算法论

莫绍揆 编著

科学出版社

算法论

莫绍揆 编著

科学出版社

内 容 简 介

本书从介绍字母、字母表、字、出现、代入、转换和映照等基本概念开始，着重讨论了演算和算法的平行性、彼此密切相关性，以及算法和演算的合成与嵌入，进而又讨论了与算法、演算直接有关的各种判定性问题。

算 法 论

莫 绍 揆 编著

责任编辑 杨家福

科学出版社出版

北京朝阳门内大街 137 号

中国科学院印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

1982 年 11 月第 一 版 开本：787×1092 1/32

1982 年 11 月第一次印刷 印张：10

印数：0001—9,000 字数：227,000

统一书号：15031·447

本社书号：2797·15—8

定价：1.55 元

序　　言

算法与演算是处理计算过程——推理过程时一般最常用的两大形式. 但是，长远以来人们只把数学理论(以及一切演绎科学)表示成一个公理系统，亦即表示成一个内容丰富、结构复杂的演算，其中虽有若干片段是表示成算法的，例如对四则(加减乘除)运算给出了计算图式，对求最大公约数给出了辗转相除法等等. 但是，一来这些只是零星片段，并没有把它们组织起来，从而把数学表示成一个大算法，二来，甚至于这些零星片段的算法也被人们认为是"笨"方法，不够巧妙，因此大家都认为，最好使用一些"精彩的"、有技巧性的方法，"万不得已"时才采用这些笨方法. 换句话说，这些零星的算法被看作是辅助性的工具，而不是研究的主要对象.

自从机器出现以后，尤其是带有自动控制、自动调整性质的机器(如自动电话、电子数字计算机、无人工厂等等)出现以后，算法的重要性便突出地显示出来了. 1936 年，杜灵 (A. M. Turing) 提出了杜灵机器的概念，第一次把算法作为一个独立的体系来研究，而不是当作辅助工具了. 以后，马尔科夫 (A. A. Марков) 又提出正规算法(即本书的换中算法)，算法的概念从而得到进一步的推广与澄清，算法的理论也就日益发展了.

目前，算法的应用是非常广泛的，好些应用极广的科目如程序设计理论、控制论等等，都可以说成是在一定意义之下的算法论的一部分，可以说成是算法论中那些直接与实践相结合的部分. 此外，既然算法与演算是互相平行的两大形式，而

数学理论已经表示成一个大演算，那末便有可能（也有必要）把整个数学理论也表示成一个大算法．如果我们朝这个方向努力，就会提出很多新问题、新概念，从而促进数学向前发展．

本书的目的却不在这里，而是强调演算与算法的平行性、彼此密切相关性，从而同时对演算与算法作出平行的、初步的理论探讨，并讨论它们对大量问题（从而对数理逻辑的一个中心问题，即所谓判定问题）的应用，这样才能矫正通常那种只讨论一种（或只讨论演算，或只讨论算法）情况的片面性，以便能够更深入地理解演算与算法的本质，更深入地理解数学乃至演绎科学的本质．

经验证明，在作这样的研究时，与其使用内容丰富、结构复杂的算法或演算，不如使用内容简单、结构原始的算法或演算更为适宜．但必须证明，这么简单的算法或演算却能够解决别的任何复杂的算法或演算所能解决的问题；这也就是本书所要讨论的一个主要内容．本书只讨论建立于组合系统之上的算法与演算，尤其是其中最原始的首尾算法与首尾演算，在一定意义上，它们比正规算法（换中算法）或演算更为原始，更值得注意．

与别的同类书籍相比，本书在许多方面还有下列不同之点．

一般书籍通常只讨论一种算法或一种演算，本书则不但同时讨论算法与演算，而且在讨论时绝不限于某一种算法或某一种演算．尤其值得提出的是，一般书都把杜灵机器理论放在递归函数理论中（最近一些讨论文法、形式语言的书中才同时讨论杜灵机器与文法，后者即演算），与别的演算、算法割裂开来，这是不够妥当的．杜灵机器本身便是一个算法，而且是建立在组合系统之上的一种算法，应该与别的演算、算法放

在一起讨论，它与(自然数的)递归函数论的情况是迥然不同的．本书对它进行了详细讨论，看来是适宜的．

好些算法书都详尽地、深入地讨论判定问题，或者把好些很特殊的（与演算、算法关系不太大的）判定问题都讨论到了．作者认为，这种处理方式固然有其好处，但它究竟离演算算法的内容太远．在本书中详细地讨论了可判定性的各种初等性质后，进而只探讨了与算法、演算直接有关的各种判定问题，没有进行更广泛、深入的探讨．这样，既能使读者对判定问题有足够的认识，又不至于超出算法与演算的范围．

本书所作的各个证明，都力求能显示出问题的本质，以便读者看了以后能够自动地推广到同类问题上去．本书所作各算法与演算都力求简单紧凑．这一点读者不难由其中的通用算法与通用演算看出来(当然，别处的算法与演算也是力求简单的)．作者希望读者在学了本书以后，在构作算法与构作演算方面能得到足够的训练．

书中所存在的不妥之处，希望读者批评指正．

目　　录

第一章　基本概念

在详细讨论演算与算法以前，有好些基本概念须加以澄清．这些基本概念看起来很直观，很容易理解，但如果不对它作进一步的分析研究，今后讨论起来就会遇到困难，以至使概念混乱不清．因此，读者务必要重视本章的讨论，决不能轻易对待．

§1　字母、字母表与字

定义　当把一个记号作为整体看待而不再加以分析时，该记号便叫做具体字母．

我们假定，两个具体字母的同型性是大家所熟知的，即任意给出两个具体字母，大家都会判定它们为同型或否，而且答案是不因人而异的．我们还假定同型性具有下列三个性质：

(1) 自反性．每个具体字母自己和自己同型．

(2) 对称性．　如果这个具体字母和那个具体字母同型，则那个具体字母和这个具体字母同型．

(3) 可传性．如果第一个具体字母与第二个具体字母同型，第二个具体字母与第三个具体字母同型，则第一个具体字母与第三个具体字母同型．

必须指出，两具体字母的同型性除满足上述三个性质外，在别的方面是没有约束的．例如，汉字中，草体的“𠂇”与楷体的“事”相差极大，但依习惯，它们是同型的；反之，“士”与

"土","日"与"曰"可以说只有毫厘之差，但依习惯，它们不是同型的. 容易看出，这样规定的同型性是满足上述三个性质的.

定义 具体字母的集合叫做具体字母表.

例如，$\{a, a, b, c\}$ 便是具体字母表，有四个具体字母为其元素(其中有两个具体字母是同型的).

定义 设有两个具体字母表，如果这个字母表中每个具体字母都和那个具体字母表中某一具体字母同型，那个具体字母表中每个具体字母亦和这个具体字母表中某个具体字母同型，我们便说这两个具体字母表是同型的.

显然，当具体字母的同型性确定以后，两个具体字母表的同型性也就确定了. 此外，两个具体字母表的同型性亦是自反的、对称的和可传的.

在下文所讨论的具体字母表都是有限的具体字母表，即其中具体字母的个数是有限的(但却是无界的，即我们并不规定每个具体字母表所含具体字母的最大个数). 故给出一个具体字母表时可以采用详细列举它所含的具体字母这个办法.

我们再假定大家都熟悉对两个具体记号作毗连运算，并都熟悉此运算的结果. 对任何两个记号均可作毗连而得出一个新记号(注意，我们故意忽视了时间上与空间上的限制，如考虑这些限制，本性质便不成立). 毗连不必一定左右毗连，也不必一定上下毗连，但为方便起见，下面只使用左右毗连. 毗连的一些重要性质，我们将详细列举于后(抽象字的毗连处).

有了毗连运算后，我们便可以定义具体字.

定义 设有具体字母表 **A**，则所谓 **A** 中具体字可以递归地定义如下：

(1) **A** 中的具体字母为 **A** 中的具体字；

(2) 如果甲、乙为两个 **A** 中的具体字，则甲、乙毗连的结果也为 **A** 中的具体字；

(3) 所谓 **A** 中具体字仅限于此.

定义 **A** 中两个具体字的同型性可递归地定义如下：

(1) 如果它们是 **A** 中同型的具体字母，则它们同型；

(2) 由同型的两对 **A** 中具体字依相同次序作毗连，所得的两个 **A** 中具体字是同型的；

(3) 两个 **A** 中具体字同型的情况仅限于此.

显然，当具体字母的同型性确定以后，**A** 中具体字的同型性也就确定了. 此外，具体字的同型性显然也满足自反性、对称性与可传性. 现在我们便利用具体字母、具体字母表与具体字的同型性来进行抽象——同一性抽象，这是因为同型性都具有自反性、对称性与可传性，故可依同型性而作同一性抽象.

我们说，由同型的具体字母可以抽象出一个相应的抽象字母，由同型的具体字母表可以抽象出一个相应的抽象字母表，由同型的具体字可以抽象出一个相应的抽象字. 例如，本段中便有好几个具体字母“由”，但只有一个抽象字母“由”.

我们说，每个具体字母(具体字母表、具体字)都是相应的抽象字母(抽象字母表、抽象字)的一个代表. 但是，我们还认为，抽象字还包括空字(不由任何抽象字母毗连而得的，亦即不含有任何抽象字母的，以下记为 Λ)，空字不是从抽象得来的，它没有任何代表.

今后，我们几乎只局限于讨论抽象字母、抽象字母表、抽象字，故形容词“抽象”二字便可省去. 当我们想讨论具体字母、具体字母表、具体字时，形容词“具体”二字必须明确标出，不能省略.

从概念上说，从具体字母表作抽象而得的抽象字母表本来和抽象字母的表(集合)是有区别的，但实际上两者没有区别. 以下我们不区别它们，通称它们为抽象字母表(简称字母表).

我们给出抽象字母(字母表、字)时，即用写出它们的代表的方法. 例如，要给出由开头四个拉丁字母所组成的字母表时，我们便写成 $\{a, b, c, d\}$.

在讨论过程中，我们往往并不讨论某些特定的字母或特定的字母表或特定的字，而往往是对未指定的字母、未指定的字母表、未指定的字而立论的. 这时我们采用下列的约定.

我们约定：在今后的讨论中，永远不对大写拉丁字母(白体及黑体)、大写俄文字母、大写哥德体字母、大小写希腊字母进行讨论；换言之，这些字母不在我们所讨论的字母范围之内. 这时我们便用：

小写希腊字母　　代　未指定的字母
白体大写拉丁字母　代　未指定的字
黑体大写拉丁字母　代　未指定的字母表.

(其余种类字母的用法以后规定). 例如，当我们说字母 α、字母 β 等等时，这是指 α, β 所代的那两个字母(可能这两个字母为 a, b 或为 x, y 或为日文字母等等)，而不是指希腊字母 α, β 本身；又如，当我们说字母表 **A**,**B**，这是指 **A**,**B** 所代的那两个字母表(这两个字母表可能为 $\{a, b\}$，也可能为日文的五十假名表)，而不是指由拉丁字母 **A**, **B** 本身所组成的两个字母表；又如，当我们说字 P, Q 时，这是指 P, Q 所代的那两个字(可能它们是 there，可能它们是两个汉字)，而不是指由 P, Q 本身所组成的字；用数理逻辑的话说，α, β, **A**, **B**, P, Q 等是语法变元，而不是被讨论的对象.

现在我们引入两个抽象字的毗连运算，显然它与两具体

字的毗连运算是相应的.

定义 设有两抽象字 P,Q,把它们的代表(这两代表便是两个具体字)作毗连得一个具体字,对此具体字作抽象所得的抽象字 R 便叫做字 P, Q 的毗连,记为 $R=\overset{\frown}{PQ}$, 简记为 $R=PQ$.

我们要求(这可看作对具体字的毗连的要求)抽象字的毗连须具有下列三个性质:

(1) 任意两字均可作毗连,其结果仍为一个字;

(2) (结合律)对任何字 P, Q, R 恒有

$$(PQ)R=P(QR);$$

(3) 设 ξ,η 为字母,而 P,Q 为字,则由 $\xi P=\eta Q$ 或 $P\xi=Q\eta$ 可以推得 $\xi=\eta$,且 $P=Q$ (注意,这反映了字母必须作为整体看待,不能再行分解).

还可指出,有了毗连运算后,可以只利用抽象字母概念而把抽象字递归定义如下:

(1) Λ (空字)为字;

(2) 如 ξ 为 (**A** 中)抽象字母,则 ξ 为 (**A** 中)字;

(3) 如 P, Q 为 (**A** 中)字,则 $\overset{\frown}{PQ}$ 为 (**A** 中)字;

(4) 所谓 (**A** 中)字也仅限于此.

对于 Λ (空字)我们要求它满足下列性质:

(1) 对任何字 P 必有

$$\Lambda P=P\Lambda=P.$$

注意,空字只有一个,因为如果有两空字 Λ 与 Λ',则有 $\Lambda=\Lambda\Lambda'=\Lambda'$.

(2) 对任何字 P, Q 与任何字母 ξ, 必有

$$\Lambda\neq P\xi Q.$$

根据关于字的递归定义,我们易得关于字的归纳原理以

及关于字函数的递归定义原理.

关于字的归纳原理：设有一个关于字 P 的命题 $\varphi(P)$. 如果我们证明了

(1) $\varphi(\Lambda)$ 是真的，

(2) 如 ξ 为 (**A** 中) 字母，则 $\varphi(\xi)$ 是真的，

(3) 由 $\varphi(Q)$ 真及 $\varphi(R)$ 真(这两者叫做归纳假设)可以推得 $\varphi(QR)$ 真，

则可以作出结论说，$\varphi(P)$ 对一切 (**A** 中)字 P 为真.

关于字函数的递归定义原理：必有一个也只有一个关于字 P 的函数 $f(P)$ 满足下列定义式(叫做原始递归式) 其中 g, h 为已知函数，而 A 为已知字：

$$\begin{cases} f(\Lambda) = A \\ f(\xi) = g(\xi) \\ f(QR) = h(Q, R, f(Q), f(R)). \end{cases}$$

这两个原理都是极易了解的，但要严格证明它们，却必须明白列出我们所使用的推理工具；这不属于本书范围，不作详细讨论.

注意，归纳原理中的 (3) 亦可改为下面的 (3′) 而仍然成立：

(3′) 由 $\varphi(Q)$ 真 (归纳假设) 可推得 $\varphi(\xi Q)$ (或推得 $\varphi(Q\xi)$) 真.

此外，递归定义的第三式亦可改为下式而递归定义原理仍然成立·

$$f(\xi Q) = h(\xi, Q, f(Q)),$$

或

$$f(Q\xi) = h(\xi, Q, f(Q)).$$

这些变形读者可以随意使用.

作为例子，我们可以定义字 P 的长度(记为 P^0) 如下：

$$\begin{cases}\Lambda^{\partial}=0\\ \xi^{\partial}=1\ (\xi\text{为任一}\mathbf{A}\text{中字母})\\ (QR)^{\partial}=Q^{\partial}+R^{\partial}.\end{cases}$$

根据字长的唯一性可知：如 $P^{\partial}=0$，则 P 必为空字；如果 $P^{\partial}=1$，则 P 必为 **A** 中字母；如果 $P^{\partial}>1$，则 P 必由多个 **A** 中字母毗连而得.

我们又可定义反字如下. 所谓 P 的反字(记为 $P^{\smile}$)，指把 P 中字母依相反次序作毗连而得的字，例如，$(abc)^{\smile}=cba$. 定义如下：

$$\begin{cases}\Lambda^{\smile}=\Lambda\\ \xi^{\smile}=\xi\\ (QR)^{\smile}=(R^{\smile}Q^{\smile}).\end{cases}$$

作为归纳证明的例子，我们今证明如下几条比较重要的定理.

定理 1 对任何字 P，Q，R，均有：

由 $PQ=PR$，可推得 $Q=R$(左消元律)

由 $QP=RP$，可推得 $Q=R$(右消元律).

[证] 今只证明左消元律，读者仿此可证明右消元律.

当 $P=\Lambda$ 时，由 $\Lambda Q=\Lambda R$ 当然可推得 $Q=R$.

当 $P=\xi$ 时，根据毗连性质(3)，由 $\xi Q=\xi R$ 可推得 $Q=R$.

当 $P=P_1P_2$ 时，由 $(P_1P_2)Q=(P_1P_2)R$，根据结合律得 $P_1(P_2Q)=P_1(P_2R)$，根据归纳假设可推得 $P_2Q=P_2R$，再根据归纳假设得 $Q=R$.

故根据关于字的归纳原理，左消元律得到证明.

定理 2 如果字 P 非空，则恒可找到字母 $\xi_1,\xi_2,\cdots,\xi_n$ 使得 $P=\xi_1\xi_2\cdots\xi_n$，右端叫做 P 的分解式，而这个 n 就是字 P 的长度 P^{∂}.

[证] 当 P 为空时，不属于讨论范围，可以认为定理成立.

如果 P 为字母 ξ，即如果 $P=\xi$，显然可取 $n=1$ 及 $\xi_1=\xi$，显见 $1=\xi^\partial$，故定理成立.

如果 $P=QR$，因 P 非空，故 Q，R 不能均空. 如果 Q，R 有一为空，则 $P=R$，或 $P=Q$，由归纳假设，定理成立. 如果 Q，R 均非空，依归纳假设应有字母 ξ_1，ξ_2，$\cdots$，ξ_l 及 ξ_{l+1}，ξ_{l+2}，$\cdots$，ξ_{l+m} 使得 $Q=\xi_1\xi_2\cdots\xi_l$ 及 $R=\xi_{l+1}\xi_{l+2}\cdots\xi_{l+m}$，这时有

$$P=QR=(\xi_1\cdots\xi_l)(\xi_{l+1}\cdots\xi_{l+m})=\xi_1\cdots\xi_l\xi_{l+1}\cdots\xi_{l+m},$$

故取 $n=l+m$ 及相应的字母，即可见到本定理第一部分成立. 显然，依归纳假设 $l=Q^\partial$，$m=R^\partial$，故 $n=Q^\partial+R^\partial=P^\partial$，故第二部分亦成立.

根据字的归纳原理，本定理得到证明.

系 任何一个非空字 P 恒可写成 ξQ 或 $R\xi$ 形（ξ 为字母），这叫做把 P 露头或把 P 露尾.

[证] 如 P 为字母，则取 $Q=R=\Lambda$ 即可，否则取 $Q=\xi_2\cdots\xi_n$ 及 $R=\xi_1\cdots\xi_{n-1}$ 即可.

定理 3 每一个非空字 P 只能唯一地表示成 $\xi_1\cdots\xi_n$ 形，即如果有

$$P=\xi_1\cdots\xi_n=\eta_1\cdots\eta_m,$$

则必 $m=n$ 且 $\xi_i=\eta_i(1\leqslant i\leqslant n)$.

[证] 当 $P=\Lambda$ 时，不属于讨论范围，故定理成立.

当 $P=\xi$ 时，如果 P 另有一分解式 R，根据空字的第二性质，R 必非空，故将 R 露头得 $R=\eta R_1$，从而 $\xi=\eta R_1$，依毗连的第三性质得 $\xi=\eta$ 且 $R_1=\Lambda$. 故 P 的任一分解式均呈 ξ 形，所以定理成立.

当 $P=\xi Q$ 时，如果 P 另有一分解式 R，则根据空字第二

性质，R必非空．今将R露头得 $R=\eta R_1$，从而 $\xi Q=\eta R_1$，根据毗连第三性质得

$$\xi=\eta \quad 且 \quad Q=R_1.$$

依归纳假设，Q(即 R_1)只有一个分解式，从而P的分解式只能是Q的唯一分解式左毗连以 ξ 的式子，故亦是唯一的．因此定理成立．

根据字的归纳原理，本定理得到证明．

以上这些关于字母、字母表、字的基本性质，读者应该熟练掌握．

这些基本概念也可用抽象代数的观点来作抽象处理，从而可以对它们获得进一步认识．在抽象代数中，我们有下列的概念．

设有一集合M与一运算$\circ$，如果：

(1) M对$\circ$是封闭的，即如果 a,b 为M的元素，则 $a\circ b$ 亦为M的元素；

(2) $\circ$服从结合律，即对M中任意元素 a，b，c 恒有

$$(a\circ b)\circ c=a\circ(b\circ c);$$

则说 $(M,\circ)$ 组成一个半群．

如果半群具有下列性质：

(3) (消元律)对M中任何元素 a，b，c 恒有：

由 $a\circ b=a\circ c$ 可推得 $b=c$ (左消元律)；

由 $b\circ a=c\circ a$ 可推得 $b=c$ (右消元律)；

则说 $(M,\circ)$ 为具有消元律的半群(或称准群)．

M中一元素 e 如果具有下列性质：

(4) 对M中任何元素 a 恒有 $a\circ e=e\circ a=a$，则 e 叫做 $(M,\circ)$ 的么元素．

M中的一个子集 $\mathbf{A}$ 如果具有下列性质：