# Глава 4

# Кодиране

## 4.1 Изчислими функции

В тази глава, освен ако не е казано друго, ще говорим за функции, множества и релации от естествени числа. С $I_k^n$, $1 \leqslant k \leqslant n$ ще означаваме функцията $I_k^n : \mathbb{N}^n \to \mathbb{N}$, действаща по правилото

$$I_k^n(a_1, \ldots, a_n) = a_k.$$

Ако $\ldots x \ldots$ е израз за естествени числа, който е верен за поне едно $x$, то с

$$\mu x[\ldots x \ldots]$$

ще означаваме най-малкото естествено число, за което израза $\mu x[\ldots x \ldots]$ е верен.

Ако $P \subseteq \mathbb{N}^n$ е $n$-местна релация, ще пишем $P(a_1, \ldots, a_n)$ вместо $(a_1, \ldots, a_n) \in P$. $P$ ще разглеждаме като предикат, т.е. изображение, съпоставящо на $(a_1, \ldots, a_n)$ истина или лъжа. С $K_P$ ще означаваме функцията $K_P : \mathbb{N}^n \to \mathbb{N}$, действаща по правилото

$$K_P(a_1, \ldots, a_n) = \begin{cases} 1, & P(a_1, \ldots, a_n), \\ 0, & \neg P(a_1, \ldots, a_n). \end{cases}$$

Ще казваме, че една функция е изчислима, ако тя може да се получи от функциия $I_k^n$, $1 \leqslant k \leqslant n$, $+$, $.$, $K_<$ чрез краен брой суперпозииции и прилагане на $\mu$-оператори. Така

**C1.** Функциите $I_k^n$, $1 \leqslant k \leqslant n$, $+$, $.$, $K_<$ са изчислими.

**C2.** Ако $F$ е $k$-местна функция изчислима функция, а $G_1, \ldots, G_k$ са изчислими $n$-местни функции, то функцията $H : \mathbb{N}^n \to \mathbb{N}$, действаща по правилото

$$H(\overline{a}) = F(G_1(\overline{a}), \ldots, G_k(\overline{a})).$$

също е изчислима.

**C3.** Ако $G$ е $n+1$ местна изчислима функция и $\forall \overline{a} \exists x (G(\overline{a}, x) = 1)$, то $n$-местната функция $F$, действаща по правилото

$$F(\overline{a}) = \mu x[G(\overline{a}, x) = 1]$$

също е изчислима.

Ще казваме, че предикатът $P$ е изчислим, ако $K_P$ и изчислима функция. Ще допълним горния списък с правила за получаване на изчислими функции, които могат да се получат от C1, C2 и C3.

**C4.** Ако $Q$ е изчислим, $k$-местен предикат и $F_1, \ldots F_k$ са $n$-местни изчислими функции, то $n$ местната релация $P$, дефинирана чрез

$$P(\overline{a}) \iff Q(F_1(\overline{a}), \ldots, F_k(\overline{a}))$$

също е изчислима.

*Доказателство.*

$$K_P(\overline{a}) = K_Q(F_1(\overline{a}), \ldots, F_k(\overline{a})).$$

□

**C5.** Ако $P$ е $n+1$-местен изчислим предикат, такъв че $\forall\overline{a}\exists x P(\overline{a},x)$, то $n$-местната функция $F$, действаща по правилото

$$F(\overline{a}) = \mu x[P(\overline{a},x)]$$

също е изчислима.

*Доказателство.*

$$F(\overline{a}) = \mu x[K_P(\overline{a},x) = 1].$$

□

Дефиниции от вида $F(\overline{a}) = \ldots$ и $P(\overline{a}) \iff$ ____, където $\ldots$ и ____ са изрази, съдържащи само вече дефинирани символи, ще наричаме явни дефиниции. Нека например $F$ е дефинирана чрез

$$F(a_1,a_2,a_3) = G(a_1, G(H(a_2),a_1)),$$

където $G$ и $H$ са изчислими функции (дефинирани преди това). Нека

$$\begin{aligned} F_1(a_1,a_2) &= H(I^2_2(a_1,a_2)); \\ F_2(a_1,a_2) &= G(F_1(a_1,a_2), I^2_1(a_1,a_2)). \end{aligned}$$

Тогава $F_1, F_2$ са изчислими и

$$F(a_1,a_2) = G(I^2_1(a_1,a_2), F_2(a_1,a_2))$$

и значи $F$ също е изчислима.

Нека сега $P$ е дефинирано чрез

$$P(a_1,a_2) \iff Q(a_1, \mu x R(x, F(a_2)),$$

където $F$, $Q$ и $R$ са изчислими и $\forall a_2 \exists x R(x,F(a_2))$. Нека

$$\begin{aligned} F_1(a_1,a_2,x) &= F(I^3_2(a_1,a_2,x)); \\ R_1(a_1,a_2,x) &\iff R(I^3_3(a_1,a_2,x), F_1(a_1,a_2,x)). \end{aligned}$$

Тогава $F_1$ и $R_1$ са изчислими, като при това $\forall a_1 \forall a_2 \exists x R_1(a_1,a_2,x)$ (защото $R_1(a_1,a_2,x) \leftrightarrow R(x,F(a_2)))$. Оттук

$$F_2(a_1,a_2) = \mu x R_1(a_1,a_2,x)$$

е изчислима. Тогава

$$P(a_1,a_2) \iff Q(I^2_1(a_1,a_2), F_2(a_1,a_2))$$

и следователно $P$ е изичислим.

В общия случай, ако една функция или предикат е дефинирана чрез явна дефиниция, в която участват само променливи, (символи за) изчислими функии и предикати, и $\mu$-оператори (приложени, така че резултатът да бъде тотална функция), то тя е изчислима.

**C6.** Константните функции са изчислими.

*Доказателство.* Нека $n > 0$ и нека с $\kappa_m$ означим $n$-местните функции, даващи $m$ за всяка стойност на аргументите си. Тогава

$$\kappa_1(\overline{a}) = \mu x[I^{n+1}_{n+1}(\overline{a},x) = 1]$$

и значи $\kappa_1$ е изчислима. Имаме

$$\kappa_0(\overline{a}) = \mu x[x < \kappa_1(\overline{a})]$$

и следователно $\kappa_0$ е изчислима. Нека сега $\kappa_m$ е изчислима. Тогава

$$\kappa_{m+1}(\overline{a}) = \mu x[\kappa_m(\overline{a}) < x]$$

и значе $\kappa_{m+1}$ също е изчислима.

□

**Забележка.** Можем да използваме константи в явни дефиниции.

**C7.** Нека $P$ и $Q$ са изчислими предикати. Тогава $\neg P$, $P \vee Q$, $P \mathbin{\&} Q$, $P \to Q$, $P \leftrightarrow Q$ са изчислими.

*Доказателство.* Имаме $K_{\neg P}(\overline{a}) = K_<(K_P(\overline{a}),1)$ и $K_{P \mathbin{\&} Q}(\overline{a}) = K_P(\overline{a})K_Q(\overline{a})$.

□

**Забележка.** Можем да използваме $\neg$, $\vee$, $\&$, $\to$ и $\leftrightarrow$ в явни дефиниции.

**C8.** Предикатите $<$, $\leqslant$, $\geqslant$, $>$ и $=$ са изчислими.

*Доказателство.* Релацията $<$ е изчислима по условие. Имаме

$$\begin{aligned} a \leqslant b &\iff \neg(b < a); \\ a > b &\iff b < a \\ a \geqslant b &\iff b \leqslant a \\ a = b &\iff (a \leqslant b)\ \&\ (b \leqslant a). \end{aligned}$$

□

Ако $\ldots$ е израз, приемащ стойност естествено число, а изразът $\_\_\_\_x\_\_\_\_$ е формула, то с $\mu x_{x<\ldots}[\_\_\_\_x\_\_\_\_]$ ще означаваме израза $\mu x[\_\_\_\_x\_\_\_\_ \vee x = \ldots]$. Ще казваме, че $\mu x_{x<\ldots}$ е ограничен $\mu$ оператор.

**C9.** Ако $P$ е $n+1$-местен изчислим предикат, то $n+1$-местната функция $F$, дефинирана чрез

$$F(b, \overline{a}) = \mu x_{x<b} P(\overline{a}, x)$$

е изчислима.

*Доказателство.* Предикатът $P(\overline{a}, x) \vee x = b$ е изчислим и $\forall b \forall \overline{a} \exists x (P(\overline{a}, x) \vee x = b)$.

□

**Забележка.** Можем да използваме ограничени $\mu$-оператори в явни дефиниции.

Нека отново $\ldots$ е израз, приемащ стойност естествено число, а изразът $\_\_\_\_x\_\_\_\_$ е формула. Дефинираме

$$\begin{aligned} \exists x_{x<\ldots}(\_\_\_\_x\_\_\_\_) &\iff \mu x_{x<\ldots}[\_\_\_\_x\_\_\_\_] < \ldots \\ \forall x_{x<\ldots}(\_\_\_\_x\_\_\_\_) &\iff \neg \exists x_{x<\ldots} \neg(\_\_\_\_x\_\_\_\_) \end{aligned}$$

$\exists x_{x<\ldots}$ и $\forall x_{x<\ldots}$ наричаме ограничени квантори. Ясно е, че $\exists x_{x<\ldots}(\_\_\_\_x\_\_\_\_)$ тогава и само тогава, когато има $x < \ldots$, за което $\_\_\_\_x\_\_\_\_$, а $\forall x_{x<\ldots}(\_\_\_\_x\_\_\_\_)$ тогава и само тогава, когато $\_\_\_\_x\_\_\_\_$ за всяко $x < \ldots$.

**C10.** Нека $P$ е $n+1$-местен изчислим предикат. Тогава $n+1$-местните предикати $Q$ и $R$, дефинирани чрез

$$\begin{aligned} Q(b, \overline{a}) &\iff \exists x_{x<b} P(\overline{a}, x), \\ R(b, \overline{a}) &\iff \forall x_{x<b} P(\overline{a}, x) \end{aligned}$$

са изчислими.

*Доказателство.* $x_{x<b} P(\overline{a}, x)$ и $x_{x<b} P(\overline{a}, x)$ имат явни дефиниции, изполвзащи $P$, $<$, огриничен $\mu$-оператор, и $\neg$ и следователно са изчислими.

□

**Забележка.** Можем да използваме ограничени квантори в явни дефиниции на изчислими функции.

Когато в индекса на ограничен $\mu$-оператор или квантор пишем $\leqslant \ldots$ ще имаме предвид $< \ldots + 1$.

Дефинираме двуместната функция $\dot{-}$ чрез $a \dot{-} b = \begin{cases} a - b, & a \geqslant b, \\ 0, & a < b \end{cases}$.

**C11.** Функцията $\dot{-}$ е изчислима.

*Доказателство.*

$$a \dot{-} b = \mu x (b + x = a \vee a < b).$$

□

**C12.** Нека $G_1, \ldots, G_k$ са $n$-местни изчислими функции, $R_1, \ldots, R_k$ са $n$-местни изчислими предикати, такива че за всяко $\overline{a}$, точно едно от $R_1(\overline{a}), \ldots, R_k(\overline{a})$ е вярно. Тогава $n$-местната функция $F$, дефинирана чрез

$$F(\overline{a}) = \begin{cases} G_1(\overline{a}), & R_1(\overline{a}); \\ G_2(\overline{a}), & R_2(\overline{a}); \\ \vdots \\ G_k(\overline{a}), & R_k(\overline{a}) \end{cases}$$

е изчислима.

*Доказателство.*

$$F(\overline{a}) = G_1(\overline{a})K_{R_1}(\overline{a}) + G_2(\overline{a})K_{R_2}(\overline{a}) + \cdots + G_k(\overline{a})K_{R_k}(\overline{a}).$$

□

**C13.** Нека $Q_1, \ldots, Q_k$ са $n$-местни изчислими предикати, а $R_1, \ldots, R_k$ са $n$-местни изчислими предикати, такива че за всяко $\overline{a}$, точно едно от $R_1(\overline{a}), \ldots, R_k(\overline{a})$ е вярно. Тогава $n$-местният предикат $P$, дефиниран чрез

$$P(\overline{a}) \iff \begin{cases} Q_1(\overline{a}), & R_1(\overline{a}); \\ Q_2(\overline{a}), & R_2(\overline{a}); \\ \vdots \\ Q_k(\overline{a}), & R_k(\overline{a}) \end{cases}$$

е изчислим.

*Доказателство.*

$$K_P(\overline{a}) = \begin{cases} K_{Q_1}(\overline{a}), & R_1(\overline{a}); \\ K_{Q_2}(\overline{a}), & R_2(\overline{a}); \\ \vdots \\ K_{Q_k}(\overline{a}), & R_k(\overline{a}) \end{cases}$$

□

**Забележка.** Тъй като $R_k$ е еквивалентен на $\neg R_1 \,\&\, \neg R_2 \,\&\cdots\&\, \neg R_{k-1}$, вместо $R_k(\overline{a})$ ще пишем „иначе“.

Да разгледаме двуместната функция $OP$, дефинирана чрез

$$OP(a, b) = (a + b)(a + b) + a + 1.$$

Тогава $OP$ е изчислима (има явна изчислима дефиниция). При това, ако $OP(a, b) = OP(a', b')$, то $a = a'$ и $b = b'$. Действително, нека $OP(a, b) = OP(a', b')$. Ако допуснем, че $a' + b' > a + b$, то

$$OP(a', b') > (a' + b')^2 \geqslant (a + b + 1)^2 = (a + b)(a + b) + 2(a + b) + 1 \geqslant OP(a, b).$$

Следователно $a' + b' = a + b$. Тогава $a' + 1 = a + 1$, т.е. $a' = a$ и значи $b' = b$.

Дефинираме двуместния предикат $\mid$ чрез

$$a \mid b \iff \exists x_{x \leqslant b}(b = ax).$$

Следователно $\mid$ е изчислим и $a \mid b$ тогава и само тогава, когато $a$ дели $b$.

Дефинираме двуместния предикат $coP$ чрез

$$coP(a, b) \iff \forall x_{x \leqslant a}(x \mid a \to x \mid b \to x = 1).$$

Следователно $coP$ е изчислим и $coP(a, b)$ тогава и само тогава, когато $coP(a, b)$ са взаимно прости. Ясно е, че

1. $coP(a, b)$ тогава и само тогава, когато $coP(b, a)$;
2. ако $a \neq 1$ и $coP(a, b)$, то $a \nmid b$;
3. ако $coP(a, b_1)$ и $coP(a, b_2)$, то $coP(a, b_1 b_2)$.

Нека сега $a_0, a_1, \ldots, a_k$ са произволни естествени числа. Нека $b_i = OP(a_i, i)$, $0 \leqslant i \leqslant k$. Тогава числата $b_0, \ldots, b_k$ са положителни и различни. Нека $s = \max\{b_0, \ldots, b_k\}$ и нека $m = s!$. Ще покажем, че числата

$$m.1 + 1, m.2 + 1, \ldots, ms + 1$$

са две по две взаимно прости. За целта да допуснем, че $p$ е просто число, такова че $p \mid (mi + 1)$ и $p \mid (mj + 1)$, $1 \leqslant i < j \leqslant s$. Тогава $p \mid m(j - i)$ и значи $p \mid m$ или $p \mid (j - i)$. Ако $p \mid (j - i)$, то $p < s$ и значи $p \mid m$. Следовотелно $p \mid m$ и тъй като $p \mid (mi + 1)$ и значи $p \mid 1$, противоречие.

Нека

$$M = (mb_0 + 1)(mb_1 + 1) \ldots (mb_k + 1).$$

Ако $y$ не е нито едно от числата $b_0, b_1, \ldots, b_k$, то $coP(my + 1, mb_i + 1)$, $0 \leqslant i \leqslant k$, и значи $coP(my + 1, M)$, откъдето $(my + 1) \nmid M$.

Следователно за всяко $y$, $1 \leqslant y \leqslant s$, е в сила

$$(my+1) \mid M \iff y = b_i \text{ за някое е } i,\ 0 \leqslant i \leqslant k,$$

Така $m.OP(a_i, i) + 1 \mid M$ (защото $OP(a_i, i) = b_i$) и ако $x < a_i$, то $OP(x, i) < OP(a_i, i) \leqslant s$, $OP(x, i)$ е различно от числата $b_0, \ldots, b_k$ и значи $m.OP(x, i) + 1 \nmid M$. Следователно

$$a_i = \mu x[m.OP(x, i) + 1 \mid M], \quad 0 \leqslant i \leqslant k.$$

Дефинираме двуместната функцията $\beta$ чрез

$$\beta(a, i) = \mu x_{x<a \dot{-} 1} \left[\exists y_{y<a} \exists z_{z<a} (a = OP(y, z) \;\&\; (yOP(x, i) + 1) \mid z)\right].$$

Ясно е, че $\beta$ е изчислима. При горните означения, ако $a = OP(m, M)$, то тогава

$$\beta(a, i) = a_i, \quad 0 \leqslant i \leqslant k.$$

Така доказахме следната теорема:

**Теорема 4.1** (Гьодел). Съществува изчислима функция $\beta$, такава че

(i) $\beta(a, i) \leqslant a \dot{-} 1$ за всяко $a$ и $i$;

(ii) за всяка редица $a_0, a_1, \ldots, a_k$ съществува $a$, такова че

$$\beta(a, i) = a_i,\ 0 \leqslant i \leqslant k.$$

Нека отбележим, че $\beta(0, i) = 0$ и $\beta(a, i) < a$ за $a \neq 0$. На всяка редица $a_1, \ldots, a_n$ съпоставяме най-малкото число $a$, за което $\beta(a, 0) = n$ и $\beta(a, i) = a_i$, $1 \leqslant i \leqslant n$. Ще наричаме това число код на редицата и ще го бележим с $\langle a_1, \ldots, a_n \rangle$. В сила е $\langle\ \rangle = 0$.

За всяко фиксирано $n$ функцията $\langle a_1, \ldots, a_n \rangle$ е изчислима, тъй като

$$\langle a_1, \ldots, a_n \rangle = \mu x[\beta(x, 0) = n \;\&\; \beta(x, 1) = 1 \;\&\; \ldots \;\&\; \beta(x, n) = a_n].$$

Полагаме

$$\begin{aligned} \mathrm{lh}(a) &= \beta(a, 0), \\ (a)_i &= \beta(a, i+1). \end{aligned}$$

Тогава, ако $a = \langle a_0, \ldots, a_{n-1} \rangle$, то $\mathrm{lh}(a) = n$ и $(a)_i = a_i$, $0 \leqslant i \leqslant n-1$. Ще пишем $(a)_{i,j}$ вместо $((a)_i)_j$.

Дефинираме едноместния предикат $Seq$ чрез

$$Seq(a) \iff \forall x_{x<a} (\mathrm{lh}(x) \neq \mathrm{lh}(a) \vee \exists i_{i<\mathrm{lh}(a)} ((x)_i \neq (a)_i)).$$

Тогава $Seq$ е изчислим. При това $Seq(a)$ тогава и само тогава, когато $a$ е код на редица.

Дефинираме двуместната функция $In$ чрез

$$In(a, k) = \mu x[\mathrm{lh}(x) = k \;\&\; \forall i_{i<k} ((x)_i = (a)_i)].$$

Функцията $In$ е изчислима, като при това ако $k < n$, то $In(\langle a_0, \ldots, a_{n-1} \rangle, k) = \langle a_0, \ldots a_{k-1} \rangle$.

Дефинираме двуместна операция $*$ чрез

$$a * b = \mu x[\mathrm{lh}(x) = \mathrm{lh}(a) + \mathrm{lh}(b) \;\&\; \forall i_{i<\mathrm{lh}(a)} ((x)_i = (a)_i) \;\&\; \forall i_{i<\mathrm{lh}(b)} ((x)_{i+\mathrm{lh}(a)} = (b)_i)].$$

Тогава $*$ е изчислима и $\langle a_0, \ldots a_{m-1} \rangle * \langle b_0, \ldots, b_{m-1} \rangle = \langle a_0, \ldots a_{m-1}, b_0, \ldots, b_{m-1} \rangle$.

С помощта на кодирането на редици можем да сведем всяка $n$-местна функция до едноместна. Нека $F$ е $n$-местна функция. С $\langle F \rangle$ ще означаваме едноместната функция, действаща по правилото

$$\langle F \rangle(a) = F((a)_0, (a)_1, \ldots, (a)_{n-1}).$$

Тогава, ако $F$ е изчислима, то и $\langle F \rangle$ също е изчислима. При това

$$F(a_1, \ldots, a_n) = \langle F \rangle(\langle a_1, \ldots, a_n \rangle).$$

По същия начин, на $n$ местен предикат $P$ съпоставяме едноместен $\langle P \rangle$, дефиниран чрез

$$\langle P \rangle(a) \iff P((a)_0, \ldots, (a)_{n-1}).$$

Тогава, ако $P$ е изчислим, то и $\langle P \rangle$ също е изчислим. Освен това $P(a_1, \ldots, a_n) \iff \langle P \rangle(\langle a_1, \ldots, a_n \rangle)$.

Нека $F$ е $n+1$-местна функция. Дефинираме $n+1$-местна функция $\overline{F}$ чрез

$$\overline{F}(\overline{a}, a) = \mu x[\mathrm{lh}(x) = a \ \&\ (x)_0 = F(\overline{a}, 0) \ \&\ \forall i_{i<a}((x)_i = F(\overline{a}, i))].$$

Тогава за всяко фиксирано $n$ имаме $\overline{F}(\overline{a}, n) = \langle F(\overline{a}, 0), \ldots, F(\overline{a}, n-1) \rangle$. При това

$$F(\overline{a}, a) = (\overline{F}(\overline{a}, a+1))_a$$

и следователно $F$ и изчислима тогава и само тогава, когато $\overline{F}$ е изчислима. Следователно $\overline{F}(\overline{a}, a)$ се определя от и съдържа информацията за $F(\overline{a}, 0)$, ..., $F(\overline{a}, a-1)$. Тогава, ако $F$ удовлетворява уравнение от вида

$$F(\overline{a}, a) = G(\overline{a}, a, \overline{F}(\overline{a}, a)),$$

то $F$ се определя рекурсивно с помоцтта на $G$.

**C14.** Ако $G$ е $n+2$-местна изчислима функция и $F$ е $n+1$-местна функция, дефинирана чрез рекурсията

$$F(\overline{a}, a) = G(\overline{a}, a, \overline{F}(\overline{a}, a)),$$

то $F$ е изчислима.

*Доказателство.* Да разгледаме $n+1$-местната функция $H$, дефинирана чрез

$$H(\overline{a}, a) = \mu x[\mathrm{lh}(x) = a \ \&\ \forall i_{i<a}((x)_i = G(\overline{a}, i, In(x, i)))].$$

Тогава $H$ е изчислима,

$$\overline{F}(\overline{a}, a) = H(\overline{a}, a)$$

и значи $F$ също е изчислима.

□