + 1$.

4б. Если в слово u входит слово вида $1^{n+1}2w_121^m2w_221^{n+1}$, где $n = l(x)$, $m > l(x)$, $|w_1| \leqslant l(x)$, $|w_2| \leqslant l(x)$, то $|w_2| = |w_1| + 1$.

Приведем формулу только для п. 4б:

$$(\forall w_1)_{w_1 \leqslant u}(\forall w_2)_{w_2 \leqslant u}(\forall z_1)_{z_1 \leqslant u}(\forall z_2)_{z_2 \leqslant u}\big((1(z_1) \mathbin{\&} 1(z_2) \mathbin{\&} \\ \mathbin{\&} (l(z_1) = l(x) + 1) \mathbin{\&} (l(z_2) > l(x)) \mathbin{\&} (l(w_1) \leqslant l(x)) \mathbin{\&} (l(w_2) \leqslant l(x)) \mathbin{\&} \\ \mathbin{\&} \mathrm{C}(z_12w_12z_22w_22z_1, u) \Rightarrow (l(w_2) = l(w_1) + 1))\big).$$

5а. Если началом слова u является слово вида $2w21^{m_1}2wa1^{m_2}2$, где $|wa| \leqslant l(x)$, $m_1 > l(x)$, $m_2 > l(x)$, то $m_2 = 2m_1 + a - n$.

5б. Если в слово u входит слово вида $1^{n+1}2w21^{m_1}2wa21^{m_2}2$, где $|wa| \leqslant l(x)$, $n = l(x)$, $m_1 > l(x)$, $m_2 > l(x)$, то $m_2 = 2m_1 + a - n$.

5в. Если концом слова u является слово вида $1^{n+1}2w21^{m_1}2wa21^{m_2}$, где $|wa| \leqslant l(x)$, $n = l(x)$, $m_1 > l(x)$, $m_2 > l(x)$, то $m_2 = 2m_1 + a - n$.

Приведем формулу только для п. 5б:

$$\begin{aligned}(\forall w)_{w\leqslant u}(\forall z_1)_{z_1\leqslant u}(\forall z_2)_{z_2\leqslant u}(\forall z_3)_{z_3\leqslant u}(\forall a)_{a\leqslant u}\big((1(z_1)\ \&\ 1(z_2)\ \&\ 1(z_3)\ \&\\ \&\ (l(z_1) = l(x)+1)\ \&\ (l(z_2) > l(x))\ \&\ (l(z_3) > l(x))\ \&\ (l(w) < l(x))\ \&\\ \&\ (a = 1 \vee a = 2)\ \&\ \mathrm{C}(z_1 2w2z_2 2wa2z_3 2, u)) \Rightarrow ((z_3 z_1 = z_2 z_2 11)\ \&\\ \&\ (a=1) \vee (z_3 z_1 = z_2 z_2 111)\ \&\ (a=2))\big).\end{aligned}$$

§ 1.3. Рудиментарное моделирование вычислений на машинах Тьюринга

1. Доказательство рудиментарности предиката $y = 2^x$, изложенное в § 1.2, приводит к некоторой общей идее, касающейся возможности обоснования рудиментарности предикатов целого семейства. Основные моменты этой идеи можно сформулировать следующим образом.

Предположим, что для словарного предиката $\pi(x)$ имеются такие действительное число α, $0 < \alpha < 1$, полином P с натуральными коэффициентами и рудиментарные предикаты $b(x, v)$, $e(x, v)$, $t(x, v, w)$, что процесс вычисления значения $\pi(x)$ можно представить в виде последовательности слов

$$v_1, \ldots, v_m, \tag{1.18}$$

где $m \leqslant P(|x|)$, $|v_i| \leqslant |x|^\alpha$ при $1 \leqslant i \leqslant m$, предикат $b(x, v)$ выделяет начало v_1 последовательности (1.18), предикат $e(x, v)$ — ее конец v_m, а предикат $t(x, v, w)$ обеспечивает правильность расположения соседних слов v_i, v_{i+1} в последовательности (1.18). Тогда рудиментарность предиката π можно установить следующим образом (чтобы не заслонять основную идею второстепенными техническими деталями, будем предполагать, что число $|x|$ достаточно велико, числа $|x|^\alpha$ и $|x|^{1-\alpha}$ целые и все слова v_i последовательности (1.18) имеют одну и ту же длину $|x|^\alpha$).

Определим, во-первых, такой рудиментарный предикат $\sigma_1(x, v, w)$, что $\sigma_1(x, v_i, v_j)$ выполняется в том и только в том случае, когда $j = i + |x|^{1-\alpha} - 1$. Для этого достаточно найти такое слово u длины $|x|$, что v есть начало слова u длины $|x|^\alpha$, w есть конец слова u длины $|x|^\alpha$ и для любых двух слов r, s длины $|x|^\alpha$ выполняется следующее условие: если слово rs входит в слово u и начинается с позиции вида $i \cdot |x|^\alpha + 1$, то имеет место $t(x, r, s)$.

Далее аналогичным образом определяем такой рудиментарный предикат $\sigma_2(x, v, w)$, что $\sigma_2(x, v_i, v_j)$ выполняется в том и только том случае, когда $j = i + (|x|^{1-\alpha} - 1)^2$. Тогда при рассмотрении соответствующего слова u длины $|x|$ вместо предиката $t(x, r, s)$ используется предикат $\sigma_1(x, r, s)$.

Вообще, продолжая по индукции, для любого натурального k определяем такой рудиментарный предикат $\sigma_k(x, v, w)$, что $\sigma_k(x, v_i, v_j)$ выполняется в том и только в том случае, когда $j = i + (|x|^{1-\alpha} - 1)^k$. Если теперь допустить, что для некоторого k справедливо равенство $m = (|x|^{1-\alpha} - 1)^k + 1$, то предикат $\sigma_k(x, v, w)$ дает возможность говорить о существовании последовательности (1.18), имея только первый и последний члены этой последовательности. Остается теперь по аргументу x с помощью предиката b выделить начало v_1 последовательности (1.18), а с помощью предиката e — ее конец v_m.

2. Изложенную выше идею естественно применить прежде всего к вычислениям на абстрактных вычислительных устройствах типа машин Тьюринга. Довольно понятно, что слова $v_1, \ldots, v_m$ должны быть кодами последовательных конфигураций для данных машин Тьюринга, причем v_1 — кодом начальной, а v_m — кодом заключительной конфигураций. Ограничения на длину слов v_i и длину последовательности (1.18) в свою очередь налагают ограничения на выбор машин Тьюринга и на способ вычисления предикатов на этих машинах.

Выберем в качестве вычислительных устройств недетерминированные двуленточные машины Тьюринга. Машины этого типа имеют входную и рабочую ленты. Входная лента служит для записи значений аргументов. Головка машины на входной ленте может только считывать символы и передвигаться по ленте в обе стороны, не выходя при этом за границы записи аргументов. На действия головки машины, расположенной на рабочей ленте, никакие ограничения не налагаются.

В качестве алфавита входной ленты возьмем алфавит $\{1, 2, *\}$, где символ $*$ играет роль разделительного и ограничительного символа. В качестве алфавита рабочей ленты можно взять любой неоднобуквенный алфавит — доказываемые далее результаты не зависят от числа букв в этом алфавите. В целях унификации обозначений в качестве алфавита рабочей ленты выберем также алфавит $\{1, 2, *\}$. В данном случае $*$ будет играть роль «пустого» символа.

Двуленточная машина Тьюринга $\mathcal{M}$ с входным и рабочим алфавитом $\{1, 2, *\}$ задается множеством состояний $Q = \{q_1, \ldots, q_s\}$ с выделенными начальным q_1 и заключительным q_s состояниями и конечным множеством команд вида

$$abq_i \to cq_j D_1 D_2, \tag{1.19}$$

где $a, b, c \in \{1, 2, *\}$, $1 \leqslant i < s$, $1 \leqslant j \leqslant s$, $D_1, D_2 \in \{L, R, S\}$. Мы будем рассматривать недетерминированный вариант машин Тьюринга, поэтому в множестве команд машины $\mathcal{M}$ может быть, вообще говоря, несколько различных команд (1.19) с одинаковой левой частью abq_i.

Команда (1.19) интерпретируется следующим образом: если машина $\mathcal{M}$ в некоторый момент времени t находится в состоянии q_i, а ее головки на входной и рабочей лентах считывают соответственно символы a и b, то в следующий момент времени $t + 1$ машина $\mathcal{M}$ будет находиться в состоянии q_j, обозреваемый символ b на рабочей ленте будет заменен символом c, а головки на входной и рабочей лентах совершат перемещения в соответствии со значениями D_1 и D_2 (L — сдвиг на одну клетку влево, R — вправо, S — отсутствие сдвига).

Чтобы вычислить на машине Тьюринга $\mathcal{M}$ словарный предикат $\pi(x_1, \ldots, x_n)$, поступаем следующим образом. Набор значений переменных $x_1, \ldots, x_n$ записываем на входной ленте машины $\mathcal{M}$ в виде слова

$$*x_1 * \ldots * x_n * . \tag{1.20}$$

Перед началом вычисления машина $\mathcal{M}$ приводится в состояние q_1, а ее головка на входной ленте устанавливается на самый левый символ $*$ (напомним, что в процессе вычисления головка на входной ленте не выходит за крайние символы $*$). Рабочая лента в начальный момент времени пуста (заполнена сплошь символами $*$). В каждый из последующих моментов времени машина $\mathcal{M}$ недетерминированным образом выбирает подходящую команду (1.19) и в соответствии с этой командой изменяет положение головок на лентах и содержимое рабочей ленты. Работа машины завершается, когда она достигает заключительного состояния q_s либо когда в программе машины нет необходимой команды.

Считаем, что машина $\mathcal{M}$ вычисляет предикат π, если при истинности значения $\pi(x_1, \ldots, x_n)$ у машины $\mathcal{M}$ имеется вычисление с начальными данными $x_1, \ldots, x_n$, которое завершается в заключительном состоянии q_s. Если же значение $\pi(x_1, \ldots, x_n)$ ложно, то всякое вычисление машины $\mathcal{M}$ (с начальными данными $x_1, \ldots, x_n$) либо бесконечно, либо завершается ввиду отсутствия необходимой команды в программе машины.

Более формально понятие вычисления на машине Тьюринга $\mathcal{M}$ можно ввести на основе понятия конфигурации. Пусть в момент времени t на входной ленте машины $\mathcal{M}$ записано слово (1.20), машина находится в состоянии q_i, головка на входной ленте обозревает k-й символ слова (1.20), $1 \leqslant k \leqslant | * x_1 * \ldots * x_n * |$, слева от головки на рабочей ленте записано слово w_1, справа — слово w_2 (сама головка обозревает первый символ слова w_2). Тогда *конфигурацией машины* $\mathcal{M}$ в момент времени t называется набор

$$(*x_1 * \ldots * x_n *, i, k, w_1, w_2). \tag{1.21}$$

Поскольку в любой момент времени на рабочей ленте символы $1, 2$ могут находиться лишь в конечном числе клеток, мы примем следующее соглашение относительно слов w_1, w_2. Слово w_1 либо начинается одним из символов $1, 2$, либо совпадает с символом $*$; слово w_2 либо заканчивается одним из символов $1, 2$, либо совпадает с символом $*$.

Пусть K — конфигурация (1.21) машины $\mathcal{M}$ в момент времени t, $i < s$, a — k-й (слева) символ слова (1.20), b — первый символ слова w_2. Тогда команда (1.19) преобразует конфигурацию K в непосредственно следующую конфигурацию:

$$K' = (*x_1 * \ldots * x_n *, j, k', w_1', w_2'),$$

где:

$$k' = \begin{cases} k-1, & \text{если} \quad D_1 = L; \\ k+1, & \text{если} \quad D_1 = R; \\ k, & \text{если} \quad D_1 = S; \end{cases}$$

$$w_1' = \begin{cases} \text{началу слова } w_1 \text{ длины } |w_1|-1, & \text{если} \quad D_2 = L \quad \text{и} \quad w_1 \neq *; \\ w_1 c, & \text{если} \quad D_2 = R \quad \text{и} \quad w_1 \neq *; \\ c, & \text{если} \quad D_2 = R \quad \text{и} \quad w_1 = *; \\ w_1 & \text{в остальных случаях;} \end{cases}$$

$$w_2' = \begin{cases} dcw_3, & \text{если } D_2 = L,\ d \text{ есть последний символ слова } w_1, \\ & w_3 \text{ есть конец слова } w_2 \text{ длины } |w_2|-1 \text{ и либо} \\ & |w_2| \geqslant 2, \text{ либо } c \neq *; \\ d, & \text{если } D_2 = L,\ d \text{ есть последний символ слова } w_1, \\ & |w_2| = 1 \text{ и } c = *; \\ w_3, & \text{если } D_2 = R,\ |w_2| \geqslant 2 \text{ и } w_3 \text{ есть конец слова } w_2 \\ & \text{длины } |w_2|-1; \\ *, & \text{если } D_2 = R \text{ и } |w_2| = 1; \\ cw_3, & \text{если } D_2 = S \text{ и } w_3 \text{ есть конец слова } w_2 \text{ длины } |w_2|-1. \end{cases}$$

Конфигурация (1.21) называется *начальной*, если $i = 1$, и *заключительной*, если $i = s$. *Вычислением на машине* $\mathcal{M}$ называется любая последовательность конфигураций

$$C = (K_0, K_1, \ldots, K_t), \tag{1.22}$$

где для любого i, $1 \leqslant i \leqslant t$, конфигурация K_i является непосредственно следующей за конфигурацией K_{i-1}. Величина t называется *временем вычисления* C. Пусть

$$l_C = \max_{0 \leqslant i \leqslant t} \{|w_1^i w_2^i|\},$$

где для любого i, $0 \leqslant i \leqslant t$, w_1^i и w_2^i суть слова на рабочей ленте, входящие в конфигурацию K_i. Величину l_C назовем *зоной вычисления* C.

Имея понятия конфигурации и вычисления на машине $\mathcal{M}$, будем говорить, что предикат $\pi(x_1, \ldots, x_n)$ вычисли́м на машине $\mathcal{M}$, если для любого набора $(x_1, \ldots, x_n)$ выполняются следующие условия.

Если значение $\pi(x_1, \ldots, x_n)$ истинно, то существует вычисление (1.22) на машине $\mathcal{M}$, в котором

$$K_0 = (*x_1 * \ldots * x_n*, 1, 1, *, *) \tag{1.23}$$

и K_t — заключительная конфигурация. Если же значение $\pi(x_1, \ldots, x_n)$ ложно, то для любого вычисления (1.22) с начальной конфигурацией K_0 вида (1.23) конфигурация K_t не является заключительной.

Пусть $T(x)$, $L(x)$ — функции натурального аргумента x с натуральными значениями. Будем говорить, что предикат $\pi(x_1, \ldots, x_n)$ вычислим на машине $\mathcal{M}$ *за время* T и *в пределах зоны* L, если предикат π вычислим на машине $\mathcal{M}$ и при истинности значения $\pi(x_1, \ldots, x_n)$

существует вычисление (1.22) с начальной конфигурацией (1.23) и заключительной конфигурацией K_t, для которого

$$t \leqslant T(|*x_1*\ldots*x_n*|), \quad l_C \leqslant L(|*x_1*\ldots*x_n*|).$$

Очевидно, что конфигурация машины $\mathcal{M}$ в момент времени t содержит в себе полную информацию, достаточную для определения функционирования машины $\mathcal{M}$ после момента времени t. Однако особенность выбранного варианта машины Тьюринга состоит в том, что содержимое входной ленты остается неизменным на протяжении всего вычисления. Это позволяет в дальнейших построениях обходиться (в конфигурации) без слова, записанного на входной ленте. Таким образом, мы приходим к понятию *неполной конфигурации* (i, k, w_1, w_2), где параметры i, k, w_1, w_2 имеют тот же смысл, что и выше.

3. Перейдем к кодированию конфигураций и вычислений словами в алфавите $\{1, 2\}$.

Пусть $a \in \{1, 2\}$ и $\mathrm{Symb}_a(x, y)$ обозначает предикат «a есть x-й (слева) символ диадического представления числа y». Следующая эквивалентность показывает, что предикат $\mathrm{Symb}_a(x, y)$ принадлежит классу $\mathbf{R}$:

$$\mathrm{Symb}_a(x, y) \equiv (\exists z)_{x \leqslant y} (\exists w)_{w \leqslant y} \big((z = 2^x - 1) \,\&\, (l(z) = l(w)) \,\&\, \mathrm{B}(w, y) \,\&\, \mathrm{E}(a, w)\big).$$

Обозначим через $\mathrm{Code}\,(w)$ функцию, которая сопоставляет каждому слову w в алфавите $\{1, 2, *\}$ слово в алфавите $\{1, 2\}$ по следующему правилу: символы 1, 2, $*$ слова w одновременно заменяются соответственно словами 111, 112, 121. Будем считать, что слову Λ функция Code сопоставляет также слово Λ.

Если множество значений функции Code рассматривать как числовое множество (имея в виду диадическое представление чисел из $\mathbb{N}$), то предикат $\mathrm{Bcode}\,(w)$ принадлежности этому множеству оказывается рудиментарным. Действительно,

$$\begin{aligned}\mathrm{Bcode}\,(x) \equiv (\exists y)_{y \leqslant x} (\forall z)_{z \leqslant x} (\forall w)_{w \leqslant x} \big((l(x) = l(y) + l(y) + l(y)) \,\&\\ \&\, ((l(z) = l(w) + l(w) + l(w)) \,\&\, \mathrm{B}(z, x)) \Rightarrow\\ \Rightarrow (\mathrm{E}(111, z) \vee \mathrm{E}(112, z) \vee \mathrm{E}(121, z))\big)\end{aligned}$$

(предикат $l(x) = l(y) + l(y) + l(y)$ можно очевидным образом получить из рудиментарного предиката $l(s) = l(t) + l(v)$).

Аналогично, если переменные x, y рассматривать одновременно и как числовые переменные, то предикат $y = \mathrm{Code}\,(x)$ также оказывается рудиментарным:

$$\begin{aligned}(y = \mathrm{Code}\,(x)) \equiv (l(y) = l(x) + l(x) + l(x)) \,\&\, (\forall z)_{z \leqslant x} (\exists w)_{w \leqslant y}\\ ((l(w) = l(z) + l(z) + l(z)) \,\&\, (\mathrm{B}(z, x) \Rightarrow \mathrm{B}(w, y)) \,\&\, \big(\mathrm{E}(1, z) \Rightarrow\\ \Rightarrow \mathrm{E}(111, w) \,\&\, (\mathrm{E}(2, z) \Rightarrow \mathrm{E}(112, w))\big).\end{aligned}$$

Пусть $K = (i, k, w_1, w_2)$ — неполная конфигурация. Обозначим через $\mathrm{Code}\,(K)$ и назовем *кодом конфигурации* K слово

$$\mathrm{Code}\,(i)221\mathrm{Code}\,(k)221\mathrm{Code}\,(w_1)221\mathrm{Code}\,(w_2),$$

где $\mathrm{Code}\,(i)$, $\mathrm{Code}\,(k)$ обозначают коды соответствующих диадических представлений чисел i, k.

Обозначим через $\mathrm{Conf}_{\mathcal{M}}(x)$ предикат «диадическое представление x является кодом неполной конфигурации машины $\mathcal{M}$». Нетрудно убедиться в том, что предикат $\mathrm{Conf}_{\mathcal{M}}(x)$ рудиментарен. В самом деле, имеем

$$\begin{aligned}\mathrm{Conf}_{\mathcal{M}}(x) \equiv (\exists i)_{i\leqslant x}(\exists k)_{k\leqslant x}(\exists x_1)_{x_1\leqslant x}(\exists x_2)_{x_2\leqslant x}(\exists x_3)_{x_3\leqslant x}(\exists x_4)_{x_4\leqslant x}\\ \big((1\leqslant i)\ \&\ (i\leqslant s)\ \&\ (1\leqslant k)\ \&\ (x_1=\mathrm{Code}\,(i))\ \&\ (x_2=\mathrm{Code}\,(k))\ \&\\ \&\ \mathrm{Bcode}\,(x_3)\ \&\ \mathrm{Bcode}(x_4)\ \&\ (x=x_1 221 x_2 221 x_3 221 x_4)\big).\end{aligned}$$

Пусть $\mathrm{Next}_{\mathcal{M}}(x_1, \ldots, x_n, y, z)$ обозначает предикат «y, z суть коды неполных конфигураций K_1, K_2 машины $\mathcal{M}$, у которой на входной ленте записано слово (1.20), и конфигурация K_2 непосредственно следует за конфигурацией K_1». Будем предполагать, что в случае, когда y есть код заключительной конфигурации, $\mathrm{Next}_{\mathcal{M}}(x_1, \ldots, x_n, y, z)$ истинно тогда и только тогда, когда $z = y$.

Лемма 1.6. *Предикат* $\mathrm{Next}_{\mathcal{M}}(x_1, \ldots, x_n, y, z)$ *принадлежит классу* $\mathbf{R}$.

Доказательство. Мы не будем выписывать целиком формулу, задающую предикат $\mathrm{Next}_{\mathcal{M}}(x_1, \ldots, x_n, y, z)$, ввиду ее громоздкости. Перечислим лишь те требования, которые должны быть учтены в этой формуле, и поясним некоторые технические моменты в ее построении.

Во-первых, необходимо найти такие y_1, y_2, y_3, y_4 и z_1, z_2, z_3, z_4 (величины y_i, z_i рассматриваются и как числа, и как диадические представления чисел), что

$$y = y_1 221 y_2 221 y_3 221 y_4, \quad z = z_1 221 z_2 221 z_3 221 z_4$$

и выполняются предикаты $\mathrm{Conf}_{\mathcal{M}}(y)$, $\mathrm{Conf}_{\mathcal{M}}(z)$. Затем находим величины y_{21}, z_{21}, удовлетворяющие равенствам

$$y_2 = \mathrm{Code}\,(y_{21}), \quad z_2 = \mathrm{Code}\,(z_{21}),$$

и проверяем выполнимость неравенств

$$y_{21} \leqslant l(x_1) + \cdots + l(x_n) + n + 1, \quad z_{21} \leqslant l(x_1) + \cdots + l(x_n) + n + 1.$$

При этом используем предикат $s = l(t) + l(v)$, рудиментарность которого следует из эквивалентности

$$(s = l(t) + l(v)) \equiv (\exists r)_{r\leqslant tv}\big(1(r)\ \&\ (l(r) = l(t) + l(v))\ \&\ (2^s - 1 = r)\big).$$

Далее необходимо проверить, что существует команда (1.19), с помощью которой неполная конфигурация с кодом z получается из неполной конфигурации с кодом y. Формализация этой проверки представляет собой основную часть формулы, задающей предикат $\mathrm{Next}_{\mathcal{M}}$. Отметим ключевые моменты в построении этой формулы.

Пусть y_{11} удовлетворяет условию $y_1 = \mathrm{Code}(y_{11})$, а w_1, w_2 — слова в алфавите $\{1, 2, *\}$, представленные кодами y_3, y_4. Аналогичный смысл имеют обозначения z_{11}, w_1', w_2'. Тогда y есть код неполной конфигурации $(y_{11}, y_{21}, w_1, w_2)$, а z — код неполной конфигурации $(z_{11}, z_{21}, w_1', w_2')$. Для всякой команды (1.19) из программы машины $\mathcal{M}$ необходимо проверить, можно ли получить с помощью этой команды неполную конфигурацию $(z_{11}, z_{21}, w_1', w_2')$ из неполной конфигурации $(y_{11}, y_{21}, w_1, w_2)$, если на входной ленте машины $\mathcal{M}$ записано слово (1.20).

Итак, зафиксируем команду (1.19) и выполним следующие действия. Сравним величины i и y_{11}. Если $i = y_{11}$, то найдем далее y_{21}-й символ d слова (1.20). Это можно осуществить последовательно: если $y_{21} = 1$, то $d = *$; если $1 < y_{21} \leqslant l(x_1) + 1$, то значение d находим, вычисляя предикаты

$$\mathrm{Symb}_1(y_{21} - 1, x_1), \quad \mathrm{Symb}_2(y_{21} - 1, x_1);$$

если $y_{21} = l(x_1) + 2$, то $d = *$; если $l(x_1) + 2 < y_{21} \leqslant l(x_1) + l(x_2) + 2$, то значение d находим, вычисляя предикаты

$$\mathrm{Symb}_1(y_{21} - l(x_1) - 2, x_2), \quad \mathrm{Symb}_2(y_{21} - l(x_1) - 2, x_2);$$

и т. д.

Найдя значение d, сравним его со значением a из команды (1.19). Если $d = a$, то определим первые три символа слова w_2 и сравним их с кодом символа b из команды (1.19). Если сравнение даст положительный результат, то команду (1.19) можно применять к неполной конфигурации $(y_{11}, y_{21}, w_1, w_2)$. Теперь необходимо проверить, что величины z_{21}, z_{22}, w_1', w_2' получаются из величин y_{11}, y_{21}, w_1, w_2 в соответствии со значениями c, j, D_1, D_2 из правой части команды (1.19). Легко проверяются соотношения: $z_{11} = j$ и

$$z_{21} = \begin{cases} y_{21} - 1, & \text{если} \quad D_1 = L; \\ y_{21} + 1, & \text{если} \quad D_1 = R; \\ y_{21}, & \text{если} \quad D_1 = S. \end{cases}$$

Несколько более сложно убедиться в правильности строения слов w_1' и w_2'. Подробная процедура их получения описана выше при определении конфигурации $(*x_1 * \ldots * x_n*, j, k', w_1', w_2')$, которая получается из конфигурации $(*x_1 * \ldots * x_n*, i, k, w_1, w_2)$ с помощью команды (1.19). Лемма доказана.

Теорема 1.3. *Пусть для предиката* $\pi(x_1, \ldots, x_n)$ *существуют такие двуленточная машина Тьюринга* $\mathcal{M}$, *полином* $P(x)$ *с натуральными коэффициентами и действительное число* α, $0 < \alpha < 1$, *что предикат* π *вычислим на машине* $\mathcal{M}$ *за время* T *и в пределах зоны* L, *где функции* T, L *при достаточно больших значениях* x *удовлетворяют неравенствам*

$$T(x) \leqslant P(x), \quad L(x) \leqslant x^\alpha. \tag{1.24}$$

Тогда предикат π *принадлежит классу* $\mathbf{R}$.

Доказательство. Пусть предикат $N_1(x_1, \ldots, x_n, y, z)$ выполняется в том и только том случае, когда существует такая последовательность $K_1, \ldots, K_t$ неполных конфигураций машины $\mathcal{M}$, что для любого i, $1 \leqslant i < t$, конфигурация K_{i+1} непосредственно следует за конфигурацией K_i, $y = \mathrm{Code}\,(K_1)$, $z = \mathrm{Code}\,(K_t)$ и

$$|\mathrm{Code}\,(K_1)222\ldots222\mathrm{Code}\,(K_t)| \leqslant |*x_1*\ldots*x_n*|. \tag{1.25}$$

Утверждается, что предикат N_1 рудиментарен.

В самом деле, существование последовательности $K_1, \ldots, K_t$ можно заменить существованием слова u вида

$$\mathrm{Code}\,(K_1)222\ldots222\mathrm{Code}\,(K_t),$$

где в силу (1.25) выполняется ограничение

$$u \leqslant 11x_1 1 \ldots 1x_n 1.$$

Как видно из определения, слово u не содержит подслов 2222. Далее, начало слова u до первого вхождения слова 222, конец слова u после последнего вхождения слова 222, а также любое подслово слова u, заключенное между соседними вхождениями слова 222, должны быть кодами неполных конфигураций машины $\mathcal{M}$. Наконец, если началом слова u является слово вида $v222z222$, либо концом слова u является слово вида $222v222z$, либо в слово u входит слово вида $222v222z222$, где слова v, z не содержат слова 222, то неполная конфигурация машины $\mathcal{M}$ с кодом z непосредственно следует за неполной конфигурацией с кодом v. Поскольку предикаты

$$\mathrm{Conf}_{\mathcal{M}}(x) \quad \text{и} \quad \mathrm{Next}_{\mathcal{M}}(x_1, \ldots, x_n, y, z)$$

являются рудиментарными, перечисленные выше условия, которым должно удовлетворять слово u, можно выразить средствами класса $\mathbf{R}$. Таким образом, предикат $N_1(x_1, \ldots, x_n, y, z)$ рудиментарен.

Пусть $l = |*x_1*\ldots*x_n*|$ (предполагается, что числа $x_1, \ldots, x_n$ заданы своими диадическими представлениями). Из неравенств (1.24), (1.25) заключаем, что существует такая положительная константа C, что при достаточно больших значениях величины $x_1 + \cdots + x_n$ предикат $N_1(x_1, \ldots, x_n, y, z)$ будет выполняться в случае существования последовательности конфигураций $K_1, \ldots, K_t$ длины t, где

$$1 \leqslant t \leqslant C \cdot l^{1-\alpha}. \tag{1.26}$$

Далее аналогично предикату $N_1(x_1, \ldots, x_n, y, z)$ определяем рудиментарный предикат $N_2(x_1, \ldots, x_n, y, z)$. Единственное отличие в определении предиката N_2 состоит в том, что вместо предиката $\mathrm{Next}_{\mathcal{M}}$ используется уже построенный предикат N_1. Для предиката N_2 неравенство (1.26) заменяется неравенством

$$1 \leqslant t \leqslant (C \cdot l^{1-\alpha} - 1)^2 + 1.$$

Вообще, пусть уже определен рудиментарный предикат $N_{m-1}(x_1, \ldots \ldots, x_n, y, z)$. Тогда описанным выше способом определяем через него рудиментарный предикат $N_m(x_1, \ldots, x_n, y, z)$, который удовлетворяет следующим условиям. Значение $N_m(x_1, \ldots, x_n, y, z)$ истинно тогда и только тогда, когда существует последовательность $K_1, \ldots, K_t$ неполных конфигураций машины $\mathcal{M}$ такая, что $y = \mathrm{Code}\,(K_1)$, $z = \mathrm{Code}\,(K_t)$, для любого i, $1 \leqslant i < t$, истинно значение $N_{m-1}(x_1, \ldots, x_n, v_i, v_{i+1})$, где $v_i = \mathrm{Code}\,(K_i)$, $v_{i+1} = \mathrm{Code}\,(K_{i+1})$, и выполняется соотношение (1.25). При этом значение t может быть выбрано из промежутка

$$1 \leqslant t \leqslant (C \cdot l^{1-\alpha} - 1)^m + 1. \tag{1.27}$$

Выберем теперь число m с таким расчетом, чтобы при достаточно больших l выполнялось неравенство

$$(C \cdot l^{1-\alpha} - 1)^m + 1 \geqslant P(l). \tag{1.28}$$

Применяя первое из неравенств (1.24), а также неравенства (1.27), (1.28), заключаем: если значение $x_1 + \cdots + x_n$ достаточно велико, y есть код начальной конфигурации машины $\mathcal{M}$, имеющей на входной ленте слово (1.20), z есть код заключительной конфигурации, то значение $N_m(x_1, \ldots, x_n, y, z)$ истинно в том и только в том случае, когда истинно значение $\pi(x_1, \ldots, x_n)$.

Кодом начальной конфигурации служит слово

$$111221111221121221121.$$

Код заключительной конфигурации начинается словом $\mathrm{Code}\,(s)221$. Поэтому при достаточно больших значениях суммы $x_1 + \cdots + x_n$ получим

$$\begin{aligned}\pi(x_1, \ldots, x_n) \equiv (\exists y)_{y \leqslant 1x_1 1 \ldots 1x_n 1} (\exists z)_{z \leqslant 1x_1 1 \ldots 1x_n 1} \\ \big((y = 111221111221121221121) \mathbin{\&} \mathrm{B}(\mathrm{Code}(s)221, z) \mathbin{\&} \\ \mathbin{\&} N_m(x_1, \ldots, x_n, y, z)\big).\end{aligned} \tag{1.29}$$

Поскольку на конечном множестве значения предиката можно задать табличным способом, на основании эквивалентности (1.29) заключаем, что предикат π принадлежит классу $\mathbf{R}$. Теорема доказана.

Теорема 1.4. *Имеет место равенство* $\mathbf{BA} = \mathbf{R}$.

Доказательство. Согласно утверждению 1.6, $\mathbf{R} \subseteq \mathbf{BA}$. В конце § 1.3 доказано также, что предикат $x + y = z$ рудиментарен. Обращаясь к определениям классов $\mathbf{BA}$ и $\mathbf{R}$, видим, что для доказательства обратного включения $\mathbf{BA} \subseteq \mathbf{R}$ достаточно установить, что рудиментарен предикат $x \cdot y = z$. Это будет сделано с использованием теоремы 1.3.

Пусть

$$a_p a_{p-1} \ldots a_0, \quad b_q b_{q-1} \ldots b_0, \quad c_r c_{r-1} \ldots c_0$$

— диадические представления чисел x, y, z (случаи $x = 0$ и $y = 0$ ввиду тривиальности мы опускаем). Положим

$$s(j) = \sum_{i=0}^{j} a_{j-i} \cdot b_i, \tag{1.30}$$

где $j = 0, 1, \ldots, r$, $a_i = 0$ при $i > p$ и $b_i = 0$ при $i > q$. Для обычного умножения чисел x и y «столбиком» *перенос* $\mathrm{tr}\,(j)$ в j-й разряд произведения определяется согласно соотношениям:

$$\mathrm{tr}\,(0) = 0, \quad \mathrm{tr}\,(j + 1) = 1/2(s(j) + \mathrm{tr}\,(j) - c_j). \tag{1.31}$$

Тогда разряды $c_1, \ldots, c_r$ произведения $x \cdot y$ выражаются следующим образом:

$$c_j = \begin{cases} 1, & \text{если } s(j) + \mathrm{tr}\,(j) \text{ — нечетное число;} \\ 2 & \text{в противном случае.} \end{cases} \tag{1.32}$$

Очевидно, что $s(j) \leqslant 4(j + 1)$. Следовательно, используя (1.31), по индукции заключаем, что $\mathrm{tr}\,(j) \leqslant 4j$. Поэтому

$$s(j) < 4l, \quad \mathrm{tr}\,(j) < 4l,$$

где

$$l = |{*}\, a_p \ldots a_0 * b_q \ldots b_0 * c_r \ldots c_0 *| = p + q + r + 7.$$

В частности, диадическое представление величин $s(j)$, $\mathrm{tr}\,(j)$ состоит из не более чем $\log_2 l + 2$ разрядов.

Опираясь на формулы (1.31), (1.32), дадим содержательное описание алгоритма, который проверяет истинность предиката $x \cdot y = z$ и может быть реализован на двуленточной машине Тьюринга $\mathcal{M}$ за полиномиальное время и в пределах зоны, по порядку равной $\log_2 l$.

Наш алгоритм носит индуктивный характер. Предположим, что на рабочей ленте машины $\mathcal{M}$ представлены в диадической записи числа j, $s(j)$ и $\mathrm{tr}\,(j)$ $(0 \leqslant j < r)$. По второй из формул (1.31) находим значение $\mathrm{tr}\,(j + 1)$. Для этого складываем «столбиком» числа $s(j)$,

$\mathrm{tr}\,(j)$ и отбрасываем в полученной сумме последний разряд c_j. Чтобы найти значение $s(j+1)$ по формуле (1.30), необходимо уметь вычислять разряды a_{j-i+1} и b_i. Рассмотрим, например, получение разряда a_{j-i+1}. Имея «текущее» значение i, вычитаем «столбиком» из $j+1$ число i. Создав на рабочей ленте копию диадического представления числа $j-i+1$, начинаем вычитать из него последовательно по единице, проводя после каждого вычитания сдвиг головки на входной ленте на одну клетку влево, начиная от второго символа $*$. Аналогично вычисляем разряд b_i. Сумму вида (1.30) образуем пошагово по мере вычисления произведений $a_{j-i+1} \cdot b_i$.

После того как найдена величина $s(j+1)$, вычисляем значение c_{j+1} по формуле (1.32) и сравниваем его со значением c_{j+1}, имеющимся на входной ленте. При совпадении значений продолжаем процесс нахождения величин $j+2$, $s(j+2)$, $\mathrm{tr}\,(j+2)$ (если только $j+1<r$). В противном случае вычисление можно либо зациклить, либо оборвать без достижения заключительного состояния. Теорема доказана.

§ 1.4. Классы FBA, FR, BPC

1. Пусть $\rho(x_1,\ldots,x_n)$ — предикат на множестве $\mathbb{N}$. Всюду определенная функция $\chi(x_1,\ldots,x_n)$ называется *характеристической функцией* предиката $\rho(x_1,\ldots,x_n)$, если она принимает лишь значения 0, 1 и имеет место эквивалентность

$$(\chi(x_1,\ldots,x_n)=1)\equiv\rho(x_1,\ldots,x_n). \tag{1.33}$$

Если Q — некоторый класс функций, то через Q_* обозначаем множество всех предикатов, у которых характеристические функции принадлежат классу Q. Предикаты множества Q_* называем *предикатами класса* Q.

Для любого $n\geqslant 1$ и любого i, $1\leqslant i\leqslant n$, обозначим через $I_i^n(x_1,\ldots,x_i,\ldots,x_n)$ *селекторную функцию*, значения которой совпадают со значениями переменной x_i. Множество всех селекторных функций I_i^n $(1\leqslant i\leqslant n,\ n=1,2,\ldots)$ обозначим через I.

Будем говорить, что класс функций Q замкнут относительно операции *суперпозиции*, если наряду с любыми функциями

$$g(y_1,\ldots,y_m),\ h_1(x_1,\ldots,x_n),\ldots,h_m(x_1,\ldots,x_n)$$

классу Q принадлежит также функция $f(x_1,\ldots,x_n)$, определяемая соотношением

$$f(x_1,\ldots,x_n)=g(h_1(x_1,\ldots,x_n),\ldots,h_m(x_1,\ldots,x_n)) \tag{1.34}$$

и называемая суперпозицией функций $g,h_1,\ldots,h_m$.

Отметим следующий факт: если класс Q содержит множество селекторных функций I и замкнут относительно операции суперпозиции, то помимо «регулярных» суперпозиций (1.34) в классе Q можно использовать и «нерегулярные» суперпозиции вида

$$g(h_1(x_1^1,\dots,x_{n_1}^1),\dots,h_m(x_1^m,\dots,x_{n_m}^m)),$$

где $x_1^1,\dots,x_{n_1}^1,\dots,x_1^m,\dots,x_{n_m}^m$ — произвольные переменные (возможно, повторяющиеся). В самом деле, если, например, переменная x_1^2 не содержится среди переменных $x_1^1,\dots,x_{n_1}^1$, то ее можно «добавить» к функции $h_1(x_1^1,\dots,x_{n_1}^1)$, образовав новую функцию

$$h_1'(x_1^1,\dots,x_{n_1}^1,x_1^2) = h_1(I_1^{n_1+1}(x_1^1,\dots,x_{n_1}^1,x_1^2),\dots,I_{n_1}^{n_1+1}(x_1^1,\dots,x_{n_1}^1,x_1^2)).$$

Положим

$$\operatorname{sg} x = \begin{cases} 0, & \text{если} \quad x=0; \\ 1, & \text{если} \quad x>0; \end{cases} \qquad \overline{\operatorname{sg}}\, x = \begin{cases} 1, & \text{если} \quad x=0; \\ 0, & \text{если} \quad x>0. \end{cases}$$

Утверждение 1.10. *Пусть класс функций Q содержит функции $x+1$, $x \dot- y$, I и замкнут относительно операции суперпозиции. Тогда класс предикатов Q_* замкнут относительно операций логики высказываний.*

Доказательство. Имеем:

$$0 = x \dot- x, \quad 1 = 0+1, \quad \overline{\operatorname{sg}}\, x = 1 \dot- x, \quad \operatorname{sg} x = \overline{\operatorname{sg}}\,\overline{\operatorname{sg}}\, x.$$

Поскольку $\overline{\operatorname{sg}} \in Q$, класс Q_*, очевидно, замкнут относительно операции отрицания. Далее,

$$x + \operatorname{sg} y = (x+1) \dot- \overline{\operatorname{sg}}\, y.$$

Имея в классе Q функцию $x + \operatorname{sg} y$, устанавливаем замкнутость класса Q_* относительно операции дизъюнкции: если χ_1, χ_2 — характеристические функции предикатов ρ_1, ρ_2, то характеристической функцией предиката $\rho_1 \vee \rho_2$ служит функция $\operatorname{sg}(\chi_1 + \operatorname{sg}\chi_2)$. Утверждение доказано.

Пусть $\rho_1(x_1,\dots,x_n),\dots,\rho_m(x_1,\dots,x_n)$ — предикаты и для любых значений i, j $(1 \leqslant i < j \leqslant m)$ предикат

$$\rho_i(x_1,\dots,x_n) \mathbin{\&} \rho_j(x_1,\dots,x_n)$$

тождественно ложен. Говорим, что функция $f(x_1,\dots,x_n)$ получена из функций

$$g_1(x_1,\dots,x_n), \quad \dots, \quad g_m(x_1,\dots,x_n), \quad g_{m+1}(x_1,\dots,x_n)$$

с помощью операции *разбора случаев по предикатам* $\rho_1,\dots,\rho_m$, если

$$f(x_1,\dots,x_n) = \begin{cases} g_1(x_1,\dots,x_n), \ \text{если } \rho_1(x_1,\dots,x_n); \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ g_m(x_1,\dots,x_n), \ \text{если } \rho_m(x_1,\dots,x_n); \\ g_{m+1}(x_1,\dots,x_n) \ \text{в остальных случаях.} \end{cases} \tag{1.35}$$

Утверждение 1.11. *Пусть класс функций Q содержит функции $\overline{\mathrm{sg}}\,x$, $x+y$, $x \cdot \mathrm{sg}\,y$, I и замкнут относительно операции суперпозиции. Тогда класс Q замкнут относительно операции разбора случаев по предикатам.*

Доказательство. Пусть функции $g_1, \ldots, g_m, g_{m+1}$ принадлежат классу Q, предикаты $\rho_1, \ldots, \rho_m$ — классу Q_* и функция f получается из функций $g_1, \ldots, g_m, g_{m+1}$ и предикатов $\rho_1, \ldots, \rho_m$ согласно соотношениям (1.35). Обозначим через $\chi_1, \ldots, \chi_m$ характеристические функции предикатов $\rho_1, \ldots, \rho_m$. Тогда

$$\begin{aligned} f(x_1, \ldots, x_n) = g_1(x_1, \ldots, x_n) \cdot \mathrm{sg}\,\chi_1(x_1, \ldots, x_n) + \ldots \\ \ldots + g_m(x_1, \ldots, x_n) \cdot \mathrm{sg}\,\chi_m(x_1, \ldots, x_n) + \\ + g_{m+1}(x_1, \ldots, x_n) \cdot \overline{\mathrm{sg}}\,\chi_1(x_1, \ldots, x_n) \cdot \ldots \cdot \overline{\mathrm{sg}}\,\chi_m(x_1, \ldots, x_n), \end{aligned}$$

и утверждение доказано.

Операция *ограниченной минимизации* — это эффективная операция, которая по любой всюду определенной функции $g(x_1, \ldots, x_n)$ дает всюду определенную функцию

$$f(x_1, \ldots, x_n, y) = (\mu z)_{z \leqslant y}(g(x_1, \ldots, x_{n-1}, z) = x_n), \tag{1.36}$$

где

$$(\mu z)_{z \leqslant y}(g(x_1, \ldots, x_{n-1}, z) = x_n) = \\ = \begin{cases} \text{наименьшему из таких значений } z, \\ \qquad \text{что } z \leqslant y \text{ и } g(x_1, \ldots, x_{n-1}, z) = x_n, \\ \qquad \text{если такое } z \text{ существует;} \\ 0 \text{ в противном случае.} \end{cases}$$

Иногда вместо схемы (1.36) будем использовать схему

$$f(x_1, \ldots, x_n, y) = (\mu z)_{z \leqslant y} \rho(x_1, \ldots, x_n, z),$$

где ρ — предикат, или

$$f(x_1, \ldots, x_n, y) = (\mu z)_{z \leqslant y}(\chi(x_1, \ldots, x_n, z) = 1),$$

где χ — характеристическая функция предиката.

2. Определим класс элементарных функций **FBA**. Исходными функциями класса **FBA** являются функции

$$x+1, \quad x \cdot y, \quad x \dot{-} y, \quad I,$$

а порождающими операциями — операции суперпозиции и ограниченной минимизации. Нетрудно видеть, что всякую функцию класса **FBA** можно ограничить сверху подходящим полиномом с натуральными коэффициентами.

Теорема 1.5. *Имеет место равенство* $\mathbf{BA} = \mathbf{FBA}_*$.

Доказательство. Сначала покажем, что $\mathbf{BA} \subseteq \mathbf{FBA}_*$. Так же, как в утверждении 1.8, устанавливаем, что в класс $\mathbf{FBA}$ входят функции 0, 1, sg, $\overline{\mathrm{sg}}$. Кроме того,

$$x + y = (x+1)(y+1) \dot{-} (xy+1), \quad |x - y| = (x \dot{-} y) + (y \dot{-} x).$$

Значит, классу $\mathbf{FBA}_*$ принадлежат предикаты $x + y = z$ и $x \cdot y = z$, поскольку их характеристическими функциями являются функции

$$\overline{\mathrm{sg}}\,|x + y - z|, \quad \overline{\mathrm{sg}}\,|x \cdot y - z|.$$

Далее, согласно утверждению 1.8. класс $\mathbf{FBA}_*$ замкнут относительно операций логики высказываний. Легко также видеть, что класс $\mathbf{FBA}_*$ замкнут относительно явных преобразований. Наконец, если

$$\sigma(x_1, \ldots, x_n, y) \equiv (\exists z)_{z \leqslant y} \rho(x_1, \ldots, x_n, z),$$

то

$$\chi_\sigma(x_1, \ldots, x_n, y) = \chi_\rho(x_1, \ldots, x_n, f(x_1, \ldots, x_n, y)),$$

где χ_σ, χ_ρ — характеристические функции предикатов σ, ρ и

$$f(x_1, \ldots, x_n, y) = (\mu z)_{z \leqslant y}(\chi_\rho(x_1, \ldots, x_n, z) = 1).$$

Таким образом, класс $\mathbf{FBA}_*$ замкнут относительно операций ограниченной квантификации и $\mathbf{BA} \subseteq \mathbf{FBA}_*$.

Обратно, индукцией по построению класса $\mathbf{FBA}$ докажем, что для любой функции $f(x_1, \ldots, x_n)$ класса $\mathbf{FBA}$ *график функции* f, т. е. предикат $f(x_1, \ldots, x_n) = y$, принадлежит классу $\mathbf{BA}$. Тогда каждый предикат класса $\mathbf{FBA}$ будет входить в класс $\mathbf{BA}$, поскольку в силу (1.33) любой предикат получается из графика своей характеристической функции подстановкой константы 1 вместо одной из переменных.

Обратимся к исходным функциям класса $\mathbf{FBA}$. Графики функций $x + 1$, $x \cdot y$, I имеют вид равенства двух полиномов с натуральными коэффициентами. На основании утверждения 1.4 они принадлежат классу $\mathbf{BA}$. Принадлежность предиката $x \dot{-} y = z$ классу $\mathbf{BA}$ установлена в § 1.1.

Пусть теперь $g, h_1, \ldots, h_m \in \mathbf{FBA}$, выполняется равенство (1.34) и графики функций $g, h_1, \ldots, h_m$ принадлежат классу $\mathbf{BA}$. Пусть, кроме того, $P_1(x_1, \ldots, x_n), \ldots, P_m(x_1, \ldots, x_n)$ — такие полиномы с натуральными коэффициентами, которые ограничивают сверху функции $h_1(x_1, \ldots, x_n)$, …, $h_m(x_1, \ldots, x_n)$. Тогда будем иметь

$$(f(x_1, \ldots, x_n) = y) \equiv (\exists y_1)_{y_1 \leqslant P_1(x_1, \ldots, x_n)} \ldots (\exists y_m)_{y_m \leqslant P_m(x_1, \ldots, x_n)}$$
$$((h_1(x_1, \ldots, x_n) = y_1) \,\&\, \ldots \,\&\, (h_m(x_1, \ldots, x_n) = y_m) \,\&\, (g(y_1, \ldots, y_m) = y)).$$

Отсюда следует, что график функции f принадлежит классу $\mathbf{BA}$.

Аналогично, если график функции $g(x_1, \ldots, x_n)$ принадлежит классу $\mathbf{BA}$, а функция $f(x_1, \ldots, x_n, y)$ получается из функции g с помощью операции ограниченной минимизации (1.36), то график функции f будет входить в класс **BA**, поскольку имеет место эквивалентность

$$(f(x_1,\ldots,x_n,y)=v)\equiv(v\leqslant y)\,\&\,((g(x_1,\ldots,x_{n-1},v)=x_n)\,\&\\ \&\,(\forall t)_{t<v}(g(x_1,\ldots,x_{n-1},t)\neq x_n)\vee(v=0)\,\&\\ \&\,(\forall t)_{t\leqslant y}(g(x_1,\ldots,x_{n-1},t)\neq x_n)).$$

3. По аналогии с классом **FBA** определим класс словарных функций **FR**. Положим (для слов x, y, z в алфавите $\{1,2\}$)

$$\operatorname{sg}x=\begin{cases}\Lambda, & \text{если} \quad x=\Lambda;\\ 1, & \text{если} \quad x\neq\Lambda;\end{cases}\qquad \overline{\operatorname{sg}}\,x=\begin{cases}1, & \text{если} \quad x=\Lambda;\\ \Lambda, & \text{если} \quad x\neq\Lambda;\end{cases}$$

$$x\dot{-}y=\begin{cases}z, & \text{если } y \text{ — такое (единственное) слово, что } z*y=x;\\ \Lambda & \text{в остальных случаях.}\end{cases}$$

Если $\rho(x_1,\ldots,x_n)$ — словарный предикат (над алфавитом $\{1,2\}$), то характеристической функцией предиката ρ считаем словарную функцию $\chi_\rho(x_1,\ldots,x_n)$, которая принимает лишь значения Λ, 1 и для которой предикат $\rho(x_1,\ldots,x_n)$ совпадает с предикатом $\chi_\rho(x_1,\ldots,x_n)=1$.

По аналогии с утверждением 1.10 доказывается

Утверждение 1.12. *Пусть класс Q словарных функций содержит функции $x*1$, $x\dot{-}y$, I и замкнут относительно операции суперпозиции. Тогда класс Q_* всех предикатов из Q замкнут относительно операций логики высказываний.*

Доказательство. Так же, как в доказательстве утверждения 1.10, получаем функции Λ, 1, sg, $\overline{\text{sg}}$, используя вместо константы 0 константу Λ. Далее образуем аналог функции $x+\operatorname{sg}y$ — функцию $x*1\dot{-}\overline{\operatorname{sg}}\,y$. С помощью полученной функции и функции $\overline{\text{sg}}$ устанавливаем замкнутость класса Q_* относительно логических операций отрицания и дизъюнкции. Утверждение доказано.

Операцию ограниченной минимизации распространяем на словарные функции, используя отношение $\leqslant$ для слов в алфавите $\{1,2\}$ и заменяя число 0 словом Λ.

Обозначим через **FR** наименьший класс словарных функций, который содержит исходные функции

$$1,\quad 2,\quad x*y,\quad x\dot{-}y,\quad I \tag{1.37}$$

и замкнут относительно операций суперпозиции и ограниченной минимизации.

Точно так же, как для класса **FBA** (см. доказательство теоремы 1.5), доказывается, что класс $\mathbf{FR}_*$ замкнут относительно операций ограниченной квантификации.

Теорема 1.6. *Имеет место равенство* $\mathbf{R} = \mathbf{FR}_*$.

Доказательство. Сначала установим включение $\mathbf{R} \subseteq \mathbf{FR}_*$. Очевидно, что словарные функции-константы принадлежат классу $\mathbf{FR}$, а класс $\mathbf{FR}_*$ замкнут относительно явных преобразований. Покажем, что в класс $\mathbf{FR}_*$ входит предикат $x * y = z$.

В самом деле, характеристическая функция предиката $x * y = z$ получается из характеристической функции предиката $v = 1$ подстановкой функции $((1 * z) \dot{-} y) \dot{-} x$ вместо переменной v. В свою очередь предикат $v = 1$ является конъюнкцией предикатов

$$\mathrm{sg}\,(v) = 1, \quad \overline{\mathrm{sg}}\,(v \dot{-} 1) = \Lambda, \quad \overline{\mathrm{sg}}\,(v \dot{-} 2) = \Lambda, \quad 12 \dot{-} v = \Lambda.$$

Их характеристические функции суть соответственно

$$\mathrm{sg}\,(v), \quad \overline{\mathrm{sg}}\,(v \dot{-} 1), \quad \overline{\mathrm{sg}}\,(v \dot{-} 2), \quad \overline{\mathrm{sg}}\,(12 \dot{-} v).$$

При доказательстве включения $\mathbf{FR}_* \subseteq \mathbf{R}$ придерживаемся соответствующей части доказательства теоремы 1.5. Устанавливаем принадлежность графиков всех функций из $\mathbf{FR}$ классу $\mathbf{R}$. Для функций 1 и $x * y$ это сделано выше, функция 2 рассматривается аналогично функции 1. В случае предиката $x \dot{-} y = z$ следует воспользоваться его представлением в форме

$$(x = z * y) \vee (z = \Lambda) \,\&\, ((\forall v)_{v \leqslant x}(x \neq v * y)).$$

Для операций суперпозиции и ограниченной минимизации принадлежность образующихся функций классу $\mathbf{R}$ устанавливается так же, как в теореме 1.5. Теорема доказана.

Следствие. *Имеет место равенство* $\mathbf{FBA} = \mathbf{FR}$.

Доказательство. В силу теоремы 1.6 множества графиков функций из классов $\mathbf{FBA}$ и $\mathbf{FR}$ совпадают. Поэтому для доказательства равенства $\mathbf{FBA} = \mathbf{FR}$ достаточно заметить, что всякую функцию $f(x_1, \ldots, x_n)$ можно получить из ее графика с помощью операции ограниченной минимизации, если только только при этом переменную в операции минимизации ограничить достаточно «большой» функцией. В случае класса $\mathbf{FBA}$ такой функцией является полином (с натуральными коэффициентами) от переменных $x_1, \ldots, x_n$, во втором случае — словарный терм от тех же переменных. Однако полиномы и словарные термы (как числовые функции) взаимно ограничивают сверху друг друга. Отсюда следует совпадение классов $\mathbf{FBA}$, $\mathbf{FR}$. Следствие доказано.

4. Идею построения классов $\mathbf{R}$ и $\mathbf{FR}$ можно применить для определения еще некоторых похожих классов. Например, словарное ограничение $x \leqslant y$, используемое при введении ограниченных кванторов и ограниченной минимизации, можно заменить ограничением $x \sqsubseteq y$, означающим «слово x есть префикс (начало) слова y». К сожалению, возникающие при этом классы предикатов и функций оказываются слишком узкими, и мы ими заниматься не будем.

Тем не менее если операцию ограниченной минимизации заменить более сильной операцией ограниченной префиксной конкатенации, то получающийся класс функций оказывается и достаточно широким, и содержательно интересным. Итак, будем говорить, что функция f получена из функции g с помощью операции *ограниченной префиксной конкатенации*,

$$f(x_1, \ldots, x_n, y) = \underset{z \sqsubseteq y}{\mathrm{Con}}\, g(x_1, \ldots, x_n, z),$$

если $f(x_1, \ldots, x_n, y)$ есть слово

$$g(x_1, \ldots, x_n, z_1) * g(x_1, \ldots, x_n, z_2) * \ldots * g(x_1, \ldots, x_n, z_l),$$

где $l = |y|$, $z_1, \ldots, z_l$ — все префиксы слова y в порядке возрастания их длин, $z_1 = \Lambda$ и $z_l = y$.

Обозначим через **BPC** наименьший класс всех функций, которые можно получить из исходных функций (1.37) с помощью операций суперпозиции и ограниченной префиксной конкатенации.

Пусть $\rho(x_1, \ldots, x_{n-1}, z)$ — предикат на множестве $\{1, 2\}^*$. Посредством $(\exists z)_{z \sqsubseteq y} \rho(x_1, \ldots, x_{n-1}, z)$ обозначим предикат, который совпадает с предикатом

$$\rho(x_1, \ldots, x_{n-1}, z_1) \vee \rho(x_1, \ldots, x_{n-1}, z_2) \vee \ldots \vee \rho(x_1, \ldots, x_{n-1}, z_l),$$

где $z_1, \ldots, z_l$ — все префиксы слова y. Аналогичным образом определим предикат $(\forall z)_{z \sqsubseteq y} \rho(x_1, \ldots, x_{n-1}, z)$. Операции перехода от предиката ρ к определенным выше предикатам с ограниченными кванторами будем называть операциями *ограниченной префиксной квантификации*.

Так же, как для класса **FR**, устанавливаем принадлежность простейших словарных функций классу **BPC** и замкнутость класса предикатов $\mathbf{BPC}_*$ относительно операций логики высказываний и явных преобразований. Нетрудно видеть, что применение операции $\mathrm{Con}_{z \sqsubseteq y}$ к функции $I_1^2(x, z)$ дает функцию $x^{|y|+1}$ (слово, полученное конкатенацией $|y| + 1$ экземпляров слова x). Далее получаем функцию $x^{|y|}$: $x^{|y|} = x^{|y|+1} \dot{-} x$ ($|y|$-я «степень» слова x).

Отметим, что предикаты $|x| = |y|$ и $|x| < |y|$ принадлежат классу $\mathbf{BPC}_*$. Это следует из вида их характеристических функций: $\overline{\mathrm{sg}}\,((1^{|x|} \dot{-} 1^{|y|}) * (1^{|y|} \dot{-} 1^{|x|}))$ и $\mathrm{sg}\,(1^{|y|} \dot{-} 1^{|x|})$. Кроме того, класс $\mathbf{BPC}_*$ замкнут относительно операций ограниченной префиксной квантификации. В самом деле, для предиката $(\exists z)_{z \sqsubseteq y} \rho(x_1, \ldots, x_{n-1}, z)$, полученного из предиката ρ с помощью операции навешивания ограниченного квантора существования, характеристической функцией будет функция $\mathrm{sg}\,(\mathrm{Con}_{z \sqsubseteq y} \chi_\rho(x_1, \ldots, x_{n-1}, z))$.

Покажем, что классу $\mathbf{BPC}_*$ принадлежат предикаты $x = y$ и $x \neq y$. Поскольку класс $\mathbf{BPC}_*$ замкнут относительно операций логики высказываний, ограничимся только предикатом $x = y$. Однако $x = y$ тогда и только тогда, когда $|x| = |y|$ и функция $(1 * x) \dot{-} y$ принимает значение 1. Однако при условии $|x| = |y|$ она принимает лишь значения 1 и Λ, поэтому для последнего предиката можно рассмотреть характеристическую функцию $\mathrm{sg}\,((1 * x) \dot{-} y)$.

Утверждение 1.13. *Класс* **BPC** *замкнут относительно операции ограниченной минимизации.*

Доказательство. Пусть

$$f(x_1, \ldots, x_n, y) = (\mu z)_{z \sqsubseteq y}(g(x_1, \ldots, x_{n-1}, z) = x_n)$$

и $g \in \mathbf{BPC}$. Обозначим через $\rho(x_1, \ldots, x_n, z)$ предикат, который выполняется в том и только в том случае, когда $g(x_1, \ldots, x_{n-1}, z) = x_n$ и никакое начало слова z, отличное от слова z, данному равенству не удовлетворяет. Принадлежность предиката ρ классу $\mathbf{BPC}_*$ вытекает из установленных выше свойств класса $\mathbf{BPC}_*$ и эквивалентности

$$\rho(x_1, \ldots, x_n, z) \equiv (g(x_1, \ldots, x_{n-1}, z) = x_n) \,\&\, (\forall v)_{v \sqsubseteq z}((v \neq z) \Rightarrow \\ \Rightarrow (g(x_1, \ldots, x_{n-1}, z) \neq x_n)).$$

Пусть χ — характеристическая функция предиката ρ. Тогда будем иметь

$$f(x_1, \ldots, x_n, y) = \operatorname*{Con}_{z \sqsubseteq y} z^{\chi(x_1, \ldots, x_n, z)}.$$

Утверждение доказано.

Легко видеть, что классу $\mathbf{BPC}_*$ принадлежат придикаты $\mathrm{B}(x, y)$, $\mathrm{E}(x, y)$, $\mathrm{C}(x, y)$, а класс **BPC** замкнут относительно операции разбора случаев по предикатам.

Обозначим через $\mathrm{first}\,(x)$, $\mathrm{last}\,(x)$ функции, которые выдают первый и последний символы слова x, если слово x непусто, и слово Λ в противном случае. Принадлежность функции first классу **BPC** вытекает из следующих соотношений:

$$\mathrm{first}\,(x) = \begin{cases} 1, & \text{если} \quad B(1, x); \\ 2, & \text{если} \quad B(2, x); \\ \Lambda & \text{если} \quad x = \Lambda. \end{cases}$$

Аналогично доказывается принадлежность функции last классу **BPC**.

Пусть $\mathrm{pref}_{|y|}(x)$ равно префиксу слова x длины $|y|$, если $|y| \leqslant |x|$, и равно Λ при $|y| > |x|$. Имеем

$$\mathrm{pref}_{|y|}(x) = \operatorname*{Con}_{z \sqsubseteq x} z^{\chi(y, z)},$$

где $\chi(y, z)$ — характеристическая функция предиката $|y| = |z|$. Таким образом, функция $\mathrm{pref}_{|y|}(x)$ принадлежит классу **BPC**.

Обозначим через $\mathrm{inv}\,(x)$ функцию, которая дает инверсию слова x (т. е. слово, составленное из символов слова x, записанных в обратном порядке). Следующая формула устанавливает принадлежность функции inv классу **BPC**:

$$\mathrm{inv}\,(x) = \operatorname*{Con}_{z \sqsubseteq 1^{|x|}} \mathrm{last}\,(\mathrm{pref}_{|1^{|x|} \dot{-} z|}(x)).$$

По аналогии с операцией ограниченной префиксной конкатенации введем операцию ограниченной суффиксной конкатенации, для которой будем использовать обозначение $\mathrm{Con}_{y \sqsupseteq z}$. Действие операции $\mathrm{Con}_{y \sqsupseteq z}$ на функцию $g(\widetilde{x}, z)$ состоит в образовании конкатенации слов $g(\widetilde{x}, z_l), \ldots, g(\widetilde{x}, z_2), g(\widetilde{x}, z_1)$, где $z_1, \ldots, z_l$ — все суффиксы слова y, выписанные в порядке возрастания длин.

Утверждение 1.14. *Класс* **BPC** *замкнут относительно операции ограниченной суффиксной конкатенации.*

Доказательство. Очевидно, что при инверсии слова суффиксы переходят в префиксы и обратно. Поэтому

$$\mathop{\mathrm{Con}}_{y \sqsupseteq z} g(\widetilde{x}, z) = \mathrm{inv}\Biggl(\mathop{\mathrm{Con}}_{z \sqsubseteq \mathrm{inv}\,(y)} g(\widetilde{x}, z)\Biggr).$$

Утверждение доказано.

Для классов функций, замкнутых относительно операции суперпозиции, важным свойством является наличие в классе функции, нумерующей пары, и «обратных» к ней функций. Мы решим эту задачу, определив соответствующие функции pair, left и right. С этой целью введем ряд словарных функций и докажем их принадлежность классу **BPC**.

Пусть $\mathrm{doub}\,(x)$ — функция, удваивающая каждый символ слова x. Имеем

$$\mathrm{doub}\,(x) = \mathop{\mathrm{Con}}_{z \sqsupseteq x} (\mathrm{first}\,(z) * \mathrm{first}\,(z)).$$

Нумерационную функцию pair определим равенством

$$\mathrm{pair}\,(x_1, x_2) = \mathrm{doub}\,(x_1) * 12 * \mathrm{doub}\,(x_2).$$

Пусть далее $\mathrm{even}\,(x)$, $\mathrm{odd}\,(x)$ — предикаты, определяющие четность и нечетность длины слова x. Для предиката even справедлива эквивалентность

$$\mathrm{even}\,(x) \equiv (\exists z)_{z \sqsubseteq x}\bigl(1^{|x|} = 1^{|z|} * 1^{|z|}\bigr).$$

Аналогичная эквивалентность справедлива для предиката odd.

Обозначим через $\mathrm{compress}\,(x)$ функцию, которая удовлетворяет тождеству $\mathrm{compress}\,(\mathrm{doub}\,(x)) = x$. Для функции compress получаем выражение

$$\mathrm{compress}\,(x) = \mathop{\mathrm{Con}}_{z \sqsubseteq x} (\mathrm{last}\,(z))^{\chi(z)},$$

где $\chi(z)$ — характеристическая функция предиката odd.

Пусть $\mathrm{left}'\,(x)$ — функция, которая по слову x вида $\mathrm{pair}\,(x_1, x_2)$ выдает слово $\mathrm{doub}\,(x_1)$. Имеем

$$\mathrm{left}'\,(x) = \mathop{\mathrm{Con}}_{z \sqsubseteq x} z^{\chi(x,z)},$$

где $\chi(x, z)$ — характеристическая функция предиката

$$\mathrm{even}\,(z)\ \&\ \mathrm{B}(z12, x).$$

Теперь получаем

$$\mathrm{left}\,(x) = \mathrm{compress}\,(\mathrm{left}'\,(x)).$$

Функцию right также получаем в два этапа:

$$\mathrm{right}'\,(x) = \mathrm{inv}\,(\mathrm{inv}\,(x) \dot{-} (21 * \mathrm{inv}\,(\mathrm{left}'\,(x)))),$$
$$\mathrm{right}\,(x) = \mathrm{compress}\,(\mathrm{right}'\,(x)).$$

Задачи и темы для дальнейших исследований

1. Пусть $\rho(x, y, z) \equiv (z$ есть показатель степени, с которым простое число p_y входит в разложение x на простые сомножители). Доказать, что $\rho \in \mathbf{BA}$.

2. Доказать замкнутость класса **BA** относительно операций навешивания ограниченных кванторов вида

$$(\exists x)_{x \leqslant \min(x_1, \ldots, x_n)}, \quad (\forall x)_{x \leqslant \min(x_1, \ldots, x_n)}.$$

3. Для любого $n \geqslant 1$ обозначим через $\mathrm{BA}\Sigma_n$ ($\mathrm{BA}\Pi_n$) множество всех предикатов класса **BA**, которые можно представить в форме (1.2), где $Q_1 = \exists$ (соответственно $Q_1 = \forall$) и последовательность $Q_1 \ldots Q_m$ содержит ровно $n-1$ перемен кванторов. Очевидно, что при любом n

$$\mathrm{BA}\Sigma_n \cup \mathrm{BA}\Pi_n \subseteq \mathrm{BA}\Sigma_{n+1} \cap \mathrm{BA}\Pi_{n+1}.$$

Являются ли иерархии

$$\mathrm{BA}\Sigma_1 \subseteq \mathrm{BA}\Sigma_2 \subseteq \ldots \subseteq \mathrm{BA}\Sigma_n \subseteq \ldots,$$
$$\mathrm{BA}\Pi_1 \subseteq \mathrm{BA}\Pi_2 \subseteq \ldots \subseteq \mathrm{BA}\Pi_n \subseteq \ldots$$

класса **BA** невырожденными?

4. Не используя теорему 1.3, доказать рудиментарность предиката «диадическое представление x является симметричным словом».

5. Установить рудиментарность предикатов $x \cdot y = z$ и $x^y = z$, не используя теорему 1.3.

6. Рассмотрим следующий класс $\mathcal{K}$ нестирающих машин Тьюринга. Машины этого класса имеют одну ленту, на которой располагаются несколько читающих головок. Каждая головка может независимо от других головок читать символы на ленте и передвигаться в обе стороны. Так же, как и для двуленточных машин Тьюринга, значения переменных $x_1, \ldots, x_n$ записываются на ленте машин класса $\mathcal{K}$ с использованием диадических представлений в виде $*x_1 * \ldots * x_n*$. В процессе вычисления головки на ленте не могут выходить за крайние символы $*$. По аналогии с двуленточными машинами Тьюринга вводим понятие предиката, вычислимого на машине класса $\mathcal{K}$. Предполагая, что машины класса $\mathcal{K}$ могут быть недетерминированными, доказать, что всякий предикат, вычислимый машиной класса $\mathcal{K}$, является рудиментарным [30].

7. Пусть L — контекстно свободный язык в алфавите $\{1, 2\}$. Доказать, что предикат принадлежности языку L является рудиментарным [32].

8. Пусть рудиментарный предикат ρ представи́м в форме

$$(\exists y_1)_{y_1 \leqslant z_1} \ldots (\exists y_m)_{y_m \leqslant z_m} \sigma(x_1, \ldots, x_n, y_1, \ldots, y_m),$$

где предикат σ получен из предиката конкатенации с помощью явных преобразований и операций логики высказываний. Доказать, что предикат ρ можно вычислить детерминированно за полиномиальное (от длины диадической записи аргументов) время [21].

9. Пусть $f(x)$ равно длине максимального блока из нулей, входящего в двоичное представление числа x. Доказать, что $f \in \mathbf{FBA}$.

10. Определим операцию $(\mathrm{Max}\, z)_{z \leqslant y}$ ограниченного максимума следующими соотношениями:

$$(\mathrm{Max}\, z)_{z \leqslant y}(f(x_1, \ldots, x_{n-1}, z) = x_n) = \\ = \begin{cases} \text{наибольшему из таких значений } z, \text{ что } z \leqslant y \\ \quad \text{и } f(x_1, \ldots, x_{n-1}, z) = x_n, \text{ если указанные} \\ \quad \text{значения } z \text{ существуют;} \\ y \text{ в противном случае.} \end{cases}$$

Доказать, что класс **FBA** совпадает с наименьшим классом функций, который содержит исходные функции $x + 1$, $x \cdot y$, $x \dot{-} y$, I и замкнут относительно операций суперпозиции и ограниченного максимума.

11. Существует ли такое натуральное число n, что всякую функцию класса **FBA** можно получить из исходных функций класса **FBA** операцией суперпозиции и не более чем n применениями операции ограниченной минимизации?

12. Рассмотрим вариант операции ограниченной конкатенации, который определяется на основе всех подслов «ограничивающего» слова y. Чтобы применение этой операции давало однозначный результат, потребуем, чтобы все подслова слова y были, например, упорядочены по следующему принципу: сначала слово Λ, затем однобуквенные подслова в порядке их появления (слева направо) в слове y, потом двубуквенные подслова в порядке их появления в слове y, и т. д.

Доказать, что класс **BPC** совпадает с классом всех функций, которые можно получить из исходных функций (1.37) с помощью операций суперпозиции и данного варианта ограниченной конкатенации.

13. Доказать, что классу **BPC** принадлежат (арифметические) функции $x + y$ и $x \dot{-} y$.

14. Можно ли в индуктивном определении класса **BPC** ограничиться (для всех функций этого класса) фиксированным числом применений операции ограниченной префиксной конкатенации?

15. Можно ли для предикатов класса $\mathbf{BPC}_*$ получить аналог представления (1.14)?

Комментарии. Ограниченно арифметические предикаты определены А.В. Кузнецовым [11]. Операцию конкатенации «как базис для арифметики» предложил рассматривать В. Куайн [41]. Рудиментарные предикаты ввел Р. Смальян [34]. Лемма 1.1 принадлежит Ю.И. Хмелевскому [35], леммы 1.2–1.5 — Н.К. Косовскому [9]. Теорема 1.2 доказана Н.К. Косовским [9]. Теорема 1.4 принадлежит В.А. Непомнящему [32]. Теорема 1.5 доказана С.В. Пахомовым [33]. Операция ограниченной префиксной конкатенации и класс функций **BPC** предложены в работе [26].

Дальнейшие результаты по ограниченно арифметическим и рудиментарным предикатам можно найти в [9, 21, 30–32, 34, 36, 37, 44, 45].

Глава II

ФУНКЦИИ, ЭЛЕМЕНТАРНЫЕ ПО СКОЛЕМУ, И КЛАССЫ ГЖЕГОРЧИКА

§ 2.1. Ограниченная рекурсия и нумерационные функции

1. Будем говорить, что всюду определенная функция $f(x_1, \ldots, x_n, y)$ получена из всюду определенных функций

$$g(x_1, \ldots, x_n), \quad h(x_1, \ldots, x_n, y, z), \quad j(x_1, \ldots, x_n, y)$$

с помощью операции *ограниченной рекурсии*, если выполняются соотношения:

$$\begin{cases} f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n), \\ f(x_1, \ldots, x_n, y+1) = h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)), \\ f(x_1, \ldots, x_n, y) \leqslant j(x_1, \ldots, x_n, y). \end{cases} \tag{2.1}$$

Первые два равенства из (2.1) образуют схему обычной примитивной рекурсии. Схему ограниченной рекурсии (2.1) можно приблизить к схеме примитивной рекурсии, освободившись в (2.1) от третьего соотношения. На этом пути существуют несколько вариантов эффективных операций, близких к операции ограниченной рекурсии. Приведем два примера подобных операций:

$$\begin{cases} f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n), \\ f(x_1, \ldots, x_n, y+1) = \min(h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)), \\ \hfill j(x_1, \ldots, x_n, y+1)); \end{cases}$$

$$\begin{cases} f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n); \\ f(x_1, \ldots, x_n, y+1) = \begin{cases} h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)), \text{ если} \\ h(x_1, \ldots, x_n, y, f(x_1, \ldots, x_n, y)) \leqslant \\ \quad \leqslant j(x_1, \ldots, x_n, y+1); \\ 0 \text{ в противном случае.} \end{cases} \end{cases}$$

Во всех дальнейших построениях вместо операции ограниченной рекурсии (2.1) можно с равным успехом воспользоваться любым из приведенных вариантов ограниченной рекурсии.

Введем еще две «ограниченные» операции: ограниченное суммирование и ограниченное мультиплицирование. Всюду определенная функция $f(x_1,\ldots,x_n,y)$ получается из всюду определенной функции $g(x_1,\ldots,x_,y)$ с помощью операции *ограниченного суммирования*, если

$$f(x_1,\ldots,x_n,y)=\sum_{i\leqslant y} g(x_1,\ldots,x_n,i). \tag{2.2}$$

Аналогично, функция $f(x_1,\ldots,x_n,y)$ получается из функции $g(x_1,\ldots,x_,y)$ с помощью операции *ограниченного мультиплицирования*, если

$$f(x_1,\ldots,x_n,y)=\prod_{i\leqslant y} g(x_1,\ldots,x_n,i). \tag{2.3}$$

2. Будем говорить, что функции $c(x,y)$, $l(x)$, $r(x)$ образуют *нумерационную тройку функций*, если справедливы тождества

$$l(c(x,y))=x,\quad r(c(x,y))=y. \tag{2.4}$$

Нумерационную тройку образуют, например, функции

$$\frac{(x+y)^2+3x+y}{2},\quad x\dot{-}\frac{1}{2}\left[\frac{[\sqrt{8x+1}\ \,]+1}{2}\right]\cdot\left[\frac{[\sqrt{8x+1}\ \,]\dot{-}1}{2}\right],$$

$$\left[\frac{[\sqrt{8x+1}\ \,]+1}{2}\right]\dot{-}\left(\left(x\dot{-}\frac{1}{2}\left[\frac{[\sqrt{8x+1}\ \,]+1}{2}\right]\cdot\left[\frac{[\sqrt{8x+1}\ \,]\dot{-}1}{2}\right]\right)+1\right)$$

или

$$2^x\cdot 3^y,\quad \exp_0(x),\quad \exp_1(x),$$

где через $\exp_i(x)$ обозначен показатель степени простого числа p_i в разложении x на простые сомножители (обычно полагают $\exp_i(0)=$ $=0$). В первом случае функции c, l, r помимо тождества (2.4) удовлетворяют также тождеству

$$c(l(x),r(x))=x, \tag{2.5}$$

во втором случае — нет.

В качестве нумерационной тройки функций мы выберем тройку

$$c(x,y)=(x+y)^2+x,\quad l(x)=x\dot{-}[\sqrt{x}\,]^2,\quad r(x)=[\sqrt{x}\,]\dot{-}l(x).$$

Нетрудно проверить, что данные функции удовлетворяют тождеству (2.4), но не удовлетворяют тождеству (2.5).

Положим

$$c^2(x_1,x_2)=c(x_1,x_2),\quad c^{n+1}(x_1,\ldots,x_{n+1})=c(c^n(x_1,\ldots,x_n),x_{n+1}),$$

$$l_1(x)=l(x),\quad l_{n+1}(x)=l(l_n(x)).$$

Опираясь на тождество (2.4), выводим, что при любом $n \geqslant 3$ справедливы тождества

$$l_{n-1}(c^n(x_1,\ldots,x_n)) = x_1, \quad r(l_{n-2}(c^n(x_1,\ldots,x_n))) = x_2, \ldots$$
$$\ldots, r(l_1(c^n(x_1,\ldots,x_n))) = x_{n-1}, \quad r(c^n(x_1,\ldots,x_n)) = x_n. \quad (2.6)$$

Утверждение 2.1. *Пусть Q — класс функций, который содержит тройку нумерационных функций c, l, r и замкнут относительно операции суперпозиции, $Q^{(1)}$ — множество всех функций одной переменной из Q. Тогда замыкание множества функций $Q^{(1)} \cup \{c\}$ относительно операции суперпозиции совпадает с классом Q.*

Доказательство. Пусть $f(x_1,\ldots,x_n)$ — функция из Q, $n \geqslant 2$ и $\widehat{f}(x)$ обозначает функцию

$$f(l_{n-1}(x), r(l_{n-2}(x)), \ldots, r(l_1(x)), r(x)),$$

принадлежащую множеству $Q^{(1)}$. Используя тождества (2.4), (2.6), получаем

$$\widehat{f}(c^n(x_1,\ldots,x_n)) = f(x_1,\ldots,x_n).$$

Утверждение доказано.

Замечание. В утверждении 2.1 в качестве операции суперпозиции используется «нерегулярная» суперпозиция, с помощью которой определяются функции c^n. Можно было бы сформулровать аналог утверждения 2.1 для «регулярной» суперпозиции, однако при этом потребовалось бы добавить к классу Q селекторные функции I. Поскольку во всех рассматриваемых далее классах многоместных функций присутствуют функции I (это относится и к уже рассмотренным классам $\mathbf{FBA}$, $\mathbf{FR}$, $\mathbf{BPC}$), мы сочли возможным сформулировать утверждение 2.1 без упоминания функций I.

Нумерационные функции c, l, r принадлежат классу $\mathbf{FBA}$. В самом деле, предикаты $[\sqrt{x}\ ] = z$, $x \mathbin{\dot{-}} y = z$ являются ограниченно арифметическими,

$$(l(x) = y) \equiv (\exists z)_{z \leqslant x}(([\sqrt{x}\ ] = z) \mathbin{\&} (z^2 + y = x)),$$
$$(r(x) = y) \equiv (\exists z)_{z \leqslant x}(\exists w)_{w \leqslant x}(([\sqrt{x}\ ] = z) \mathbin{\&} (l(x) = w) \mathbin{\&} (z \mathbin{\dot{-}} w = y))$$

и

$$l(x) = (\mu y)_{y \leqslant x}(l(x) = y), \quad r(x) = (\mu y)_{y \leqslant x}(r(x) = y).$$

§ 2.2. Функции, элементарные по Сколему

1. С помощью операции ограниченного суммирования (и суперпозиции) можно определить различные классы «элементарных» функций: всё зависит от выбора исходных функций класса. Однако наименьшим «естественным» и нетривиальным классом здесь является класс $\mathbf{Sk}$

функций, *элементарных по Сколему*. В качестве исходных функций класса **Sk** мы возьмем функции

$$x+1, \quad x \dot{-} y, \quad I. \tag{2.7}$$

Порождающими операциями класса **Sk** будут операции суперпозиции и ограниченного суммирования.

Из определения класса **Sk** нетрудно вывести, что каждая функция, принадлежащая классу **Sk**, ограничена сверху подходящим полиномом с натуральными коэффициентами.

Утверждение 2.2. *Пусть Q — произвольный класс функций, который содержит функции* (2.7) *и замкнут относительно операций суперпозиции и ограниченного суммирования. Тогда класс Q содержит функции $x+y$, $x \cdot y$ и замкнут относительно операции ограниченной минимизации, класс предикатов Q_* содержит предикаты $x+y=z$, $xy=z$ и замкнут относительно явных преобразований, операций логики высказываний и ограниченной квантификации.*

Доказательство. Имеем:

$$x(y+1) = \sum_{i \leqslant y} I_1^2(x,i), \quad xy = x(y+1) \dot{-} x,$$

$$x+y = (x+1)(y+1) \dot{-} (xy+1).$$

Принадлежность функций $\overline{\mathrm{sg}}\, x$, $|x-y|$ классу Q, предикатов $x+y=z$, $xy=z$ классу Q_* и замкнутость класса Q_* относительно операций логики высказываний установлены в утверждении 1.8 и теореме 1.5. Замкнутость класса Q_* относительно явных преобразований очевидна. Пусть, далее, функция $f(x_1,\ldots,x_n,y)$ определяется через функцию $g(x_1,\ldots,x_n)$ с помощью операции ограниченной минимизации (1.36). Положим

$$h(x_1,\ldots,x_n,y) = \sum_{i \leqslant y} \overline{\mathrm{sg}}\, |g(x_1,\ldots,x_{n-1},i) - x_n|.$$

Тогда функция $h(x_1,\ldots,x_n,y)$ монотонно не убывает по y и, кроме того, если z — наименьшее число из отрезка $[0,y]$, для которого $h(x_1,\ldots,x_n,z) > 0$ (в этом случае будет $h(x_1,\ldots,x_n,z) = 1$), то $f(x_1,\ldots,x_n,z) = z$. Следовательно, функция

$$\sum_{i \leqslant y} i \cdot h(x_1,\ldots,x_n,i) \cdot \overline{\mathrm{sg}}\, h(x_1,\ldots,x_n,i \dot{-} 1)$$

совпадает с функцией $f(x_1,\ldots,x_n,y)$. Таким образом, класс Q замкнут относительно операции ограниченной минимизации.

Если χ_ρ есть характеристическая функция предиката ρ и

$$\sigma(x_1, \ldots, x_n, y) \equiv (\exists z)_{z \leqslant y} \rho(x_1, \ldots, x_n, z),$$

то характеристической функцией предиката σ служит функция

$$\chi_\rho(x_1, \ldots, x_n, (\mu z)_{z \leqslant y} \rho(x_1, \ldots, x_n, z)).$$

Отсюда вытекает, что класс Q_* замкнут относительно операций ограниченной квантификации. Утверждение доказано.

Следствие. *В условиях утверждения* 2.2 *имеет место включение* $\mathbf{FBA} \subseteq Q$. *В частности*, $\mathbf{FBA} \subseteq \mathbf{Sk}$.

Оказывается, что при определении класса $\mathbf{Sk}$ операцию ограниченного суммирования не обязательно использовать в полном объеме, достаточно ограничиться более слабой ее формой, носящей название операции суженного ограниченного суммирования. Будем говорить, что функция $f(x_1, \ldots, x_n, y)$ получена из функции $g(x_1, \ldots, x_n, z)$ с помощью операции *суженного ограниченного суммирования*, если

$$f(x_1, \ldots, x_n, y) = \sum_{i \leqslant y} (1 \dot{-} g(x_1, \ldots, x_n, i)) = \sum_{i \leqslant y} \overline{\mathrm{sg}}\, g(x_1, \ldots, x_n, i).$$

Понятно, что операция суженного ограниченного суммирования при наличии функции $1 \dot{-} x = \overline{\mathrm{sg}}\, x$ выразима через операции ограниченного суммирования и суперпозиции. Поэтому если обозначить через $\mathbf{Sk}'$ класс функций, который получается из исходных функций (2.7), дополненных функцией $x \cdot y$, с помощью операций суперпозиции и суженного ограниченного суммирования, то будем иметь $\mathbf{Sk}' \subseteq \mathbf{Sk}$.

Теорема 2.1. *Справедливо равенство* $\mathbf{Sk}' = \mathbf{Sk}$.

Доказательство. Достаточно установить, что $\mathbf{Sk} \subseteq \mathbf{Sk}'$. В свою очередь это включение вытекает из замкнутости класса $\mathbf{Sk}'$ относительно операции ограниченного суммирования. Пусть поэтому функция $f(x_1, \ldots, x_n, y)$ получается из функции $g(x_1, \ldots, x_n, z)$ с помощью операции ограниченного суммирования (2.2). Замечаем, что если

$$z \geqslant \max_{i \leqslant y} \{g(x_1, \ldots, x_n, i)\},$$

то $f(x_1, \ldots, x_n, y)$ совпадает с числом решений неравенства

$$g(x_1, \ldots, x_n, i) > j$$

в области $0 \leqslant i \leqslant y$, $0 \leqslant j \leqslant z$. Иными словами,

$$f(x_1, \ldots, x_n, y) = \sum_{i \leqslant y} \sum_{j \leqslant z} \overline{\mathrm{sg}}\, ((j+1) \dot{-} g(x_1, \ldots, x_n, i)).$$

В последнем соотношении двойную сумму можно заменить одинарной суммой $\sum\limits_{k \leqslant yz+y+z}$, если значения i, j определить по формулам

$$i = \mathrm{rm}\,(k, y+1), \quad j = \left[\frac{k}{y+1}\right].$$

Таким образом, для завершения доказательства теоремы остается установить принадлежность классу $\mathbf{Sk}'$ функций $x+y$, $\mathrm{rm}\,(x,y)$, $[x/y]$ (вместо переменной z следует выбрать полином с натуральными коэффициентами, который ограничивает сверху функцию $\max\limits_{i \leqslant y}\{g(x_1, \ldots, x_n, i)\}$).

Принадлежность функции $x+y$ классу $\mathbf{Sk}'$ доказывается так же, как в теореме 1.5. Далее имеем:

$$\left[\frac{k}{y+1}\right] = \sum_{i \leqslant k} \overline{\mathrm{sg}}\,((i+1)(y+1) \dot{-} k),$$

$$\mathrm{rm}\,(k, y+1) = k \dot{-} (y+1)\left[\frac{k}{y+1}\right].$$

Теорема доказана.

Под операцией *одноместного ограниченного суммирования* будем понимать операцию ограниченного суммирования (2.2), применяемую к функциям одной переменной.

Обозначим через $\mathbf{Sk}''$ класс функций, который содержит исходные функции

$$1, \quad x+y, \quad l(x) = x \dot{-} [\sqrt{x}\ ]^2, \quad I$$

и порождается операциями суперпозиции и одноместного ограниченного суммирования.

Теорема 2.2. *Справедливо равенство* $\mathbf{Sk}'' = \mathbf{Sk}$.

Доказательство. Как установлено ранее, $l \in \mathbf{FBA}$ и $\mathbf{FBA} \subseteq \mathbf{Sk}$. Поэтому $\mathbf{Sk}'' \subseteq \mathbf{Sk}$. Чтобы доказать обратное включение, достаточно установить принадлежность классу $\mathbf{Sk}''$ функции $x \dot{-} y$ и замкнутость класса $\mathbf{Sk}''$ относительно операции ограниченного суммирования.

Определим функцию $x \div y$ соотношениями

$$x \div y = \begin{cases} x - y, & \text{если} \quad x \geqslant y; \\ 3x + y + 3, & \text{если} \quad x < y. \end{cases}$$

Поскольку

$$(x+y)^2 + 5x + 3y + 4 = (x+y+2)^2 + x - y,$$

при $x \geqslant y$ будем иметь

$$(x+y+2)^2 \leqslant (x+y+2)^2 + x - y < (x+y+3)^2.$$

Следовательно, при $x \geqslant y$

$$l((x+y)^2 + 5x + 3y + 4) = x - y.$$

Напротив, если $x < y$, то из соотношений

$$(x+y+1)^2 < (x+y+1)^2 + 3x + y + 3 = \\ = (x+y+2)^2 + x - y < (x+y+2)^2$$

следует, что

$$l((x+y)^2 + 5x + 3y + 4) = 3x + y + 3.$$

Таким образом,

$$x \div y = l((x+y)^2 + 5x + 3y + 4).$$

Далее, нетрудно убедиться, что функция $(x+y)^2 + 5x + 3y + 4$ принадлежит классу $\mathbf{Sk}''$. В самом деле,

$$(x+y)^2 + 5x + 3y + 4 = (x+y)^2 + 3(x+y) + 2 + [(x+1) + (x+1)].$$

Функция $(x+y)^2 + 3(x+y) + 2$ получается подстановкой функции $x+y$ вместо переменной z в функцию $z^2 + 3z + 2$. В свою очередь

$$z^2 + 3z + 2 = \sum_{i \leqslant z} (2i + 2).$$

Итак, функция $x \div y$ входит в класс $\mathbf{Sk}''$.

Пока не доказана принадлежность функции $x \dot{-} y$ классу $\mathbf{Sk}''$, функцию $x \div y$ можно в определенных случаях использовать вместо функции $x \dot{-} y$. Так, в класс $\mathbf{Sk}''$ входит функция x^2, поскольку

$$x^2 = ((x^2 + 3x + 2) \div (2x + 2)) \div x.$$

Имея функцию x^2, устанавливаем вхождение функции $c(x,y) = (x+y)^2 + x$ в класс $\mathbf{Sk}''$. Далее образуем функции $\operatorname{sg} x$, $\overline{\operatorname{sg}}\, x$ и $[\sqrt{x}\,]$:

$$\operatorname{sg} x = l(x^2 + 1), \quad \overline{\operatorname{sg}}\, x = l(2 \cdot \operatorname{sg} x + 2), \quad [\sqrt{x}\,] = \left(\sum_{i \leqslant x} \overline{\operatorname{sg}}\, l(i) \right) \div 1.$$

Функция $l(x)$ по определению входит в класс $\mathbf{Sk}''$. Чтобы образовать теперь тройку нумерационных функций, можно использовать вместо функции $r(x)$ функцию $r'(x) = [\sqrt{x}\,] \div l(x)$. Действительно, если $n = c(x,y)$, то

$$[\sqrt{n}\,] = x + y, \quad l(n) = x, \quad x + y \geqslant x$$

и потому $r'(n) = r(n) = y$.

Докажем замкнутость класса $\mathbf{Sk}''$ относительно операции ограниченного суммирования (2.2). При этом, имея тройку нумерационных функций c, l, r', можно ограничиться случаем $n=1$. В самом деле, если $n \geqslant 2$, то для заданной функции $g(x_1, \ldots, x_n, y)$ образуем функцию

$$\widehat{g}(x, y) = g(l_{n-1}(x), r'(l_{n-2}(x)), \ldots, r'(l_1(x)), r'(x), y),$$

применяем к ней операцию ограниченного суммирования

$$f_1(x, y) = \sum_{i \leqslant y} \widehat{g}(x, i)$$

и получаем функцию f:

$$f(x_1, \ldots, x_n, y) = f_1(c^n(x_1, \ldots, x_n), y).$$

Итак, пусть $n=1$ и функция $f(x, y)$ получается из функции $g(x, y)$ с помощью операции ограниченного суммирования (2.2) (индекс 1 у переменной x_1 опускаем). Имеем

$$\sum_{i \leqslant y} g(x, i) = \sum_{i \leqslant y} g(l(c(x, y)), i) = \sum_{(c(x,y))^2 \leqslant j \leqslant (c(x,y))^2 + y} g(l([\sqrt{j}\,]), l(j)).$$

Однако для любых функций G, s, t выполняется соотношение

$$\sum_{s(n) \leqslant j \leqslant s(n)+t(n)} G(j) = \left(G(s(n)) + \sum_{j \leqslant s(n)+t(n)} G(j) \right) \div \sum_{j \leqslant s(n)} G(j).$$

Отсюда следует, что класс $\mathbf{Sk}''$ замкнут относительно операции ограниченного суммирования.

Остается доказать принадлежность функции $x \dot{-} y$ классу $\mathbf{Sk}''$. Сначала образуем в классе $\mathbf{Sk}''$ функцию xy:

$$x(y+1) = \sum_{i \leqslant y} I_1^2(x, i), \quad xy = x(y+1) \div x.$$

Далее замечаем, что

$$((x \div y) + y) \div x = \begin{cases} 0, \text{ если } x \geqslant y; \\ 2x + 2y + 3, \text{ если } x < y. \end{cases}$$

Следовательно, вводя функцию d, получаем

$$d(x, y) = \overline{\mathrm{sg}}\,(((x \div y) + y) \div x) = \begin{cases} 1, & \text{если } x \geqslant y; \\ 0, & \text{если } x < y. \end{cases}$$

Доказательство теоремы теперь завершается равенством

$$x \dot{-} y = (x \div y) \cdot d(x, y).$$

Напомним, что при $n \geqslant 2$ для произвольной функции $f(x_1, \ldots, x_n)$ через $\widehat{f}(x)$ мы обозначили функцию

$$f(l_{n-1}(x), r(l_{n-2}(x)), \ldots, r(l_1(x)), r(x)),$$

где
$$l_1(x) = l(x), \quad l_{m+1}(x) = l(l_m(x)).$$
При $n = 1$ положим $\widehat{f}(x) = f(x)$.

Теорема 2.2 допускает следующее обобщение.

Теорема 2.3. *Пусть Q — множество функций, которое состоит из исходных функций* (2.7) *класса* $\mathbf{Sk}$ *и функций $f_1, f_2, \ldots$, а Q' есть замыкание множества Q относительно операций суперпозиции и ограниченного суммирования. Тогда Q' совпадает с замыканием Q'' системы функций*
$$1, \quad x+y, \quad l(x), \quad I, \quad \widehat{f_1}, \quad \widehat{f_2}, \ldots \tag{2.8}$$
относительно операций суперпозиции и одноместного ограниченного суммирования.

Доказательство. Очевидно, что $Q'' \subseteq Q'$. По теореме 2.2 получаем $\mathbf{Sk} \subseteq Q''$. Поскольку $c \in \mathbf{Sk}$, будет также выполняться включение
$$\{f_1, f_2, \ldots\} \subseteq Q''.$$
Следовательно, $Q \subseteq Q''$. Замкнутость класса Q'' относительно операции ограниченного суммирования устанавливается так же, как и в теореме 2.2. Теорема доказана.

2. Обозначим через Ω набор из трех операций, действующих на множестве одноместных функций: сложение двух функций $((f + g)(x) = f(x) + g(x))$, композиция двух функций $(f(g)(x) = f(g(x)))$ и одноместное ограниченное суммирование.

Следующая теорема показывает, как можно порождать все одноместные функции некоторого класса, не выходя за рамки множества одноместных функций.

Теорема 2.4. *Пусть*
$$Q = \{x+1,\ x \dot{-} y,\ I,\ f_1,\ f_2, \ldots\},$$
а Q' — замыкание множества Q относительно операций суперпозиции и ограниченного суммирования. Тогда одноместные функции класса Q' и только они могут быть получены из функций
$$1, \quad l(x), \quad \widehat{f_1}(x), \quad \widehat{f_2}(x), \ldots \tag{2.9}$$
с помощью операций Ω.

Доказательство. В пределах доказательства этой теоремы назовем одноместную функцию *допустимой*, если ее можно получить из функций системы (2.9) с помощью операций Ω. Очевидно, что все допустимые функции принадлежат классу Q'. Поэтому для доказательства теоремы достаточно установить, что все одноместные функции из Q' допустимы.

Расширим понятие допустимости на функции многих переменных. Будем говорить, что при $n \geqslant 2$ n-местная функция $g(x_1, \ldots, x_n)$ *допустима*, если для любых одноместных допустимых функций $h_1(x), \ldots \ldots, h_n(x)$ функция $g(h_1(x), \ldots, h_n(x))$ также является допустимой. Докажем теперь более общее утверждение, из которого будет следовать теорема:

все функции класса Q' являются допустимыми.

С этой целью воспользуемся теоремой 2.3 и представим класс Q' в виде замыкания системы функций (2.8) относительно операций суперпозиции и одноместного ограниченного суммирования. Отметим, что функции 1, $l(x)$, $\widehat{f}_1(x)$, $\widehat{f}_2(x), \ldots$ допустимы очевидным образом. Функция $x + y$ также допустима, поскольку для любых двух допустимых функций $h_1(x)$, $h_2(x)$ функция $h_1(x) + h_2(x)$ есть результат применения операции сложения из Ω к функциям $h_1(x)$, $h_2(x)$. Из соотношения

$$I_i^n(h_1(x), \ldots, h_i(x), \ldots, h_n(x)) = h_i(x)$$

вытекает допустимость всех функций I_i^n при $n \geqslant 2$.

Пусть функции $g_0, g_1, \ldots, g_m$ допустимы и

$$h(x_1, \ldots, x_n) = g_0(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)).$$

Если $j_1(x), \ldots, j_n(x)$ — произвольные допустимые функции, то допустимыми будут функции

$$k_1(x) = g_1(j_1(x), \ldots, j_n(x)), \ \ldots, \ k_m(x) = g_m(j_1(x), \ldots, j_n(x))$$

и, следовательно, функция $g_0(k_1(x), \ldots, k_m(x))$, которая совпадает с функцией $h(j_1(x), \ldots, j_n(x))$. При этом допустимость функций $k_i(x)$ обосновывается по-разному: при $n \geqslant 2$ следует воспользоваться определением многоместных допустимых функций, а при $n = 1$ — применить операцию композиции из Ω к допустимым функциям g_i и j_i. Аналогичное замечание необходимо сделать при обосновании допустимости функции $g_0(k_1(x), \ldots, k_m(x))$.

Таким образом, операция суперпозиции сохраняет допустимость функций.

Для завершения доказательства теоремы остается показать, что функция $I_1^1(x)$ допустима. Здесь необходимо проанализировать начало доказательства теоремы 2.2 и убедиться в том, что при доказательстве принадлежности функций $x + 1$ и $x \dot{-} y$ классу $\mathbf{Sk}''$ используются лишь функции 1, $l(x)$, $x + y$. Теперь получаем

$$I_1^1(x) = (x + 1) \dot{-} 1.$$

Пусть $\exp(x, y)$ есть показатель степени простого числа p_y, с которым оно входит в разложение x на простые сомножители. В дальнейшем нам понадобится включение $\exp \in \mathbf{Sk}$. Оно устанавливается следующим образом.

Обозначим через $\chi(x)$ характеристическую функцию предиката $\mathrm{Pr}\,(x)$. Как показано в гл. I, $\mathrm{Pr} \in \mathbf{BA}$. Поэтому $\chi \in \mathbf{Sk}$. Положим

$$d(x) = \sum_{i \leqslant x} \chi(i).$$

Функция $d(x)$ дает количество простых чисел, заключенных в отрезке $[0, x]$. В теории чисел известно, что величина p_x асимптотически не превосходит $x \ln x$. Поэтому можно выбрать такую натуральную константу C, что для всех значений x будет выполняться неравенство

$$p_x \leqslant x^2 + C.$$

Следовательно, функция

$$p_x = (\mu y)_{y \leqslant x^2 + C} (\mathrm{Pr}\,(y) \,\&\, (d(y) = x + 1)),$$

рассматриваемая от переменной x, принадлежит классу $\mathbf{Sk}$.

Обозначим через $\rho(p, x, y)$ предикат «y есть максимальная степень простого числа p, делящая x». Имеем

$$\rho(p, x, y) \equiv \mathrm{Dp}\,(y, p) \,\&\, (y|x) \,\&\, \neg(yp|x).$$

Эта формула показывает, что $\rho \in \mathbf{BA}$. Если

$$g(x, y) = (\mu z)_{z \leqslant x} \rho(p_y, x, z),$$

то $g(x, y)$ равно максимальной степени простого числа p_y, делящей x. Теперь получаем

$$\exp\,(x, y) = \left(\sum_{i \leqslant x} \varphi(i, g(x, y)) \right) \dot{-} 1,$$

где $\varphi(s, t)$ — характеристическая функция предиката $s|t$.

§ 2.3. Классы Гжегорчика

1. На основе операций суперпозиции и ограниченной рекурсии можно дать определение целой серии классов «элементарных» функций.

Пусть $\mathcal{E}^0$ обозначает наименьший класс функций, который содержит исходные функции

$$0, \quad x + 1, \quad I \tag{2.10}$$

и замкнут относительно операций суперпозиции и ограниченной рекурсии.

Классы $\mathcal{E}^1$, $\mathcal{E}^2$, $\mathcal{E}^3$ определим аналогичным образом, добавляя к исходным функциям (2.10) соответственно функции $x + y$, $x \cdot y$, x^y (считаем, что $0^0 = 1$). Классы $\mathcal{E}^0$, $\mathcal{E}^1$, $\mathcal{E}^2$, $\mathcal{E}^3$ суть первые четыре класса из счетной последовательности классов, образующей иерархию Гжегорчика множества всех примитивно рекурсивных функций.

Идею, заложенную в определении классов Гжегорчика, можно легко обобщить в различных направлениях. Мы воспользуемся обобщением, предложенным А.П. Бельтюковым [3].

Пусть f — произвольная всюду определенная функция. Через $\mathcal{E}f$ обозначим наименьший класс функций, который содержит исходные функции (2.10), функции $\max(x, y)$, f и замкнут относительно операций суперпозиции и ограниченной рекурсии. Очевидно, что для любой функции f имеет место включение $\mathcal{E}^0 \subseteq \mathcal{E}f$.

Пусть E^0 — множество всех таких всюду определенных функций $f(x)$, что $f(x) \geqslant x + 1$, функция $f(x)$ монотонно не убывает и график функции f, т. е. предикат $f(x) = y$, принадлежит классу $\mathcal{E}^0_*$. В дальнейшем будем рассматривать классы «элементарных» функций, имеющие вид $\mathcal{E}f$, где $f \in E^0$.

Если f — одноместная функция, а i — натуральное число, то через $f^{\langle i \rangle}$ будем обозначать i-кратную суперпозицию функции f, т. е. функцию

$$f^{\langle i \rangle}(x) = \underbrace{f(f(\ldots f}_{i}(x)\ldots)).$$

Из определений классов $\mathcal{E}^0$, $\mathcal{E}f$, E^0 легко выводится следующее

Утверждение 2.3. *Для любой функции $g(x_1, \ldots, x_n)$ из класса $\mathcal{E}^0$ найдутся такие натуральные числа i, $1 \leqslant i \leqslant n$, и k, что*

$$g(x_1, \ldots, x_i, \ldots, x_n) \leqslant x_i + k.$$

Если $f \in E^0$, то для любой функции $g(x_1, \ldots, x_n)$ из класса $\mathcal{E}f$ найдется такое натуральное число i, что

$$g(x_1, \ldots, x_n) \leqslant f^{\langle i \rangle}(\max(x_1, \ldots, x_n)).$$

Утверждение 2.4. *Класс $\mathcal{E}^0$ содержит функции $x \dot{-} y$ и $x \cdot \mathrm{sg}\, y$. Класс $\mathcal{E}^0_*$ и классы вида $(\mathcal{E}f)_*$ замкнуты относительно операций логики высказываний.*

Доказательство. Сначала ограниченной рекурсией определим в классе $\mathcal{E}^0$ функцию $x \dot{-} 1$:

$$\begin{cases} 0 \dot{-} 1 = 0, \\ (x+1) \dot{-} 1 = I^1_1(x), \\ x \dot{-} 1 \leqslant I^1_1(x). \end{cases}$$

Затем образуем функцию $x \dot{-} y$:

$$\begin{cases} x \dot{-} 0 = I^1_1(x), \\ x \dot{-} (y+1) = (x \dot{-} y) \dot{-} 1, \\ x \dot{-} y \leqslant I^2_1(x, y). \end{cases}$$

Далее получаем

$$\begin{cases} x \cdot \operatorname{sg} 0 = 0, \\ x \cdot \operatorname{sg}(y+1) = x, \\ x \cdot \operatorname{sg} y \leqslant x. \end{cases}$$

Замкнутость классов $\mathcal{E}^0_*, (\mathcal{E}f)_*$ относительно операций логики высказываний следует теперь из утверждения 1.8.

Утверждение 2.5. *Класс $\mathcal{E}^0$ и классы вида $\mathcal{E}f$ замкнуты относительно операций суженного ограниченного суммирования и ограниченной минимизации. Класс $\mathcal{E}^0_*$ и классы вида $(\mathcal{E}f)_*$ замкнуты относительно операций ограниченной квантификации.*

Доказательство. Мы рассмотрим только класс $\mathcal{E}^0$, классы $\mathcal{E}f$ рассматриваются аналогично.

Соотношение

$$x + \operatorname{sg} y = (x+1) \dot{-} (1 \dot{-} y)$$

показывает, что классу $\mathcal{E}^0$ принадлежит функция $x + \operatorname{sg} y$. Если теперь $g(x_1, \ldots, x_n, z)$ есть функция из класса $\mathcal{E}^0$ и

$$h(x_1, \ldots, x_n, y) = \sum_{i \leqslant y} (1 \dot{-} g(x_1, \ldots, x_n, i)),$$

то функцию h получаем в классе $\mathcal{E}^0$ ограниченной рекурсией с использованием функции $x + \operatorname{sg} y$:

$$\begin{cases} h(x_1, \ldots, x_n, 0) = 1 \dot{-} g(x_1, \ldots, x_n, 0), \\ h(x_1, \ldots, x_n, y+1) = h(x_1, \ldots, x_n, y) + \operatorname{sg}(1 \dot{-} g(x_1, \ldots, x_n, y+1)), \\ h(x_1, \ldots, x_n, y) \leqslant y + 1. \end{cases}$$

Таким образом, класс $\mathcal{E}^0$ замкнут относительно операции суженного ограниченного суммирования.

Пусть $\rho(x_1, \ldots, x_n, z)$ — предикат класса $\mathcal{E}^0_*$, χ_ρ — его характеристическая функция и

$$\sigma(x_1, \ldots, x_n, y) \equiv (\exists z)_{z \leqslant y} \rho(x_1, \ldots, x_n, z).$$

Тогда характеристическая функция χ_σ предиката σ определяется по формуле

$$\chi_\sigma(x_1, \ldots, x_n, y) = \operatorname{sg} \sum_{i \leqslant y} (1 \dot{-} \overline{\operatorname{sg}}\, \chi_\rho(x_1, \ldots, x_n, i)).$$

Используя утверждение 2.4, получаем, что класс $\mathcal{E}^0$ замкнут также относительно операции навешивания ограниченного квантора общности.

Предположим, что функция g принадлежит классу $\mathcal{E}^0$, а функция h получается из функции g с помощью операции ограниченной минимизации:

$$h(x_1, \ldots, x_n, y) = (\mu z)_{z \leqslant y} (g(x_1, \ldots, x_{n-1}, z) = x_n).$$

Имеем

$$(h(x_1,\ldots,x_n,y)=w)\equiv(w\leqslant y)\,\&\,(g(x_1,\ldots,x_{n-1},w)=x_n)\,\&\\ \&\,(\forall z)_{z<w}(g(x_1,\ldots,x_{n-1},z)\neq x_n)\vee(w=0)\,\&\\ \&\,(\forall z)_{z\leqslant y}(g(x_1,\ldots,x_{n-1},z)\neq x_n).$$

Поскольку характеристическими функциями предикатов $x<y$, $x=y$ служат функции

$$\mathrm{sg}\,(y\dot{-}x),\quad \overline{\mathrm{sg}}\,(x\dot{-}y+\mathrm{sg}\,(y\dot{-}x)),$$

предикат $h(x_1,\ldots,x_n,y)=w$ принадлежит классу $\mathcal{E}^0_*$.

Пусть $\chi(x_1,\ldots,x_n,y,w)$ — его характеристическая функция. Положим

$$h_1(x_1,\ldots,x_n,y,w)=\sum_{i\leqslant w}(1\dot{-}\overline{\mathrm{sg}}\,\chi(x_1,\ldots,x_n,y,i)).$$

Тогда $h_1\in\mathcal{E}^0$ и, кроме того,

$$h(x_1,\ldots,x_n,y)=\sum_{i\leqslant y}(1\dot{-}h_1(x_1,\ldots,x_n,y,i)).$$

Таким образом, класс $\mathcal{E}^0$ замкнут относительно операции ограниченной минимизации. Утверждение доказано.

2. Утверждение 2.6. *Пусть $f\in E^0$, $g(x_1,\ldots,x_n)$ — функция из класса $\mathcal{E}f$. Тогда найдутся такое натуральное число i и такая функция $h(x_1,\ldots,x_n,y)$ из класса $\mathcal{E}^0$, что при любом a из $\mathbb{N}$ справедливо соотношение*

$$g(x_1,\ldots,x_n)=h(x_1,\ldots,x_n,f^{\langle i\rangle}(\max\,(x_1,\ldots,x_n))+a).$$

Доказательство. Проведем индукцию по построению функции g в классе $\mathcal{E}f$.

Если $g\in\{0,x+1,I\}$, то утверждение очевидно. Рассмотрим функцию $\max(x_1,x_2)$. Предикат $\max(x_1,x_2)=y$ принадлежит классу $\mathcal{E}^0_*$, поскольку он является конъюнкцией предикатов

$$x_1\leqslant y,\quad x_2\leqslant y,\quad (x_1=y\vee x_2=y).$$

Положим

$$h(x_1,x_2,y)=(\mu z)_{z\leqslant y}(\max\,(x_1,x_2)=z).$$

Тогда $h\in\mathcal{E}^0$ и, кроме того,

$$h(x_1,x_2,y)=\begin{cases}\max\,(x_1,x_2), \text{ если } y\geqslant\max\,(x_1,x_2);\\ 0 \text{ в противном случае.}\end{cases}$$

Поэтому ввиду условия $f(x)\geqslant x+1$ при любом $a\in\mathbb{N}$ будем иметь

$$\max\,(x_1,x_2)=h(x_1,x_2,f^{\langle 1\rangle}(\max\,(x_1,x_2))+a).$$

Аналогичным образом поступаем с функцией $f(x)$. Предикат $f(x) = y$ по определению класса E^0 входит в класс $\mathcal{E}^0_*$. Определяем в классе $\mathcal{E}^0$ функцию

$$h(x, y) = (\mu z)_{z \leqslant y}(f(x) = z)$$

и получаем, что при любом $a \in \mathbb{N}$

$$f(x) = h(x, f^{\langle 1 \rangle}(x) + a).$$

Предположим теперь, что функции $g_0, g_1, \ldots, g_m$ принадлежат классу $\mathcal{E}f$,

$$g(x_1, \ldots, x_n) = g_0(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n)),$$

а числа $i_0, i_1, \ldots, i_m$ и функции $h_0, h_1, \ldots, h_m$ из класса $\mathcal{E}^0$ выбраны так, что при любом j, $1 \leqslant j \leqslant m$, и любых $a_0, a_1, \ldots, a_m$ из множества $\mathbb{N}$

$$g_0(y_1, \ldots, y_m) = h_0(y_1, \ldots, y_m, f^{\langle i_0 \rangle}(\max(y_1, \ldots, y_m)) + a_0),$$

$$g_j(x_1, \ldots, x_n) = h_j(x_1, \ldots, x_n, f^{\langle i_j \rangle}(\max(x_1, \ldots, x_m)) + a_j).$$

Согласно утверждению 2.3 найдутся такие числа $k_1, \ldots, k_m$, что при любом j, $1 \leqslant j \leqslant m$, выполняется неравенство

$$g_j(x_1, \ldots, x_n) \leqslant f^{\langle k_j \rangle}(\max(x_1, \ldots, x_n)).$$

Если $i = \max(i_0, i_1, \ldots, i_m, k_1, \ldots, k_m)$ и

$$h(x_1, \ldots, x_n, y) = h_0(h_1(x_1, \ldots, x_n, y), \ldots, h_m(x_1, \ldots, x_n, y), y),$$

то, пользуясь монотонностью функции f, при любом $a \in \mathbb{N}$ будем иметь

$$g(x_1, \ldots, x_n) = h(x_1, \ldots, x_n, f^{\langle 2i \rangle}(\max(x_1, \ldots, x_n)) + a).$$

Предположим, что g_0, g_1, g_2 суть функции класса $\mathcal{E}f$,

$$\begin{cases} g(x_1, \ldots, x_n, 0) = g_0(x_1, \ldots, x_n), \\ g(x_1, \ldots, x_n, x_{n+1} + 1) = g_1(x_1, \ldots, x_n, x_{n+1}, g(x_1, \ldots, x_n, x_{n+1})), \\ g(x_1, \ldots, x_n, x_{n+1}) \leqslant g_2(x_1, \ldots, x_n, x_{n+1}), \end{cases}$$

а числа i_0, i_1, i_2 и функции h_0, h_1 из класса $\mathcal{E}^0$ выбраны так, что соотношения

$$g_0(x_1, \ldots, x_n) = h_0(x_1, \ldots, x_n, f^{\langle i_0 \rangle}(\max(x_1, \ldots, x_n)) + a_0),$$
$$g_1(x_1, \ldots, x_{n+2}) = h_1(x_1, \ldots, x_{n+2}, f^{\langle i_1 \rangle}(\max(x_1, \ldots, x_{n+2})) + a_1),$$
$$g_2(x_1, \ldots, x_{n+1}) \leqslant f^{\langle i_2 \rangle}(\max(x_1, \ldots, x_{n+1}))$$

справедливы при любых a_0, a_1 из множества $\mathbb{N}$. Из определения функции g и последнего неравенства следует, что

$$g(x_1, \ldots, x_{n+1}) \leqslant f^{\langle i_2 \rangle}(\max(x_1, \ldots, x_{n+1})).$$

Пользуясь утверждением 2.4, убеждаемся, что функция h, определенная соотношениями

$$\begin{cases} h(x_1,\ldots,x_n,0,y) = \begin{cases} h_0(x_1,\ldots,x_n,y), \text{ если } h_0(x_1,\ldots,x_n,y) \leqslant y; \\ 0 \text{ в противном случае}; \end{cases} \\ h(x_1,\ldots,x_n,x_{n+1}+1,y) = \\ \qquad = \begin{cases} h_1(x_1,\ldots,x_n,x_{n+1},h(x_1,\ldots,x_{n+1},y),y), \text{ если} \\ \qquad h_1(x_1,\ldots,x_n,x_{n+1},h(x_1,\ldots,x_{n+1},y),y) \leqslant y; \\ 0 \text{ в противном случае}; \end{cases} \\ h(x_1,\ldots,x_{n+1},y) \leqslant y, \end{cases}$$

принадлежит классу $\mathcal{E}^0$. Если теперь положить $i = \max(i_0, i_1, i_2)$, то согласно определению функций h_0, h_1, h при любом $a \in \mathbb{N}$ будем иметь

$$g(x_1,\ldots,x_{n+1}) = h(x_1,\ldots,x_{n+1}, f^{\langle 2i\rangle}(\max(x_1,\ldots,x_{n+1})) + a).$$

Утверждение доказано.

Утверждение 2.7. *Пусть $f \in E^0$. Тогда класс $\mathcal{E}f$ совпадает с наименьшим классом функций $\mathcal{E}'f$, который содержит исходные функции* 0, I *и замкнут относительно операций суперпозиции, ограниченной рекурсии вида*

$$\begin{cases} g(x_1,\ldots,x_n,0) = h(x_1,\ldots,x_n), \\ g(x_1,\ldots,x_n,y+1) = j(x_1,\ldots,x_n,y,g(x_1,\ldots,x_n,y)), \\ g(x_1,\ldots,x_n,y) \leqslant f^{\langle i\rangle}(\max(x_1,\ldots,x_n,y)) \end{cases} \tag{2.11}$$

и ограниченной минимизации вида

$$g(x_1,\ldots,x_n) = (\mu y)_{y \leqslant f^{\langle i\rangle}(\max(x_1,\ldots,x_n))}(h(x_1,\ldots,x_n,y) \neq 0), \tag{2.12}$$

где неравенство $h(x_1,\ldots,x_n,y) \neq 0$ выполняется хотя бы для одного y, не превосходящего $f^{\langle i\rangle}(\max(x_1,\ldots,x_n))$.

Доказательство. Очевидно, что класс $\mathcal{E}f$ замкнут относительно операции ограниченной рекурсии вида (2.11). Замкнутость класса $\mathcal{E}f$ относительно операции ограниченной минимизации вида (2.12) следует из утверждений 2.4, 2.5 и замкнутости класса $\mathcal{E}f$ относительно суперпозиции. Поэтому $\mathcal{E}'f \subseteq \mathcal{E}f$.

Обратно, докажем, что класс $\mathcal{E}'f$ содержит функции $\max$, f и замкнут относительно операции ограниченной рекурсии (2.1).

Из утверждения 2.3 следует, что в схеме ограниченной рекурсии (2.1) вместо функций j можно рассматривать функции вида $f^{\langle i\rangle}(\max(x_1,\ldots,x_n))$. Таким образом, класс $\mathcal{E}'f$ замкнут относительно операции ограниченной рекурсии (2.1).

Далее, как установлено при доказательстве утверждения 2.4, функцию $x \dot{-} y$ можно определить ограниченной рекурсией через функции 0 и I. Иными словами, $(x \dot{-} y) \in \mathcal{E}'f$. Поскольку

$$x + 1 = (\mu y)_{y \leqslant f^{\langle 1\rangle}(x)}(y \dot{-} x \neq 0),$$

функция $x+1$ также принадлежит классу $\mathcal{E}'f$. Отсюда следует, что $\mathcal{E}^0 \subseteq \mathcal{E}'f$. Предикаты

$$\max(x_1, x_2) = y, \quad f(x) = y$$

входят в класс $\mathcal{E}^0_*$. Пусть $\chi_1(x_1, x_2, y)$, $\chi_2(x, y)$ — соответственно их характеристические функции. Тогда будем иметь:

$$\max(x_1, x_2) = (\mu y)_{y \leqslant f^{\langle 1 \rangle}(\max(x_1, x_2))}(\chi_1(x_1, x_2, y) \neq 0),$$
$$f(x) = (\mu y)_{y \leqslant f^{\langle 1 \rangle}(x)}(\chi_2(x, y) \neq 0).$$

Утверждение доказано.

Утверждение 2.8. *Имеет место включение* $\mathbf{BA} \subseteq \mathcal{E}^0_*$.

Доказательство. В силу утверждений 2.4, 2.5 достаточно установить, что классу $\mathcal{E}^0_*$ принадлежат предикаты $x+y=z$ и $xy=z$. Как нетрудно убедиться, справедлива эквивалентность

$$(x+y=z) \equiv (((z+1) \dot{-} x) \dot{-} y = 1).$$

Поэтому предикат $x+y=z$ входит в класс $\mathcal{E}^0_*$. Определим далее в классе $\mathcal{E}^0$ функцию $z \dot{-} xy$:

$$\begin{cases} z \dot{-} x \cdot 0 = z, \\ z \dot{-} x \cdot (y+1) = (z \dot{-} xy) \dot{-} x, \\ z \dot{-} xy \leqslant z. \end{cases}$$

Теперь получаем

$$(xy = z) \equiv ((z+1) \dot{-} xy = 1).$$

Утверждение доказано.

Как уже отмечалось, $\mathcal{E}^0 \subseteq \mathcal{E}f$ для любой функции f. В частности, $\mathcal{E}^0 \subseteq \mathcal{E}(x+1)$. Однако функция $\max(x_1, x_2)$, принадлежащая классу $\mathcal{E}(x+1)$, не входит в класс $\mathcal{E}^0$, поскольку не может быть ограничена функциями вида $x_1 + C$ и $x_2 + C$. Таким образом, $\mathcal{E}^0 \subset \mathcal{E}(x+1)$. Вместе с тем справедливо

Утверждение 2.9. *Имеет место равенство* $\mathcal{E}^0_* = (\mathcal{E}(x+1))_*$.

Доказательство. Включение $\mathcal{E}^0_* \subseteq (\mathcal{E}(x+1))_*$ очевидно. Установим обратное включение.

Пусть $g(x_1, \ldots, x_n)$ — произвольная функция класса $\mathcal{E}(x+1)$, принимающая лишь значения 0 и 1. Согласно утверждению 2.6 найдутся такие натуральное число i и функция $h(x_1, \ldots, x_n, y)$ из класса $\mathcal{E}^0$, что

$$g(x_1, \ldots, x_n) = h(x_1, \ldots, x_n, \max(x_1, \ldots, x_n) + i).$$

Отсюда

$$(g(x_1,\ldots,x_n)=1)\equiv \bigvee_{1\leqslant j\leqslant n}(x_j=\max(x_1,\ldots,x_n))\,\&\\ \&\,(h(x_1,\ldots,x_n,x_j+i)=1).$$

Предикат $x_j=\max(x_1,\ldots,x_n)$ принадлежит классу **BA** (см. утверждение 1.3) и, значит, классу $\mathcal{E}^0_*$; предикат $h(x_1,\ldots,x_n,x_j+i)=1$ также, очевидно, принадлежит классу $\mathcal{E}^0_*$, причем класс $\mathcal{E}^0_*$ замкнут относительно операций логики высказываний (утверждение 2.4). Следовательно, в класс $\mathcal{E}^0_*$ входит предикат $g(x_1,\ldots,x_n)=1$. Так как функция g принимает лишь значения 0 и 1, она совпадает с характеристической функцией предиката $g(x_1,\ldots,x_n)=1$. Утверждение доказано.

Утверждение 2.10. *При* $i=1,2,3$ *класс* $\mathcal{E}^i$ *совпадает с классом* $\mathcal{E}f_i$, *где*

$$f_1(x)=2(x+1),\quad f_2(x)=(x+1)^2,\quad f_3(x)=2^x.$$

Доказательство. Поскольку $\mathcal{E}^0\subset\mathcal{E}^1\subset\mathcal{E}^2\subset\mathcal{E}^3$ и классу $\mathcal{E}^0$ принадлежит функция $\min(x,y)$:

$$\min(x,y)=x\dot{-}(x\dot{-}y),$$

функция $\min$ будет входить в каждый из классов $\mathcal{E}^1$, $\mathcal{E}^2$, $\mathcal{E}^3$. Принадлежность функции $\max$ данным классам вытекает из следующих соотношений:

$$\max(x,y)=(x+y)\dot{-}\min(x,y),\quad x+y=((x+1)(y+1)\dot{-}xy)\dot{-}1,$$
$$x+y=(x+1)^{y+1}\dot{-}(((x+1)^{y+1}\dot{-}x)\dot{-}y).$$

Из очевидных включений

$$f_1\in\mathcal{E}^1,\quad f_2\in\mathcal{E}^2,\quad f_3\in\mathcal{E}^3$$

следует далее, что

$$\mathcal{E}f_1\subseteq\mathcal{E}^1,\quad \mathcal{E}f_2\subseteq\mathcal{E}^2,\quad \mathcal{E}f_3\subseteq\mathcal{E}^3.$$

Обратно, схемы ограниченных рекурсий

$$\begin{cases}x+0=x,\\ x+(y+1)=(x+y)+1,\\ x+y\leqslant f_1(\max(x,y)),\end{cases}\qquad \begin{cases}x\cdot 0=0,\\ x\cdot(y+1)=x\cdot y+x,\\ x\cdot y\leqslant f_2(\max(x,y)),\end{cases}$$

$$\begin{cases}x^0=1,\\ x^{y+1}=x^y\cdot x,\\ x^y\leqslant f_3^{\langle 2\rangle}(\max(x,y))\end{cases}$$

и неравенства

$$f_1(x)\leqslant f_2^{\langle 2\rangle}(x),\quad f_2(x)\leqslant f_3^{\langle 2\rangle}(x)$$

показывают, что функции $x + y$, $x \cdot y$, x^y принадлежат соответственно классам $\mathcal{E}f_1$, $\mathcal{E}f_2$, $\mathcal{E}f_3$. Утверждение доказано.

Утверждение 2.11. *Имеет место включение* $\mathbf{Sk} \subseteq \mathcal{E}^2$.

Доказательство. Функция $x \dot{-} y$ принадлежит классу $\mathcal{E}^0$ и, значит, классу $\mathcal{E}^2$. Поэтому для доказательства достаточно установить, что класс $\mathcal{E}^2$ замкнут относительно операции ограниченного суммирования.

Пусть $g \in \mathcal{E}^2$ и функция $f(x_1, \ldots, x_n, y)$ получается из функции g согласно формуле (2.2). Поскольку функция $x + y$ входит в класс $\mathcal{E}^2$, функцию f можно получить из функций класса $\mathcal{E}^2$ с помощью операции примитивной рекурсии:

$$\begin{cases} f(x_1, \ldots, x_n, 0) = g(x_1, \ldots, x_n, 0), \\ f(x_1, \ldots, x_n, y + 1) = f(x_1, \ldots, x_n, y) + g(x_1, \ldots, x_n, y + 1). \end{cases}$$

Остается указать в классе $\mathcal{E}^2$ функцию, которая ограничивает сверху функцию f.

Согласно утверждениям 2.3 и 2.10 существует такое натуральное число i, что

$$g(x_1, \ldots, x_n) \leqslant f_2^{\langle i \rangle}(\max(x_1, \ldots, x_n, y)).$$

Отсюда и из определения функции f получаем, что

$$\begin{aligned} f(x_1, \ldots, x_n, y) \leqslant (y + 1) \cdot f_2^{\langle i \rangle}(\max(x_1, \ldots, x_n, y)) \leqslant \\ \leqslant f_2(\max(x_1, \ldots, x_n, y)) \cdot f_2^{\langle i \rangle}(\max(x_1, \ldots, x_n, y)) \leqslant \\ \leqslant f_2^{\langle i+1 \rangle}(\max(x_1, \ldots, x_n, y)). \end{aligned}$$

Утверждение доказано.

3. Пусть f, g — одноместные функции. Будем писать $f \leqslant {}_{\mathcal{E}} g$, если существует такое число i, что

$$f(x) \leqslant g^{\langle i \rangle}(x). \tag{2.13}$$

Запись $f < {}_{\mathcal{E}} g$ означает, что $f \leqslant {}_{\mathcal{E}} g$ и существует такое число i, что при любом j выполняется неравенство $f^{\langle j \rangle} < {}_{\mathrm{ae}} g^{\langle i \rangle}$, где $s < {}_{\mathrm{ae}} t$ есть сокращение для формулы

$$(\exists x_0)(\forall x)_{x \geqslant x_0}(s(x) < t(x)).$$

Утверждение 2.12. *Если* $f, g \in E^0$, *то* $f \leqslant {}_{\mathcal{E}} g$ *в том и только в том случае, когда* $\mathcal{E}f \subseteq \mathcal{E}g$. *Если же* $f < {}_{\mathcal{E}} g$, *то* $\mathcal{E}f \subset \mathcal{E}g$.

Доказательство. Пусть $f \leqslant {}_{\mathcal{E}} g$ и, следовательно, для некоторого i выполняется неравенство (2.13). Очевидно, что для доказательства соотношения $\mathcal{E}f \subseteq \mathcal{E}g$ достаточно утановить, что функция f входит в класс $\mathcal{E}g$. Из $f \in E^0$ следует, что предикат $f(x) = y$ принадлежит классу $\mathcal{E}^0$, а из $\mathcal{E}^0 \subseteq \mathcal{E}g$ — что он содержится и в классе $\mathcal{E}g$. Положим

$$h(x, y) = (\mu z)_{z \leqslant y}(f(x) = z).$$

В силу утверждения 2.5 функция h принадлежит классу $\mathcal{E}g$. Пользуясь неравенством (2.13), получаем

$$f(x) = h(x, g^{\langle i \rangle}(x)).$$

Обратно, если $\mathcal{E}f \subseteq \mathcal{E}g$, то в силу утверждения 2.3 найдется такое i, что будет справедливо неравенство (2.13).

Предположим теперь, что $f <_{\mathcal{E}} g$. Поскольку, в частности, $f \leqslant_{\mathcal{E}} g$, по доказанному получаем, что $\mathcal{E}f \subseteq \mathcal{E}g$. Функция g не может входить в класс $\mathcal{E}f$, так как это противоречит утверждению 2.3 и соотношению $f <_{\mathcal{E}} g$. Утверждение доказано.

Напомним, что через $f_2(x)$ мы обозначили функцию $(x+1)^2$.

Теорема 2.5. *Пусть* $f, g \in E^0$, $f <_{\mathcal{E}} g \leqslant_{\mathcal{E}} f_2$ *и* $(\mathcal{E}f)_* = (\mathcal{E}g)_*$. *Тогда* $\mathcal{E}^0_* = (\mathcal{E}g)_*$.

Доказательство. Без ограничения общности можно считать, что

$$(\forall i)(f^{\langle i \rangle} <_{\mathrm{ae}} g), \quad (\forall x)_{x \geqslant b}(g(x+1) \leqslant x^k)$$

для некоторых b и k из $\mathbb{N}$.

Пусть $\mathbf{x}$ обозначает набор $(x', \widehat{x}, x^{(k)}, \ldots, x^{(0)})$, $\overline{\mathbf{x}}$ — набор $(\mathbf{x}_1, \ldots$ $\ldots, \mathbf{x}_n)$. Положим

$$\begin{aligned}
&r(\mathbf{x}) = \min\left(g(x'+1), \sum_{i \leqslant k} x^{(i)} \cdot \widehat{x}^i\right),\\
&\overline{r}(\mathbf{x}) = (r(\mathbf{x}_1), \ldots, r(\mathbf{x}_n)),\\
&g'(z) = (\mu y)(g(y) \geqslant z) \dot{-} 1,\\
&\widehat{e}(z) = \lceil \sqrt[k]{z}\, \rceil,
\end{aligned}$$

где через $\lceil a \rceil$ обозначено целое, ближайшее сверху к числу a. При $z > 1$ определим разряды $e^{(k)}(z), \ldots, e^{(0)}(z)$ разложения числа z по степеням $\widehat{e}(z)$:

$$e^{(i)}(z) = \left[\frac{\mathrm{rm}(z, (\widehat{e}(z))^{i+1})}{(\widehat{e}(z))^i}\right].$$

Положим также

$$e^{(i)}(0) = 0, \quad e^{(0)}(1) = 1, \quad e^{(i)}(1) = 0 \quad \text{при } i > 0.$$

Определим далее

$$\begin{aligned}
&\mathbf{e}(z) = (g'(z), \widehat{e}(z), e^{(k)}(z), \ldots, e^{(0)}(z)),\\
&\overline{\mathbf{e}}(z) = (\mathbf{e}(z_1), \ldots, \mathbf{e}(z_n)).
\end{aligned}$$

Из приведенных определений следует, что

$$r(\mathbf{e}(z)) = z, \quad e^{(i)}(z) \leqslant \widehat{e}(z), \quad \max\{\overline{r}(\overline{\mathbf{x}})\} \leqslant g(\max(\overline{\mathbf{x}}) + 1)$$

и для некоторого c из $\mathbb{N}$ —

$$g(\max(\mathbf{e}(z))) \leqslant \max(c, z),$$

поскольку

$$g(\lceil \sqrt[k]{z}\, \rceil) \leqslant g([\, \sqrt[k]{z}\,] + 1) \leqslant [\, \sqrt[k]{z}\,]^k \leqslant z$$

при $z \geqslant b^k$.

Нетрудно видеть, что функция $\min(u, r(\mathbf{x}))$ принадлежит классу $\mathcal{E}^0$. В самом деле, по определению

$$\min(u, r(\mathbf{x})) = \min\left(u, g(x'+1), \sum_{i \leqslant k} x^{(i)} \cdot \widehat{x}^i\right).$$

Предикат

$$\min\left(u, \sum_{i \leqslant k} x^{(i)} \cdot \widehat{x}^i\right) = y$$

входит в класс $\mathbf{BA}$ (напомним, что число k фиксировано), предикат $g(x'+1) = y$ по определению принадлежит классу $\mathcal{E}^0_*$,

$$\min(u, r(\mathbf{x})) = (\mu y)_{y \leqslant u}\left((g(x'+1) = y) \vee \left(\min\left(u, \sum_{i \leqslant k} x^{(i)} \cdot \widehat{x}^i\right) = y\right)\right)$$

и потому функция $\min(u, r(\mathbf{x}))$ входит в класс $\mathcal{E}^0$.

Пусть $\varphi(z_1, \ldots, z_n)$ — функция из класса $\mathcal{E}g$, принимающая лишь значения 0 и 1. Согласно утверждению 2.6 найдутся такие натуральное число i и функция φ_1 из класса $\mathcal{E}^0$, что для любого $a \in \mathbb{N}$ будет

$$\varphi(z_1, \ldots, z_n) = \varphi_1(g^{\langle i \rangle}(\max(z_1, \ldots, z_n)) + a, z_1, \ldots, z_n).$$

Положим

$$\psi(v, \overline{\mathbf{x}}) = \varphi_1(v, \min(v, r(\mathbf{x}_1)), \ldots, \min(v, r(\mathbf{x}_n))).$$

По доказанному функция ψ принадлежит классу $\mathcal{E}^0$. Поскольку $x <_{\mathrm{ae}} g(x)$, для достаточно больших c будем иметь

$$\begin{aligned}\varphi(\overline{z}) = \varphi_1(g^{\langle i \rangle}(\max(\overline{r}(\overline{\mathbf{e}}(\overline{z})))), \overline{r}(\overline{\mathbf{e}}(\overline{z}))) = \psi(g^{\langle i \rangle}(\max(\overline{r}(\overline{\mathbf{e}}(\overline{z})))), \overline{\mathbf{e}}(\overline{z})) =\\ = \psi(g^{\langle i \rangle}(g(\max(\overline{r}(\overline{\mathbf{e}}(\overline{z})) + 1)), \overline{\mathbf{e}}(\overline{z}))) = \psi(g^{\langle i+2 \rangle}(\max(c, \overline{\mathbf{e}}(\overline{z}))), \overline{\mathbf{e}}(\overline{z})),\end{aligned}$$

где $\overline{z} = (z_1, \ldots, z_n)$. Функция $\psi(g^{\langle i+2 \rangle}(\max(c, \overline{\mathbf{x}})), \overline{\mathbf{x}})$ принадлежит классу $\mathcal{E}g$. Можно считать, что она принимает лишь значения 0 и 1. По условию теоремы $(\mathcal{E}g)_* = (\mathcal{E}f)_*$. Поэтому согласно утвержению 2.6 найдутся такое число j и функция ω из класса $\mathcal{E}^0$, что при любом $a \in \mathbb{N}$ выполняется равенство

$$\varphi(\overline{z}) = \omega(f^{\langle j \rangle}(\max(\overline{\mathbf{e}}(\overline{z}))) + a, \overline{\mathbf{e}}(\overline{z})).$$

Так как

$$(\forall j)(f^{\langle j \rangle} <_{\mathrm{ae}} g),$$

найдется такое c_1, что при любом $a \in \mathbb{N}$ верно равенство

$$\varphi(\overline{z}) = \omega(g(\max(c_1, \overline{\mathbf{e}}(\overline{z}))) + a, \overline{\mathbf{e}}(\overline{z})).$$

Определим функцию τ из класса $\mathcal{E}^0$ соотношением

$$\tau(v, \overline{z}) = \omega(v, \overline{\mathbf{e}}(\overline{z})).$$

Тогда при любом $a \in \mathbb{N}$ будем иметь

$$\varphi(\overline{z}) = \tau(g(\max(c_1, \overline{\mathbf{e}}(\overline{z}))) + a, \overline{z}).$$

Учитывая, что $g(x+1) \leqslant x^k$ при $x \geqslant b$, получаем: найдется такое число d, что выполняется равенство

$$\varphi(\overline{z}) = \tau(\max(d, \overline{z}), \overline{z}).$$

Поскольку функция φ принимает лишь значения 0 и 1, на основании утверждения 2.9 приходим к выводу, что $\tau(\max(d, \overline{z}), \overline{z}) \in \mathcal{E}^0$. Теорема доказана.

Следствие. *Если $\mathcal{E}^1_* = \mathcal{E}^2_*$, то $\mathcal{E}^0_* = \mathcal{E}^2_*$.*

Как доказано в утверждении 2.8, $\mathbf{BA} \subseteq \mathcal{E}^0_*$. Кроме того, очевидно, что $\mathcal{E}^0_* \subseteq \mathcal{E}^2_*$. Какое из этих включений строгое, неизвестно, однако вариант

$$\mathbf{BA} = \mathcal{E}^0_*, \quad \mathcal{E}^0_* \subset \mathcal{E}^2_* \tag{2.14}$$

невозможен. В самом деле, класс $\mathbf{BA}$ замкнут относительно подстановок полиномов с натуральными коэффициентами (следствие из теоремы 1.1). С другой стороны, в силу утверждения 2.6 каждый предикат класса $\mathcal{E}^2_*$ можно получить из подходящего предиката класса $\mathcal{E}^0_*$ подстановкой полинома с натуральными коэффициентами вместо одной из переменных. Таким образом, одновременное выполнение соотношений (2.14) невозможно.

§ 2.4. Соотношение между классами Sk_* и $\mathcal{E}^0_*$

Из сравнения скоростей роста функций в классах $\mathbf{Sk}$ и $\mathcal{E}^0$ легко следует, что $\mathbf{Sk} \not\subseteq \mathcal{E}^0$. В самом деле, классу $\mathbf{Sk}$ принадлежит, например, функция x^2, тогда как любая функция $f(x)$ из класса $\mathcal{E}^0$ ограничена сверху функцией вида $x + C$, где C — натуральная константа.

Более трудным является вопрос о соотношении между классами $\mathbf{Sk}_*$ и $\mathcal{E}^0_*$. Априори не очевидно, что операция ограниченного суммирования позволяет определить в классе $\mathbf{Sk}_*$ предикат, не входящий в класс $\mathcal{E}^0_*$. И действительно, как будет установлено ниже, имеет место включение $\mathbf{Sk}_* \subseteq \mathcal{E}^0_*$. При доказательстве этого утверждения будут использованы некоторые хорошо известные факты из теории чисел.

Отметим два простых утверждения относительно функций и предикатов из класса $\mathcal{E}^0$, которыми мы будем пользоваться в дальнейшем. Во-первых, класс $\mathcal{E}^0$ (а также классы $\mathcal{E}f$) замкнут относительно операции изменения значения функции в конечном числе точек. Это следует из того, что классу $\mathcal{E}^0$ принадлежат функции $x + \mathrm{sg}\, y$, $x \cdot \mathrm{sg}\, y$, $\mathrm{sg}\, |x - y|$ (ср. с доказательством утверждения 1.9).

Во-вторых, класс $\mathcal{E}^0_*$ замкнут относительно операций навешивания ограниченных кванторов вида $(Qx)_{x \leqslant \max(y_1, \dots, y_m)}$. Это есть следствие утверждений 2.5 и 2.9.

Положим $q_1(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2$ и для $k \geqslant 1$ определим

$$\begin{aligned} q_{k+1}(x_1, \dots, x_{4^{k+1}}) = q_1(&q_k(x_1, \dots, x_{4^k}), q_k(x_{4^k+1}, \dots, x_{2.4^k}), \\ &q_k(x_{2.4^k+1}, \dots, x_{3.4^k}), q_k(x_{3.4^k+1}, \dots, x_{4^{k+1}})). \end{aligned}$$

Согласно известной теореме Лагранжа каждое число из $\mathbb{N}$ представимо в виде суммы четырех квадратов чисел из $\mathbb{N}$. Иными словами, функция q_1 принимает все значения из $\mathbb{N}$. Более того, как нетрудно видеть, если переменные x_1, x_2, x_3, x_4 независимо друг от друга принимают все значения от 0 до x, то функция $q_1(x_1, x_2, x_3, x_4)$ заведомо принимает все значения от 0 до x^2. Вообще, если переменные $x_1, \dots, x_{4^k}$ независимо принимают все значения из отрезка $[0, x]$, то функция $q_k(x_1, \dots, x_{4^k})$ заведомо принимает все значения из отрезка $[0, 2^{2^k}]$.

В дальнейшем выражение $q_k(x_1, \dots, x_{4^k})$ записываем в виде $q_k(\overline{x})$.

Отметим, что функция q_k представляет собой полином с натуральными коэффициентами. Поэтому при любых k и m предикаты вида

$$q_k(\overline{x}) = q_m(\overline{y}), \quad q_k(\overline{x}) \leqslant q_m(\overline{y})$$

принадлежат классу $\mathbf{BA}$ и, следовательно, классу $\mathcal{E}^0_*$.

Функция $q_k(\overline{x})$ принимает каждое значение, отличное от 0, на нескольких наборах. Введем предикат ν_k, который выделяет те наборы, где функция q_k принимает значение $q_k(\overline{x})$ «впервые». Для этого определим линейный порядок на множестве $\mathbb{N}^{4^k}$. Зададим его с помощью нумерационной функции c^{4^k}. Именно, будем считать, что $(a_1, \dots, a_{4^k}) \leqslant (b_1, \dots, b_{4^k})$, если

$$c^{4^k}(a_1, \dots, a_{4^k}) \leqslant c^{4^k}(b_1, \dots, b_{4^k}).$$

Предикат ν_k определим в классе $\mathbf{BA}$ формулой

$$\begin{aligned} \nu_k(x_1, \dots, x_{4^k}) \equiv (\forall y_1)_{y_1 \leqslant \max(x_1, \dots, x_{4^k})} \dots (\forall y_{4^k})_{y_{4^k} \leqslant \max(x_1, \dots, x_{4^k})} \\ ((c^{4^k}(y_1, \dots, y_{4^k}) < c^{4^k}(x_1, \dots, x_{4^k})) \Rightarrow \\ \Rightarrow (q_k(y_1, \dots, y_{4^k}) \neq q_k(x_1, \dots, x_{4^k}))). \end{aligned}$$

Теорема 2.6. *Для любой функции $f(x_1, \dots, x_n)$ из класса $\mathbf{Sk}$ и любых натуральных чисел $k_1, \dots, k_n$ функция*

$$\mathrm{rm}\,(f(q_{k_1}(\overline{x}^1), \dots, q_{k_n}(\overline{x}^n)), y) \tag{2.15}$$

принадлежит классу $\mathcal{E}^0$.

Доказательство. Проведем индукцию по построению функций в классе **Sk**.

Каждый из предикатов

$$\operatorname{rm}(q_k(\overline{x})+1, y) = z, \quad \operatorname{rm}(I_i^n(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n)), y) = z, \\ \operatorname{rm}\,(q_{k_1}(\overline{x}^1) \dot{-} q_{k_2}(\overline{x}^2), y) = z \tag{2.16}$$

принадлежит классу **BA** и, следовательно, классу $\mathcal{E}^0$. Соответствующие функции

$$\operatorname{rm}(q_k(\overline{x})+1, y), \quad \operatorname{rm}(I_i^n(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n)), y), \\ \operatorname{rm}(q_{k_1}(\overline{x}^1) \dot{-} q_{k_2}(\overline{x}^2), y)$$

получаются из предикатов (2.16) с помощью операции ограниченной минимизации $(\mu z)_{z\leqslant y}$.

Пусть $g_0, g_1, \ldots, g_m \in \mathbf{Sk}$,

$$f(x_1, \ldots, x_n) = g_0(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$$

и для функций $g_0, g_1, \ldots, g_m$ утверждение теоремы доказано. Как отмечалось в § 2.2, всякая функция из класса **Sk** ограничена сверху подходящим полиномом с натуральными коэффициентами. В частности, это справедливо для функций

$$g_1(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n)), \ \ldots, \ g_m(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n)).$$

Пусть $x = \max\{\overline{x}^1, \ldots, \overline{x}^n\}$. Выберем число s таким образом, чтобы множество значений функции $q_s(\overline{y})$, принимаемых ею в кубе $0 \leqslant y_1, \ldots, y_{4^s} \leqslant x$, при любом i, $1 \leqslant i \leqslant m$, и достаточно больших x содержало множество значений функции

$$g_i(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n)),$$

принимаемых в кубе

$$0 \leqslant x_j \leqslant x \quad (x_j \in \{\overline{x}^1, \ldots, \overline{x}^n\}).$$

Например, можно взять такое s, что при любом i, $1 \leqslant i \leqslant m$, и достаточно больших значениях x выполняется неравенство

$$x^{2^s} \geqslant \max_{x_j \leqslant x} g_i(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n)).$$

Тогда, исключая, быть может, конечное число наборов, будем иметь

$$\begin{aligned}(\operatorname{rm}(f(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n)), y) = z) \equiv \\ \equiv (\exists y_1^1)_{y_1^1 \leqslant x} \ldots (\exists y_{4^s}^1)_{y_{4^s}^1 \leqslant x} \ldots (\exists y_1^m)_{y_1^m \leqslant x} \ldots (\exists y_{4^s}^m)_{y_{4^s}^m \leqslant x} \\ ((q_s(\overline{y}^1) = g_1(q_{k_1}(\overline{x}^1) \ldots, q_{k_n}(\overline{x}^n))) \,\&\, \ldots \,\& \\ \&\, (q_s(\overline{y}^s) = g_m(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n))) \,\& \\ \&\, (\operatorname{rm}(g_0(q_s(\overline{y}^1), \ldots, q_s(\overline{y}^m)), y) = z)),\end{aligned}$$

где положено

$$\overline{y}^1 = (y_1^1, \ldots, y_{4^s}^1),\ \ldots,\ \overline{y}^m = (y_1^m, \ldots, y_{4^s}^m).$$

По предположению индукции функция

$$\mathrm{rm}\,(g_0(q_s(\overline{y}^1), \ldots, q_s(\overline{y}^m)), y)$$

принадлежит классу $\mathcal{E}^0$. Кроме того, класс $\mathcal{E}_*^0$ замкнут относительно операций ограниченной квантификации, а класс $\mathcal{E}^0$ — относительно операции ограниченной минимизации. Поэтому для доказательства принадлежности функции (2.15) классу $\mathcal{E}^0$ достаточно установить, что в класс $\mathcal{E}_*^0$ входят предикаты

$$q_s(\overline{y}^i) = g_i(q_{k_1}(\overline{x}^1) \ldots, q_{k_n}(\overline{x}^n)). \tag{2.17}$$

Согласно известной китайской теореме об остатках проверку равенства (2.17) можно заменить проверкой системы равенств

$$\begin{array}{l}
\mathrm{rm}\,(q_s(\overline{y}^i), p_0) = \mathrm{rm}\,(g_i(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n)), p_0), \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\mathrm{rm}\,(q_s(\overline{y}^i), p_r) = \mathrm{rm}\,(g_i(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n)), p_r),
\end{array}$$

где $p_0, \ldots, p_r$ — последовательные простые числа, а число r выбрано с таким расчетом, чтобы выполнялось соотношение

$$p_0 \cdot \ldots \cdot p_r > \max\,(q_s(\overline{y}^i), g_i(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n))).$$

Мы выберем число r с большим запасом: числами $p_0, \ldots, p_r$ будут все простые числа из отрезка $[0, x]$. Как известно, количество простых чисел из отрезка $[0, x]$ асимптотически равно $x/\ln x$. Поэтому при достаточно больших значениях x выполняется неравенство

$$\prod_{p_j \leqslant x} p_j > \left[\frac{x}{\ln x}\right]!$$

Очевидно, что функция, стоящая в правой части этого неравенства, растет быстрее любого полинома от x. Поэтому если пренебречь конечным числом наборов, то будет справедлива эквивалентность

$$\begin{aligned}
&(q_s(\overline{y}^i) = g_i(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n))) \equiv \\
&\quad \equiv (\forall p)_{p \leqslant x}(\mathrm{Pr}\,(p) \Rightarrow (\mathrm{rm}\,(q_s(\overline{y}^i), p) = \mathrm{rm}\,(g_i(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n)), p))).
\end{aligned}$$

Предикаты $\mathrm{Pr}\,(p)$ и $\mathrm{rm}\,(q_s(\overline{y}^i), p) = z$ принадлежат классу $\mathbf{BA}$, а предикат

$$\mathrm{rm}\,(g_i(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n)), p) = z$$

входит в класс $\mathcal{E}_*^0$ по предположению индукции. Значит, принимая во внимание возможность изменять значения функций из класса $\mathcal{E}^0$ в конечном числе наборов, приходим к выводу, что функция (2.15) принадлежит классу $\mathcal{E}^0$.

Пусть теперь $g \in \mathcal{E}^0$,

$$f(x_1, \ldots, x_n, x_{n+1}) = \sum_{i \leqslant x_{n+1}} g(x_1, \ldots, x_n, i)$$

и для функции g утверждение теоремы справедливо. Положим

$$x = \max\{\overline{x}^1, \ldots, \overline{x}^n, \overline{x}^{n+1}\}.$$

Выберем число s с таким расчетом, чтобы множество значений функции $q_s(y_1, \ldots, y_{4^s})$, принимаемых ею в кубе $0 \leqslant y_1, \ldots, y_{4^s} \leqslant x$, при достаточно больших x целиком содержало в себе множество значений функции

$$f(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n), q_{k_{n+1}}(\overline{x}^{n+1})),$$

принимаемых в кубе

$$0 \leqslant x_j \leqslant x \quad (x_j \in \{\overline{x}^1, \ldots, \overline{x}^n, \overline{x}^{n+1}\}).$$

Тогда, пренебрегая, быть может, конечным числом наборов, получим

$$\begin{aligned}(\mathrm{rm}\,(f(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n), q_{k_{n+1}}(\overline{x}^{n+1})), y) = z) \equiv \\ \equiv (\exists y_1)_{y_1 \leqslant x} \ldots (\exists y_{4^s})_{y_{4^s} \leqslant x}((q_s(y_1, \ldots, y_{4^s}) = \\ = \sum_{i \leqslant q_{k_{n+1}}(\overline{x}^{n+1})} g(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n), i)) \;\&\; (\mathrm{rm}\,(q_s(y_1, \ldots, y_{4^s}), y) = z)).\end{aligned}$$

Предикат $\mathrm{rm}\,(q_s(y_1, \ldots, y_{4^s}), y) = z$ принадлежит классу $\mathbf{BA}$, класс $\mathcal{E}^0_*$ замкнут относительно операций ограниченной квантификации, а класс $\mathcal{E}^0$ — относительно операции ограниченной минимизации. Поэтому для доказательства принадлежности функции

$$\mathrm{rm}\,(f(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n), q_{k_{n+1}}(\overline{x}^{n+1}), y))$$

классу $\mathcal{E}^0$ достаточно установить, что в класс $\mathcal{E}^0_*$ входит предикат

$$q_s(\overline{y}) = \sum_{i \leqslant q_{k_{n+1}}(\overline{x}^{n+1})} g(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n), i). \tag{2.18}$$

Как и в случае суперпозиции, если исключить конечное число наборов, то равенство (2.18) можно заменить системой равенств

$$\mathrm{rm}\,(q_s(\overline{y}), p_j) = \mathrm{rm}\left(\sum_{i \leqslant q_{k_{n+1}}(\overline{x}^{n+1})} g(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n), i), p_j\right), \tag{2.19}$$

где p_j пробегает множество всех простых чисел из отрезка $[0, x]$. Правую часть равенства (2.19) можно, очевидно, переписать в виде

$$\sum_{i \leqslant q_{k_{n+1}}(\overline{x}^{n+1})} \mathrm{rm}\,(g(q_{k_1}(\overline{x}^1), \ldots, q_{k_n}(\overline{x}^n), i), p_j), \tag{2.20}$$

где суммирование проводится по модулю p_j. Чтобы теперь воспользоваться индуктивным предположением, сумму (2.20) следовало бы представить в виде

$$\sum_{i_1\leqslant x,\ldots,i_{4^t}\leqslant x} \mathrm{rm}\,(g(q_{k_1}(\overline{x}^1),\ldots,q_{k_n}(\overline{x}^n),q_t(i_1,\ldots,i_{4^t})),p_j), \tag{2.21}$$

где $t=k_{n+1}$. Однако этому препятствуют два обстоятельства. Во-первых, в кубе $0\leqslant i_1,\ldots,i_{4^t}\leqslant x$ функция $q_t(i_1,\ldots,i_{4^t})$ принимает любое значение, отличное от 0, на нескольких наборах. А во-вторых, в том же кубе функция $q_t(i_1,\ldots,i_{4^t})$ может принимать значения, бо́льшие чем $q_{k_{n+1}}(\overline{x}^{n+1})$.

Чтобы избавиться в сумме (2.21) от нежелательных слагаемых, обозначим через $h(i_1,\ldots,i_{4^t},\overline{x}^{n+1})$ характеристическую функцию предиката

$$\nu_t(i_1,\ldots,i_{4^t})\,\&\,(q_t(i_1,\ldots,i_{4^t})<q_{k_{n+1}}(\overline{x}^{n+1})),$$

принадлежащую классу $\mathcal{E}^0$. Теперь сумму (2.20) преобразуем в «исправленную» сумму

$$\sum_{i_1\leqslant x,\ldots,i_{4^t}\leqslant x} \mathrm{rm}\,(g(q_{k_1}(\overline{x}^1),\ldots,q_{k_n}(\overline{x}^n),q_t(i_1,\ldots,i_{4^t})),p_j)\times$$
$$\times\, h(i_1,\ldots,i_{4^t},\overline{x}^{n+1}), \tag{2.22}$$

где суммирование проводится по модулю p_j.

Заменим в (2.22) переменную p_j переменной p и обозначим через

$$g_1(\overline{x}^1,\ldots,\overline{x}^n,\overline{x}^{n+1},i_1,\ldots,i_{4^t},p)$$

функцию, стоящую под знаком $\sum$. Согласно индуктивному предположению $g_1\in\mathcal{E}^0$ (функция h принимает лишь значения $0,1$ и потому совпадает с функцией $\mathrm{sg}\,h$). Суммирование в (2.22) по модулю p можно провести в классе $\mathcal{E}^0$. Для этого вместо обычной функции сложения следует воспользоваться функцией $\mathrm{rm}\,(x+y,p)$, которая принадлежит классу $\mathcal{E}^0$. Обозначим через $f_1(\overline{x}^1,\ldots,\overline{x}^n,\overline{x}^{n+1},p)$ функцию, выражаемую формулой (2.22), когда $p_j=p$. Тогда, как мы убедились, $f_1\in\mathcal{E}^0$. Теперь систему равенств (2.19) можно заменить предикатом

$$(\forall p)_{p\leqslant x}(\mathrm{Pr}\,(p)\Rightarrow(\mathrm{rm}\,(q_s(y_1,\ldots,y_{4^s}),p)=f_1(\overline{x}^1,\ldots,\overline{x}^n,\overline{x}^{n+1},p))),$$

входящим в класс $\mathcal{E}_*^0$. Теорема доказана.

Следствие. *Имеет место соотношение* $\mathbf{Sk}_*\subseteq\mathcal{E}_*^0$.

Доказательство. Мы докажем чуть более общий факт: если $f(x_1,\ldots,x_n)\in\mathbf{Sk}$ и для некоторой функции $g(x_1,\ldots,x_n)$ из класса $\mathcal{E}^0$ выполняется неравенство

$$f(x_1,\ldots,x_n)\leqslant g(x_1,\ldots,x_n),$$

то $f\in\mathcal{E}^0$.

В самом деле, согласно теореме 2.6 функция

$$h(x_1^1, \dots, x_4^1, \dots, x_1^n, \dots, x_4^n, y) = \mathrm{rm}\,(f(q_1(x_1^1, \dots, x_4^1), \dots, q_1(x_1^n, \dots, x_4^n)), y)$$

принадлежит классу $\mathcal{E}^0$. Поэтому в класс $\mathcal{E}_*^0$ будет входить предикат

$$\begin{aligned}(\exists x_1^1)_{x_1^1 \leqslant x_1} \dots (\exists x_4^1)_{x_4^1 \leqslant x_1} \dots (\exists x_1^n)_{x_1^n \leqslant x_n} \dots (\exists x_4^n)_{x_4^n \leqslant x_n} \\ ((x_1 = q_1(x_1^1, \dots, x_4^1)) \,\&\, \dots \,\&\, (x_n = q_1(x_1^n, \dots, x_4^n)) \,\&\, \\ \&\, (y = h(x_1^1, \dots, x_4^1, \dots, x_1^n, \dots, x_4^n, y + 1))),\end{aligned}$$

который совпадает с предикатом $f(x_1, \dots, x_n) = y$. Теперь получаем

$$f(x_1, \dots, x_n) = (\mu y)_{y \leqslant g(x_1, \dots, x_n)}(f(x_1, \dots, x_n) = y).$$

Следствие доказано.

§ 2.5. Функции, элементарные по Кальмару

Так же, как с операцией ограниченного суммирования, с использованием операции ограниченного мультиплицирования можно определить различные классы «элементарных» функций. По ряду причин при построении «наименьшего» класса, основанного на операции ограниченного мультиплицирования, наряду с данной операцией необходимо рассматривать также операции суперпозиции и ограниченного суммирования. Таким образом, мы приходим к классу $\mathbf{K}$ функций, *элементарных по Кальмару*: $\mathbf{K}$ есть наименьший класс функций, который содержит исходные функции (2.7) и замкнут относительно операций суперпозиции, ограниченного суммирования и ограниченного мультиплицирования.

Из определения сразу следует, что $\mathbf{Sk} \subset \mathbf{K}$.

Теорема 2.7. *Справедливо равенство* $\mathbf{K} = \mathcal{E}^3$.

Доказательство. Покажем сначала, что $\mathbf{K} \subseteq \mathcal{E}^3$. Исходные функции $x + 1$ и I класса $\mathbf{K}$ по определению входят в класс $\mathcal{E}^3$. Функция $x \dot{-} y$ входит в класс $\mathbf{Sk}$ и, следовательно, в силу включений $\mathbf{Sk} \subseteq \mathcal{E}^2 \subset \mathcal{E}^3$ также и в класс $\mathcal{E}^3$.

Установим, что класс $\mathcal{E}^3$ замкнут относительно операции ограниченного суммирования. Пусть $g \in \mathcal{E}^3$ и функция $f(x_1, \dots, x_n, y)$ получается из функции g по формуле (2.2). Согласно утверждениям 2.3 и 2.10 найдется такое натуральное число k, что

$$g(x_1, \dots, x_n, i) \leqslant f_3^{\langle k \rangle}(\max\,(x_1, \dots, x_n, i)),$$

где $f_3(x) = 2^x$. Поэтому

$$\sum_{i \leqslant y} g(x_1, \dots, x_n, i) \leqslant (y + 1) \cdot f_3^{\langle k \rangle}(\max\,(x_1, \dots, x_n, y)).$$

Обозначим функцию, стоящую в правой части этого неравенства, через $h(x_1, \dots, x_n, y)$. Очевидно, что $h \in \mathcal{E}^3$. Теперь функцию f можно определить ограниченной рекурсией в классе $\mathcal{E}^3$:

$$\begin{cases} f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n, 0), \\ f(x_1, \dots, x_n, y+1) = f(x_1, \dots, x_n, y) + g(x_1, \dots, x_n, y+1), \\ f(x_1, \dots, x_n, y) \leqslant h(x_1, \dots, x_n, y). \end{cases}$$

Аналогичным образом устанавливаем замкнутость класса $\mathcal{E}^3$ относительно операции ограниченного мультиплицирования. При этом в качестве ограничивающей функции следует взять функцию

$$(f_3^{\langle k \rangle}(\max(x_1, \dots, x_n, y)))^{y+1}.$$

Перейдем к доказательству включения $\mathcal{E}^3 \subseteq \mathbf{K}$. Очевидно, что для этого достаточно утановить принадлежность функции x^y классу $\mathbf{K}$ и замкнутость класса $\mathbf{K}$ относительно операции ограниченной рекурсии.

Имеем

$$x^{y+1} = \prod_{i \leqslant y} I_1^2(x, i).$$

Функция $[x/y]$ принадлежит классу $\mathbf{Sk}$ и, значит, классу $\mathbf{K}$. Далее получаем

$$x^y = \left[\frac{x^{y+1}}{x}\right].$$

Пусть функция $f(x_1, \dots, x_n, y)$ определяется через функции g, h, j согласно схеме ограниченной рекурсии (2.1) и g, h, j входят в класс $\mathbf{K}$. Для упрощения выкладок рассмотрим случай $n = 1$, а вместо переменной x_1 будем писать x. Функцию $j(x, y)$ будем считать монотонной по y (иначе можно перейти к функции $j'(x, y) = \sum_{i \leqslant y} j(x, i)$).

Из соотношений (2.1) следует, что равенство $f(x, y) = z$ выполняется в том и только в том случае, когда найдутся такие числа $a_0, a_1, \dots, a_y$, не превосходящие величины $j(x, y)$, что

$$a_0 = g(x), \quad a_y = z,$$

и для любого i, $0 \leqslant i < y$, справедливо равенство

$$a_{i+1} = h(x, i, a_i)$$

(очевидно, что в этом случае $a_i = f(x, i)$). Вместо последовательности $a_0, a_1, \dots, a_y$ рассмотрим одно число

$$b_y = p_0^{a_0} \cdot p_1^{a_1} \cdot \ldots \cdot p_y^{a_y},$$

где $p_0, \ldots, p_y$ — последовательные простые числа. Известно, что величина p_y асимптотически растет как $y \ln y$. Поэтому существует такое натуральное число C, что при любом y из $\mathbb{N}$ выполняется неравенство

$$p_y \leqslant y \ln y + C.$$

Отсюда следует, что можно подобрать такое натуральное число C_1, что

$$p_0 \cdot p_1 \cdot \ldots \cdot p_y \leqslant (y^2 + C_1)^{y+1}.$$

А так как все числа $a_0, a_1, \ldots, a_y$ не превосходят величины $j(x, y)$, для числа b_y получим оценку

$$b_y \leqslant (y^2 + C_1)^{(y+1)\cdot j(x,y)}.$$

Понятно, что правая часть этого неравенства есть функция из $\mathbf{K}$. Обозначим ее через $j_1(x, y)$. Теперь получаем

$$\begin{aligned}(f(x,y) = z) \equiv (\exists b)_{b \leqslant j_1(x,y)} (\forall i)_{i \leqslant y} ((\exp(b, 0) = g(x)) \ \& \\ \& \ (\exp(b, y) = z)) \ \& \ ((i < y) \Rightarrow (\exp(b, i+1) = h(x, i, \exp(b, i))))),\end{aligned}$$

где $\exp(b, i)$ есть показатель числа p_i в разложении b на простые множители. В конце § 2.2 установлено, что функция $\exp(b, i)$ принадлежит классу $\mathbf{Sk}$. Согласно утверждению 2.2 предикат $f(x, y) = z$ входит в класс $\mathbf{K}_*$. Функция $f(x, y)$ получается из этого предиката с помощью операций ограниченной минимизации и суперпозиции. Еще раз обращаясь к утверждению 2.2, завершаем доказательство теоремы.

Обозначим через $\mathbf{K}'$ наименьший класс функций, который содержит исходные функции (2.7), функцию 2^x и замкнут относительно операций суперпозиции и ограниченного суммирования. Очевидно, что $\mathbf{Sk} \subset \mathbf{K}' \subseteq \mathbf{K}$.

Утверждение 2.13. *Имеет место равенство* $\mathbf{K}' = \mathbf{K}$.

Доказательство. Понятно, что для доказательства утверждения достаточно установить, что класс $\mathbf{K}'$ замкнут относительно операции ограниченного мультиплицирования.

Пусть функция $f(x_1, \ldots, x_n, y)$ получается из функции g по формуле (2.3) и $g \in \mathbf{K}'$. Покажем, что $f \in \mathbf{K}'$. Для упрощения выкладок рассмотрим случай $n = 1$, полагая $x = x_1$. Имеем

$$\begin{aligned}(f(x,y) = z) \equiv (\exists i)_{i \leqslant y} ((g(x, i) = 0) \ \& \ (z = 0)) \ \vee \\ \vee \ (\forall i)_{i \leqslant y} (\forall j)_{j \leqslant h(x,y,z)} ((g(x, i) \neq 0) \ \& \ (z \neq 0) \ \& \\ \& \ (\exp(z, j) = \sum_{k \leqslant y} \exp(g(x, k), j))),\end{aligned}$$

где

$$h(x, y, z) = z + \sum_{i \leqslant y} g(x, i).$$

Согласно утверждению 2.2 предикат $f(x,y) = z$ принадлежит классу $\mathbf{K}'_*$. Выбрав теперь подходящее число k, получаем

$$f(x,y) = (\mu z)_{z \leqslant f_3^{\langle k \rangle}(\max(x,y))}(f(x,y) = z),$$

где $f_3(x) = 2^x$. Утверждение доказано.

Следствие. *Все одноместные функции класса* $\mathbf{K}$ *и только они могут быть получены из функций* 1, $l(x)$, 2^x *с помощью операций* Ω.

Доказательство. Достаточно воспользоваться представлением класса $\mathbf{K}$ в виде $\mathbf{K}'$ и применить теорему 2.4.

Доказанное следствие позволяет сделать определенные выводы о возможности получения всех функций класса $\mathbf{K}$ из конечного числа функций этого класса с помощью одной только операции суперпозиции (конечная порождаемость класса $\mathbf{K}$ относительно операции суперпозиции).

Пусть $f(x)$ — произвольная всюду определенная функция. Функцию

$$f^\iota(x) = \prod_{i \leqslant x} p_i^{f(i)}$$

назовем *изображением* функции f. Очевидно, что

$$\exp(f^\iota(x), x) = f(x). \tag{2.23}$$

Кроме того, если функция f принадлежит классу $\mathbf{K}$, то, как нетрудно видеть, функция f^ι также принадлежит классу $\mathbf{K}$.

Попытаемся заменить действие операций из Ω на одноместные функции действием подходящих функций на соответствующие изображения. Пусть

$$g(x) = f_1(x) + f_2(x).$$

Тогда функцию $g^\iota(x)$ можно получить из функций f_1^ι, f_2^ι по формуле

$$g^\iota(x) = \prod_{i \leqslant x} p_i^{\exp(f_1^\iota(x), i) + \exp(f_2^\iota(x), i)}.$$

Следовательно, если определить функцию $h_+(x,y,z)$ в классе $\mathbf{K}$ соотношением

$$h_+(x,y,z) = \prod_{i \leqslant x} p_i^{\exp(y,i) + \exp(z,i)}, \tag{2.24}$$

то получим

$$h_+(x, f_1^\iota(x), f_2^\iota(x)) = g^\iota(x).$$

Аналогичным образом, если

$$g(x) = f_2(f_1(x)),$$

то функцию g^ι можно определить в виде

$$g^\iota(x) = h_s(x, f_1^\iota(x), f_2^\iota(v)), \tag{2.25}$$

где
$$h_s(x,y,z) = \prod_{i\leqslant x} p_i^{\exp(z,\exp(y,i))}$$
и v удовлетворяет неравенству
$$v \geqslant \max_{j\leqslant x}\{f_1(j)\}.$$

Наконец, если
$$g(x) = \sum_{i\leqslant x} f(i),$$
то функцию g^ι получаем по формуле
$$g^\iota(x) = h_\sigma(x, f^\iota(x)), \tag{2.26}$$
где функция h_σ определятся в классе $\mathbf{K}$ равенством
$$h_\sigma(x,y) = \prod_{i\leqslant x} p_i^{\sum\limits_{j\leqslant i}\exp(y,j)}.$$

В теореме 2.8 под суперпозицией мы понимаем «нерегулярную» суперпозицию (см. об этом в начале § 1.4).

Теорема 2.8. *Класс* $\mathbf{K}$ *совпадает с замыканием системы функций*
$$\begin{gathered} 1^\iota(x),\quad l^\iota(x),\quad (2^x)^\iota,\quad h_+(x,y,z),\quad h_s(x,y,z),\\ h_\sigma(x,y),\quad \exp(x,y),\quad c(x,y) \end{gathered} \tag{2.27}$$
относительно операции суперпозиции.

Доказательство. Как мы убедились ранее, все функции системы (2.27) принадлежат классу $\mathbf{K}$. Покажем, что одноместные функции из $\mathbf{K}$ можно получить из функций системы (2.27) с помощью операции суперпозиции. Для этого, используя следствие из утверждения 2.13, индукцией по построению одноместных функций класса $\mathbf{K}$ установим, что для всякой функции $f(x)$ из $\mathbf{K}$ функция $f^\iota(x)$ принадлежит замыканию системы (2.27) относительно операции суперпозиции.

Это, очевидно, справедливо для функций 1, $l(x)$ и 2^x. Шаг индукции обосновываем с помощью формул (2.24)–(2.26). При этом необходимо заметить, что переменную v в формуле (2.25) можно заменить любой функцией $d(x)$, удовлетворяющей неравенству
$$d(x) \geqslant \max_{j\leqslant x}\{f_1(j)\}.$$
По условиям теоремы эту функцию необходимо получить в виде суперпозиции функций системы (2.27). Однако любая одноместная функция из $\mathbf{K}$ мажорируется подходящей суперпозицией функции 2^x.

Функция $1^\iota(x)$, в свою очередь, мажорирует функцию 2^x. Поэтому в качестве функции $d(x)$ можно взять некоторую суперпозицию функции $1^\iota(x)$.

Имея теперь все изображения одноместных функций из $\mathbf{K}$, с помощью функции exp по формуле (2.23) получаем все одноместные функции из $\mathbf{K}$. Завершаем доказательство теоремы, обращаясь к утверждению 2.1.

Задачи и темы для дальнейших исследований

1. Доказать, что классу $\mathbf{Sk}$ принадлежат следующие функции:

а) $h_1(x,y) = x * y$ (диадическое представление $h_1(x,y)$ является конкатенацией диадических представлений чисел x и y),

б) $h_2(x) =$ числу единиц в двоичном представлении x,

в) $h_3(x) =$ наименьшему y такому, что $f_3^{\langle y\rangle}(1) \geqslant x$, где $f_3(x) = 2^x$ и $f_3^{\langle 0\rangle}(x) = x$.

2. Пусть $a_{11},\dots,a_{1n},\dots,a_{m1},\dots,a_{mn},b_1,\dots,b_m$ — рациональные числа. Доказать, что классу $\mathbf{Sk}$ принадлежит функция $f(x)$, равная числу целых решений системы неравенств

$$\begin{gathered} a_{11}x_1 + \dots + a_{1n}x_n \leqslant b_1, \\ \dots\dots\dots\dots\dots\dots\dots \\ a_{m1}x_1 + \dots + a_{mn}x_n \leqslant b_m \end{gathered}$$

в кубе $0 \leqslant x_1,\dots,x_n \leqslant x$.

3. Доказать, что операции ограниченного суммирования и ограниченного мультиплицирования не выводят за пределы класса $\mathcal{E}f$, если только функции, получающиеся в результате применения операций, ограничены сверху подходящими функциями класса $\mathcal{E}f$.

4. Пусть $f,g \in E^0$ и $f <_{\mathcal{E}} g$. Доказать, что:

а) найдется такая функция h из множества E^0, что $\mathcal{E}f \subset \mathcal{E}h \subset \mathcal{E}g$,

б) найдутся такие функции h_1, h_2 из множества E^0, что

$$\mathcal{E}f \subset \mathcal{E}h_1 \subset \mathcal{E}g, \quad \mathcal{E}f \subset \mathcal{E}h_1 \subset \mathcal{E}g, \quad \mathcal{E}h_1 \nsubseteq \mathcal{E}h_2, \quad \mathcal{E}h_2 \nsubseteq \mathcal{E}h_1.$$

5. Доказать, что если $f,g \in E^0$, $f_2(x) \leqslant_{\mathcal{E}} f$, $f_2 \leqslant_{\mathcal{E}} g$, то:

а) $f \leqslant_{\mathcal{E}} g \Leftrightarrow (\mathcal{E}f)_* \subseteq (\mathcal{E}g)_*$,

б) $f <_{\mathcal{E}} g \Leftrightarrow (\mathcal{E}f)_* \subset (\mathcal{E}g)_*$,

где $f_2(x) = (x+1)^2$ [2].

6. Какие из перечисленных ниже включений являются строгими:

а) $\mathbf{FBA}_* \subseteq Q_*$, где $Q \in \{\mathbf{Sk}, \mathcal{E}^0, \mathcal{E}^1, \mathcal{E}^2\}$,

б) $\mathbf{Sk}_* \subseteq Q_*$, где $Q \in \{\mathcal{E}^0, \mathcal{E}^1, \mathcal{E}^2\}$,

в) $\mathcal{E}^0_* \subseteq \mathcal{E}^1_*$, $\quad \mathcal{E}^0_* \subseteq \mathcal{E}^2_*$, $\quad \mathcal{E}^1_* \subseteq \mathcal{E}^2_*$?

7. Доказать, что все одноместные функции класса $\mathcal{E}^2$ и только они могут быть получены из функций x^2+x+1, $l(x)$ с помощью операций сложения, суперпозиции и ограниченного итерирования, где последняя операция есть следующий вариант ограниченной рекурсии:

$$\begin{cases} f(0) = 0, \\ f(x+1) = g(f(x)), \\ f(x) \leqslant h(x). \end{cases}$$

8. Доказать утверждение: для всякой функции $g(x_1, \ldots, x_n)$ из класса $\mathbf{K}$ найдутся такая функция $g'(x_1, \ldots, x_n, y)$ из класса $\mathbf{Sk}$ и такое натуральное число k, что

$$g(x_1, \ldots, x_n) = g'(x_1, \ldots, x_n, f_3^{\langle k \rangle}(\max(x_1, \ldots, x_n))),$$

где $f_3(x) = 2^x$.

9. Доказать, что класс $\mathbf{K}$ совпадает с наименьшим классом функций, который содержит исходные функции $x+1$, 2^x, xy, $x \dot{-} y$, I и замкнут относительно операции суперпозиции и хотя бы одной из следующих операций:

а) ограниченной минимизации,

б) ограниченного максимума (см. задачу 10 из гл. I),

в) суженного ограниченного суммирования,

г) ограниченного мультиплицирования,

д) суженного ограниченного мультиплицирования, т. е. операции

$$\prod_{i \leqslant y} (1 \dot{-} f(x_1, \ldots, x_n, i)).$$

10. Пусть $(\mathrm{Con}\, z)_{z \leqslant y}$ — операция ограниченной конкатенации, которая переводит функцию $g(x_1, \ldots, x_n, y)$ в функцию

$$f(x_1, \ldots, x_n, y) = (\mathrm{Con}\, z)_{z \leqslant y} g(x_1, \ldots, x_n, z),$$

где диадическое представление значения $f(x_1, \ldots, x_n, y)$ получается последовательной конкатенацией значений

$$g(x_1, \ldots, x_n, y), g(x_1, \ldots, x_n, y-1), \ldots, g(x_1, \ldots, x_n, 0),$$

выписанных слева направо в порядке убывания параметра y.

Доказать, что класс $\mathbf{K}$ можно получить в виде замыкания исходного множества функций $x+1$, $x \dot{-} y$, xy, I относительно операций суперпозиции и ограниченной конкатенации.

11. Пусть K_2 есть множество всех функций, каждая из которых получается из исходных функций 0, $x+1$, I операцией суперпозиции и не более чем двумя применениями операции примитивной рекурсии. Доказать, что $K_2 \subseteq \mathbf{K}$. Верно ли, что это включение собственное?

12. Доказать аналог теоремы 2.8, используя вместо функций $f^{\iota}(x)$ функции

$$\sum_{i \leqslant x} f(i) \cdot y^i.$$

13. Доказать, что класс $\mathbf{K}$ порождается суперпозициями функций каждой из систем

$$\{x+1,\ x^y,\ [x/y],\ \varphi(x,y)\}, \quad \{x \dot{-} 1,\ [x/y],\ 2^{x+y},\ \sigma(x)\},$$

где $\varphi(x,y)$ равно наименьшему номеру нулевого разряда в представлении числа y в позиционной системе с основанием x (при $x = 0, 1$ можно принять $\varphi(x,y) = 0$), а $\sigma(x)$ равно числу единиц в двоичном представлении числа x [17, 20].

14. Рассмотрим следующий вариант ограниченной словарной рекурсии:

$$\begin{cases} f(x_1,\ldots,x_n,\Lambda) = g(x_1,\ldots,x_n), \\ f(x_1,\ldots,x_n,y*1) = h_1(x_1,\ldots,x_n,y,f(x_1,\ldots,x_n,y)), \\ f(x_1,\ldots,x_n,y*2) = h_2(x_1,\ldots,x_n,y,f(x_1,\ldots,x_n,y)), \\ f(x_1,\ldots,x_n,y) \leqslant j(x_1,\ldots,x_n,y), \end{cases}$$

где переменные $x_1,\ldots,x_n,y$ принимают значения в множестве всех слов в алфавите $\{1,2\}$, а отношение $\leqslant$, как в гл. I, рассматривается между числами, заданными диадическими представлениями. Пусть $x^{|y|}$ есть функция, которая сопоставляет слову x слово, образованное конкатенацией $|y|$ экземпляров слова x (при $y = \Lambda$ полагаем $x^{|y|} = \Lambda$). Обозначим через $\mathbf{C}$ наименьший класс функций, который содержат функции Λ, 1, 2, $x*y$, $x^{|y|}$, I и замкнут относительно операций суперпозиции и ограниченной словарной рекурсии.

Доказать, что класс $\mathbf{C}$ имеет конечный базис по суперпозиции.

Комментарии. Класс функций, элементарных по Сколему, введен в [43]. Теорема 2.2 принадлежит Н.К. Косовскому [7]. Операция ограниченной рекурсии и классы $\mathcal{E}^n$ иерархии Гжегорчика определены в [6]. Теорема 2.5 доказана А.П. Бельтюковым [3]. Теорема 2.6 установлена в [16]. Идея доказательства теоремы 2.8 принадлежит Д. Рёддингу [42] и Ч. Парсонсу [40].

Глава III

МАШИННОЕ ОПИСАНИЕ КЛАССОВ

§ 3.1. Стековые регистровые машины

Следуя [3], определим абстрактные вычислительные устройства, которые будем называть *стековыми регистровыми машинами* (сокращенно: машины SRM). Память машины SRM состоит из *входных регистров*, которые будем обозначать $x_1, \ldots, x_n$, *регистров стека* $t_0, t_1, \ldots, t_k$, *рабочего регистра* r и *нулевого регистра* 0. В каждом регистре, за исключением регистра 0, на каждом шаге работы машины может находиться любое число из $\mathbb{N}$. В нулевом регистре постоянно содержится число 0.

Работа машины определяется *программой*, которая состоит из конечного числа *команд*. Каждая команда в программе снабжена некоторой *меткой*, при этом разные команды помечены различными метками. Команды могут быть одного из следующих трех типов:

1) $r := z$, где z имеет вид x_i, t_j, r или 0;

2) $t_i := t_i + 1$;

3) **if** $z_1 = z_2$ **then go to** L_i **else go to** L_j,

где z_1, z_2 имеют вид x_p, t_q, r или 0, а L_i, L_j — метки программы.

Команда 1) носит название *команды засылки*. При ее выполнении содержимое регистра z засылается в регистр r. Содержимое всех регистров, кроме регистра r, при этом не меняется. После выполнения этой команды машина переходит к выполнению следующей (согласно нумерации меток) команды.

Команда 2) называется *командой приращения*. При ее выполнении содержимое регистра t_i увеличивается на 1. Одновременно содержимое всех регистров t_j, где $j < i$, обращается в 0. Содержимое остальных регистров, отличных от регистров $t_0, \ldots, t_i$, не меняется. После выполнения команды 2) машина переходит к выполнению следующей команды программы.

Команда 3) является *командой перехода*. При ее выполнении проверяется равенство содержимого регистров z_1, z_2, и машина переходит либо к команде с меткой L_i, либо к команде с меткой L_j. При выполнении команды 3) содержимое всех регистров остается неизменным.

Программа машины SRM представляет собой список команд C_i, помеченных различными метками L_i:

$$(L_1 : C_1;\ L_2 : C_2; \ldots;\ L_s : C_s).$$

Программы машин SRM подчиняются двум ограничениям. Во-первых, последняя команды программы не может быть командой перехода. Во-вторых, для всякого i в программе машины встречается не более одного вхождения команды $t_i := t_i + 1$.

В начале работы машины SRM в рабочем регистре и регистрах стека находятся нули. Нулевой регистр, как отмечалось, постоянно содержит 0. Если на машине вычисляется n-местная функция, то число входных регистров машины равно n, и в начале вычисления в регистры $x_1, \ldots, x_n$ помещаются значения соответствующих переменных. В дальнейшем содержимое входных регистров не меняется. Работа машины начинается с команды, помеченной меткой L_1, и заканчивается после выполнения команды, помеченной меткой L_s. При этом результатом работы считается содержимое рабочего регистра после выполнения команды C_s.

В дальнейшем при сокращенной записи программ будем использовать простейшие конструкции языков программирования: неполные условные и составные операторы, операторы безусловного перехода. Для обозначения начала и конца оператора применяем круглые скобки. Считаем, что за пределами составных операторов все метки этих операторов недоступны.

Пусть $\mathcal{M}$ — машина SRM, имеющая n входных регистров. Результат работы машины над входными значениями $x_1, \ldots, x_n$ будем обозначать через $\mathcal{M}(x_1, \ldots, x_n)$. *Зоной вычисления* машины $\mathcal{M}$ на входе $x_1, \ldots, x_n$ (обозначение $\mathrm{SPACE}_{\mathcal{M}}(x_1, \ldots, x_n)$) считаем наибольшее из значений всех регистров, достигнутое в процессе вычисления значения $\mathcal{M}(x_1, \ldots, x_n)$. Пусть $f(x), g(x_1, \ldots, x_n)$ — всюду определенные функции. Говорим, что функция g *вычислима* на машине $\mathcal{M}$ в пределах зоны f, если

$$g(x_1, \ldots, x_n) = \mathcal{M}(x_1, \ldots, x_n)$$

и

$$\mathrm{SPACE}_{\mathcal{M}}(x_1, \ldots, x_n) \leqslant f(\max(x_1, \ldots, x_n)).$$

Множество всех всюду определенных функций, вычислимых на машинах SRM в пределах зоны f, обозначим через $\mathrm{SRM}(\mathrm{SPACE}, f)$.

§ 3.2. Вычисления на машинах SRM с ограничениями на зону

Теорема 3.1. *Если $f \in E^0$, то*

$$\mathcal{E}f = \bigcup_{i \geqslant 1} \mathrm{SRM}(\mathrm{SPACE}, f^{\langle i \rangle}).$$

Доказательство. Включение левой части равенства в правую часть докажем индукцией по построению функций в классе $\mathcal{E}f$, используя представление класса $\mathcal{E}f$ из утверждения 2.7. Функции 0 и $I_i^n(x_1, \ldots, x_n)$ вычисляются машинами SRM с программами $(r := 0)$ и $(r := x_i)$ в пределах зоны $f^{\langle 1 \rangle}$.

Предположим, что функции $h_0, h_1, \ldots, h_m$ вычислимы на машинах SRM с программами $\Delta_0, \Delta_1, \ldots, \Delta_m$ в пределах зоны $f^{\langle i \rangle}$ и

$$g(x_1, \ldots, x_n) = h_0(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n)).$$

Без ограничения общности можно считать, что программы $\Delta_0, \Delta_1, \ldots, \Delta_m$ используют различные регистры стека и начинаются с команды $r := 0$. Пусть d — наибольший из номеров регистров стека в программах $\Delta_0, \Delta_1, \ldots, \Delta_m$, а $t_j := r$ есть сокращение для блока

$$(L: \ \mathbf{if}\ t_j \neq r\ \mathbf{then}\ (t_j := t_j + 1;\ \mathbf{go\ to}\ L)).$$

Пусть далее программа Δ_0' получается из программы Δ_0 заменой входных регистров x_j регистрами t_{d+j}. Тогда функция $g(x_1, \ldots, x_n)$ вычисляется машиной SRM с программой

$$(\Delta_m; t_{d+m} := r; \ldots; \Delta_1; t_{d+1} := r; \Delta_0')$$

в пределах зоны $f^{\langle 2i \rangle}$.

Предположим, что функции h, j вычислимы на машинах SRM с программами Γ, Δ в пределах зоны $f^{\langle i \rangle}$ и функция $g(x_1, \ldots, x_n, x_{n+1})$ получается из функций h, j, $f^{\langle i \rangle}$ операцией ограниченной рекурсии (2.11). Будем считать, что программы Γ, Δ используют различные регистры стека. Пусть d — наибольший из номеров регистров стека программ Γ, Δ, а программа Δ' получается из программы Δ заменой x_{n+1} на t_{d+2} и x_{n+2} на t_{d+1}. Тогда функция $g(x_1, \ldots, x_n, x_{n+1})$ вычисляется машиной SRM с программой

$$(\Gamma; L: \ \mathbf{if}\ t_{d+2} \neq x_{n+1}\ \mathbf{then}$$
$$(t_{d+2} := t_{d+2} + 1; t_{d+1} := r; r := 0; \Delta';\ \mathbf{go\ to}\ L))$$

в пределах зоны $f^{\langle 2i \rangle}$.

Предположим, что функция h вычислима на машине SRM с программой Γ в пределах зоны $f^{\langle i \rangle}$ и функция $g(x_1, \ldots, x_n)$ получается из функции h операцией ограниченной минимизации (2.12). Пусть d — наибольший из номеров регистров стека программы Γ, а программа Γ' получается из программы Γ заменой x_{n+1} на t_{d+1}. Тогда функция $g(x_1, \ldots, x_n)$ вычисляется на машине SRM с программой

$$(L: \ \Gamma';\ \mathbf{if}\ r = 0\ \mathbf{then}\ (t_{d+1} := t_{d+1} + 1;\ \mathbf{go\ to}\ L); r := t_{d+1})$$

в пределах зоны $f^{\langle 2i \rangle}$.

Докажем теперь, что при любом $i \geqslant 1$ имеет место включение

$$\mathrm{SRM}(\mathrm{SPACE}, f^{\langle i \rangle}) \subseteq \mathcal{E}f.$$

С этой целью расширим понятие машины SRM, резрешив команды вида

$$r := g(x_1, \ldots, x_n, t_0, \ldots, t_k, r),$$

$$\textbf{if } g(x_1, \ldots, x_n, t_0, \ldots, t_k, r) = 0 \textbf{ then go to } L_j \textbf{ else go to } L_l,$$

где g — произвольная функция из класса $\mathcal{E}f$. Полученный класс машин обозначим через SRM_f. Для завершения доказательства теоремы достаточно установить, что

$$\mathrm{SRM}_f(\mathrm{SPACE}, f^{\langle i\rangle}) \subseteq \mathcal{E}f.$$

Напомним, что для любого j программа машины SRM_f содержит не более одного вхождения команды приращения $t_j := t_j + 1$. Очевидно, что после выполнения команды приращения по содержимому регистров стека можно однозначным образом установить, содержимое какого именно регистра было увеличено последним. Поэтому, полагая $\overline{x} = (x_1, \ldots, x_n)$, $\overline{t} = (t_0, \ldots, t_k)$, программу любой машины SRM_f с входными регистрами $x_1, \ldots, x_n$ и регистрами стека $t_0, \ldots, t_k$ можно записать в следующем виде:

$$\begin{aligned}
(L :\ & \textbf{if } g_0(\overline{x}, \overline{t}, r) = 0 \textbf{ then } (r := h_0(\overline{x}, \overline{t}, r);\ t_0 := t_0 + 1;\ \textbf{go to } L));\\
& (\textbf{if } g_1(\overline{x}, \overline{t}, r) = 0 \textbf{ then } (r := h_1(\overline{x}, \overline{t}, r);\ t_1 := t_1 + 1;\ \textbf{go to } L));\\
& \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
& (\textbf{if } g_k(\overline{x}, \overline{t}, r) = 0 \textbf{ then } (r := h_k(\overline{x}, \overline{t}, r);\ t_k := t_k + 1;\ \textbf{go to } L));\\
& (r := h_{k+1}(\overline{x}, \overline{t}, r)),
\end{aligned} \tag{3.1}$$

где $g_0, \ldots, g_k$ — функции из класса $\mathcal{E}^0$, осуществляющие «сравнения» значений $\overline{x}$, $\overline{t}$, r, а $h_0, \ldots, h_{k+1}$ — функции из класса $\mathcal{E}f$.

Дальнейшее доказательство проводим индуцией по k. Положим $\overline{t}_1 = (t_1, \ldots, t_k)$. Пусть машина SRM_f с программой (3.1) работает в пределах зоны $f^{\langle i\rangle}$. Если содержимое регистра t_0 было равно 0 при некотором прохождении метки L, то при первом после этого выходе из первой строки программы (3.1) новые значения t_0 и r, которые мы обозначим через $\tau_0(\overline{x}, \overline{t}_1, r)$ и $\rho(\overline{x}, \overline{t}_1, r)$, будут определяться равенствами

$$\varphi(\overline{x}, \overline{t}_1, 0, r) = \min\,(f^{\langle i\rangle}(\max\,(\overline{x})), r),$$

$$\varphi(\overline{x}, \overline{t}_1, t_0 + 1, r) = \min\,(f^{\langle i\rangle}(\max\,(\overline{x})), h_0(\overline{x}, \overline{t}, \varphi(\overline{x}, \overline{t}, r))),$$

$$\tau_0(\overline{x}, \overline{t}_1, r) = (\mu t_0)_{t_0 \leqslant f^{\langle i\rangle}(\max\,(\overline{x}))}(g_0(\overline{x}, \overline{t}, \varphi(\overline{x}, \overline{t}_1, t_0, r)) \neq 0),$$

$$\rho(\overline{x}, \overline{t}_1, r) = \varphi(\overline{x}, \overline{t}_1, \tau_0(\overline{x}, \overline{t}_1, r), r).$$

Здесь функция $\varphi(\overline{x}, \overline{t}_1, t_0, r)$, определяемая ограниченной рекурсией в классе $\mathcal{E}f$ (функция min в ее определении «не позволяет» выйти за пределы класса $\mathcal{E}f$), задает содержимое регистра r в момент достижения значения t_0 нулевым регистром стека.

Из определений следует, что функции τ_0, ρ принадлежат классу $\mathcal{E}f$.

После выхода из первой строки программы (3.1) при следующем прохождении метки L содержимое регистра t_0 вновь станет равным 0. Поэтому если в программе (3.1) подставить во все функции g_j, h_j $(j \geqslant 1)$ вместо t_0 и r функции $\tau_0(\overline{x}, \overline{t}_1, r)$, $\rho(\overline{x}, \overline{t}_1, r)$ соответственно и убрать первую строку программы, то получим программу эквивалентной машины SRM_f, имеющей на один регистр стека меньше. Остается заметить, что при $k = 0$ машина вычисляет функцию $h_1(\overline{x}, \tau_0(\overline{x}, 0), \rho(\overline{x}, 0))$, входящую в класс $\mathcal{E}f$. Теорема доказана.

Следствие. *При $j = 1, 2, 3$ класс Гжегорчика $\mathcal{E}^j$ совпадает с классом*
$$\bigcup_{i \geqslant 1} \mathrm{SRM}(\mathrm{SPACE}, f_j^{\langle i \rangle}), \tag{3.2}$$
где $f_1(x) = 2(x+1)$, $f_2(x) = (x+1)^2$, $f_3(x) = 2^x$.

Что касается класса $\mathcal{E}^0$, то в силу утверждений 2.5 и 2.9 класс $\mathcal{E}^0$ будет совпадать с множеством всех функций $g(x_1, \ldots, x_n)$ из (3.2), где $j = 0$, $f_0(x) = x + 1$ и функция g ограничена сверху некоторой функцией из класса $\mathcal{E}^0$.

Теорему 3.1 можно использовать для получения некоторой информации об «алгебраическом» строении классов вида $\mathcal{E}f$. Один из важных вопросов в этом направлении — нахождение условий, при которых класс $\mathcal{E}f$ порождается с помощью операции суперпозиции конечной системой функций (подробнее об этом будет сказано в § 3.4). Пока мы установим связь между существованием конечной порождающей системы в множестве $(\mathcal{E}f)^{(1)}$ всех одноместных функций из $\mathcal{E}f$ и объемом класса $(\mathcal{E}f)_*$.

Теорема 3.2. *Пусть $f, g \in E^0$, множество $(\mathcal{E}f)^{(1)}$ порождается суперпозициями функций $\varphi_0, \ldots, \varphi_k$ из $(\mathcal{E}f)^{(1)}$ и $f <_{\mathcal{E}} g$. Тогда $(\mathcal{E}f)_* \subset \subset (\mathcal{E}g)_*$.*

Доказательство. Без ограничения общности можно считать, что
$$(\forall i)(f^{\langle i \rangle} <_{\mathrm{ae}} g).$$
Определим в классе SRM машину $\mathcal{M}$, которая будет вычислять характеристическую функцию предиката, не входящего в класс $(\mathcal{E}f)_*$. Для любого x из $\mathbb{N}$ машина $\mathcal{M}$ вычисляет значения $g(x)$, $l(x) = x \dot{-} [\sqrt{x}]^2$ и помещает их в два регистра стека с наибольшими номерами. Затем $\mathcal{M}$ последовательно находит разряды $(k+2)$-ичного представления $a_m \ldots a_0$ числа $l(x)$ (т. е. $l(x) = \sum\limits_{i \leqslant m} a_i (k+2)^i$ и $a_m \neq 0$) и вычисляет значение
$$1 \dot{-} \varphi_{b_m}(\ldots \varphi_{b_0}(x) \ldots),$$
где $b_0 = a_0 \dot{-} 1, \ldots, b_m = a_m \dot{-} 1$, следя при этом за тем, чтобы промежуточные результаты не превосходили значения $g(x)$. Нетрудно видеть, что в итоге образуется функция, не принадлежащая классу $\mathcal{E}f$.

В самом деле, пусть функция $\varphi(x)$ принадлежит классу $\mathcal{E}f$ и принимает лишь значения 0 и 1. Согласно условию теоремы найдутся такие значения $b_0, \ldots, b_m$, не превосходящие k, что

$$\varphi(x) = \varphi_{b_m}(\ldots \varphi_{b_0}(x) \ldots).$$

Поскольку функции $\varphi_0, \ldots, \varphi_k$ принадлежат классу $\mathcal{E}f$, найдутся такие число i и машины $\mathcal{M}_0, \ldots, \mathcal{M}_k$, что функции $\varphi_0, \ldots, \varphi_k$ вычислимы на машинах $\mathcal{M}_0, \ldots, \mathcal{M}_k$ в пределах зоны $f^{\langle i \rangle}$. Следовательно, суперпозицию $\varphi_{b_m}(\ldots \varphi_{b_0}(x) \ldots)$ можно вычислить последовательным применением машин $\mathcal{M}_{b_0}, \ldots, \mathcal{M}_{b_m}$ в пределах зоны $f^{\langle i(m+1) \rangle}$. По условию теоремы

$$f^{\langle i(m+1) \rangle} <_{\mathrm{ae}} g.$$

Значит, существует такое число x_0, что

$$(\forall x)_{x \geqslant x_0}(f^{\langle i(m+1) \rangle}(x) < g(x)).$$

Пусть y_0 — число, $(k+2)$-ичное представление которого имеет вид $(b_m+1)\ldots(b_0+1)$. Если $x = c(y_0, x_0) = (y_0+x_0)^2 + y_0$, то описанный выше процесс применения машины $\mathcal{M}$ к аргументу x даст значение

$$1 \dot{-} \varphi_{b_m}(\ldots \varphi_{b_0}(x) \ldots) = 1 \dot{-} \varphi(x),$$

отличное от $\varphi(x)$. Тем самым установлено, что машина $\mathcal{M}$ вычисляет функцию, не входящую в класс $\mathcal{E}f$. Теорема доказана.

§ 3.3. Универсальные функции

Пусть Q — некоторое множество всюду определенных функций, $Q^{(n)}$ — подмножество множества Q, состоящее из всех функций от n переменных. Будем говорить, что всюду определенная функция $U(z, x_1, \ldots, x_n)$ является *универсальной функцией* для множества функций $Q^{(n)}$, если выполняются следующие условия:

1) для всякого числа a из $\mathbb{N}$ функция $U(a, x_1, \ldots, x_n)$ принадлежит множеству $Q^{(n)}$;

2) для всякой функции $q(x_1, \ldots, x_n)$ из множества $Q^{(n)}$ найдется такое число a, что n-местная функция $U(a, x_1, \ldots, x_n)$ совпадает с функцией $q(x_1, \ldots, x_n)$.

Нетрудно видеть, что множество функций Q, включающее в себя хотя бы одну из функций $x+1$, $\overline{\mathrm{sg}}\, x$ и замкнутое относительно операции суперпозиции (включая отождествление переменных), ни при каком n не может содержать функцию $U(z, x_1, \ldots, x_n)$, универсальную для множества функций $Q^{(n)}$. Действительно, для получения противоречия достаточно образовать функции

$$U(x_1, x_1, \ldots, x_n) + 1, \quad \overline{\mathrm{sg}}\, U(x_1, x_1, \ldots, x_n).$$

В следующей теореме приведены достаточно широкие условия, при которых класс $\mathcal{E}g$ содержит универсальные функции для множеств $(\mathcal{E}f)^{(n)}$. Напомним, что посредством $f_2(x)$ мы обозначили функцию $(x+1)^2$.

Теорема 3.3. *Пусть* $f, g \in E^0$, $f_2 \leqslant {}_{\mathcal{E}}f$ *и* $f < {}_{\mathcal{E}}g$. *Тогда при любом* $n \geqslant 1$ *класс* $\mathcal{E}g$ *содержит функцию, универсальную для множества функций* $(\mathcal{E}f)^{(n)}$.

Доказательство. Заметим, во-первых, что теорему достаточно доказать лишь для случая $n = 1$. В самом деле, из условия $f_2 \leqslant {}_{\mathcal{E}}f$ и утверждений 2.10, 2.12 следует, что $\mathcal{E}^2 \subseteq \mathcal{E}f$. Классу $\mathcal{E}^2$ принадлежит тройка нумерационных функций c, l, r. Если при $n \geqslant 2$ функция $h(x_1, \ldots, x_n)$ входит в класс $\mathcal{E}f$, то в него входит также функция

$$\widehat{h}(x) = h(l_{n-1}(x), r(l_{n-2}(x)), \ldots, r(l_1(x)), r(x)). \tag{3.3}$$

Обратно, функция h получается из функции $\widehat{h}$ с помощью подстановки нумерационной функции c^n:

$$h(x_1, \ldots, x_n) = \widehat{h}(c^n(x_1, \ldots, x_n)). \tag{3.4}$$

Поэтому если функция $U_1(z, x)$ является универсальной функцией для множества функций $(\mathcal{E}f)^{(1)}$, то при $n \geqslant 2$ на основании соотношений (3.3), (3.4) универсальной функцией для множества $(\mathcal{E}f)^{(n)}$ служит функция

$$U_n(z, x_1, \ldots, x_n) = U_1(z, c^n(x_1, \ldots, x_n)).$$

Наметим теперь общий план дальнейшего доказательства теоремы. Сначала мы построим некоторую нумерацию всех машин SRM с одним входным регистром. Затем с помощью нумерационной функции c определим кодирование конфигураций машин SRM. Далее в классе $\mathcal{E}^0$ найдем такую функцию $\mathrm{Init}\,(x, y)$, что

$$\mathrm{Init}\,(x,y) = \begin{cases} \text{коду начальной конфигурации любой машины с одним} \\ \qquad \text{входным регистром, содержащим } x, \text{ если этот код} \\ \qquad \text{не превосходит } y; \\ 0 \text{ в противном случае.} \end{cases}$$

После этого в классе $\mathcal{E}^0$ построим ключевую функцию $\mathrm{Next}\,(z, x, y)$, которая обладает следующими свойствами. Если z есть номер машины $\mathcal{M}$ с одним входным регистром, а x — код незаключительной конфигурации машины $\mathcal{M}$, то $\mathrm{Next}\,(z, x, y)$ равно коду непосредственно следующей конфигурации машины $\mathcal{M}$, если только этот код не превосходит y. В противном случае значением $\mathrm{Next}\,(z, x, y)$ служит 0. Отметим также, что $\mathrm{Next}\,(z, x, y)$ сохраняет код заключительной конфигурации.

С помощью функции Next ограниченной рекурсией в классе $\mathcal{E}^0$ определим функцию $\mathrm{N}\,(z, x, y, t)$, которая аналогична функции Next, однако дает код конфигурации машины $\mathcal{M}$ после t тактов работы.

Наконец, в классе $\mathcal{E}^0$ будет определена функция $\mathrm{Yield}\,(x)$, дающая по коду x конфигурации машины SRM содержимое ее рабочего регистра.

Покажем, как с использованием функций Init, N, Yield и g построить в классе $\mathcal{E}g$ функцию, универсальную для множества функций $(\mathcal{E}f)^{(1)}$.

Можно считать, что

$$(\forall j)(f^{\langle j\rangle} <_{\mathrm{ae}} g). \tag{3.5}$$

Положим

$$U(z,x) = \mathrm{Yield}\,(\mathrm{N}\,(z, \mathrm{Init}\,(x, \max\,(z, g(x))), \max\,(z, g(x)), \max\,(z, g(x)))).$$

Докажем, что $U(z,x)$ является функцией, универсальной для множества функций $(\mathcal{E}f)^{(1)}$.

Пусть функция $h(x)$ из класса $\mathcal{E}f$ вычислима на машине $\mathcal{M}$ с номером z_h в пределах зоны $f^{\langle i\rangle}$. Как будет видно из построения нумерации машин SRM с одним входным регистром, число регистров стека и число команд в программе машины $\mathcal{M}$ меньше числа z_h. Поэтому значение $h(x)$ в пределах зоны $f^{\langle i\rangle}(x)$ машина $\mathcal{M}$ вычислит за время, не превосходящее величины

$$(f^{\langle i\rangle}(x))^{z_h} \cdot z_h. \tag{3.6}$$

Коды конфигураций машины $\mathcal{M}$, работающей со входом x, не будут превосходить величины

$$c^{k+5}(f^{\langle i\rangle}(x), \ldots, f^{\langle i\rangle}(x), s), \tag{3.7}$$

где $k+1$ — число регистров стека машины $\mathcal{M}$, а s — число команд в ее программе. Так как $f_2 \leqslant_{\mathcal{E}} f$, найдется такое число j (зависящее от машины $\mathcal{M}$), что каждая из величин (3.6), (3.7) ограничена сверху функцией $f^{\langle j\rangle}(x)$. Применяя (3.5), видим, что существует такое x_0, что

$$(\forall x)_{x\geqslant x_0}(f^{\langle j\rangle}(x) < g(x)).$$

Следовательно, при $x \geqslant x_0$ в качестве верхней границы для времени вычисления $h(x)$ на машине $\mathcal{M}$ и для кодов конфигураций, возникающих при этом, можно взять значение $g(x)$. В частности, при $x \geqslant x_0$ функция $\mathrm{Init}\,(x, \max\,(z_h, g(x)))$ будет давать код начальной конфигурации машины $\mathcal{M}$, содержащей во входном регистре x, а функция

$$\mathrm{N}\,(z_h, \mathrm{Init}\,(x, \max\,(z_h, g(x)), \max\,(z_h, g(x)), \max\,(z_h, g(x))))$$

— номер соответствующей заключительной конфигурации машины $\mathcal{M}$. В итоге при $x \geqslant x_0$ получим

$$\begin{aligned} h(x) = \mathrm{Yield}\,(\mathrm{N}(z_h,&\\ &\mathrm{Init}\,(x, \max(z_h, g(x)), \max\,(z_h, g(x)), \max\,(z_h, g(x)))))). \end{aligned} \tag{3.8}$$

Остается позаботиться о значениях функции $U(z_h, x)$ при $x < x_0$. Здесь мы применим известный технический прием. Понятно, что функцию h можно вычислить на бесконечном числе машин SRM, имеющих даже такое же число регистров стека, что и машина $\mathcal{M}$. Для этого достаточно дописать к программе машины $\mathcal{M}$ «фиктивные» команды (например вида $r := r$), к которым машина не будет обращаться в процессе вычисления. Очевидно, что время вычисления при этом не изменится. Можно также считать, что добавление «фиктивных» команд не влияет на оценку кодов конфигураций. В таком случае вместо номера z_h машины $\mathcal{M}$ следует взять достаточно большой номер z'_h машины $\mathcal{M}'$, эквивалентной машине $\mathcal{M}$, с таким расчетом, чтобы значение z'_h служило бы при $x < x_0$ верхней оценкой времени вычисления значений $h(x)$ и кодов конфигураций, возникающих при этом.

Приступая к деталям доказательства теоремы, начнем с нумерации машин SRM, имеющих один входной регистр. Итак, пусть $\mathcal{M}$ — машина SRM с одним входным регистром x, регистрами стека $t_0, t_1, \ldots, t_k$, рабочим регистром r, нулевым регистром 0 и программой

$$(L_1 : C_1; \quad L_2 : C_2; \quad \ldots; \quad L_s : C_s),$$

где $L_1, \ldots, L_s$ — метки программы, а $C_1, \ldots, C_s$ — команды. Сопоставим регистрам $0, r, x, t_0, \ldots, t_k$ натуральные числа $1, 3, 7, \ldots, 2^{k+4} - 1$, имеющие соответственно диадические представления $1, 11, 111, \ldots, 1^{k+4}$.

Пусть C_j есть команда засылки $r := z$, где $z \in \{0, r, x, t_0, \ldots, t_k\}$, и регистру z сопоставлено натуральное число $2^m - 1$ (с диадическим представлением 1^m). Тогда команде C_j сопоставляем натуральное число, имеющее диадическое представление $1^j 2112 1^m$. Пусть команда C_j имеет вид $t_i := t_i + 1$. Сопоставляем ей натуральное число с диадическим представлением $1^j 2 1^{i+4}$. Если же C_j есть команда перехода

$$\textbf{if } z_1 = z_2 \textbf{ then go to } L_i \textbf{ else go to } L_l$$

и регистрам z_1, z_2 сопоставлены натуральные числа $2^p - 1, 2^q - 1$, то команде C_j сопоставляем натуральное число, имеющее диадическое представление $1^j 2 1^p 2 1^q 2 1^i 2 1^l$. Наконец, номером машины $\mathcal{M}$ объявляем натуральное число с диадическим представлением $d_1 22 d_2 22 \ldots 22 d_s$, где $d_1, \ldots, d_s$ суть диадические представления номеров команд $C_1, \ldots, C_s$.

Нетрудно понять, что по виду диадического представления номера команды можно однозначным образом определить тип команды (засылка, приращение или переход) — достаточно найти число разделительных символов 2. Более того, с помощью рудиментарных предикатов можно определить также, является ли данное число номером некоторой машины SRM с одним входным регистром. Поскольку структура диадических представлений номеров машин SRM весьма простая, мы не будем выписывать соответствующие формулы, которые задают перечисленные рудиментарные предикаты.

Применяя теперь технику рудиментарных предикатов и пользуясь утверждением 2.8, определяем в классе $\mathcal{E}^0$ такие функции $T(x)$, $R(x,y)$, $C(x,y)$, что:

$$T(x)=\begin{cases} i, & \text{если } x \text{ есть номер команды типа } i\ (i=1,2,3);\\ 0, & \text{если } x \text{ не является номером команды;}\end{cases}$$

$$R(x,y)=\begin{cases} 2^m-1, & \text{если диадическое представление числа } x \text{ имеет}\\ & \text{вид } 1^j21121^m \text{ или } 1^j21^m,\ \text{где } j,m\geqslant 1;\\ 2^{m_y}-1, & \text{если диадическое представление числа } x \text{ имеет}\\ & \text{вид } 1^j21^{m_0}21^{m_1}21^{m_2}21^{m_3},\ y\leqslant 3;\\ & j,m_0,m_1,m_2,m_3\geqslant 1;\\ 0 & \text{в остальных случаях;}\end{cases}$$

$$C(x,y)=\begin{cases} \text{номеру команды с меткой } L_y,\ \text{если } x \text{ есть номер}\\ \qquad \text{некоторой машины SRM и диадическое представление}\\ \qquad \text{числа } x \text{ содержит команду с меткой } L_y;\\ 0 \text{ в остальных случаях.}\end{cases}$$

Конфигурацией машины $\mathcal{M}$ в момент времени t назовем упорядоченный набор $(t_k',\ldots,t_0',x',r',0,j)$, где $t_k',\ldots,t_0',x',r'$ — содержимое соответствующих регистров машины $\mathcal{M}$ в момент времени t, а j — номер метки выполняемой в момент t команды программы машины $\mathcal{M}$.

Кодом конфигурации $(t_k',\ldots,t_0',x',r',0,j)$ считаем число

$$c^{k+5}(t_k',\ldots,t_0',x',r',0,j).$$

Как вытекает из определения, код начальной конфигурации любой машины $\mathcal{M}$ с одним входным регистром равен

$$c^{k+5}(0,\ldots,0,x,0,0,1)= \\ =(x^2(x^2+1)(x^4+x^2+1)+1)^2+x^2(x^2+1)(x^4+x^2+1).$$

Поэтому функцию $\mathrm{Init}\,(x,y)$ можно определить соотношениями

$$\mathrm{Init}\,(x,y)= \\ =\begin{cases} (x^2(x^2+1)(x^4+x^2+1)+1)^2+x^2(x^2+1)(x^4+x^2+1),\ \text{если}\\ \qquad (x^2(x^2+1)(x^4+x^2+1)+1)^2+x^2(x^2+1)(x^4+x^2+1)\leqslant y;\\ 0 \text{ в противном случае.}\end{cases}$$

Поскольку предикат

$$\rho(x,y,z)\equiv(z=(x^2(x^2+1)(x^4+x^2+1)+1)^2+x^2(x^2+1)(x^4+x^2+1))$$

принадлежит классу **BA**, а функция $\mathrm{Init}\,(x,y)$ получается из этого предиката с помощью операции ограниченной минимизации $(\mu z)_{z\leqslant y}$, функция Init принадлежит классу $\mathcal{E}'$.

Исходя из определения кода конфигурации, нетрудно также определить в классе $\mathcal{E}^0$ функцию Yield:

$$\mathrm{Yield}\,(x) = r(l_2(x)).$$

Заметим, что в класс $\mathcal{E}^0$ входит функция двух переменных $l_y(x)$:

$$\begin{cases} l_0(x) = x, \\ l_{y+1}(x) = l(l_y(x)), \\ l_y(x) \leqslant x. \end{cases}$$

Перейдем к определению функции $\mathrm{Next}\,(z, x, y)$ в классе $\mathcal{E}^0$. Пусть z есть номер некоторой машины, а x — код ее конфигурации. Находим $r(x)$ — номер метки команды, содержащейся в конфигурации с кодом x. Величина $C(z, r(x))$ есть номер команды $C_{r(x)}$, содержащейся в программе с номером z. Вычисляем значение $i = T(C(z, r(x)))$. Возможны следующие случаи.

• $i = 1$. Тогда команда $C_{r(x)}$ есть команда засылки. Именно, в рабочий регистр необходимо заслать содержимое регистра с номером $2^m - 1$, где $2^m - 1 = R(C(z, r(x)), 0)$. Это содержимое равно $r(l_m(x))$ (рудиментарность предиката $v = 2^u$ доказана в конце § 1.2). Следовательно, величину $\mathrm{Next}\,(z, x, y)$ в этом случае следует определить так:

$$\mathrm{Next}(z, x, y) = \begin{cases} x, \ \text{если команда } C_{r(x)} \text{ является последней} \\ \qquad \text{командой в программе с номером } z \\ \qquad \text{и } x \leqslant y; \\ c^4(l_3(x), r(l_m(x)), 0, r(x)+1), \ \text{если} \\ \qquad c^4(l_3(x), r(l_m(x)), 0, r(x)+1) \leqslant y \text{ и команда } C_{r(x)} \\ \qquad \text{не является последней в программе} \\ \qquad \text{с номером } z; \\ 0 \text{ в остальных случаях.} \end{cases}$$

• $i = 2$. Тогда команда $C_{r(x)}$ есть команда приращения регистра стека, имеющего номер $2^m - 1 = R(C(z, r(x)), 0)$. Содержимое этого регистра равно $r(l_m(x))$. Величину $\mathrm{Next}\,(z, x, y)$ в этом случае определим согласно соотношениям:

$$\mathrm{Next}\,(z, x, y) =$$
$$= \begin{cases} c^{m+2}(l_{m+1}(x), r(l_m(x)) + 1, r(l_{m-1}(x)), \ldots, r(l_1(x)), r(x)+1), \\ \qquad \text{если } c^{m+2}(l_{m+1}(x), r(l_m(x)) + 1, r(l_{m-1}(x)), \ldots, r(l_1(x)), \\ \qquad r(x)+1) \leqslant y; \\ 0 \text{ в противном случае.} \end{cases}$$

В последней формуле встречается «неограниченная» функция c^{m+2}. В классе $\mathcal{E}^0$ ее можно определить, построив сначала в $\mathcal{E}^0$ с помощью ограниченной рекурсии функцию h:

$$\begin{cases} h(x,y,z,0) = \begin{cases} c(l_{m+1}(x), r(l_m(x))+1), \\ \qquad \text{если } c(l_{m+1}(x), r(l_m(x))+1) \leqslant y, \\ 0 \text{ в противном случае;} \end{cases} \\ h(x,y,z,v+1) = \begin{cases} c(h(x,y,z,v), r(l_{m \dot{-} (v+1)}(x))), \text{ если} \\ \qquad c(h(x,y,z,v), r(l_{m \dot{-} (v+1)}(x))) \leqslant y; \\ 0 \text{ в противном случае;} \end{cases} \\ h(x,y,z,v) \leqslant y. \end{cases}$$

Далее получаем

$$\mathrm{Next}\,(z,x,y) = \begin{cases} x, \text{ если } C_{r(x)} \text{ есть последняя команда} \\ \quad \text{в программе с номером } z \text{ и } x \leqslant y; \\ c(h(x,y,z,m \dot{-} 1), r(x)+1), \text{ если} \\ \quad c(h(x,y,z,m \dot{-} 1), r(x)+1) \leqslant y \\ \quad \text{и } C_{r(x)} \text{ не является последней командой} \\ \quad \text{в программе с номером } z; \\ 0 \text{ в остальных случаях.} \end{cases}$$

• $i = 3$. Тогда команда $C_{r(x)}$ есть команда перехода. Вычисляем величины

$$2^{m_j} - 1 = R(C(z, r(x)), j), \quad j = 0, 1, 2, 3.$$

Находим содержимое регистров с номерами m_0 и m_1:

$$a_0 = r(l_{m_0}(x)), \quad a_1 = r(l_{m_1}(x)).$$

Далее полагаем

$$\mathrm{Next}\,(z,x,y) = \begin{cases} c(l(x), 2^{m_2}-1), \text{ если } a_0 = a_1 \text{ и } c(l(x), 2^{m_2}-1) \leqslant y; \\ c(l(x), 2^{m_3}-1), \text{ если } a_0 \neq a_1 \text{ и } c(l(x), 2^{m_3}-1) \leqslant y; \\ 0 \text{ в остальных случаях.} \end{cases}$$

Имея функцию Next, определим, наконец, в классе $\mathcal{E}^0$ ограниченной рекурсией функцию $\mathrm{N}\,(z,x,y,t)$:

$$\begin{cases} \mathrm{N}\,(z,x,y,0) = \mathrm{Next}\,(z,x,y), \\ \mathrm{N}\,(z,x,y,t+1) = \begin{cases} \mathrm{Next}\,(z, \mathrm{N}\,(z,x,y,t), y), \text{ если} \\ \qquad \mathrm{Next}\,(z, \mathrm{N}\,(z,x,y,t), y) \leqslant y; \\ 0 \text{ в противном случае;} \end{cases} \\ \mathrm{N}\,(z,x,y,t) \leqslant y. \end{cases}$$

Теорема доказана.

Следствие 1. *В условиях теоремы* $(\mathcal{E}f)_* \subset (\mathcal{E}g)_*$.

Следствие 2. *При любом* $n \geqslant 1$ *класс* $\mathcal{E}^3$ *содержит функцию, универсальную для множества функций* $(\mathcal{E}^2)^{(n)}$.

§ 3.4. Конечные базисы по суперпозиции

Пусть Q — некоторый класс функций, замкнутый относительно операции суперпозиции, и $Q_0 \subseteq Q$. Будем говорить, что система Q_0 *порождает* класс Q (относительно операции суперпозиции), если замыкание системы Q_0 относительно операции суперпозиции совпадает с классом Q. Конечные порождающие системы класса Q принято называть (конечными) *базисами по суперпозиции* в классе Q.

Следует отметить два обстоятельства, связанные с конечными базисами по суперпозиции. Во-первых, конечный базис по суперпозиции может и не быть независимой системой. Иными словами, некоторые функции базиса могут выражаться через другие функции базиса с помощью операции суперпозиции. Во-вторых, если класс Q не состоит только из одноместных функций, то, говоря о конечном базисе по суперпозиции в классе Q, мы допускаем в качестве суперпозиций так называемые «нерегулярные» суперпозиции (см. об этом в начале § 1.4). В противном случае, как нетрудно понять, из конечного набора функций с помощью операции суперпозиции можно получить лишь функции от ограниченного числа переменных.

Теорема 3.4. *Пусть $f \in E^0$ и $f_2 \leqslant_{\mathcal{E}} f$. Тогда класс $\mathcal{E}f$ имеет конечный базис по суперпозиции.*

Доказательство. Установим, что конечный базис по суперпозиции в классе $\mathcal{E}f$ образует система функций

$$0, \quad x+1, \quad c(x,y), \quad f(x), \quad \mathrm{Init}\,(x,y), \quad \mathrm{N}\,(x,y,z,w), \quad \mathrm{Yield}\,(x), \tag{3.9}$$

где функции Init, N, Yield из класса $\mathcal{E}^0$ определены в доказательстве теоремы 3.3.

Во-первых, из условия $f_2 \leqslant_{\mathcal{E}} f$ следует, что $\mathcal{E}^2 \subseteq \mathcal{E}f$. Поэтому все функции системы (3.9) входят в класс $\mathcal{E}f$. Далее, пусть $h(x)$ — произвольная функция класса $\mathcal{E}f$, а $\mathcal{M}$ — машина типа SRM, которая вычисляет функцию $h(x)$ в пределах зоны $f^{\langle i\rangle}(x)$. Если z_h — номер машины $\mathcal{M}$, то, как установлено в доказательстве теоремы 3.3, функция h выражается формулой (3.8). При этом вместо функции $\max\,(z_h, g(x))$ можно выбрать любую функцию из класса $\mathcal{E}f$, которая превосходит коды всех конфигураций машины $\mathcal{M}$, возникающие в процессе вычисления значений $h(x)$, а также время вычисления значения $h(x)$. Из доказательства теоремы 3.3 видно, что такой функцией может служить подходящая суперпозиция функций $f(x)$ и $f_2(x) = (x+1)^2$. Поскольку $f_2 \leqslant_{\mathcal{E}} f$, функцию f_2 в этой суперпозиции можно заменить функцией f. Таким образом, функцию h можно представить формулой вида

$$h(x) = \mathrm{Yield}\,(\mathrm{N}\,(z_h, \mathrm{Init}\,(x, f^{\langle k\rangle}(x)), f^{\langle k\rangle}(x), f^{\langle k\rangle}(x))).$$

Остается заметить, что любую натуральную константу можно получить суперпозицией функций 0 и $x+1$. Для получения функций от произвольного числа переменных из класса $\mathcal{E}f$ необходимо воспользоваться функцией $c(x,y)$ и применить утверждение 2.1. Теорема доказана.

Используя примерно те же идеи, что и при доказательстве теорем 3.3 и 3.4, можно установить, что в условиях теоремы 3.4 множество всех одноместных функций из $\mathcal{E}f$ также имеет конечный базис по суперпозиции. Мы получим этот результат в виде следствия из теоремы 3.4 и одного общего факта о конечных базисах, содержащегося в теореме 3.5 (для упрощения записи в доказательстве теоремы 3.5 операцию суперпозиции для одноместных функций будем изображать знаком $\circ$).

Теорема 3.5. *Пусть Q — произвольный класс функций, который содержит нумерационные функции c, l, r и замкнут относительно операции суперпозиции, $Q^{(1)}$ — множество всех одноместных функций из Q. Тогда класс Q имеет конечный базис по суперпозиции в том и только в том случае, когда конечный базис по суперпозиции имеет множество $Q^{(1)}$.*

Доказательство. В одну сторону утверждение теоремы почти очевидно: если $Q^{(1)}$ имеет конечный базис B_1 по суперпозиции, то в силу утверждения 2.1 система $B_1 \cup \{c\}$ будет представлять собой конечный базис по суперпозиции в классе Q.

Обратно, пусть B — конечный базис по суперпозиции в классе Q. Обозначим через B_1 конечное множество функций из $Q^{(1)}$, которое для любой функции $f(x_1,\ldots,x_n)$ из B содержит функцию

$$f^*(x) = c(f(r\circ l^{\langle n\rangle}(x), r\circ l^{\langle n-1\rangle}(x), \ldots r\circ l(x)), x), \tag{3.10}$$

а также функции

$$l(x), \quad c(x,x), \quad c(x,r(x)), \quad c(l^{\langle 2\rangle}(x), r(x)), \quad c(r\circ l(x), r(x)),$$
$$c^3(l^{\langle 2\rangle}(x), l\circ r\circ l(x), r(x)), \quad c^3(l^{\langle 2\rangle}(x), r^{\langle 2\rangle}\circ l(x), r(x)).$$

Докажем, что замыкание $[B_1]$ множества B_1 относительно операции суперпозиции совпадает с множеством $Q^{(1)}$.

Пусть $f_1(x),\ldots,f_n(x)$ — произвольные функции, полученные суперпозициями функций l, r. Установим сначала, что множеству $[B_1]$ принадлежит функция

$$c^{n+1}(f_1(x),\ldots,f_n(x),x).$$

В самом деле, если применять к функции $c(x,x)$ функции

$$c(l^{\langle 2\rangle}(x), r(x)), \quad c(r\circ l(x), r(x))$$

в той последовательности, в которой функция $f_1(x)$ порождается функциями l, r, то получим функцию

$$g_1(x) = c(f_1(x), x).$$

Применение функции $c(x, r(x))$ к функции $g_1(x)$ дает функцию

$$g_1'(x) = c^3(f_1(x), x, x).$$

Далее образуем функцию

$$g_2(x) = c^3(f_1(x), f_2(x), x),$$

действуя на функцию $g_1'(x)$ функциями

$$c^3(l^{\langle 2\rangle}(x), l \circ r \circ l(x), r(x)), \quad c^3(l^{\langle 2\rangle}(x), r^{\langle 2\rangle} \circ l(x), r(x))$$

в той последовательности, в которой функция $f_2(x)$ получается из функций l, r. Вновь применяем к функции $g_2(x)$ функцию $c(x, r(x))$, получаем функцию

$$g_2'(x) = c^4(f_1(x), f_2(x), x, x),$$

и т. д.

Из доказанного утверждения вытекает следующий факт.

Пусть $f_1(x), \ldots, f_n(x)$ — *произвольные функции, полученные суперпозициями функций* l, r, $h(x_1, \ldots, x_n) \in Q$, *и множеству* $[B_1]$ *принадлежит функция*

$$h^*(x) = c(h(r \circ l^{\langle n\rangle}(x), \ldots, r \circ l(x)), x).$$

Тогда множеству $[B_1]$ *будет принадлежать функция*

$$h_1(x) = c(h(f_1(x), \ldots, f_n(x)), x).$$

Действительно, если применить к функции $h^*(x)$ сначала функцию $c(x, r(x))$, а затем функцию

$$c^3(l^{\langle 2\rangle}(x), r^{\langle 2\rangle} \circ l(x), r(x)),$$

то получим функцию

$$h_1'(x) = c^3(h(r \circ l^{\langle n\rangle}(x), \ldots, r \circ l(x)), r(x), x).$$

По доказанному функция

$$g(x) = c^{n+2}(l(x), f_1(x), \ldots, f_n(x), x)$$

принадлежит множеству $[B_1]$. Положив $h_1''(x) = h_1' \circ g(x)$, будем иметь

$$h_1''(x) = c^3(h(f_1(x), \ldots, f_n(x)), x, g(x)).$$

Остается теперь заметить, что

$$h_1(x) = l \circ h_1''(x).$$

Мы хотим далее индукцией по построению функций в классе Q доказать следующее утверждение: если функция $f(x_1, \ldots, x_n)$ принадлежит классу Q, то множеству $[B_1]$ принадлежит функция $f^*(x)$, определяемая равенством (3.10). Базис индукции справедлив по определению множества B_1.

Прежде чем провести индуктивный переход, разложим общую «нерегулярную» операцию суперпозиции на четыре более простые операции. Именно, заметим, что любая суперпозиция функций может быть представлена в виде последовательного применения следующих четырех операций (см. [12, 13]).

1. Операция циклической перестановки переменных, которая при $n \geqslant 2$ по функции $f(x_1, \ldots, x_n)$ дает функцию

$$g(x_1, \ldots, x_n) = f(x_2, \ldots, x_n, x_1).$$

2. Операция транспозиции первых двух переменных, которая при $n \geqslant 2$ по функции $f(x_1, \ldots, x_n)$ дает функцию

$$g(x_1, \ldots, x_n) = f(x_2, x_1, x_3, \ldots, x_n).$$

3. Операция отождествления первых двух переменных, которая при $n \geqslant 2$ по функции $f(x_1, \ldots, x_n)$ дает функцию

$$g(x_1, \ldots, x_{n-1}) = f(x_1, x_1, x_2, \ldots, x_{n-1}).$$

4. Операция подстановки одной функции вместо первой переменной другой функции, которая по функциям $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_m)$ дает функцию

$$h(x_1, \ldots, x_{m+n-1}) = f(g(x_1, \ldots, x_m), x_{m+1}, \ldots, x_{m+n-1}). \tag{3.11}$$

Возвращаясь к индуктивному переходу, замечаем, что если для функции f из класса Q функция f^* принадлежит множеству $[B_1]$, а функция g получается из функции f с помощью одной из операций 1–3, то в силу установленного выше факта множеству $[B_1]$ будет принадлежать и функция g^*.

Пусть теперь функция h получается из функций f и g согласно равенству (3.11), а функции f^*, g^* принадлежат множеству $[B_1]$. По доказанному в множество $[B_1]$ входят функции

$$f_1(x) = c(f(l^{\langle n\rangle}(x), r \circ l^{\langle n-1\rangle}(x), \ldots, r \circ l(x)), x),$$
$$g_1(x) = c(g(r \circ l^{\langle m+n-1\rangle}(x), \ldots, r \circ l^{\langle n\rangle}(x)), x).$$

Применяя к функции $f_1(x)$ последовательно функции

$$c(x, r(x)), \quad c^3(l^{\langle 2\rangle}(x), r^{\langle 2\rangle} \circ l(x), r(x)),$$

принадлежащие множеству B_1, получим функцию

$$f_2(x) = c^3(f(l^{\langle n\rangle}(x), r \circ l^{\langle n-1\rangle}(x), \ldots, r \circ l(x)), r(x), x). \tag{3.12}$$

Как и в начале доказательства теоремы, из функции $g_1(x)$ с помощью функций

$$c(x, r(x)), \quad c^3(l^{\langle 2\rangle}(x), l \circ r \circ l(x), r(x)), \quad c^3(l^{\langle 2\rangle}(x), r^{\langle 2\rangle} \circ l(x), r(x)),$$

входящих в множество B_1, получаем функцию

$$g_2(x) = c^{n+1}(g(r \circ l^{\langle m+n-1\rangle}(x), \ldots, r \circ l^{\langle n\rangle}(x)), r \circ l^{\langle n-1\rangle}(x), \ldots \\ \ldots, r \circ l(x), x). \quad (3.13)$$

Если теперь определить

$$h'(x) = f_2 \circ g_2(x),$$

то, опираясь на представления (3.12) и (3.13), будем иметь

$$h'(x) = c^3(f(g(r \circ l^{\langle m+n-1\rangle}(x), \ldots, r \circ l^{\langle n\rangle}(x)), r \circ l^{\langle n-1\rangle}(x), \ldots \\ \ldots, r \circ l(x)), x, g_2(x)).$$

Следовательно, функцией $h^*(x)$ будет функция $l \circ h'(x)$.

Завершим доказательство теоремы. Возьмем произвольную функцию $f(x)$ из класса Q. Как установлено выше, в множество $[B_1]$ входит функция

$$f^*(x) = c(f \circ r \circ l(x), x).$$

Тогда

$$l \circ f^*(x) = f \circ r \circ l(x).$$

Остается заметить, что функция $f(x)$ получается из функции $c^3(x,x,x)$ применением к ней функции $f \circ r \circ l(x)$. В свою очередь функция $c^3(x,x,x)$ получается суперпозицией функций $c(x,x)$ и $c(x, r(x))$. Теорема доказана.

Из теорем 3.4 и 3.5 вытекает

Следствие. *Пусть $f \in E^0$ и $f_2 \leqslant {}_{\mathcal{E}} f$. Тогда множество всех одноместных функций из класса $\mathcal{E}f$ имеет конечный базис по суперпозиции.*

Конечные базисы по суперпозиции, построенные в теоремах 2.8, 3.4 и 3.5, содержат не менее семи функций. Возникает вопрос о минимальном числе функций в базисе и о минимальном числе переменных у функций базиса. Ответ на этот вопрос дает теорема 3.6.

Теорема 3.6. *Пусть класс функций Q содержит функции c, l, r, замкнут относительно операции суперпозиции и имеет конечный базис по суперпозиции. Тогда множество $Q^{(1)}$ всех одноместных функций из Q имеет базис по суперпозиции, состоящий из двух функций. Если, кроме того, в класс Q входят функции $x+1$ и $x \dot{-} y$, то класс Q имеет базис, состоящий из одной двуместной функции.*

Доказательство. Согласно теореме 3.5 множество $Q^{(1)}$ имеет конечный базис по суперпозиции $\{b_1(x), \ldots, b_s(x)\}$. Положим

$$d_1(x) = r(x), \quad d_2(x) = c^{s+1}(b_1(x), \ldots, b_s(x), l(x)).$$

Очевидно, что

$$\{d_1, d_2\} \subset Q^{(1)}, \quad d_1 \circ d_2(x) = l(x).$$

С помощью функций l, r получаем из функции d_2 функции $b_1, \ldots, b_s$. Таким образом, $[\{d_1, d_2\}] = Q^{(1)}$.

Пусть теперь $\{x+1, x \dot{-} y\} \subset Q$. Имеем:

$$0 = x \dot{-} x, \quad 1 = 0+1, \quad \overline{\mathrm{sg}}\, x = 1 \dot{-} x, \quad \mathrm{sg}\, x = \overline{\mathrm{sg}}\,\overline{\mathrm{sg}}\, x,$$

$$x + y = c(x,y) \dot{-} ((c(x,y) \dot{-} x) \dot{-} y), \quad |x-y| = (x \dot{-} y) + (y \dot{-} x),$$

$$x^2 = c(0,x), \quad 2xy = ((c(x,y) \dot{-} x^2) \dot{-} y^2) \dot{-} x, \quad x \cdot \mathrm{sg}\, y = 2x \cdot \mathrm{sg}\, y \dot{-} x.$$

Положим

$$d(x,y) = \begin{cases} x+1, & \text{если } x = y; \\ d_1(x), & \text{если } x+1 = y; \\ d_2(y), & \text{если } x = y+1; \\ c(x,y) & \text{в остальных случаях.} \end{cases}$$

Согласно утверждению 1.9 функция d входит в класс Q. Далее получаем:

$$x+1 = d(x,x), \quad d_1(x) = d(x, x+1), \quad d_2(x) = d(x+1, x).$$

Пользуясь тем, что функции d_1, d_2 образуют базис класса $Q^{(1)}$, суперпозициями d_1, d_2 определяем функции

$$c(x,x), \quad c(x,x)+2, \quad d_3(x) = c(l^{\langle 2\rangle}(x), l(r(x) \dot{-} 2)).$$

Нетрудно убедиться в том, что при любых x, y выполняется неравенство

$$|c(x,x) - c(y,y) - 2| \geqslant 2.$$

Поэтому

$$d(c(x,x), c(y,y)+2) = c(c(x,x), c(y,y)+2).$$

Следовательно,

$$d_3 \circ d(c(x,x), c(y,y)+2) = c(x,y).$$

Система $\{d_1, d_2, c\}$, очевидно, образует базис по суперпозиции в классе Q. Теорема доказана.

Замечание. Нетрудно видеть, что множество $Q^{(1)}$ не может иметь базиса по суперпозиции, состоящего из одной функции. В самом деле, пусть это не так и функция $f(x)$ образует базис множества $Q^{(1)}$. Тогда для некоторого натурального k должно быть, в частности, $0 = f^{\langle k\rangle}(x)$. Значит, при любом $m \geqslant k$ функция $f^{\langle m\rangle}(x)$ будет константой. Следовательно, суперпозициями функции f можно получить менее k функций, отличных от констант. Однако функция $c(x,x)$ строго монотонна, отлична от функции x и потому суперпозициями функции $c(x,x)$ можно определить, например, бесконечное число монотонных функций. Противоречие показывает, что базис по суперпозиции множества $Q^{(1)}$ не может состоять только из одной функции.

Задачи и темы для дальнейших исследований

1. Доказать аналог теоремы 3.1 для варианта машин SRM, в котором отсутствуют ограничения на число вхождений команд вида $t_i := t_i + 1$ в программу машины, а функция f удовлетворяет соотношению $f_2 \leqslant_{\mathcal{E}} f$, где $f_2(x) = (x+1)^2$.

2. Многоленточной машиной Минского [29] называется нестирающая машина Тьюринга $\mathcal{M}$, которая имеет k односторонних (бесконечных вправо) лент $L_1, \ldots, L_k$. В клетках каждой из лент $L_1, \ldots, L_k$ записана одна и та же бесконечная двоичная последовательность $100\ldots$, которая не меняется в процессе вычисления. На каждой из лент находится одна считывающая головка. В процессе вычисления головки машины $\mathcal{M}$ могут независимо передвигаться в обе стороны, не выходя при этом за левый конец ленты, содержащий символ 0. Машина $\mathcal{M}$ имеет множество состояний $\{q_0, q_1, \ldots, q_{s-1}\}$, в котором выделены начальное состояние q_1 и заключительное состояние q_0. Программа машины $\mathcal{M}$ состоит из команд вида

$$e_1 \ldots e_k q_i \to d_1 \ldots d_k q_j,$$

где $e_1, \ldots, e_k \in \{0, 1\}$, $i \neq 0$, $d_1, \ldots, d_k \in \{-1, 0, 1\}$ и $d_l \neq -1$ при $e_l = 1$. Здесь $e_1, \ldots, e_k$ — символы, обозреваемые головками машины на лентах $L_1, \ldots, L_k$, а $d_1, \ldots, d_k$ — движения головок на лентах. Предполагается, что машина $\mathcal{M}$ детерминирована.

Числа на лентах машины $\mathcal{M}$ задаются положением головок, числу 0 соответствует крайняя левая клетка ленты. Всюду определенная функция $g(x_1, \ldots, x_n)$ вычислима на машине $\mathcal{M}$, если $k \geqslant n$ и для любого набора $(x_1, \ldots, x_n)$ машина $\mathcal{M}$, начиная работу в состоянии q_1 с числами $x_1, \ldots, x_n, 0, \ldots, 0$, представленными на лентах $L_1, \ldots, L_k$, завершает работу в состоянии q_0 с числом $g(x_1, \ldots, x_n)$, представленным на ленте L_1.

Пусть $f(x)$ — всюду определенная функция. Говорим, что машина $\mathcal{M}$ вычисляет функцию $g(x_1, \ldots, x_n)$ в пределах зоны f, если максимальное из чисел, представленных на лентах машины $\mathcal{M}$ в процессе вычисления значения $g(x_1, \ldots, x_n)$, не превосходит значения $f(\max(x_1, \ldots, x_n))$. Через $\mathrm{MIN}\,(\mathrm{SPACE}, f)$ обозначим множество всех всюду определенных функций, которые вычислимы на машинах Минского в пределах зоны f.

Доказать утверждение: если $f \in E^0$ и $f_2 \leqslant_{\mathcal{E}} f$, то

$$\mathcal{E}f = \bigcup_{i \geqslant 1} \mathrm{MIN}\,(\mathrm{SPACE}, f^{\langle i \rangle}).$$

3. Пользуясь представлением класса $\mathcal{E}f$ из теоремы 3.1 (либо аналогичными представлениями из задач 1, 2), доказать, что при условии $f_2 \leqslant_{\mathcal{E}} f$ любую функцию класса $\mathcal{E}f$ можно получить из функций $x+1$, $[\sqrt{x}\,]$, $x \dot{-} y$, xy, $f(x)$ с помощью операции суперпозиции и не более чем однократным применением операции ограниченной рекурсии.

4. Разработать на основе машин SRM систему понятий и технику относительных вычислений для доказательства соответствующего обобщения теоремы 3.1.

5. Определим следующий вариант машин SRM — машины SRM$^-$. Машины SRM$^-$ не имеют рабочего регистра, регистра 0 и команд вида $r := z$, но имеют команды перехода, содержащие условия вида

$$z = c, \quad z_1 = z_2 + z_3, \quad z_1 = z_2 \cdot z_3,$$

где c — произвольное число из $\mathbb{N}$, а $z, z_i \in \{x_1, \dots, x_n, t_0, \dots, t_k\}$. Результат работы машины SRM$^-$ записывается в регистре стека с наибольшим номером. Класс функций $\mathrm{SRM}^-(\mathrm{SPACE}, f)$, вычислимых на машинах SRM$^-$, определяется так же, как и для машин SRM.

Доказать [3], что при любом $i \geqslant 1$, класс **BA** совпадает с множеством всех предикатов, содержащихся в любом из классов

$$\mathrm{SRM}^-(\mathrm{SPACE}, f_0^{\langle i \rangle}), \quad \mathrm{SRM}^-(\mathrm{SPACE}, f_1^{\langle i \rangle}), \quad \mathrm{SRM}^-(\mathrm{SPACE}, f_2^{\langle i \rangle}),$$

где $f_0(x) = x + 1$, $f_1(x) = 2(x+1)$, $f_2(x) = (x+1)^2$.

6. Пусть для любого $i \geqslant 1$ выполняется равенство

$$b_i(x) = x + \lceil x^{1-1/i} \rceil + 1,$$

где $\lceil a \rceil$ есть ближайшее сверху целое к числу a. Доказать [3], что при любом $i \geqslant 1$ справедливо равенство

$$\mathcal{E}_*^0 = (\mathcal{E} b_i)_*.$$

Комментарии. Теоремы 3.1, 3.2 принадлежат А.П. Бельтюкову [3]. Варианты теоремы 3.4 доказаны в [15, 20]. Теорема 3.5 установлена в [20].

Глава IV

ПРОСТОЙ БАЗИС ПО СУПЕРПОЗИЦИИ В КЛАССЕ $\mathcal{E}^2$

В гл. III было доказано, что при некоторых ограничениях на функцию f класс $\mathcal{E}f$ имеет конечный базис по суперпозиции. В основе доказательства теоремы 3.4 лежит «арифметизация» вычислений на машинах типа SRM. Проводимая арифметизация выполнена с использованием ключевых функций $\mathrm{Init}\,(x,y)$, $\mathrm{N}\,(x,y,z,w)$ и $\mathrm{Yield}\,(x)$. И хотя с содержательной точки зрения определения этих функций достаточно прозрачны, техническая сторона определений получается весьма громоздкой и занимает несколько страниц. Возникает естественный вопрос: нельзя ли подобную арифметизацию выполнить с использованием только хорошо известных «арифметических» функций?

По-видимому, трудно надеяться на решение этой задачи в общих условиях теоремы 3.4 и в терминах «совсем простых» арифметических функций. Тем не менее оригинальный подход к решению задачи был предложен С.А. Волковым [5]. Далее мы ограничимся рассмотрением только класса $\mathcal{E}^2$, хотя принципиально метод С.А. Волкова применим к любому классу $\mathcal{E}f$, удовлетворяющему условиям теоремы 3.4.

§ 4.1. Основные понятия и формулировка центрального результата

Мы будем свободно пользоваться следующими функциями, которые определены в предыдущих главах и принадлежат классу $\mathcal{E}^2$:

$$\mathrm{sg},\quad \overline{\mathrm{sg}},\quad x+y,\quad x\cdot y,\quad x\dot{-}y,\quad [x/y],\quad \mathrm{rm}\,(x,y).$$

Определим в классе классе $\mathcal{E}^2$ еще несколько необходимых функций. Функцию $\min\,(x,2^y)$ зададим следующей ограниченной рекурсией:

$$\begin{cases} \min\,(x,2^0) = x\dot{-}(x\dot{-}1), \\ \min\,(x,2^{y+1}) = 2\min\,(x,2^y)\cdot\overline{\mathrm{sg}}\,(2\min\,(x,2^y)\dot{-}x) + \\ \qquad\qquad\qquad\qquad + x\cdot\mathrm{sg}\,(2\min\,(x,2^y)\dot{-}x), \\ \min(x,2^y)\leqslant x. \end{cases}$$

Функцию $[\log_2 x]$ получим в виде $g(x,x)$, где функция g определяется ограниченной рекурсией

$$\begin{cases} g(x,0)=0, \\ g(x,y+1)=g(x,y)+\operatorname{sg}(x \dot{-} \min(x,2^y)), \\ g(x,y)\leqslant x \end{cases}$$

(отметим, что для введенной функции $[\log_2 x]$ выполняется равенство $[\log_2 0]=0$).

Функцию $x\wedge y$ определим как поразрядную конъюнкцию двоичных представлений чисел x и y. Именно, если $a_n a_{n-1}\ldots a_0$, $b_n b_{n-1}\ldots, b_0$ — двоичные (не диадические!) представления чисел x и y (при несовпадения длин двоичных представлений старшие разряды двоичного представления меньшего числа считаем равными нулю), то двоичное представление числа $x\wedge y$ есть $(a_n\cdot b_n)(a_{n-1}\cdot b_{n-1})\ldots(a_0\cdot b_0)$.

Определим функцию $R(x,y)$ как циклический сдвиг двоичного представления числа x на y разрядов вправо. Иными словами, пусть $R(0,y)=0$, $R(1,y)=1$, а если $a_n a_{n-1}\ldots a_0$ — двоичное представление x, причем $n\geqslant 1$ и $a_n=1$, то $R(x,y)$ есть $a_{n+y}a_{n+y-1}\ldots a_{1+y}a_y$, где сложение проводится по модулю $n+1$.

Нетрудно установить, что обе функции $x\wedge y, R(x,y)$ принадлежат классу $\mathcal{E}^2$. Проделаем это для функции $x\wedge y$.

Если $\min(z,2^v)<z$, то $\min(z,2^v)=2^v$. Поэтому при $\min(2x+1,2^v)<2x+1$ функция

$$[\operatorname{rm}(x,2\min(2x+1,2^v))/\min(2x+1,2^v)]$$

даёт v-й разряд двоичного представления числа x. Обозначим эту функцию через $g(x,v)$. Тогда

$$x\wedge y=\sum_{v\leqslant x}\min(2x+1,2^v)\cdot g(x,v)\cdot g(y,v)\cdot\operatorname{sg}((2x+1)\dot{-}\min(2x+1,2^v)).$$

Пусть $V(x_1,\ldots,x_m)$ — функция из класса $\mathcal{E}^2$ и $F\subseteq\mathcal{E}^2$. Будем говорить, что функция V является *квазиуниверсальной* в классе $\mathcal{E}^2$ относительно множества функций F, если для любой функции $f(\widetilde{y})$ из класса $\mathcal{E}^2$ найдутся такие функции $g_1(\widetilde{y}),\ldots,g_m(\widetilde{y}),h(z,\widetilde{y})$ из множества F, что

$$f(\widetilde{y})=h(V(g_1(\widetilde{y}),\ldots,g_m(\widetilde{y})),\widetilde{y}).$$

Определим функцию $Q(x,p_1,p_2,c_1,c_2,t)$ следующей примитивной рекурсией:

$$\begin{cases} Q(x,p_1,p_2,c_1,c_2,0)=x, \\ Q(x,p_1,p_2,c_1,c_2,t+1)=Q(x,p_1,p_2,c_1,c_2,t)+R(p_2,c_2t), \\ \qquad\qquad\qquad\text{если } Q(x,p_1,p_2,c_1,c_2,t)\wedge R(p_1,c_1t)=0, \\ Q(x,p_1,p_2,c_1,c_2,t+1)=Q(x,p_1,p_2,c_1,c_2,t) \text{ в противном случае.} \end{cases}$$

Поскольку

$$Q(x,p_1,p_2,c_1,c_2,t)\leqslant x+2p_2t,$$

функция Q определена ограниченной рекурсией в классе $\mathcal{E}^2$ и, следовательно, $Q \in \mathcal{E}^2$.

Центральным результатом этой главы является следующая теорема.

Теорема 4.1. *Функция $Q(x, p_1, p_2, c_1, c_2, t)$ является квазиуниверсальной в классе $\mathcal{E}^2$ относительно замыкания по суперпозиции системы функций*

$$x + 1, \quad x \cdot y, \quad \min(x, 2^y), \quad x \dot{-} y, \quad [x/y], \quad [\log_2 x]. \tag{4.1}$$

Следствие. *Функция Q вместе с функциями* (4.1) *образует базис по суперпозиции в классе $\mathcal{E}^2$.*

§ 4.2. Конфигурации и коды конфигураций машин Минского

Доказательство теоремы 4.1 фактически будет состоять в том, что с помощью функций системы (4.1) и функции Q будет проведена арифметизация вычислений на некотором типе абстрактных вычислительных устройств — *машинах Минского*. Машины Минского определены нами в задаче 2 из гл. III. Так же, как в приведенном там определении, будем считать, что машина Минского $\mathcal{M}$ имеет k бесконечных вправо лент и s состояний, которые будем обозначать числами $0, 1, \ldots, s-1$. Состояние 1 считаем начальным, состояние 0 — заключительным. Программа машины $\mathcal{M}$ состоит из команд вида

$$e_1 \ldots e_k q \to d_1 \ldots d_k q', \tag{4.2}$$

где

$$\begin{array}{ll} e_1, \ldots, e_k \in \{0, 1\}, & q, q' \in \{0, 1, \ldots, s-1\}, \\ q \neq 0, & d_1, \ldots, d_k \in \{-1, 0, 1\} \end{array}$$

и $d_i \neq -1$, если $e_i = 1$. Предполагаем, что для каждого набора $(e_1, \ldots, e_k) \in \{0, 1\}^k$ и любого $q \in \{1, \ldots, s-1\}$ в программе машины $\mathcal{M}$ имеется ровно одна команда (4.2) с левой частью $e_1 \ldots e_k q$.

Если машина Минского $\mathcal{M}$ вычисляет всюду определенную функцию от переменных $x_1, \ldots, x_n$, то время вычисления (число тактов работы машины $\mathcal{M}$ до попадания в заключительное состояние) будем обозначать через $T_{\mathcal{M}}(x_1, \ldots, x_n)$.

Так же, как в случае машин типа SRM, класс $\mathcal{E}^2$ можно описать в терминах вычислений на машинах Минского [15, 20].

Теорема 4.2. *Класс $\mathcal{E}^2$ совпадает с множеством всех всюду определнных функций, которые вычислимы за полиномиальное время. Иными словами, всюду определенная функция $f(x_1, \ldots, x_n)$ принадлежит классу $\mathcal{E}^2$ в том и только том случае, когда существуют машина Минского $\mathcal{M}$ и полином $P(x_1, \ldots, x_n)$ с натуральными коэффициентами такие, что машина $\mathcal{M}$ вычисляет функцию f и при этом*

$$T_{\mathcal{M}}(x_1, \ldots, x_n) \leqslant P(x_1, \ldots, x_n).$$

То, что каждая функция из класса $\mathcal{E}^2$ вычислима на подходящей машине Минского за полиномиальное время, доказывается индукцией по построению функций в классе $\mathcal{E}^2$. При этом используются стандартные приемы программирования на машинах Тьюринга (Минского). Обратное включение устанавливается чуть более сложно — здесь необходима арифметизация вычислений на машинах Минского. Однако эта часть доказательства фактически будет выполнена в оставшейся части главы. Стоит лишь еще раз отметить, что для полного обоснования следствия из теоремы 4.1 необходимо доказывать принадлежность функции Q и функций (4.1) классу $\mathcal{E}^2$ — либо в рамках исходного определения класса $\mathcal{E}^2$, либо с помощью полиномиальных вычислений на машинах Минского.

Назовем машину Минского *приведенной*, если в каждом состоянии дальнейшие действия машины определяются только информацией с одной из лент (зависящей от состояния). Иными словами, программа приведенной k-ленточной машины Минского состоит из команд вида

$$e_i q \to d_1 \dots d_k q',$$

где $1 \leqslant i \leqslant k$ и число i зависит только от состояния q.

Нетрудно понять, как произвольную k-ленточную машину Минского $\mathcal{M}$ можно преобразовать в эквивалентную приведенную k-ленточную машину $\mathcal{M}'$. Для этого достаточно в машине $\mathcal{M}'$ вместо каждого состояния машины $\mathcal{M}$ ввести 2^k состояний, которые будут «запоминать» все двоичные наборы длины k (все возможные комбинации обозреваемых символов на k лентах машины $\mathcal{M}$). Каждый шаг работы машины $\mathcal{M}$ будет при этом моделироваться k шагами работы машины $\mathcal{M}'$. Таким образом, из теоремы 4.2 выводится

Следствие. *Класс $\mathcal{E}^2$ состоит в точности из всех функций, которые вычислимы на приведенных машинах Минского за полиномиальное время.*

Конфигурацией k-ленточной машины Минского $\mathcal{M}$ в момент времени t будем называть вектор $(x_1, \dots, x_k; q)$, где x_i — номер клетки, в которой в момент t находится i-я головка машины $\mathcal{M}$ $(1 \leqslant i \leqslant k)$, а q — ее состояние в момент t.

В дальнейшем мы будем рассматривать всюду определенные вектор-функции вида

$$F:\ \mathbb{N}^k \times \{0, 1, \dots, s-1\} \to \mathbb{N}^k \times \{0, 1, \dots, s-1\}. \tag{4.3}$$

Пусть $(x_1, \dots, x_k; q)$ — конфигурация машины Минского $\mathcal{M}$ и (4.2) — команда из программы машины $\mathcal{M}$, причем

$$e_1 = \overline{\mathrm{sg}}\,(x_1), \dots, e_k = \overline{\mathrm{sg}}\,(x_k). \tag{4.4}$$

Команда (4.2) преобразует конфигурацию $(x_1, \ldots, x_k; q)$ в непосредственно следующую конфигурацию $(x_1 + d_1, \ldots, x_k + d_k; q')$. В целом процесс преобразования конфигураций машины Минского $\mathcal{M}$ можно задать с помощью вектор-функции $\mathrm{Con}_{\mathcal{M}}$ вида (4.3). При этом

$$\mathrm{Con}_{\mathcal{M}}(x_1, \ldots, x_k; q) = (x_1 + d_1, \ldots, x_k + d_k; q'),$$

если в программе машины $\mathcal{M}$ содержится команда (4.2) и выполняются соотношения (4.4), и

$$\mathrm{Con}_{\mathcal{M}}(x_1, \ldots, x_k; 0) = (x_1, \ldots, x_k; 0)$$

(напомним, что 0 — заключительное состояние машины $\mathcal{M}$).

Вектор-функцию F вида (4.3) назовем *простой*, если существуют целые (не обязательно натуральные) числа $a_1, \ldots, a_k$, а также числа i $(1 \leqslant i \leqslant k)$ и $q', q'' \in \{0, 1, \ldots, s-1\}$, такие, что

$$F(x_1, \ldots, x_k; q) = \\ = \begin{cases} (x_1 + a_1, \ldots, x_k + a_k; q'), & \text{если } x_i = 0 \text{ и } q = q''; \\ (x_1, \ldots, x_k; q) & \text{в противном случае.} \end{cases} \tag{4.5}$$

По техническим причинам удобно также ввести вектор-функции F для значения $i = 0$, полагая $x_0 = 0$.

Нетрудно видеть, что справедливо следующее

Утверждение 4.1. *Для любой приведенной k-ленточной машины Минского $\mathcal{M}$ существуют натуральные числа s, m и простые вектор-функции $F_1, \ldots, F_m$ вида* (4.5), *такие, что*

$$\mathrm{Con}_{\mathcal{M}}(\widetilde{x}; q) = F_1(F_2(\ldots F_m(\widetilde{x}; q) \ldots)).$$

Число x будем называть (w, l)-*кодом конфигурации* $(x_1, \ldots, x_k; q)$, если двоичные разряды числа x с $l(i-1)$-го по $(li-1)$-й образуют двоичную запись числа x_i $(1 \leqslant i \leqslant k)$, а разряды с kl-го по $(kl + w - 1)$-й — двоичную запись числа q. Отметим, что (w, l)-код конфигурации не определяется однозначно.

Функцию f одной переменной будем называть *простой*, если существуют такие числа $u, v \in \mathbb{N}$, что для любого $x \in \mathbb{N}$

$$f(x) = \begin{cases} x + v, & \text{если } x \wedge u = 0; \\ x & \text{в противном случае.} \end{cases}$$

Утверждение 4.2. *Пусть F — простая вектор-функция вида* (4.5), *где $|a_1|, \ldots, |a_k| \leqslant 1$, w, l — натуральные числа и $2^w \geqslant s$.*

Пусть, далее, f_1, f_2, f_3 — простые функции, которые определяются следующими параметрами u_1, v_1, u_2, v_2, u_3, v_3:

$$\begin{aligned}
&u_1 = 0,\\
&v_1 = (2^w - q'')2^{lk},\\
&u_2 = \begin{cases} (2^w - 1)2^{lk} + (2^l - 1)2^{l(i-1)}, & \text{если } i > 0,\\ (2^w - 1)2^{lk}, & \text{если } i = 0, \end{cases}\\
&v_2 = 2^{lk+w} + (2^w + q' - q'')2^{lk} + \sum_{j=1}^{k} a_j 2^{l(j-1)},\\
&u_3 = 0,\\
&v_3 = q''2^{lk}.
\end{aligned}$$

Тогда для любых векторов $(x_1, \ldots, x_k; q), (y_1, \ldots, y_k; q^*)$ и натурального числа x: если

$$x_1, \ldots, x_k, y_1, \ldots, y_k < 2^l,$$

$$(y_1, \ldots, y_k; q^*) = F(x_1, \ldots, x_k; q),$$

$$x \text{ — } (w, l)\text{-}\textit{код конфигурации } (x_1, \ldots, x_k; q),$$

то $f_3(f_2(f_1(x)))$ — (w, l)-код конфигурации $(y_1, \ldots, y_k; q^*)$.

Доказательство. Заметим, прежде всего, что все числа u_j, v_j $(1 \leqslant j \leqslant 3)$ неотрицательны.

Пусть $f_1(x)$, $f_2(f_1(x))$, $f_3(f_2(f_1(x)))$ — (w, l)-коды конфигураций K_1, K_2, K_3 и

$$K_j = (x_{j1}, \ldots, x_{jk}; q_j), \quad 1 \leqslant j \leqslant 3.$$

Очевидно, что

$$f_1(x) = x + (2^w - q'')2^{lk}.$$

Следовательно,

$$K_1 = (x_1, \ldots, x_k; q - q'')$$

(здесь и далее в доказательстве сложение и вычитание чисел q, q', q'', q_j выполняется по модулю 2^w).

Докажем, что

$$(f_1(x) \wedge u_2) = 0 \equiv (x_i = 0 \text{ и } q = q''). \tag{4.6}$$

В самом деле, если $i \neq 0$, то в двоичной записи числа u_2 единицы расположены в разрядах с $l(i-1)$-го по $(li-1)$-й и с lk-го по $(lk + w - 1)$-й. Отсюда следует, что $f_1(x) \wedge u_2 = 0$ тогда и только тогда, когда в соответствующих разрядах числа $f_1(x)$ расположены нули, т. е.

$$(f_1(x) \wedge u_2 = 0) \equiv (x_{1i} = 0 \text{ и } q_1 = 0).$$

Однако $q_1 = q - q''$ и $x_{1i} = x_i$, что приводит к эквивалентности (4.6).

В случае $i = 0$ (напомним, что по предположению $x_0 = 0$) путем аналогичных рассуждений получаем, что

$$(f_1(x) \wedge u_2 = 0) \equiv (q = q'').$$

Следовательно, вновь приходим к эквивалентности (4.6).

Пусть $f_1(x) \wedge u_2 = 0$, т. е. $x_i = 0$ и $q = q''$. Тогда согласно определению функции F выполняются равенства $y_j = x_j + a_j$ $(1 \leqslant j \leqslant k)$. Поскольку $f_1(x)$ есть (w, l)-код конфигурации K_1, будет справедлива цепочка сравнений

$$f_1(x) \equiv q_1 2^{lk} + \sum_{j=1}^{k} x_{1j} 2^{l(j-1)} \equiv$$
$$\equiv (q - q'')2^{lk} + \sum_{j=1}^{k} x_j 2^{l(j-1)} \equiv \sum_{j=1}^{k} x_j 2^{l(j-1)} \pmod{2^{lk+w}}.$$

Значит,

$$f_2(f_1(x)) \equiv f_1(x) + v_2 \equiv (q' - q'')2^{lk} + \sum_{j=1}^{k} (x_j + a_j) 2^{l(j-1)} \equiv$$
$$\equiv (q' - q'')2^{lk} + \sum_{j=1}^{k} y_j 2^{l(j-1)} \pmod{2^{lk+w}}.$$

Однако при любом j, $1 \leqslant j \leqslant k$, выполняется неравенство $y_j < 2^l$. Поэтому

$$K_2 = (y_1, \ldots, y_k; q' - q'').$$

Если же $f_1(x) \wedge u_2 \neq 0$, то, очевидно, при любом j, $1 \leqslant j \leqslant k$, будем иметь $y_j = x_j$. Кроме того,

$$f_2(f_1(x)) = f_1(x)$$

и

$$K_2 = K_1 = (x_1, \ldots, x_k; q - q'') = (y_1, \ldots, y_k; q - q'').$$

Далее, из определения функции f_3 следует, что

$$f_3(f_2(f_1(x))) = f_2(f_1(x)) + v_3 = f_2(f_1(x)) + q'' 2^{lk}.$$

Значит,

$$q_3 = q_2 + q''$$

и при любом j, $1 < j \leqslant k$,

$$x_{3j} = x_{2j} = y_j.$$

Если $x_i = 0$ и $q = q''$, то

$$q_3 = q_2 + q'' = (q' - q'') + q'' = q = q^*.$$

В противном случае

$$q_3 = q_2 + q'' = (q - q'') + q'' = q = q^*.$$

Таким образом,

$$K_3 = (y_1, \ldots, y_k; q^*),$$

и утверждение доказано.

Следствие. *Пусть $\mathcal{M}$ — приведенная машина Минского. Тогда существует такое натуральное число w, что для любого натурального числа l найдутся простые одноместные функции f_1, f_2, f_3, такие, что если векторы $(x_1, \ldots, x_k; q)$, $(y_1, \ldots, y_k; q')$ и натуральное число x удовлетворяют условиям*

$$x_1, \ldots, x_k, y_1, \ldots, y_k < 2^l,$$
$$(y_1, \ldots, y_k; q') = \mathrm{Con}_{\mathcal{M}}(x_1, \ldots, x_k; q),$$
$$x \text{ — } (w, l)\text{-код конфигурации } (x_1, \ldots, x_k; q),$$

то $f_3(f_2(f_1(x)))$ — (w, l)-код конфигурации $(y_1, \ldots, y_k; q')$.

§ 4.3. Вывод свойств функции Q

Обозначим через $h_c(x)$ число, двоичную запись которого образуют c младших разрядов числа x ($h_0(x) = 0$ и $h_c(x) = x$, если двоичная запись числа x имеет менее c разрядов). Отметим, что для любых x, y выполняется соотношение

$$h_c(x + y) = h_c(h_c(x) + h_c(y)).$$

Утверждение 4.3. *Пусть $r \geqslant 1$,*

$$u_0, \ldots, u_{r-2}, \quad v_0, \ldots, v_{r-2}$$

— натуральные числа и для любого $i \geqslant 0$:

$$f_i(x) = \begin{cases} x + v_{\mathrm{rm}(i,r)}, & \text{если } x \wedge u_{\mathrm{rm}(i,r)} = 0; \\ x & \text{в противном случае} \end{cases}$$

при $\mathrm{rm}\,(i, r) \neq r - 1$;

$$f_i(x) = x$$

при $\mathrm{rm}\,(i, r) = r - 1$.

Пусть, далее, для натуральных чисел t_0, p_1, p_2, c_1, c_2, x, u_{r-1}, v_{r-1} выполняются следующие условия:

$$t_0 \geqslant 1, \tag{4.7}$$
$$u_{r-1} = 2^{c_1} - 1, \tag{4.8}$$
$$2^{c_2 - 1} \leqslant v_{r-1} < 2^{c_2}, \tag{4.9}$$

$$p_1 = \sum_{i=0}^{r-1} 2^{c_1 i} u_i, \tag{4.10}$$

$$p_2 = \sum_{i=0}^{r-1} 2^{c_2 i} v_i, \tag{4.11}$$

$$x + 2p_2 t_0 < 2^{c_1}, \tag{4.12}$$

$$x + t_0 \max(v_0, \ldots, v_{r-2}) < 2^{c_2}, \tag{4.13}$$

$$u_i < 2^{c_2} \quad (0 \leqslant i \leqslant r-2), \tag{4.14}$$

$$c_1 \geqslant c_2, \tag{4.15}$$

$$x \geqslant 1. \tag{4.16}$$

Тогда

$$h_{c_2}(Q(x, p_1, p_2, c_1, c_2, t_0)) = f_{t_0-1}(f_{t_0-2}(\ldots f_0(x)\ldots)).$$

Доказательство. Пусть

$$g(t,x) = \begin{cases} f_{t-1}(f_{t-2}(\ldots f_0(x)\ldots)), & \text{если } t > 0;\\ x, & \text{если } t = 0.\end{cases}$$

Очевидно, что при всех t

$$g(t+1) \leqslant g(t) + \max(v_0, \ldots, v_{r-2}).$$

Из этого неравенства и из (4.13), (4.16) получаем, что

$$0 < g(t) < 2^{c_2}. \tag{4.17}$$

Кроме того, очевидно, что при $t < t_0$ будет

$$g(t) + \max(v_0, \ldots, v_{r-2}) < 2^{c_2}. \tag{4.18}$$

Далее по индукции доказываем, что для всех $t \leqslant t_0$ справедливо равенство

$$h_{c_2}(Q(x, p_1, p_2, c_1, c_2, t)) = g(t).$$

Базис индукции верен, поскольку

$$Q(x, p_1, p_2, c_1, c_2, 0) = x$$

и $x < 2^{c_2}$ (см. (4.13)).

Предполагая, что доказываемое равенство верно при $t < t_0$, докажем его для значения $t+1$. Из (4.7) и (4.13) следует, что $v_0 \ldots, v_{r-2} < 2^{c_2}$, а из (4.9) — что $v_{r-1} < 2^{c_2}$. Аналогично, из (4.14) и (4.8) получаем, что $u_0, \ldots, u_{r-1} < 2^{c_1}$. Таким образом, при всех j, $0 \leqslant j < r$, выполняются неравенства

$$u_j < 2^{c_1}, \quad v_j < 2^{c_2}.$$

Отсюда и из (4.10), (4.11) следует, что разряды двоичной записи числа p_1 с $(c_1 j)$-го по $(c_1(j+1)-1)$-й образуют двоичную запись числа u_j, а разряды двоичной записи числа p_2 с $(c_2 j)$-го по $(c_2(j+1)-1)$-й — двоичную запись числа v_j $(0 \leqslant j < r)$. Вместе с тем соотношения (4.8), (4.9) показывают, что двоичные записи чисел p_1 и p_2 имеют $c_1 r$ и $c_2 r$ разрядов соответственно. Отсюда заключаем, что при любом натуральном t справедливы равенства

$$h_{c_1}(R(p_1, c_1 t)) = u_{\mathrm{rm}\,(t,r)}, \tag{4.19}$$

$$h_{c_2}(R(p_2, c_2 t)) = v_{\mathrm{rm}\,(t,r)}. \tag{4.20}$$

Используя определение функции Q и (4.12), замечаем далее, что

$$Q(x, p_1, p_2, c_1, c_2, t) \leqslant x + 2p_2 t \leqslant x + 2p_2 t_0 < 2^{c_1}.$$

Следовательно, если $\mathrm{rm}\,(t,r) \neq r-1$, то

$$Q(x, p_1, p_2, c_1, c_2, t) \wedge R(p_1, c_1 t) = Q(x, p_1, p_2, c_1, c_2, t) \wedge h_{c_1}(R(p_1, c_t)) = \\ = Q(x, p_1, p_2, c_1, c_2, t) \wedge u_{\mathrm{rm}\,(t,r)}.$$

Из предположения индукции и из (4.14) следует, что

$$Q(x, p_1, p_2, c_1, c_2, t) \wedge u_{\mathrm{rm}\,(t,r)} = g(t) \wedge u_{\mathrm{rm}\,(t,r)}.$$

Таким образом, если $\mathrm{rm}\,(t,r) \neq r-1$, то

$$Q(x, p_1, p_2, c_1, c_2, t) \wedge R(p_1, c_1 t) = g(t) \wedge u_{\mathrm{rm}\,(t,r)}. \tag{4.21}$$

Если $\mathrm{rm}\,(t,r) = r-1$, то

$$h_{c_2}(Q(x, p_1, p_2, c_1, c_2, t)) \wedge h_{c_2}(R(p_1, c_1 t)) = \\ = h_{c_2}(Q(x, p_1, p_2, c_1, c_2, t)) \wedge h_{c_2}(h_{c_1}(R(p_1, c_1 t))) = \\ = g(t) \wedge h_{c_2}(u_{\mathrm{rm}\,(t,r)}) = g(t) \wedge h_{c_2}(u_{r-1}) = \\ = g(t) \wedge h_{c_2}(2^{c_1}-1) = g(t) \wedge (2^{c_2}-1) \neq 0.$$

Здесь первое равенство следует из (4.15), второе — из предположения индукции и (4.19), третье — из соотношения $\mathrm{rm}\,(t,r) = r-1$, четвертое — из (4.8), пятое — из (4.15) и последнее неравенство — из (4.17). Следовательно, если $\mathrm{rm}\,(t,r) = r-1$, то

$$Q(x, p_1, p_2, c_1, c_2, t) \wedge R(p_1, c_1 t) \neq 0. \tag{4.22}$$

Таким образом, из (4.21) и (4.22) получаем, что

$$Q(x, p_1, p_2, c_1, c_2, t+1) = \\ = \begin{cases} Q(x, p_1, p_2, c_1, c_2, t) + R(p_2, c_2 t), & \text{если } g(t) \wedge u_{\mathrm{rm}\,(t,r)} = 0 \\ & \text{и } \mathrm{rm}\,(t,r) \neq r-1; \\ Q(x, p_1, p_2, c_1, c_2, t) & \text{в противном случае.} \end{cases}$$

Заметим, что при $\mathrm{rm}\,(t,r) \neq r-1$ из свойств функции h_{c_2}, индуктивного предположения и (4.20), (4.18) следует, что

$$\begin{aligned} h_{c_2}(Q(x,p_1,p_2,c_1,c_2,t) + R(p_2,c_2t)) = \\ = h_{c_2}(h_{c_2}(Q(x,p_1,p_2,c_1,c_2,t)) + h_{c_2}(R(p_2,c_2t))) = \\ = h_{c_2}(g(t) + v_{\mathrm{rm}\,(t,r)}) = g(t) + v_{\mathrm{rm}\,(t,r)}. \end{aligned}$$

Таким образом,

$$h_{c_2}(Q(x,p_1,p_2,c_1,c_2,t+1)) = \\ = \begin{cases} g(t) + v_{\mathrm{rm}\,(t,r)}, & \text{если } g(t) \wedge u_{\mathrm{rm}\,(t,r)} = 0 \text{ и } \mathrm{rm}\,(t,r) \neq r-1, \\ g(t) & \text{в противном случае.} \end{cases}$$

Следовательно,

$$h_{c_2}(Q(x,p_1,p_2,c_1,c_2,t+1)) = g(t+1),$$

и утверждение доказано.

§ 4.4. Доказательство основной теоремы

Обозначим через Φ замыкание системы функций (4.1) относительно операции суперпозиции. Имеем:

$$0 = x \dot{-} x, \quad x + y = (x+1)\cdot(y+1) \dot{-} (xy+1).$$

Следовательно, множеству Φ принадлежат все полиномы с целыми коэффициентами, принимающие натуральные значения при любых натуральных значениях переменных (при наличии в полиноме отрицательных коэффициентов из «положительной» части полинома следует с помощью функции $\dot{-}$ вычесть «отрицательную» часть полинома).

Пусть функция $f(y_1,\ldots,y_n)$ принадлежит классу $\mathcal{E}^2$ Гжегорчика. Тогда по следствию из теоремы 4.2 существуют приведенная машина Минского $\mathcal{M}$ и полином $t(y_1,\ldots,y_n)$ с натуральными коэффициентами, такие, что машина $\mathcal{M}$ вычисляет функцию f и выполняется неравенство

$$T_{\mathcal{M}}(y_1,\ldots,y_n) \leqslant t(y_1,\ldots,y_n).$$

Пусть машина $\mathcal{M}$ имеет k лент. Будем предполагать, что все значения функции t не менее 1.

Выберем для машины $\mathcal{M}$ натуральное число w так, чтобы выполнялись условия следствия из утверждения 4.2. Положим

$$m(y_1,\ldots,y_n) = t(y_1,\ldots,y_n) + \sum_{i=1}^{n} y_i.$$

Функция m, очевидно, принадлежит множеству Φ. Заметим, что на первых $t(y_1, \ldots, y_n)$ шагах работы машины $\mathcal{M}$ (на входном наборе $(y_1, \ldots, y_n)$) головки машины будут находиться в клетках с номерами, не превосходящими значения $m(y_1, \ldots, y_n)$. Пусть

$$l(y_1, \ldots, y_n) = [\log_2 m(y_1, \ldots, y_n)] + 1.$$

Тогда, очевидно,

$$m(y_1, \ldots, y_n) < 2^{l(y_1, \ldots, y_n)}.$$

Далее, если в начальный момент времени на первых n лентах машины $\mathcal{M}$ находятся числа $y_1, \ldots, y_n$ и $(y'_1, \ldots, y'_n; q')$ — конфигурация машины $\mathcal{M}$ в момент времени

$$t' \leqslant t(y_1, \ldots, y_n),$$

то, конечно, будут выполняться неравенства

$$y'_1, \ldots, y'_n < 2^{l(y_1, \ldots, y_n)}.$$

Тогда согласно следствию из утверждения 4.2 найдутся функции

$$u_0(\widetilde{y}), \quad u_1(\widetilde{y}), \quad u_2(\widetilde{y}), \quad v_0(\widetilde{y}), \quad v_1(\widetilde{y}), \quad v_2(\widetilde{y}) \tag{4.23}$$

(которые представимы полиномами от $2^{l(\widetilde{y})}$ с целыми коэффициентами), такие, что если $(y'_1, \ldots, y'_n; q')$ — конфигурация машины $\mathcal{M}$ в момент времени $t' < t(\widetilde{y})$ и x — ее $(w, l(\widetilde{y}))$-код, то $(w, l(\widetilde{y}))$-код непосредственно следующей конфигурации есть

$$\varphi_{\widetilde{y}}(x) = f_{2,\widetilde{y}}(f_{1,\widetilde{y}}(f_{0,\widetilde{y}}(x))),$$

где

$$f_{i,\widetilde{y}}(x) = \begin{cases} x + v_i(\widetilde{y}), & \text{если } x \wedge u_i(\widetilde{y}) = 0; \\ x & \text{в противном случае.} \end{cases}$$

Обозначим через $\psi_{\widetilde{y}}$ $t(\widetilde{y})$-кратную суперпозицию функции $\varphi_{\widetilde{y}}$. Тогда если x есть $(w, l(\widetilde{y}))$-код начальной конфигурации $(y_1, \ldots, y_n, 0, \ldots, 0; 1)$ машины Минского $\mathcal{M}$, то $\psi_{\widetilde{y}}(x)$ будет $(w, l(\widetilde{y}))$-кодом ее конфигурации в момент времени $t(\widetilde{y})$, т. е. $(w, l(\widetilde{y}))$-кодом заключительной конфигурации.

Понятно, что

$$2^{l(\widetilde{y})} = \min\,(2m(\widetilde{y}), 2^{l(\widetilde{y})})$$

и потому функция $2^{l(\widetilde{y})}$ принадлежит множеству Φ. Следовательно, множеству Φ принадлежат все функции (4.23).

Пусть

$$x(\widetilde{y}) = (2^w + 1)(2^{l(\widetilde{y})})^k + \sum_{i=1}^{n} (2^{l(\widetilde{y})})^{i-1} y_i.$$

Очевидно, что $x(\widetilde{y})$ есть $(w, l(\widetilde{y}))$-код начальной конфигурации $(y_1, \ldots, y_n, 0, \ldots, 0; 1)$ и функция $x(\widetilde{y})$ принадлежит множеству Φ.

Положим
$$z(\widetilde{y}) = \psi_{\widetilde{y}}(x(\widetilde{y})).$$
Определим функции $u_3(\widetilde{y})$, $v_3(\widetilde{y})$, $p_1(\widetilde{y})$, $p_2(\widetilde{y})$, $c_1(\widetilde{y})$, $c_2(\widetilde{y})$, $t'(\widetilde{y})$ следующими соотношениями:
$$\begin{aligned}
&t'(\widetilde{y}) = 4t(\widetilde{y}),\\
&c_2(\widetilde{y}) = \left[\log_2\left(x(\widetilde{y}) + \sum_{i\leqslant 2} u_i(\widetilde{y}) + t'(\widetilde{y})\sum_{i\leqslant 2} v_i(\widetilde{y})\right)\right] + 1,\\
&v_3(\widetilde{y}) = 2^{c_2(\widetilde{y})-1},\\
&p_2(\widetilde{y}) = \sum_{i\leqslant 2}(2^{c_2(\widetilde{y})})^i v_i(\widetilde{y}),\\
&c_1(\widetilde{y}) = [\log_2(x(\widetilde{y}) + 2t'(\widetilde{y})p_2(\widetilde{y}))] + 1,\\
&u_3(\widetilde{y}) = 2^{c_1(\widetilde{y})} - 1,\\
&p_1(\widetilde{y}) = \sum_{i\leqslant 2}(2^{c_1(\widetilde{y})})^i u_i(\widetilde{y}).
\end{aligned}$$
Положим $f_{3,\widetilde{y}}(x) = x$. Тогда при $r = 4$ функции (4.23), последовательность функций
$$f_{0,\widetilde{y}}, f_{1,\widetilde{y}}, f_{2,\widetilde{y}}, f_{3,\widetilde{y}}, f_{0,\widetilde{y}}, f_{1,\widetilde{y}}, f_{2,\widetilde{y}}, f_{3,\widetilde{y}}, \ldots$$
и функции
$$t'(\widetilde{y}),\ p_1(\widetilde{y}),\ p_2(\widetilde{y}),\ c_1(\widetilde{y}),\ c_2(\widetilde{y}),\ x(\widetilde{y}),\ u_3(\widetilde{y}),\ v_3(\widetilde{y})$$
удовлетворяют условиям утверждения 4.3. Следовательно, будем иметь
$$z(\widetilde{y}) = h_{c_2(\widetilde{y})}(Q(x(\widetilde{y}), p_1(\widetilde{y}), p_2(\widetilde{y}), c_1(\widetilde{y}), c_2(\widetilde{y}), t'(\widetilde{y}))),$$
т. е.
$$z(\widetilde{y}) = \mathrm{rm}\,(Q(x(\widetilde{y}), p_1(\widetilde{y}), p_2(\widetilde{y}), c_1(\widetilde{y}), c_2(\widetilde{y}), t'(\widetilde{y})), 2^{c_2(\widetilde{y})}).$$
Понятно, что функции $c_1(\widetilde{y})$, $c_2(\widetilde{y})$ принадлежат множеству Ф. Кроме того,
$$\begin{aligned}
&2^{c_2(\widetilde{y})} = \min\left(2\left(x(\widetilde{y}) + \sum_{i\leqslant 3} u_i(\widetilde{y}) + t'(\widetilde{y})\sum_{i\leqslant 3} v_i(\widetilde{y})\right), 2^{c_2(\widetilde{y})}\right),\\
&2^{c_1(\widetilde{y})} = \min\,(2(x(\widetilde{y}) + 2t'(\widetilde{y})p_2(\widetilde{y})), 2^{c_1(\widetilde{y})}).
\end{aligned}$$
Поэтому функции $2^{c_1(\widetilde{y})}$, $2^{c_2(\widetilde{y})}$ также принадлежат множеству Ф. Значит, в множество Ф входят функции $p_1(\widetilde{y})$, $p_2(\widetilde{y})$, $u_3(\widetilde{y})$, $v_3(\widetilde{y})$. Поскольку $z(\widetilde{y})$ есть $(w, l(\widetilde{y}))$-код заключительной конфигурации машины Минского $\mathcal{M}$, имеет место равенство
$$f(\widetilde{y}) = \mathrm{rm}\,(z(\widetilde{y}), 2^{l(\widetilde{y})}).$$

Заметим, что функция

$$h(x, \widetilde{y}) = \mathrm{rm}\,(\mathrm{rm}\,(x, 2^{c_2(\widetilde{y})}), 2^{l(\widetilde{y})})$$

принадлежит множеству Φ. Следовательно, равенство

$$f(\widetilde{y}) = h(Q(x(\widetilde{y}), p_1(\widetilde{y}), p_2(\widetilde{y}), c_1(\widetilde{y}), c_2(\widetilde{y}), t'(\widetilde{y})), \widetilde{y})$$

завершает доказательство теоремы 4.1.

Задачи и темы для дальнейших исследований

1. Определим вариант машины Минского, которая не имеет внутренних состояний (машина Минского БВП [25]). Команды k-ленточной машины Минского БВП имеют вид $\{0,1\}^k \to \{-1,0,1\}^k$, где входной и выходной векторы размерности k интерпретируются так же, как для обычной машины Минского. Вместо заключительного состояния в множестве $\{0,1\}^k$ выделяются некоторые наборы, которые объявляются заключительными наборами, и машина Минского заканчивает работу, как только набор значений, читаемых ее k головками на лентах, становится заключительным набором.

Доказать, что класс $\mathcal{E}^2$ совпадает с классом всех функций, вычислимых на машинах Минского БВП за полиномиальное время. Использовать этот результат для упрощения доказательства теоремы 4.1.

2. Исследовать схему построения функции Q на предмет дальнейшего упрощения самой функции Q, а также сокращения и упрощения системы функций (4.1).

Комментарии. Конечный базис по суперпозиции в классе $\mathcal{E}^2$ впервые построен в [14]. Применять машины Минского для получения конечных базисов в классах Гжегорчика предложено в [15] (см. также [20]). Построение конечного базиса в классе $\mathcal{E}^2$ на основе машин SRM выполнено в [23]. Теорема 2.1 доказана С.А. Волковым в [5].

Глава V

ПРОСТЫЕ БАЗИСЫ ПО СУПЕРПОЗИЦИИ В КЛАССЕ ФУНКЦИЙ, ЭЛЕМЕНТАРНЫХ ПО КАЛЬМАРУ

Для класса **K** функций, элементарных по Кальмару (класс $\mathcal{E}^3$ иерархии Гжегорчика), проблема построения конечного базиса по суперпозиции получила «окончательное» решение: были найдены четыре «самые простые» арифметические функции (принадлежащие классу **K**), суперпозиции которых порождают весь класс **K**. Эти функции суть

$$x + y, \quad x \dot{-} y, \quad [x/y], \quad 2^x.$$

Данную систему функций в дальнейшем будем обозначать через S.

§ 5.1. Построение простейших функций

Сначала покажем, как из функций системы S суперпозициями получить функции-константы $0, 1, \ldots$, функции sg, $\overline{\mathrm{sg}}$, $|x-y|$, xy, x^y, $\mathrm{rm}\,(x,y)$, $\binom{x}{y}$, где $\binom{x}{y}$ — биномиальный коэффициент, который будем рассматривать при $x \geqslant y$, полагая $\binom{0}{0} = 0$.

Очевидно, что

$$0 = x \dot{-} x, \quad 1 = 2^0, \quad \overline{\mathrm{sg}}\,(x) = 1 \dot{-} x, \quad \mathrm{sg}\,(x) = \overline{\mathrm{sg}}\,(\overline{\mathrm{sg}}\,(x)),$$

$$|x - y| = (x \dot{-} y) + (y \dot{-} x).$$

Константы $2, 3, \ldots$ получаем из константы 1 с помощью функции $x + y$.

Покажем, как суперпозициями функций системы S получить функцию xy. Предположим, что $x, y > 0$, а функция $b(x,y)$ удовлетворяет неравенству

$$b(x,y) \geqslant xy(xy+1). \tag{5.1}$$

Разделим $b(x,y)$ на xy с остатком:

$$b(x,y) = a(x,y) \cdot xy + r(x,y), \tag{5.2}$$

где $a(x,y)$ — целая часть, а $r(x,y)$ — остаток от деления $b(x,y)$ на xy. Далее разделим $r(x,y)$ на x с остатком:

$$r(x,y) = p(x,y)\cdot x + q(x,y),$$

где $0 \leqslant q(x,y) < x$. Так как $0 \leqslant r(x,y) < xy$, то $p(x,y) < y$. Следовательно, функцию $b(x,y)$ можно представить в виде

$$b(x,y) = a(x,y)\cdot xy + p(x,y)\cdot x + q(x,y). \tag{5.3}$$

Из неравенств (5.1) и $r(x,y) < xy$ следует, что $a(x,y) \geqslant xy$. Поэтому из (5.2) получаем

$$\left[\frac{b(x,y)}{a(x,y)}\right] = xy. \tag{5.4}$$

Функцию $b(x,y)$ мы выберем чуть позже, а пока заметим, что из (5.3) и неравенств

$$q(x,y) < x, \quad p(x,y) < y$$

вытекают соотношения

$$\left[\frac{b(x,y)}{x}\right] = a(x,y)\cdot y + p(x,y), \quad \left[\frac{[b(x,y)/x]}{y}\right] = a(x,y). \tag{5.5}$$

Таким образом, если выбрать в классе $[S]$ функцию $b(x,y)$ с условием (5.1), то на основании соотношений (5.4), (5.5) получим, что в класс $[S]$ входит функция, совпадающая с функцией xy при $x,y > 0$.

Чтобы обойти нежелательные случаи $x = 0$ и $y = 0$, определим сначала по указанной выше схеме не функцию xy, а функцию $(x+1)(y+1)$. В качестве функции $b(x,y)$, удовлетворяющей неравенству

$$b(x,y) \geqslant (x+1)(y+1)((x+1)(y+1)+1),$$

в классе $[S]$ можно выбрать, например, функцию 2^{x+y+3}. Имея теперь функцию $(x+1)(y+1)$, легко получить функцию xy:

$$xy = (x+1)(y+1) \dot{-} (x+y+1).$$

Для функции $\mathrm{rm}\,(x,y)$ имеем соотношение

$$\mathrm{rm}\,(x,y) = x \dot{-} [x/y]y.$$

Получим функцию x^y. Заметим, что для любых $x,y > 0$ справедливы соотношения

$$2^{xy+x+1} - x > x^y,$$

$$2^{(xy+x+1)y} = (x + 2^{xy+x+1} - x)^y = \sum_{i=0}^{y} \binom{y}{i} x^{y-i}(2^{xy+x+1} - x)^i.$$

Поэтому

$$x^y = \mathrm{rm}\,(2^{(xy+x+1)y}, 2^{xy+x+1} \dot{-} x).$$

Функция x^y определена данной формулой при всех $x,y \geqslant 0$. Из нее, в частности, следует, что $x^0 = 1$ при любом $x \geqslant 0$.

Рассмотрим биномиальные коэффициенты $\binom{x}{y}$. Чтобы не вводить ограничения $x \geqslant y$, будем рассматривать биномиальные коэффициенты вида $\binom{x+y}{x}$. Поскольку

$$(1+w)^{x+y} = 1 + \binom{x+y}{1}w + \ldots + \binom{x+y}{x-1}w^{x-1} + w^x \sum_{i=x}^{x+y} \binom{x+y}{i} w^{i-x},$$

а при $x + y \geqslant 1$ и любом $w \geqslant 2^{x+y}$ выполняются неравенства

$$1 + \binom{x+y}{1}w + \ldots + \binom{x+y}{x-1}w^{x-1} < w^x, \qquad \binom{x+y}{x} < 2^{x+y},$$

будем иметь

$$\binom{x+y}{x} = \mathrm{rm}\left(\left[\frac{(1+w)^{x+y}}{w^x} \right], w \right).$$

В частности,

$$\binom{x+y}{x} = \mathrm{rm}\left(\left[\frac{(1+2^{x+y})^{x+y}}{2^{x(x+y)}} \right], 2^{x+y} \right).$$

В дальнейшем, получая новые функции в классе $[S]$, мы не будем особо заботиться о значениях этих функций при некоторых выделенных значениях переменных. В самом деле, если, например, в классе $[S]$ получены функции $f(x,y)$, $g(y)$ и мы хотим «исправить» значения $f(1,y)$ на значения $g(y)$, то в классе $[S]$ достаточно образовать функцию

$$f(x,y) \cdot \mathrm{sg}\,|x-1| + g(y) \cdot \overline{\mathrm{sg}}\,|x-1|.$$

§ 5.2. Построение функций нод, $\exp_2$, σ

Пусть нод$\,(x,y)$ есть наибольший общий делитель чисел x, y, если $x + y > 0$, и нод$\,(0,0) = 0$; $\exp_2 x$ есть показатель числа 2 в разложении x на простые множители, если $x > 0$, и $\exp_2 0 = 0$. Через $\sigma(x)$ обозначаем функцию, равную числу единиц в двоичной записи x.

Лемма 5.1. *Пусть* $a, b > 0$. *Тогда* нод$\,(a,b)$ *равен числу решений уравнения*

$$ax = by, \tag{5.6}$$

удовлетворяющих неравенствам

$$1 \leqslant x \leqslant b, \quad 1 \leqslant y \leqslant a. \tag{5.7}$$

Доказательство. Уравнение (5.6), очевидно, эквивалентно уравнению

$$\frac{ax}{\text{нод}\,(a,b)} = \frac{by}{\text{нод}\,(a,b)}, \tag{5.8}$$

где коэффициенты

$$\frac{a}{\text{нод}\,(a,b)}, \quad \frac{b}{\text{нод}\,(a,b)}$$

взаимно просты. Нетрудно понять, что все решения уравнения (5.8) имеют вид
$$\left(\frac{bt}{\text{нод}\,(a,b)}, \frac{at}{\text{нод}\,(a,b)}\right),$$
где $t = 0, \pm 1, \pm 2, \ldots$ Решения уравнения (5.8), удовлетворяющие неравенствам (5.7), получаются при $t = 1, 2, \ldots, \text{нод}\,(a,b)$. Лемма доказана.

Для $a, b > 0$ положим
$$F(a,b) = \sum_{x=1}^{b}\sum_{y=1}^{a} 2^{ab(ax-by)}.$$

Лемма 5.2. *При любых $a, b > 0$ справедливо соотношение*
$$F(a,b) = \frac{(2^{a^2b(b+1)} - 2^{a^2b})(2^{a^2b^2} - 1)}{(2^{a^2b} - 1)(2^{ab^2} - 1)2^{a^2b^2}}. \tag{5.9}$$

Доказательство. Суммируя геометрические прогрессии, получаем
$$\sum_{x=1}^{b}\sum_{y=1}^{a} 2^{ab(ax-by)} =$$
$$= \sum_{x=1}^{b}\sum_{y=1}^{a} 2^{a^2bx}\cdot 2^{-ab^2y} = \sum_{x=1}^{b} 2^{a^2bx}\sum_{y=1}^{a} 2^{-ab^2y} = \sum_{x=1}^{b} 2^{a^2bx} \times$$
$$\times \left(\frac{2^{-ab^2} - 2^{-ab^2(a+1)}}{1 - 2^{-ab^2}}\right) = \left(\frac{2^{a^2b(b+1)} - 2^{a^2b}}{2^{a^2b} - 1}\right)\left(\frac{2^{-ab^2} - 2^{-ab^2(a+1)}}{1 - 2^{-ab^2}}\right) =$$
$$= \left(\frac{2^{a^2b(b+1)} - 2^{a^2b}}{2^{a^2b} - 1}\right)\left(\frac{1 - 2^{-a^2b^2}}{2^{ab^2} - 1}\right) = \frac{(2^{a^2b(b+1)} - 2^{a^2b})(2^{a^2b^2} - 1)}{(2^{a^2b} - 1)(2^{ab^2} - 1)2^{a^2b^2}}.$$
Лемма доказана.

Лемма 5.3. *Для любых $a, b > 0$ справедливо соотношение*
$$\text{нод}\,(a,b) = \mathrm{rm}\,([F(a,b)], 2^{ab}).$$

Доказательство. Положим
$$P(a,b) = \{(x,y):\ 1 \leqslant x \leqslant b,\ 1 \leqslant y \leqslant a,\ ax - by > 0\},$$
$$N(a,b) = \{(x,y):\ 1 \leqslant x \leqslant b,\ 1 \leqslant y \leqslant a,\ ax - by < 0\}.$$
Используя лемму 5.1, получаем
$$F(a,b) = \sum_{x=1}^{b}\sum_{y=1}^{a} 2^{ab(ax-by)} = \sum_{(x,y)\in P(a,b)} 2^{ab(ax-by)} + \text{нод}\,(a,b) +$$
$$+ \sum_{(x,y)\in N(a,b)} 2^{ab(ax-by)} < \sum_{(x,y)\in P(a,b)} 2^{ab(ax-by)} + \text{нод}\,(a,b) +$$
$$+ \sum_{(x,y)\in N(a,b)} 2^{-ab} < \sum_{(x,y)\in P(a,b)} 2^{ab(ax-by)} + \text{нод}\,(a,b) + 1.$$

Таким образом,

$$[F(a,b)] = \sum_{(x,y)\in P(a,b)} 2^{ab(ax-by)} + \text{нод}\,(a,b),$$

откуда непосредственно вытекает утверждение леммы.

Из формулы (5.9) видно, что операцию вычитания можно выполнить в пределах множества $\mathbb{N}$, т. е. с помощью функции $\dot{-}$. Применяя теперь лемму 5.3, получаем нод $\in [S]$.

Лемма 5.4. *Для любого $a > 0$ справедливо соотношение*

$$\exp_2 a = \left[\frac{\mathrm{rm}\,(\text{нод}\,(a, 2^a)^{a+1}, (2^{a+1}-1)^2)}{2^{a+1}-1}\right]. \tag{5.10}$$

Доказательство. Очевидно, что

$$\text{нод}\,(a, 2^a) = 2^{\exp_2 a}.$$

Используя далее биномиальное разложение, получаем

$$\begin{aligned}(2^{\exp_2 a})^{a+1} &= (2^{a+1})^{\exp_2 a} = \\ &= (1 + 2^{a+1} - 1)^{\exp_2 a} = \sum_{i=0}^{\exp_2 a} \binom{\exp_2 a}{i} (2^{a+1}-1)^i = \\ &= (2^{a+1}-1)^2 \sum_{i=2}^{\exp_2 a} \binom{\exp_2 a}{i} (2^{a+1}-1)^{i-2} + (2^{a+1}-1)\exp_2 a + 1,\end{aligned}$$

откуда справедливость леммы следует при $\exp_2 a \geqslant 1$. При $\exp_2 a = 0$ (в частности, при $a = 0$) формула (5.10) проверяется непосредственно. Лемма доказана.

Из теоремы Куммера (см. приложение 5.1) вытекает, что $\sigma(x) = \exp_2 \binom{2x}{x}$ при $x > 0$. Поэтому $\sigma \in [S]$.

§ 5.3. Однократные экзистенциальные представления предикатов

При рассмотрении предикатов на множестве $\mathbb{N}$ мы будем использовать логическую связку конъюнкцию и квантор существования. Нас будут интересовать представления предикатов $\rho(x_1, \ldots, x_n)$ в виде

$$(\exists z_1)\ldots(\exists z_r)((2^{z_1} = z_2)\ \&\ \ldots\ \&\ (2^{z_{2k-1}} = z_{2k})\ \& \\ \&\ (D(x_1, \ldots, x_n, z_1, \ldots, z_r) = 0)), \tag{5.11}$$

где $2k \leqslant r$ и D — полином с целыми коэффициентами, которое мы будем называть *экзистенциальным* представлением. Экзистенциальное представление (5.11) назовем *однократным*, если для любого набора $(a_1, \ldots, a_n)$, удовлетворяющего предикату (5.11), существует ровно один набор значений переменных $z_1, \dots, z_r$, который выполняет предикат (5.11).

Понятно, что для экзистенциального представления (5.11) можно найти (вообще говоря, неэффективным образом) такую всюду определенную функцию $w(x_1, \dots, x_n)$, что представление (5.11) будет эквивалентно представлению

$$(\exists z_1)_{z_1 \leqslant w(x_1,\dots,x_n)} \dots (\exists z_r)_{z_r \leqslant w(x_1,\dots,x_n)} ((2^{z_1} = z_2) \mathbin{\&} \dots \\ \dots \mathbin{\&} (2^{z_{2k-1}} = z_{2k}) \mathbin{\&} (D(x_1, \dots, x_n, z_1, \dots, z_r) = 0)) \quad (5.12)$$

(здесь значения переменных $z_1, \dots, z_r$ разыскиваются не во всем множестве $\mathbb{N}$, а только в его начальном отрезке $\{0, 1, \dots, w(x_1, \dots, x_n)\}$). В этом представлении вместо функции $w(x_1, \dots, x_n)$ можно взять, разумеется, любую бóльшую функцию $w'(x_1, \dots, x_n)$.

Далее нам понадобятся монотонные функции $w_l(x_1, \dots, x_n)$ специального вида:

$$w_1(x_1, \dots, x_n) = 2^{x_1 + \dots + x_n}, \quad w_{l+1}(x_1, \dots, x_n) = 2^{w_l(x_1,\dots,x_n)}.$$

С использованием функций w_l определим класс предикатов R: предикат ρ принадлежит классу R тогда и только тогда, когда ρ имеет однократное экзистенциальное представление (5.11), в котором переменные $z_1, \dots, z_r$ можно ограничить некоторой функцией $w_l(x_1, \dots, x_n)$ (т. е. при $w = w_l$ для предиката ρ имеет место однократное представление (5.12)).

Из определения класса R легко вывести, что R замкнут относительно операции конъюнкции. В самом деле, пусть предикаты $\rho_1(x_1, \dots, x_n)$, $\rho_2(x_1, \dots, x_n)$ класса R определяются формулами (в целях упрощения формул часть переменных опускаем)

$$(\exists z_1)_{z_1 \leqslant w_l} \dots (\exists z_r)_{z_r \leqslant w_l} ((2^{z_1} = z_2) \mathbin{\&} \dots \mathbin{\&} (2^{z_{2k-1}} = z_{2k}) \mathbin{\&} (D_1 = 0)),$$

$$(\exists v_1)_{v_1 \leqslant w_l} \dots (\exists v_p)_{v_p \leqslant w_l} ((2^{v_1} = v_2) \mathbin{\&} \dots \mathbin{\&} (2^{v_{2m-1}} = v_{2m}) \mathbin{\&} (D_2 = 0)),$$

где наборы переменных $\{z_1, \dots, z_r\}$ и $\{v_1 \dots, v_p\}$ не пересекаются. Тогда предикат

$$\rho_1(x_1, \dots, x_n) \mathbin{\&} \rho_2(x_1, \dots, x_n)$$

имеет однократное экзистенциальное представление

$$(\exists z_1)_{z_1 \leqslant w_l} \dots (\exists z_r)_{z_r \leqslant w_l} (\exists v_1)_{v_1 \leqslant w_l} \dots (\exists v_p)_{v_p \leqslant w_l} \& ((2^{z_1} = z_2) \mathbin{\&} \dots \\ \dots \mathbin{\&} (2^{z_{2k-1}} = z_{2k}) \mathbin{\&} (2^{v_1} = v_2) \mathbin{\&} \dots \mathbin{\&} (2^{v_{2m-1}} = v_{2m}) \mathbin{\&} (D_1^2 + D_2^2 = 0)).$$

(Нетрудно понять, что установленный факт будет верным и в том случае, когда отношения ρ_1, ρ_2 зависят от различных переменных.)

Лемма 5.5. *Пусть*

$$f(x_1,\dots,x_n)=g(h_1(x_1,\dots,x_n),\dots,h_m(x_1,\dots,x_n)),$$

предикаты

$$y=g(y_1,\dots,y_m),\quad y=h_1(x_1,\dots,x_n),\dots,y=h_m(x_1,\dots,x_n) \tag{5.13}$$

принадлежат классу R и каждая из функций $g,h_1,\dots,h_m$ ограничена сверху некоторой функцией типа w_l. Тогда предикат $y=$ $=f(x_1,\dots,x_n)$ принадлежит классу R.

Доказательство. Будем предполагать, что каждая из функций $h_1,\dots,h_m$ ограничена сверху одной и той же функцией w_i. Тогда справедлива эквивалентность

$$(y=f(x_1,\dots,x_n))\equiv(\exists y_1)_{y_1\leqslant w_i(x_1,\dots,x_n)}\dots(\exists y_m)_{y_m\leqslant w_i(x_1,\dots,x_n)}$$
$$((y_1=h_1(x_1,\dots,x_n))\,\&\dots\&\,(y_m=h_m(x_1,\dots,x_n))\,\&\,(y=g(y_1,\dots,y_m))),$$

в которой при выполнении равенства $y=f(x_1,\dots,x_n)$ значения переменных $y_1,\dots,y_m$ в пределах множества $\{0,1,\dots,w_i(x_1,\dots,x_n)\}$ находятся однозначно. Понятно, что в этой эквивалентности функцию w_i можно заменить любой большей функцией w_j. Далее для каждого из предикатов (5.13) строим соответствующее экзистенциальное представление в классе R, пользуемся замкнутостью класса R относительно операции конъюнкции, ограничениями для функций $g,h_1,\dots,h_m$, функциями типа w_l и тем, что суперпозиции функций типа w_l мажорируются функциями того же типа. Лемма доказана.

Теорема 5.1. *Если $f(x_1,\dots,x_n)\in[S]$, то предикат $y=$ $=f(x_1,\dots,x_n)$ принадлежит классу R.*

Доказательство. Проведем индукцию по построению функций в классе $[S]$. Рассмотрим исходные функции множества S. Имеем:

$$(y=x_1+x_2)\equiv(y-x_1-x_2=0),\quad (y=2^x)\equiv(y-2^x=0).$$

Последнюю формулу легко привести к стандартному виду (5.12) введением новых переменных z_1, z_2:

$$(y=2^x)\Leftrightarrow(\exists z_1)_{z_1\leqslant w_1(x)}(\exists z_2)_{z_2\leqslant w_1(x)}((2^{z_1}=z_2)\,\&$$
$$\&\,((x-z_1)^2+(y-z_2)^2=0)).$$

В дальнейшем подобные очевидные преобразования мы опускаем.

При рассмотрении функции $x_1 \dot{-} x_2$ используем логическую связку дизъюнкцию (которая не входит в заключительное выражение). Для отношения $y = x_1 \dot{-} x_2$ имеем следующую цепочку эквивалентностей:

$$\begin{aligned}
&(y = x_1 \dot{-} x_2) \equiv (x_1 \geqslant x_2) \mathbin{\&} (x_1 = x_2 + y) \vee (x_1 < x_2) \mathbin{\&} (y = 0) \equiv \\
&\equiv (\exists z_1)((x_1 = x_2 + z_1) \mathbin{\&} (x_1 = x_2 + y)) \vee (\exists z_2)((x_1 + z_2 + 1 = x_2) \mathbin{\&} (y = 0)) \equiv \\
&\equiv (\exists z)((x_1 - x_2 - z = 0) \& (x_1 - x_2 - y = 0) \vee (x_1 + z + 1 - x_2 = 0) \& (y = 0)) \equiv \\
&\equiv (\exists z)((x_1 - x_2 - z)^2 + (x_1 - x_2 - y)^2 = 0 \vee (x_1 + z + 1 - x_2)^2 + y = 0) \equiv \\
&\equiv (\exists z)(\{(x_1 - x_2 - z)^2 + (x_1 - x_2 - y)^2\} \cdot \{(x_1 + z + 1 - x_2)^2 + y\} = 0).
\end{aligned}$$

Последняя формула в этой цепочке дает однократное экзистенциальное представление предиката $y = x_1 \dot{-} x_2$, в котором переменную z можно ограничить, например, функцией $w_1(x_1, x_2)$.

Для функции $[x_1/x_2]$ нужное представление получим в два этапа. Сначала рассмотрим функцию $[x_1/(x_2 + 1)]$:

$$\begin{aligned}
&(y = [x_1/(x_2 + 1)]) \equiv ((x_2 + 1)y \leqslant x_1) \mathbin{\&} ((x_2 + 1)(y + 1) > x_1) \equiv \\
&\equiv (\exists z_1)_{z_1 \leqslant w_1(x_1, x_2)} (\exists z_2)_{z_2 \leqslant w_1(x_1, x_2)} (((x_2 + 1)y + z_1 = x_1) \mathbin{\&} \\
&\qquad \mathbin{\&} ((x_2 + 1)(y + 1) = x_1 + z_2 + 1)).
\end{aligned}$$

Далее имеем

$$[x_1/x_2] \equiv [x_1/((x_2 \dot{-} 1) + 1)]$$

(напомним, что $[x/0] = x$). Доказательство теоремы завершаем обращением к лемме 5.5.

§ 5.4. Суммирование экспоненциально полиномиальных выражений

Лемма 3.6. *Пусть числа $v_0, \ldots, v_s, w$ удовлетворяют неравенствам*

$$0 \leqslant v_0, \ldots, v_s < 2^w \tag{5.14}$$

и q — количество нулей в последовательности $v_0, \ldots, v_s$. Тогда

$$\sigma\biggl(\sum_{i \leqslant s} (2^{2w} - 2^w v_i + v_i - 1) 2^{2wi}\biggr) = w(s + 1 + q). \tag{5.15}$$

Доказательство. Из неравенств (5.14) вытекает, что при любом $i \leqslant s$ выполняются соотношения

$$0 \leqslant 2^{2w} - 2^w v_i + v_i - 1 < 2^{2w}.$$

Поэтому в выражении

$$\sum_{i \leqslant s} (2^{2w} - 2^w v_i + v_i - 1) 2^{2wi}$$

числа

$$2^{2w} - 2^w v_i + v_i - 1$$

можно рассматривать как «цифры» в позиционной системе счисления с основанием 2^{2w}. Отсюда сразу следует, что

$$\sigma\Bigg(\sum_{i\leqslant s}(2^{2w} - 2^w v_i + v_i - 1)2^{2wi}\Bigg) = \sum_{i\leqslant s}\sigma(2^{2w} - 2^w v_i + v_i - 1).$$

Если $v_i = 0$, то, очевидно,

$$\sigma(2^{2w} - 2^w v_i + v_i - 1) = 2w.$$

В противном случае

$$\sigma(2^{2w} - 2^w v_i + v_i - 1) = \sigma(2^w - v_i) + \sigma(v_i - 1) = w,$$

поскольку двоичное представление числа $2^w - v_i$ получается из двоичного представления числа v_i сохранением младших двоичных разрядов вплоть до первого единичного разряда и инвертированием остальных двоичных разрядов вплоть до w-го, а двоичное представление числа $(v_i - 1)$ — из двоичного представления v_i инвертированием младших разрядов вплоть до первого единичного разряда и сохранением остальных двоичных разрядов. Отсюда вытекает доказываемое равенство (5.15).

Лемма 5.7. *Пусть $D(x_1, \ldots, x_n, z_1, \ldots, z_r)$ — полином с целыми коэффициентами и $d(x_1, \ldots, x_n, t)$ есть число наборов $(z_1, \ldots, z_r)$, принадлежащих кубу*

$$0 \leqslant z_1, \ldots, z_r \leqslant t \tag{5.16}$$

и удовлетворяющих отношению

$$(2^{z_1} = z_2)\,\&\ldots\&\,(2^{z_{2k-1}} = z_{2k})\,\&\,(D(x_1, \ldots, x_n, z_1, \ldots, z_r) = 0),$$

где $2k \leqslant r$. Тогда функция d принадлежит классу $[S]$.

Доказательство. Положим

$$E(x_1, \ldots, x_n, z_1, \ldots, z_r) = \\ = (2^{z_1} - z_2)^2 + \ldots + (2^{z_{2k-1}} - z_{2k})^2 + D^2(x_1, \ldots, x_n, z_1, \ldots, z_r).$$

Функция E неотрицательна, и, очевидно, $d(x_1, \ldots, x_n, t)$ равно числу решений уравнения

$$E(x_1, \ldots, x_n, z_1, \ldots, z_r) = 0,$$

лежащих в кубе (5.16). Мы хотим применить лемму 5.6 к последовательности значений функции E, принимаемых ею в кубе (5.16). С этой целью положим (см. сумму в левой части равенства (5.15))

$$F(x_1, \ldots, x_n, t, w) = \sum_{0\leqslant z_1,\ldots,z_r\leqslant t}(2^{2w} - 1 - (2^w - 1)E(x_1, \ldots, x_n, z_1, \ldots, z_r)) \times \\ \times 2^{2w(z_1(t+1)^{r-1} + z_2(t+1)^{r-2} + \ldots + z_{r-1}(t+1) + z_r)}. \tag{5.17}$$

Если выбрать величину w так, чтобы в кубе (5.16) выполнялось неравенство
$$E(x_1, \dots, x_n, z_1, \dots, z_r) < 2^w, \tag{5.18}$$

то на основании леммы 5.6 будем иметь

$$\sigma(F(x_1, \dots, x_n, t, w)) = w((t+1)^r + 1 + d(x_1, \dots, x_n, t)),$$

откуда

$$d(x_1, \dots, x_n, t) = \left[\frac{\sigma(F(x_1, \dots, x_n, t, w))}{w}\right] \dot{-} ((t+1)^r + 1).$$

Поскольку переменные $z_1, \dots, z_r$ удовлетворяют неравенствам (5.16), для выполнения неравенства (5.18) значение w можно выбрать как функцию (от переменных $x_1, \dots, x_n, t$), принадлежащую классу $[S]$. Следовательно, чтобы завершить доказательство леммы, достаточно показать, что функция F принадлежит классу $[S]$.

Учитывая структуру функции E, сумму, стоящую в правой части равенства (5.17), можно представить как конечную линейную комбинацию (с коэффициентами — полиномами от переменных $x_1, \dots, x_n$) сумм вида
$$\sum_{z_1 \leqslant t} \dots \sum_{z_r \leqslant t} z_1^{i_1} \dots z_r^{i_r} 2^{z_1 p_1(t,w) + \dots + z_r p_r(t,w)}, \tag{5.19}$$

где $i_1, \dots, i_r$ — натуральные числа, а $p_1, \dots, p_r$ — полиномы с натуральными коэффициентами. Сумму (5.19) можно далее переписать в виде

$$\prod_{k=1}^{r} \sum_{z_k \leqslant t} z_k^{i_k} 2^{z_k p_k(t,w)}. \tag{5.20}$$

Для сумм вида
$$\sum_{z \leqslant t} z^i q^z$$

в комбинаторике (см. приложение 5.2) хорошо известны формулы типа

$$\frac{Q_i(q, q^t, t)}{(q-1)^{i+1}},$$

где Q_i — полином с целыми коэффициентами. Таким образом, сумма (5.19), равная (5.20), также будет представима в виде произведения выражений типа
$$\frac{Q_{i_k}(2^{p_k(t,w)}, 2^{t p_k(t,w)}, t)}{(2^{p_k(t,w)} - 1)^{i_k+1}}.$$

Остается заметить, что во всех приведенных выше формулах вычитание можно выполнить в пределах множества $\mathbb{N}$, т. е. с помощью функции $\dot{-}$.

Теорема 5.2. *Пусть функция* $f(x_1, \ldots, x_n)$ *удовлетворяет условию*
$$\max_{i_1 \leqslant x_1, \ldots, i_n \leqslant x_n} f(i_1, \ldots, i_n) \leqslant w_l(x_1, \ldots, x_n), \tag{5.21}$$
предикат $y = f(x_1, \ldots, x_n)$ *принадлежит классу* R *и*
$$g(x_1, \ldots, x_n) = \sum_{i \leqslant x_n} f(x_1, \ldots, x_{n-1}, i).$$
Тогда $g \in [S]$.

Доказательство. В самом деле, учитывая неравенство (5.21), заключаем, что величина $g(x_1, \ldots, x_n)$ равна числу троек (i, j, y), принадлежащих кубу
$$0 \leqslant i, j, y \leqslant w_l(x_1, \ldots, x_n)$$
и удовлетворяющих предикату
$$(i \leqslant x_n) \,\&\, (y = f(x_1, \ldots, x_{n-1}, i)) \,\&\, (j < y).$$
Очевидно также, что $g(x_1, \ldots, x_n)$ будет равна числу пятерок (i, i_1, j, j_1, y) из куба
$$0 \leqslant i, i_1, j, j_1, y \leqslant w_l(x_1, \ldots, x_n),$$
которые удовлетворяют предикату
$$(i + i_1 = x_n) \,\&\, (y = f(x_1, \ldots, x_{n-1}, i)) \,\&\, (j + j_1 + 1 = y). \tag{5.22}$$
Пользуясь далее принадлежностью предиката $y = f(x_1, \ldots, x_{n-1}, i)$ классу R, получаем его однократное экзистенциальное представление:
$$\begin{aligned}(y = f(x_1, \ldots, x_{n-1}, i)) \equiv \\ \equiv (\exists z_1) \ldots (\exists z_r)((2^{z_1} = z_2) \,\&\, \ldots \,\&\, (2^{z_{2k-1}} = z_{2k}) \,\&\, \\ \&\, (D(x_1, \ldots, x_{n-1}, i, y, z_1, \ldots, z_r) = 0)).\end{aligned} \tag{5.23}$$
Будем предполагать, что число l с самого начала выбрано так, что при $i \leqslant x_n$ переменные $z_1, \ldots, z_r$ в представлении (5.23) можно ограничить функцией $w_l(x_1, \ldots, x_n)$ (ввиду соотношения (5.21) функцию w_l считаем зависящей только от переменных $x_1, \ldots, x_n$). Тогда из (5.22), (5.23) следует, что $g(x_1, \ldots, x_n)$ есть число решений системы уравнений
$$\begin{aligned}(2^{z_1} = z_2) \,\&\, \ldots \,\&\, (2^{z_{2k-1}} = z_{2k}) \,\&\, ((x_n - i - i_1)^2 + (y - j - j_1 - 1)^2 + \\ + D^2(x_1, \ldots, x_{n-1}, i, y, z_1, \ldots, z_r) = 0),\end{aligned}$$
заключенных в кубе
$$0 \leqslant i, i_1, j, j_1, y, z_1, \ldots, z_r \leqslant w_l(x_1, \ldots, x_n).$$
Теперь применяем лемму 5.7. Теорема доказана.

Напомним, что в гл. II мы обозначили через $\mathbf{K}'$ наименьший класс функций, который содержит функции $x+1$, $x \dot{-} y$, 2^x, I и замкнут относительно операций суперпозиции и ограниченного суммирования. В утверждении 2.13 было доказано, что класс $\mathbf{K}'$ совпадает с классом $\mathbf{K}$.

Теорема 3.3. *Базис по суперпозиции в классе* $\mathbf{K}$ *образует система функций* S.

Доказательство. Включение $[S] \subseteq \mathbf{K}$ очевидно. При доказательстве обратного включения воспользуемся равенством $\mathbf{K} = \mathbf{K}'$. В теореме 5.1 установлено, что для всякой функции $f(\widetilde{x})$ из $[S]$ (в частности, для любой исходной функции класса $\mathbf{K}'$) предикат $y = f(\widetilde{x})$ принадлежит классу R. Множество $[S]$ по определению замкнуто относительно операции суперпозиции, а теорема 5.2 показывает, что оно также замкнуто относительно операции ограниченного суммирования. Таким образом, $\mathbf{K}' \subseteq [S]$, и теорема доказана.

Следствие. *Базис по суперпозиции в классе* $\mathbf{K}$ *образует система функций*
$$x+y,\ x^2,\ \mathrm{rm}\,(x,y),\ 2^x \tag{5.24}$$

Доказательство. Достаточно установить, что суперпозициями функций системы (5.24) можно получить функции $x \dot{-} y$ и $[x/y]$.

Имеем:
$$0 = \mathrm{rm}\,(x,x), \quad 1 = 2^0, \quad \overline{\mathrm{sg}}\,(x) = \mathrm{rm}\,(2^x,2), \quad x \cdot \overline{\mathrm{sg}}\,(y) = \mathrm{rm}\,(x, \mathrm{sg}\,(y))$$
(напомним, что $\mathrm{rm}\,(x,0) = x$).

Положим
$$f(x,y) = \mathrm{rm}\,(2^{x+y}+x, 2^{x+y}+y).$$
Тогда
$$f(x,y) = \begin{cases} x-y, & \text{если } x \geqslant y, \\ 2^{x+y}+x & \text{в противном случае.} \end{cases}$$
Поскольку
$$\mathrm{rm}\,(2^x,2^y) = \begin{cases} 0, & \text{если } x \geqslant y, \\ 2^x & \text{в противном случае,} \end{cases}$$
получаем
$$x \dot{-} y = \mathrm{rm}\,(f(x,y), \mathrm{sg}\,(\mathrm{rm}\,(2^x,2^y))).$$
Далее имеем
$$2xy = ((x+y)^2 \dot{-} x^2) \dot{-} y^2.$$
При $y > 0$ справедливо равенство
$$[x/y] = \mathrm{rm}\,(2(x+1)(x \dot{-} \mathrm{rm}\,(x,y)), 2(x+1)y \dot{-} 1).$$
Согласно нашему определению функция $[x/y]$ должна быть равна x при $y = 0$. Поэтому полученную функцию $[x/y]$ следует сложить с функцией $x \cdot \overline{\mathrm{sg}}(y)$. Следствие доказано.

Чтобы достаточно полно оценить значение полученного результата, приведем еще одно определение класса $\mathbf{K}$. Оно не столь конкретно, как имеющиеся в гл. II индуктивные определения. Скорее, оно в содержательных терминах описывает объем класса $\mathbf{K}$. Итак, пусть имеется некоторый класс $\{\mathcal{M}\}$ универсальных абстрактных вычислительных устройств (машин), которые позволяют вычислять произвольные частично рекурсивные функции. Это могут быть, например, машины Тьюринга различного типа (в частности, машины Минского), машины с произвольным доступом к памяти, машины типа SRM, нормальные алгорифмы Маркова и т. п. И пусть для вычислений на машинах класса $\{\mathcal{M}\}$ определены понятия времени вычисления и объема памяти. Тогда $\mathbf{K}$ можно определить как класс всех всюду определенных функций, которые вычислимы на машинах из $\{\mathcal{M}\}$ за время (или с объемом памяти), не превосходящее некоторой функции w_l.

Комментарии. Идея о порождении класса $\mathbf{K}$ системой функций S высказана в [18]. Принадлежность функции σ множеству $[S]$ установлена С. Маззанти [39]. Приведенное выше доказательство теоремы 3.3 появилось в [24].

Приложение 5.1. Биномиальные коэффициенты и теорема Куммера

Как известно, для любых x, y и любого натурального n справедливо равенство
$$(x+y)^n = \sum_{m=0}^{n} \binom{n}{m} x^m y^{n-m},$$
где $\binom{n}{m}$ — биномиальный коэффициент:
$$\binom{n}{m} = \frac{n!}{m!(n-m)!},$$
$n! = n(n-1)\cdot\ldots\cdot 1,\ 0! = 1.$

Для простого числа p обозначим через $\exp_p n$ показатель степени числа p в разложении n на простые множители.

Теорема Куммера. *Если p — простое число, то показатель*
$$\exp_p \binom{m+n}{m}$$
равен количеству переносов из разряда в разряд при сложении m и n в позиционной системе счисления с основанием p.

Доказательство. Из соотношения
$$\binom{m+n}{m} = \frac{(m+n)!}{m!n!}$$

следует, что

$$\exp_p \binom{m+n}{m} = \exp_p((m+n)!) - \exp_p(m!) - \exp_p(n!).$$

Однако

$$\exp_p(k!) = \left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \ldots,$$

поскольку среди чисел $1, 2, \ldots, k$ ровно $\left[\frac{k}{p}\right]$ делятся на p, ровно $\left[\frac{k}{p^2}\right]$ делятся на p^2, и т. д. Поэтому

$$\exp_p \binom{m+n}{m} = \sum_{k \geqslant 1} \left(\left[\frac{m+n}{p^k}\right] - \left[\frac{m}{p^k}\right] - \left[\frac{n}{p^k}\right] \right).$$

Остается заметить, что в этой сумме каждое слагаемое равно 1 или 0 в зависимости от того, происходит ли перенос из $(k-1)$-го разряда в k-й или нет. Теорема доказана.

Приложение 5.2. Суммирование обобщенной геометрической прогрессии

Пусть

$$G_n(q,t) = \sum_{i=0}^{t} i^n \cdot q^i \qquad (q > 1). \tag{5.25}$$

$G_0(q,t)$ есть обычная геометрическая прогрессия и потому

$$G_0(q,t) = \frac{q^{t+1}-1}{q-1}.$$

Докажем по индукции, что для любого $n \geqslant 0$ имеется полином P_n с целыми коэффициентами такой, что

$$G_n(q,t) = \frac{P_n(q, q^t, t)}{(q-1)^{n+1}}.$$

Базис индукции рассмотрен выше. Подставим теперь $t+1$ вместо t в (5.25) и продифференцируем по q:

$$\frac{\partial}{\partial q} G_n(q, t+1) = \sum_{i=0}^{t+1} i^{n+1} \cdot q^{i-1} = \sum_{i=0}^{t} (i+1)^{n+1} \cdot q^i =$$
$$= \sum_{i=0}^{t} \sum_{j=0}^{n+1} \binom{n+1}{j} i^j \cdot q^i = \sum_{j=0}^{n+1} \binom{n+1}{j} G_j(q,t).$$

Полиномы P_n можно теперь найти на основе рекуррентного соотношения

$$G_{n+1}(q,t) = \frac{\partial}{\partial q} G_n(q,t+1) - \sum_{j=0}^{n} \binom{n+1}{j} G_j(q,t).$$

Комментарии. Впервые «явный» базис по суперпозиции в классе $\mathbf{K}$ построен Ч. Парсонсом [40]. В [17, 18] число функций в базисе удалось довести до 4, а сами функции были существенно упрощены. Кроме того, была предложена новая идея построения конечных базисов по суперпозиции, которая впоследствии привела к появлению базиса S. Технические леммы 5.1–5.4 доказаны С. Маззанти [39]. Идея рассмотрения однократных экспоненциально диофантовых представлений перечислимых предикатов принадлежит Ю.В. Матиясевичу [27]. Использовать однократные экзистенциальные представления предикатов в качестве основного средства при построении конечных базисов в классе $\mathbf{K}$ предложено в [24]. Из этой работы заимствовано также доказательство основного результата главы V. Лемма 5.6 установлена Ю.В. Матиясевичем [28].

Список литературы

1. *Бельтюков А. П.* Итеративное описание класса $\mathcal{E}^1$ иерархии Гжегорчика // Зап. научн. сем. ЛОМИ. 1976. Т. 66. С. 3–14.
2. *Бельтюков А. П.* Максимальная последовательность классов, преобразуемых примитивной рекурсией в данный класс // Зап. научн. сем. ЛОМИ. 1977. Т. 68. С. 3–18.
3. *Бельтюков А. П.* Машинное описание и иерархия начальных классов Гжегорчика // Зап. научн. сем. ЛОМИ. 1979. Т. 88. С. 30–46.
4. *Виноградов А. К.*, *Косовский Н. К.* Иерархия диофантовых представлений примитивно рекурсивных предикатов // Вычисл. техника и вопр. кибернетики. Вып. 12. — Л.: ЛГУ, 1975. — С. 99–107.
5. *Волков С. А.* Пример простой квазиуниверсальной функции в классе $\mathcal{E}^2$ иерархии Гжегорчика // Дискр. матем. 2006. Т. 18, № 4. С. 31–44.
6. *Гжегорчик А.* Некоторые классы рекурсивных функций // Проблемы математической логики. — М.: Мир, 1970. — С. 9–49.
7. *Косовский Н. К.* Возможности операций одноместного суммирования и одноместного ограниченного умножения // Зап. научн. сем. ЛОМИ. 1975. Т. 49. С. 3–6.
8. *Косовский Н. К.* О классах функций, определимых с помощью операции суммирования // Вычисл. техника и вопр. кибернетики. Вып. 14. — Л.: ЛГУ, 1978. — С. 54–60.
9. *Косовский Н. К.* Элементы математической логики и ее приложения к теории субрекурсивных алгоритмов. — Л.: ЛГУ, 1981.
10. *Косовский Н. К.* Основы теории элементарных алгоритмов. — Л.: ЛГУ, 1987.
11. *Кузнецов А. В.* К теореме о канонической форме для ординально-рекурсивных функций // *Гудстейн Р. Л.* Математическая логика. — М.: ИЛ, 1961. — С. 149–154.
12. *Мальцев А. И.* Итеративные алгебры и многообразия Поста // Алгебра и логика. 1966. Т. 5, № 2. С. 5–24.
13. *Мальцев А. И.* Итеративные алгебры Поста. — Новосибирск: НГУ, 1976.
14. *Марченков С. С.* Устранение схем рекурсий в классе $\mathcal{E}^2$ Гжегорчика // Матем. заметки. 1969. Т. 5, № 5. С. 561–568.
15. *Марченков С. С.* Об ограниченных рекурсиях // Math. Balkanica. 1972. Т. 2. С. 124-142.
16. *Марченков С. С.* О функциях, элементарных по Сколему // Матем. заметки. 1975. Т. 17, № 1. С. 133-141.
17. *Марченков С. С.* Об одном базисе по суперпозиции в классе функций, элементарных по Кальмару // Матем. заметки. 1980. Т. 27, № 3. С. 321–332.

18. *Марченков С.С.* Простые примеры базисов по суперпозиции в классе функций, элементарных по Кальмару // Banach Cent. Publ. 1989. T. 25. C. 119–126.
19. *Марченков С.С.* О представлении словарных предикатов из арифметической иерархии // Дискр. матем. 1990. Т. 2, № 1. С. 87–93.
20. *Марченков С.С.* Базисы по суперпозиции в классах рекурсивных функций // Математические вопросы кибернетики. Вып. 3. — М.: Наука, 1991. — С. 115–139.
21. *Марченков С.С.* О сложности вычисления рудиментарных предикатов // Дискр. матем. 2000. Т. 12, № 4. С. 83–98.
22. *Марченков С.С.* Позитивные ВЕ-представления словарных предикатов // Дискр. анализ и исслед. опер. Сер. 1. 2001. Т. 8, № 4. С. 68–75.
23. *Марченков С.С.* Элементарные рекурсивные функции. М.: МЦНМО, 2003.
24. *Марченков С.С.* Суперпозиции элементарных арифметических функций // Дискр. анализ и исслед. опер. Сер. 1. 2006. Т. 13, № 4. С. 33–48.
25. *Марченков С.С.* О сложности класса $\mathcal{E}^2$ Гжегорчика // Дискр. матем. 2010. Т. 22, № 1. С. 5–16.
26. *Марченков С.С.* Об элементарных словарных функциях, получаемых на основе ограниченной префиксной конкатенации // Дискр. матем. 2015. Т. 27, № 3. С. 44–55.
27. *Матиясевич Ю.В.* Новое доказательство теоремы об экспоненциально диофантовом представлении перечислимых предикатов // Зап. научн. сем. ЛОМИ. 1976. Т. 60. С. 75–92.
28. *Матиясевич Ю.В.* Один класс критериев простоты, формулируемых в терминах делимости биномиальных коэффициентов // Зап. научн. сем. ЛОМИ. 1977. Т. 67. С. 167–183.
29. *Минский М.* Вычисления и автоматы. — М., Мир, 1971.
30. *Непомнящий В.А.* Рудиментарная интерпретация двуленточных тьюринговых вычислений // Кибернетика. 1970. № 2. С. 29–35.
31. *Непомнящий В.А.* Рудиментарные предикаты и тьюринговы вычисления // ДАН СССР. 1970. Т. 195, № 2. С. 282–284.
32. *Непомнящий В.А.* Рудиментарное моделирование недетерминированных тьюринговых вычислений // Кибернетика. 1973. № 2. С. 23–29.
33. *Пахомов С.В.* Доказательство несовпадения классов простых примитивно рекурсивных функций // Зап. научн. сем. ЛОМИ. 1977. Т. 68. С. 115–122.
34. *Смальян Р.* Теория формальных систем. — М.: Наука, 1981.
35. *Хмелевский Ю.И.* Уравнения в свободной полугруппе // Тр. МИАН СССР. 1971. Т. 107. С. 3–288.
36. *Allender E.*, *Gore V.* Rudimentary reductions revisited // Inform. Process. Letters. 1991. V. 40, No. 2. P. 89–95.
37. *Atserias A.* The descriptive complexity of the fixed-points of bounded formulas // Lect. Notes Comput. Sci. 2000. V. 1862. P. 172–186.
38. *Kalmár L.* Egyszerű példa eldönthetetlen aritmetikai problémára // Matematikai és Fizikai Lapok. 1943. Köt. 50. Ol. 1–23.
39. *Mazzanti S.* Plain bases for classes of primitive recursive functions // Math. Logic Quart. 2002. V. 48, Is. 1. P. 93–104.

40. *Parsons Ch*. Hierarchies of primitive recursive functions // Z. math. Logik u. Grundlag. Math. 1968. Bd. 14, No. 4. S. 357–376.
41. *Quine W*. Concatenation as a basis for arithmetic // J. Symb. Logic. 1946. V. 11, Is. 4. P. 105–114.
42. *Rödding D*. Über die Eliminierbarkeit von Definitionsschemata in der Theorie der rekursiven Funktionen // Z. math. Logik u. Grundlag. Math. 1964. Bd. 10, No. 4. S. 315–330.
43. *Skolem Th*. Proof of some theorems on recursively enumerable sets // Notre Dame J. Formal Logic. 1962. V. 3, No. 2. P. 65–74.
44. *Volger H*. The role of rudimentary relations in complexity theory // Mém. Soc. Math. France. Sér. 2. 1984. V. 16. P. 41–51.
45. *Wrathall C*. Rudimentary predicates and relative computability // SIAM J. Comp. 1978. V. 7, No. 2. P. 194–209.

Предметный указатель