

计算模型导引|2018复习

Yang Luo

Spring 2018

一 递归函数

1.1 数论函数 (P1)

本源函数 \mathcal{IF} :

- 零函数 Z
- 后继函数 S
- 投影函数 P_i^n

1.2 配对函数 (P7)

配对函数: 设 $pg(x, y) : \mathbb{N}^2 \rightarrow \mathbb{N}$, $K(x) : \mathbb{N} \rightarrow \mathbb{N}$, $L(x) : \mathbb{N} \rightarrow \mathbb{N}$ 为数论函数, 若它们对于任意 $x, y \in \mathbb{N}$, 满足: $K(pg(x, y)) = x$, $L(pg(x, y)) = y$, 则称 pg 为配对函数, K 和 L 分别为左函数和右函数, $\{pg, K, L\}$ 为配对函数组。

1.3 初等函数 (P14)

初等函数 \mathcal{EF} :

- $\mathcal{IF} \subset \mathcal{EF}$
- $x + y, x - y, x \times y, \lfloor x/y \rfloor \in \mathcal{EF}$
- \mathcal{EF} 对于复合, 有界叠加算子 $\sum[\cdot]$ 和有界迭乘算子 $\prod[\cdot]$ 封闭
- $x \times y, N(x), N^2(x)$
- \mathcal{EF} 对于 μ -算子和 max -算子封闭
- $x^y, \sqrt[y]{x}, rs(x, y)$
- $\tau(x)$: x 的因子的数目
- $prime(x)$: 判断 x 是否为素数
- $\pi(x)$: 不超过 x 的素数个数
- $P(n)$: 枚举第 n 个素数
- $ep(n, x)$: x 的素因子分解式中 P_n 的指数

1.4 原始递归函数 (P25)

(P25) 原始递归函数: 类 \mathcal{PRF} 是满足一下条件的最小集合: (1) $\mathcal{IF} \subseteq \mathcal{PRF}$ (2) \mathcal{PRF} 对于复合, 带参原始递归算子和无参原始递归算子封闭。

原始递归函数 (\mathcal{PRF}) :

- $add(x, y)$
- $pred(x, y)$
- $sub(x, y)$
- $diff(x, y)$
- $mul(x, y)$
- $sq(x)$
- $N(x)$
- $N^2(x)$
- $sqr(x) = \lfloor \sqrt{x} \rfloor$
- $E(x) = x - \lfloor \sqrt{x} \rfloor^2$

(P30) 原始复迭函数类 (\mathcal{IIF}) : (1) $\mathcal{IF} \subseteq \mathcal{IIF}$ (2) \mathcal{IIF} 对于复合、原始复迭算子 $It[\cdot]$ 、弱原始复迭算子 $Itw[\cdot]$ 封闭。

(P32) 定理1.47: $\mathcal{IIF} = \mathcal{PRF}$

(P33) 串值递归

(P34) 联立递归、变参递归

(P35) 多重递归

(P36) Ackermann函数

1.5 递归函数 (P40)

正则函数、正则 μ -算子、 μ -算子、一般递归函数 (\mathcal{GRF})、部分递归函数 (\mathcal{RF})

1.6 不可计算数论函数类

- (P102) 集合 $\mathcal{N} = \{M : M \text{有} \beta - n f\}$
- (P100, P102) 在 λ -演算中, 等价关系 $=_\beta$ 是不可判定的 (存在 $M, N \in \Lambda$ 使得 $m = \lceil M \rceil, n = \lceil N \rceil$ 且 $M =_\beta N$)
- (P136) 停机问题: 存在Turing机使 $n = \#M$ 且 M 对于一切输入皆停机

1.7 第二大题分类情况

- \mathcal{EF} : 1. 向下取整类型 2. Godel的 β -函数 3. π 的十进制展开中的第 n 个数字 4. e 的十进制展开中的第 n 个数字 (hint: 1. $\pi/4 = 1 - 1/3 + 1/5 - 1/7 + \dots$ 2. $e = \sum_{i=0}^n (1/i!)$)
- $\mathcal{PRF} - \mathcal{EF}$: 1. 类似 $G(x) = 2^{2^{\dots^x}}$
- $\mathcal{GRF} - \mathcal{PRF}$: 1. Ackermann函数
- $\mathcal{RF} - \mathcal{GRF}$: 1. $f: \mathbb{N} \rightarrow \mathbb{N}$ 为处处无定义的函数 2. 存在无定义的函数 (P40 μ -算子定义)
- 不可计算数论函数类: 见1.6

三 λ —演算

3.1 λ —演算的语法 (P70)

约定3.3 :

1. x, y, z 表示任意变元
2. M, N, L 表示任意 λ —项
3. $M \equiv N$ 表示M和N语法恒同
4. 通常采用以下省略括号表示法
 1. 左结合: $FM_1M_2 \dots M_n \equiv (\dots ((FM_1)M_2) \dots M_n)$
 2. $\lambda x_1x_2 \dots x_n. M \equiv (\lambda x_1(\lambda x_2(\dots (\lambda x_n M) \dots)))$
5. 设 $P \equiv MN_1 \dots N_k$, 其中 $k \geq 0$, 当 $k = 0$ 时, $P \equiv M$
6. 设 $P \equiv \lambda x_1 \dots x_n. M$, 其中 $k \geq 0$, 当 $k = 0$ 时, $P \equiv M$

3.2 转换 (P74)

形式理论 $\lambda\beta$ 由以下的公理和规则组成:

公理:

- $(\rho)M = M$
- $(\beta)(\lambda x. M)N = M[x := N]$

规则:

- $(\sigma) \frac{M=N}{N=M}$
- $(\tau) \frac{M=N, N=L}{M=L}$
- $(\mu) \frac{M=N}{ZM=ZN}$
- $(\nu) \frac{M=N}{MZ=NZ}$
- $(\xi) \frac{M=N}{\lambda x. M = \lambda x. N}$

(P76) 标准组合子:

- $I \equiv \lambda x. x$
- $K \equiv \lambda xy. x$
- $K^* \equiv \lambda xy. y$
- $S \equiv \lambda xyz. xz(yz)$

(P76) 定义3.14

- 形式理论 $\lambda\beta + ext$ 是在形式理论 $\lambda\beta$ 中加入下述规则(ext): $(ext)Mx = Nx \Rightarrow M = N$, 其中 $x \notin FV(MN)$
- 形式理论 $\lambda\beta\eta$ 是在形式理论 $\lambda\beta$ 中加入下述公理(η): $(\eta)\lambda x. Mx = M$, 其中 $x \notin FV(M)$

3.3 规约 (P77)

关系	性质	读法	备注
\rightarrow_R	合拍	一步 R -规约	R 的合拍闭包
\twoheadrightarrow_R	规约	R -规约	\rightarrow_R 的自反、传递闭包
$=_R$	同余	R -转换	\twoheadrightarrow_R 的对称闭包

$\beta - nf$:

- $(\lambda x. xx)y$ 不是 $\beta - nf$, 但 yy 是它的 $\beta - nf$
- $\Omega \equiv (\lambda x. xx)(\lambda x. xx)$ 不是 $\beta - nf$, 也无 $\beta - nf$
- $(\lambda u. v)\Omega$ 不是 $\beta - nf$, 但它有 $\beta - nf$, 而且有无穷 β -化归链

3.5 不动点定理 (P91)

(P91) 定理3.22 (不动点) 定理: 对于任意的 $F \in \Lambda$, 存在 $Z \in \Lambda$, 使得 $FZ =_\beta Z$ 。

3.6 递归函数的 λ -可定义性 (P93)

(P93) Church数项: 对于 $n \in \mathbb{N}$, Church数项 $[n]$ 定义为 $[n] \equiv \lambda f x. f^n x$

λ -可定义函数类:

- 一般递归函数 λ -可定义的
- 本源函数
- 对复合封闭, 对原始递归封闭

部分 λ -定义函数:

- 本源函数
- 后继函数 S
- 前驱函数 $PRED$
- 选择函数 D

$D[0] =_\beta U_1^2$, $D[n+1] =_\beta U_2^2$, 因此 $D[0]MN =_\beta M$, $D[n+1]MN =_\beta N$

3.7 与递归论对应的结果 (P98)

(P99) 定理3.42 第二不动点定理: $\forall F. \exists Z. F[Z] =_{\beta} Z$

3.8 第三大题套路

一般是对给定的数论函数 $f(x)$, 构造 $F \in \Lambda^{\circ}$ 其 λ -定义 $f(x)$ 。

做题套路:

1. 首先将 $f(x)$ 写成原始递归式/弱原始递归式形式 $f(0) = a, f(x+1) = g(f(x))$
2. 可知 $f(x) = g^n(a)$, 那么 $F[x] =_{\beta} [g^n(a)] =_{\beta} G^n[a] \equiv [n]G[a] \equiv (\lambda x. xG[a])[n]$
3. 构造 $G[x]$ 使其 λ -定义 $g(x)$

□

3.9 第四大题套路

在已有的公理系统中加入一个额外公理(*), 使用规则和标准组合子推出对任何 $M, N \in \Lambda$, $\lambda\beta + (*) \vdash M = N$ 。

- 套路1: $(*)\lambda x. x = \lambda x. xx$, 对于接收一个参数的, 一般参数代入 K , 然后添加 M , 得到 $M =$ 标准组合子复合, N 同理, 得到 $M = N$ 。
- 套路2: $(*)\lambda xy. xy = \lambda xy. yx$, 对于接收两个参数的, 一般参数代入 KI , 然后添加 MN , 得到 $M = N$ 。
- 2004年题: $(*)x(yz) = (xy)z, \lambda\beta + (*) \vdash M = N$ 。 KII 代入两边得到 $K(II) \equiv KII \Rightarrow KI = I$, 两边加 M 得到 $KIM = IM \Rightarrow I = M$, 同理 $I = N$, 那么有 $M = N$ 。

五 Turing机

5.1 Turing机的形式描述 (P119)

(P120) 定义5.1 (Turing机): 设 $D \subset \{0, 1\} \times \mathbb{N}^*$ 为有穷集, 函数 $d: D \rightarrow \{0, 1\}$, $p: D \rightarrow \{-1, 0, 1\}$, $s: D \rightarrow \mathbb{N}^*$ 。三元组 (d, p, s) 被称为一个Turing机, 记作 $M = (d, p, s)$ 。称集合 D 为 M 的论域 $Dom(M)$, 函数 d 为 M 的“印-抹”函数, 函数 p 为 M 的位置函数, 函数 s 为 M 的状态函数。
 \overline{sdf}

(P122) 定义5.6 (Turing-可计算): 设 M 为机器, $f: \mathbb{N}^n \rightarrow \mathbb{N}$ 为 n 元数论全函数。若对于任意 $(x_1, x_2, \dots, x_n) \in \mathbb{N}^n$, M 输入 (x_1, \dots, x_n) 可输出 $f(x_1, \dots, x_n)$, 则称机器 M 计算了函数 f 。当存在机器 M 计算函数 f 时, 称函数 f 为Turing-可计算。

5.2 Turing机的计算能力 (P125)

(P126) 引理5.4: 设 $f: \mathbb{N} \rightarrow \mathbb{N}$, $g: \mathbb{N}^k \rightarrow \mathbb{N}$, 若 f, g 皆为Turing-可计算, 则 $h(\mathbf{x}) = f(g(\mathbf{x}))$ 为Turing-可计算。

已有的机器：

- `copy_k`：拷贝当前所指的值
- `compress`：将 0^n 压缩到0
- `erase`：抹去当前值
- `shiftrl`
- `shiftr`
- `double`

5.3 可判定性与停机问题（P136）

（P139）停机问题：是否存在能行过程（effective procedure）来判定机器对所有输入皆停机。

回答：答案是否定的，即停机问题不可判定。

5.4 通用Turing机（P139）

问题：什么是通用Turing机？

回答：（P144）存在机器 U 使对任何机器 M 和任何

$(n_1, n_2, \dots, n_k) \in n^k, M | \overline{(n_1, n_2, \dots, n_k)} \rightarrow \bar{y} \Leftrightarrow U | \overline{(\#M, n_1, \dots, n_k)} \rightarrow \bar{y}$

则称机器 U 为通用Turing机，通用性是指这样的机器能模拟任何其他Turing机。

5.5 Church-Turing论题（P145）

定理5.29（基本定理）：目前已知的各种刻画能行可计算的模型给出了相同的可计算函数类。

Church-Turing论题：直觉能行可计算（部分）函数类等同于Turing-可计算（部分）函数类。

总之，计算概念的可视化是20世纪的重大科学进展之一。

5.6 停机问题叙述套路



停机问题证明

- 假设存在停机问题判断算法: **bool Halt(p)**

- **p**为特定程序

- 给定某邪恶程序

```
void Evil() {
    if (!Halt(Evil)) return;
    else while(1);
}
```

- **Halt(Evil)**的返回值是什么?

- 如果为真, 则**Evil**不停机, 矛盾
- 如果为假, 则**Evil**停机, 矛盾

9

对于给定的一个机器 M , 设计机器 $Evil$, 当 $Evil$ 检测到 M 判断为停机时, 则保持不停机; 否则停机, 得出矛盾。

5.7 一些常用图灵机

- $f(x) = 2x$

	0	1
1	XXX	0R2
2	1L7	0R3
3	0R4	1R3
4	1L5	1R4
5	0L6	1L5
6	1R2	1L6
7	0R8	1L7
8	XXX	XXX

1. 去掉一根棍子 2-5. copy1 6. 中间连起来

	0	1
1	XXX	0R2
2	1C8	0R3
3	0R4	1R3
4	1R5	1R4
5	1L6	XXX
6	0L7	1L6
7	0R2	1L7
8	XXX	XXX

1.去掉一根棍子 2-7.去掉一根，加上两根

	0	1
1	XXX	0R2
2	0R3	1R2
3	1R4	1R3
4	1R5	XXX
5	0L6	XXX
6	0L7	1L6
7	0R8	1L7
8	0R9	1C1
9	XXX	0R10
10	XXX	XXX

1-8.去掉一根棍子，加上两根棍子 9.去掉一根棍子

- 棍子数*2

	0	1
1	0R7	0R2
2	0R3	1R2
3	1R4	1R3
4	1L5	XXX
5	0L6	1L5
6	0R1	1L6
7	XXX	XXX

- $f = 3x$

	0	1
1	XXX	0R2
2	1L8	0R3
3	0R4	1R3
4	1R5	1R4
5	1L6	XXX
6	0L7	1L6
7	1R2	1L7
8	0R9	1L8
9	XXX	XXX

1.去掉一根棍子 2-7.去掉一根棍子，加两根棍子，中间连起来

- copy_1 (习题5.2)

	0	1
1	0R6	0R2
2	0R3	1R2
3	1L4	1R3
4	0L5	1L4
5	1R1	1L5
6	XXX	XXX

- $f(x) = \lfloor x/2 \rfloor$

	0	1
1	XXX	0R2
2	1C8	0R3
3	1C8	0R4
4	0R5	1R4
5	1L6	1R5
6	0L7	1L6
7	0R2	1L7
8	XXX	XXX

1.去掉一根 2-7.每去掉两根，加一根

	0	1
1	0L6	0R2
2	0L3	1R2
3	1L6	0L4
4	1R5	1L4
5	0L6	1C1
6	0R7	1L6
7	XXX	XXX

1-3.头里去一根，尾巴上去一根 4-5.最前面加一根

	0	1
1	0R7	0R2
2	1C7	0R3
3	0R4	1R3
4	1L5	1R4
5	0L6	1L5
6	0R1	1L6
7	XXX	XXX

1-6. 去掉两根棍子，加一根棍子

- $f(x) = \lfloor x/3 \rfloor$

	0	1
1	0L7	0R2
2	0L3	1R2
3	1L7	0L4
4	1L7	0L5
5	1R6	1L5
6	0L7	1C1
7	0R8	1L7
8	XXX	XXX

1-6. 前面去1根棍子，后面去3根棍子，最前面加1根棍子

- $f(x) = x - y$ (习题5.11)

	0	1
1	0R12	0R2
2	0R3	1R2
3	0L9	1R4
4	0L5	1R4
5	XXX	0L6
6	0L7	1L6
7	0R12	1L8
8	0R1	1L8
9	0L10	XXX
10	1L11	1L10
11	1C14	XXX
12	0R13	XXX
13	1C14	0R13
14	XXX	XXX

- $f(x, y) = xy$ (习题5.3)

	0	1
1	XXX	0R2
2	0R3	1R2
3	0L4	1R3
4	XXX	0L5
5	0L6	1L5
6	0R7	1L6
7	0R16	0R8
8	0R9	1R8
9	0L14	0R10
10	0R11	1R10
11	1L12	1R11
12	0L13	1L12
13	1R9	1L13
14	0L15	1L14
15	0R7	1L15
16	1C17	0R16
17	XXX	XXX

1-7. x减一根, y减一根 8-15.复制一份y 16.加一根

- $f(x) = x^2$

	0	1
1	XXX	0R2
2	0L7	0R3
3	0R4	1R3
4	1L5	1R4
5	0L6	1L5
6	1R2	1L6
7	0R8	1L7
8	0R17	0R9
9	0R10	1R9
10	0L15	0R11
11	0R12	1R11
12	1L13	1R12
13	0L14	1L13
14	1R10	1L14
15	0L16	1L15
16	0R8	1L16
17	1C18	0R17
18	XXX	XXX

- $f(x) = \lfloor x^{\frac{1}{2}} \rfloor$

◦	1	XXX	0R2
	2	1C28	0R3
	3	0R12	1R4
	4	0R5	1R4
	5	1R6	1R20
	6	0R7	XXX
	7	1R8	1R7
	8	1L9	XXX
	9	0L10	1L9
	10	0L11	1L10
	11	0R2	1L11
	12	1R24	1R13
	13	0R14	1R13
	14	0L15	0R16
	15	1R25	XXX
	16	0R17	0R16
	17	0L18	0R17
	18	0L19	0L18
	19	0R26	1L19
	20	0R21	1R20
	21	0L5	1R22
◦	22	1L23	1R22
	23	XXX	0L9
	24	0L26	XXX
	25	0R25	0R16
	26	0L26	1L27
	27	1C28	1L27
	28	XXX	XXX

- $f(x) = x/y$

	0	1
1	XXX	0R2
2	0R3	1R2
3	0L4	1R3
4	XXX	0L5
5	0L18	1L6
6	0R7	1L6
7	0R13	0L8
8	0L9	1L8
9	0R10	1L9
10	0R16	0R11
11	0R12	1R11
12	1R7	1R12
13	1L14	1R13
14	0L15	1L14
15	0R7	1L15
16	0R17	0R16
17	1C19	0R17
18	1C19	0L18
19	XXX	XXX