中 国 科 学
1984 年 6 月　　A 辑　　第 6 期

形式证明的复杂性

洪 加 威
（北京市计算中心，北京工业大学二分校）

摘　要

本文提出了在形式证明系统中，证明长度、深度和宽度的概念，并且证明了长度的对数、深度和宽度三者之间是线性相关的．说明了任何定理的证明都可以高度地并行化，是一个与确定型计算截然不同的结论．

一、引　言

欧几里得的公理化方法以及 Gödel (1931) 的不完全性定理，给了数学和数理逻辑以深远的影响．半个世纪以来，数学家建立了一门理论的可证明性理论．但是仅仅研究理论的可证明性是不够的，还需要研究现实的可证明性，即研究证明复杂程度如何．我们研究的目的是要阐明证明的一些基本性质，加速证明的进程．

从计算的观点来看，要加快计算的进程，主要的方法是并行化．是否每个计算问题都可以高度并行化呢？看来答案是否定的[1]．但是对于数学的证明而言，本文却给出了一个肯定的回答：如果一个定理有一个长度为 L 的证明(相当于串行时间)，那末一定有一个深度不超过 $c\log L$ 的证明(深度相当于并行时间，c 是一个仅和公理系统有关的常数)．

作为非确定型计算的数学证明，比起确定型的计算困难得多．可是数学家为什么能写出那么长而复杂的证明呢？可能正是由于这种可并行性．实际上，这表现为对前人的继承，多人的分工合作，以及每个人思维本身的并行性．也许定理的机器证明也应当走这一条并行化的道路．

这一想法来源于作者“论计算的相似性与对偶性”一文[2]中的非确定型定理 1．

本文则进一步提出一个一般的形式证明系统(正规系统)，并且定义了证明的长度、深度和宽度，所谓证明的长度，就是把证明写出来以后字符的个数．所谓证明的深度，就是把它推导出来的层次数．

所谓证明的宽度，就是假定把证明写在一条只读带上，为了检验它是不是一个正确的形式证明所需机器的最小内存．这里的长度、宽度和深度分别相当于非确定型计算所需的串行时间、空间和并行时间，所以都是一些稳定的概念．

本文 1983 年 6 月 10 日收到．

证明的长、宽、深三者之间有什么关系呢？我们发现，证明的长度取对数就相当于深度.换言之，对任何一个正规系统 N_1，都存在一个与之等价的系统 N_2，使得对任何公式 w，若它在 N_1 中的证明长度为 L，则它在 N_2 中的深度不大于 $c\log L$，这里 c 是一个与 w 无关的常数．反过来，对任何正规系统 N_2，也都存在与之等价的系统 N_1，使对任何可证公式 w 而言，若它在 N_2 中深度为 D，则在 N_1 中证明长度的对数 $\log L \leqslant cD$．我们还发现证明的宽度和证明长度的对数之间也有这种线性关联的关系．本文的主要结果就是证明了证明长度的对数、深度和宽度三者之间是线性关联的．

需要注意的是，本文所讨论的形式数学并非数学的全貌．

二、正规形式证明系统

任何形式证明系统总是从某些公理或公理模式出发，运用某些推理规则一步步得到新的公式的一个重写系统．这里重要的是：1)这个形式证明系统要有足够的一般性．2)推理的每一步又应该是初等的(不然的话我们可以在一步之内得出任何可以得出的结论)．既然是一个重写系统，我们用一个非确定型的图灵机器来完成从某些字出发改写成另外一些字的工作，而且允许记录下某些中间信息．但是要求在每一个地方，改写和扫描的总次数不超过一个固定的常数 r．

定义 1. 一个正规(形式证明)系统是一个非确定型的图灵机器．它有 k 条双向只读输入带，k 条双向只读辅助输入带，k 条工作带，一条单向只写输出带和一条单向只写辅助输出带；它的输入、输出和工作字母表都是 Σ；它的所有带头改变方向的总次数不超过一个固定的常数 r；它的停机状态分为接受和拒绝两种，对任何输入和任何一系列非确定的选择都会最后停机．如果开始工作时第 i 个输入带的内容是 w_i，第 i 个辅助输入带上的内容是 w_i'，那末当机器进入一个接受状态时，它的输出带上的内容(辅助输出带上的内容)就叫做由前提 $w_1,\cdots,w_k$ 和辅助前提 $w_1',\cdots,w_k'$ 直接推出的结论(辅助结论)．

定义 2. 设在字母表 Σ 上给出了一个正规系统 N，我们递归地定义可证公式（又称为定理，下同)和辅助公式的集合如下：

1) 空字是可证公式，也是辅助公式．

2) 若 $w(w')$ 是由可证公式 $w_1,\cdots,w_k$ 为前提，辅助公式 $w_1',\cdots,w_k'$ 为辅助前提而得到的直接结论(辅助结论)，则 $w(w')$ 是可证公式(辅助公式)．

3) 所有辅助公式和可证公式均可使用 1 或 2 在有限次内得到．

定义 3. 如果它们可证公式集相等，则两个正规系统称作等价的．

例 1. 在由命题变元 a，b，命题联结词 $\sim$，$\supset$，以及括号所构成的命题演算系统中，有三条公理：

1) $(A\supset(B\supset A))$,

2) $((A\supset(B\supset C))\supset((A\supset B)\supset(A\supset C)))$,

3) $(((\sim A)\supset(\sim B))\supset(B\supset A))$

和一条推理规则 (modus ponens)

$$\frac{(A\supset B),\ A}{B}$$

所构成．其中 A，B、C 等都代表一个“合乎语法”的公式．

为了说明它只是正规系统的一个特例，我们构造一个非确定型图灵机 N，使得由它推出的公式恰是全体恒真命题，推出的辅助公式恰是全体合乎语法的公式．N 非确定地执行下列工作之一：

1）在辅助输出带上写下符号串 (a) 或 (b)．

2）如果辅助输入之一是字符串 A，则在辅助输出带上写下 $(\sim A)$ 或 (A)．

3）如果辅助输入是 A 和 B，则在辅助输出带上写下 $(A\supset B)$．

4）如果辅助输入是 A 和 B，则在输出带上写下 $(A\supset(B\supset A))$ 或 $(((\sim A)\supset(\sim B))\supset(B\supset A))$．

5）如果辅助输入是 A，B 和 C，则在输出带上写下 $((A\supset(B\supset C))\supset((A\supset B)\supset(A\supset C)))$．

6）如果输入是 A 和 $(A\supset B)$，则在输出带上写下 B．

以上 1),2),3) 是为了构造合乎语法的公式，4)，5) 对应于三条公理模式，6)对应于推理规则 modus ponens．为了完成上述的每一步，N 的各带头改变方向的总次数都不超过八次．

我们不难验证各种命题演算和谓词演算系统，Post 系统等都是正规系统的例子．为了说明正规系统中每一步推理仍然具有某种初等的性质，我们证明下面的引理．

引理 1. 设 w 是由前提 $w_1,\cdots,w_k$ 和辅助前题 $w_1',\cdots,w_k'$ 推出的直接结论或直接辅助结论，则

$$|w|\leqslant c(|w_1|+\cdots+|w_k|+|w_1'|+\cdots+|w_k'|),$$

此处 $|w|$ 代表 w 的长度，c 是一个仅依赖于正规系统的常数．

证．正规系统中的非确定图灵机 N 的计算可以分成不超过 r 个阶段，在每一个阶段中，任何带头都不改变方向．因为 N 一共只有有穷多个内部状态，Σ 只有有穷多个字母，所以 N 在常数步之内必须把工作带或输入带头向前走一格，否则就会陷入一个无穷的死循环．换句话说，每过若干步就必须走过一个曾经用过的方格．如果用 $S(i)$ 表示第 i 个阶段中输入带和工作带内容的总长，用 $t(i)$ 表示第 i 个阶段计算的总步数，则有关系式

$$t(i)\leqslant c_1S(i-1),$$

$$S(i)\leqslant t(i)+S(i-1)\leqslant(c_1+1)S(i-1),$$

c_1 是常数．于是，输出的长度 $|w|$ 满足

$$|w|\leqslant\sum_{i=1}^{r}t(i)\leqslant c(|w_1|+\cdots+|w_k|+|w_1'|+\cdots+|w_k'|),$$

c 是某个只依赖于 N 的常数．这一结果不仅对于输出的长度，就是对于工作带上的中间结果的长度也是正确的．引理 1 证毕．

由此可见，正规系统的每一次直接推导，只借助一个有穷非确定图灵机作不超过 r 次的扫描和改写，而且改写的中间结果和结论的长度都不超过输入总长的一个常数倍．

三、证明的长度、深度和宽度的关系

在本节中将介绍本文的主要结果．

定义 4. 设 N 是一个正规系统．N 中的一个证明是由一串用分隔符“,”分开的有穷多个

公式组成的序列. 其中每个公式都是一个N中的定理或辅助公式，并且每个公式或者是一个空字，或者是由前面的若干公式作为前提得到的直接结论(当它是一条定理的情形)，或者是由前面的若干公式作为前提得到的辅助直接结论(当它是一个辅助公式的情形). 最后一个公式应该是一条定理，被称作该证明的结论. 该公式串被称为这条定理的一个证明. 证明中全体符号的总数叫做该证明的长度. 一条定理的证明长度被定义为其最短证明的长度.

定义 5. 在一个证明中，空公式的深度为 1. 如果一个公式是一组前提的直接推论，则该公式的深度定义为该组前提中深度的最大值再加一. 如果该公式是好几组前提的直接结论(即由不同的前提组都可以直接推出该公式)，则取上述方法得到的各值中的最小者. 一个可证公式的深度被定义为以它为结论的所有证明中深度的最小值.

证明复杂性的另一种度量，就是证明的宽度. 假定给了一串符号，它是不是N中的一个证明呢? 我们可以把它存在一个只读寄存器中(例如图灵机的只读带上)，然后用一架确定型机器M来检验，称M为N的一个检验系统. 那末，为了检验一个符号串是否构成一个证明所需要的最小工作内存加上输入长度的对数，就定义为该证明相对于M的宽度. 为什么要加上输入长度的对数呢? 因为一般说来，要有一个对数长度的计数器，才能记住正在扫描的输入符号的位置. 所以这个假定是合理的. 由此得到下面的定义.

定义 6. 设N是一个正规系统，M是它的一个检验系统，即检验一个字符串 $w\in(\Sigma\cup\{,\})^*$ 是否构成N中的一个证明的确定型图灵机器. M作用在w上所使用工作空间与 $\log|w|$ 之和称为(关于M)的宽度.

所以，宽度总是相对于一个固定的检验系统M. 只是有时为了说话方便才省去这几个字. 严格地讲，我们在第一节中讲到的结果，可以表述为下面三个定理.

定理 1. 对于任何正规系统 N_1 都存在一个等价的正规系统 N_2，使对任何可证公式 f 而言，若 f 在 N_1 中的深度为 D，则在 N_2 中证明长度 L 的对数 $\log L$ 不大于 cD，c 是一个仅依赖于 N_1 的常数；反之，对任何正规系统 N_2，都存在一个与之等价的正规系统 N_1，使对任何可证公式 f 而言，若 f 在 N_2 中的证明长度为 L，则 f 在 N_1 中的深度不大于 $c_1\log L$，c_1 是一个仅依赖于 N_2 的常数.

把定理 1 中的深度 D 换成宽度 W，就得到一个与之对偶的定理:

定理 2. 对任何正规系统 N_1 和它的一个检验系统 M，都存在与之等价的正规系统 N_2，对任何可证公式 f，若 f 在 N_1 中关于 M 的宽度为 W，则 f 在 N_2 中的证明长度的对数不大于 cW，c 是一个仅依赖于 N_1 的常数；反之，对任何正规系统 N_2，都存在与之等价的正规系统 N_1 和它的一个检验系统 M，使对任何可证公式 f 而言，若 f 在 N_2 中的证明长度为 L，则 f 在 N_1 中相对于 M 的宽度不大于 $c_1\log L$，c_1 是一个仅依赖于 N_2 的常数.

定理 3. 对任何正规系统 N_1 都存在一个与之等价的正规系统 N_2 及其检验系统 M，对任何可证公式 f，若 f 在 N_1 中深度为 D，则在 N_2 中相对于 M 的宽度不大于 D；反之，对任何正规系统 N_2 及其检验系统 M，都存在一个等价的正规系统 N_1，使得对任何可证公式 f 而言，若 f 在 N_2 中相对于 M 的宽度为 W，则在 N_1 中的深度不大于 W.

四、从非确定图灵机构造正规系统

设 T 是一个 k 带非确定图灵机，它的状态集合为 Q，工作字母表为 Σ，包含空格符号 $\sqcup$. 那

么一个部分瞬时描述（PID）是如下形式的字：

$$x_1qy_1\Delta x_2qy_2\Delta\cdots\Delta x_kqy_k,$$

其中Δ是不属于$\Sigma\cup Q$的一个字母，$q\in Q$，$x_iy_i\in\Sigma^*$．它表示在某个瞬时，机器处于状态q，x_iy_i是第i条带上的内容的一个子字．第i条带的带头正扫描着y_i的最左符号．注意，x_iy_i不见得是带上的全部内容，只是带头附近的内容，所以称为部分瞬时描述．

为了描述图灵机T的一个简单动作，可根据T的下一动作函数写出一组基本推演式：

$$\alpha_1\Delta\alpha_2\Delta\cdots\Delta\alpha_k\to\beta_1\Delta\beta_2\Delta\cdots\Delta\beta_k,\tag{1}$$

其中每对$\alpha_i\to\beta_i$具有下列三种形式之一：

1）$b_iqa_i\to b_iq'a_i'$，

2）$b_iqa_i\to b_ia_i'q'$，

3）$b_iqa_i\to q'b_ia_i'$．

此处q，$q'\in Q$，a_i，a_i'，$b_i\in\Sigma$．(1)式的意思为：若机器T正处于状态q，它的第i个带头正扫描着符号a_i，$i=1,2,\cdots,k$，那么T可以做下面的动作：把它扫描的第i条带上的符号a_i改成a_i'，$(i=1,2,\cdots,k)$；把自己的状态由q改为q'；不改变第i个带头的位置（当情形1成立），把第i个带头右移一格（当情形2成立），或者把第i个带头左移一格（当情形3成立）．

对于任一非确定图灵机T，基本推演式的集合是有限的，记为$\mathscr{D}_0$．图灵机的活动可由部分推演式的集合$\mathscr{D}$来刻划，其定义如下：

1）$\mathscr{D}_0\subset\mathscr{D}$．

2）若$I\to J$及$J\to K$属于$\mathscr{D}$，则$I\to K$也属于$\mathscr{D}$．

3）若$x_1qy_1\Delta\cdots\Delta x_kqy_k\to x_1'q'y_1'\Delta\cdots\Delta x_k'q'y_k'$属于$\mathscr{D}$，则$u_1x_1qy_1v_1\Delta\cdots\Delta u_kx_kqy_kv_k\to u_1x_1'q'y_1'v_1\Delta\cdots\Delta u_kx_k'q'y_k'v_k$也属于$\mathscr{D}$，此处$u_1\cdots u_kv_1\cdots v_k\in\Sigma^*$．

4）$\mathscr{D}$中元素均可由以上三条得到．

非形式地讲，1)描写了T的一步动作；2)可把各动作串联起来；3)则用于扩充部分瞬时描述的范围，本身不对应T的动作．不难用归纳法证明：若$\alpha_1\Delta\cdots\Delta\alpha_k\to\beta_1\Delta\cdots\Delta\beta_k$属于$\mathscr{D}$，则$|\alpha_i|=|\beta_i|$，且$\alpha_1\Delta\cdots\Delta\alpha_k$和$\beta_1\Delta\cdots\Delta\beta_k$都是部分瞬时描述．

图灵机T从初始状态q_0出发，开始的时候，第一条带上的内容为字$w\in(\Sigma-\{\sqcup\})^*$，其余的带上全为空格符$\sqcup$．如果$T$最终进入某一接受状态$q_t\in Q_t$，我们就说$T$接受了输入$w$．形式地讲，如果$u_1q_0wv_1\Delta u_2q_0v_2\Delta\cdots\Delta u_kq_0v_k\to x_1q_iy_1\Delta\cdots\Delta x_kq_iy_k$属于$\mathscr{D}$，并且$u_1\cdots u_kv_1\cdots v_k\in\{\sqcup\}^*$，$q_i\in Q_t$，就说$T$接受输入$w$．

现在我们从T出发，构造一个正规系统N_2，使得对任何w而言，T接受w当且仅当w是N_2所推出的结论．N_2非确定地执行下列任务之一：

1）在辅助输出带上写下$\mathscr{D}_0$中任一基本推演式．

2）如果有两个辅助输入$I\to J$和$J\to K$，则在辅助输出带上输出$I\to K$．

3）如果辅助输入为$\alpha_1\Delta\cdots\Delta\alpha_k\to\beta_1\Delta\cdots\Delta\beta_k$，则非确定地选取$u_i$，$v_i\in\Sigma^*$，并在辅助输出带上写下$u_1\alpha_1v_1\Delta\cdots\Delta u_k\alpha_kv_k\to u_1\beta_1v_1\Delta\cdots\Delta u_k\beta_kv_k$．但输出长不超过输入长的一个常数倍．

4）如果辅助输入为$u_1q_0wv_1\Delta u_2q_0v_2\Delta\cdots\Delta u_kq_0v_k\to J$，其中$J$的内部状态属于$Q_t$，且

$u_1\cdots u_k v_1\cdots v_k \in \{\sqcup\}^*$，则在输出带上写下 ω(作为结论).

引理 2. N_2 的可证公式集恰为 T 所接受的语言.

证. 只需要证：N_2 的辅助公式集恰为 $\mathscr{D}$. 其实，N_2 用第一条可以得到 $\mathscr{D}_0$ 中任一基本推演式，再用 2),3)两条可得 $\mathscr{D}$ 中任一部分推演式. 反过来，N_2 的辅助公式也都属于 $\mathscr{D}$. 引理 2 证毕.

引理 3. 系统 N_2 中的任何一个证明都可以在对数空间中验证. 换言之，存在一个确定型图灵机 M，在对数空间中判定任何字符串是否构成 N_2 的一个证明.

证. 设输入为 $f_0, f_1, f_2, \cdots, f_n$，总长为 L_1. M 依次检查各个 $f_i(i = 0, 1, 2, \cdots, n)$ 是否一个辅助公式或可证公式(不难区别，有→号的一定是一个辅助公式，否则不是). 因为在 N_2 所执行的 4 条任务中，只有第 2 条用到两个前题，故可逐个试验 i^2 个可能的前提对，这只需两个长度 $\log n$ 的计数器. 在选定了前提后，为了检验 f_i 是否可由它们推出，$O(\log L_1)$ 的空间是足够的. 引理 3 证毕.

设 $f \in \Sigma^*$ 被 T 在时间 L 内接受，那么每条带上只有那些距离带头初始位置不超过 L 的方格可能被用到. 所以我们可以假定，一个完全的瞬时描述形为 $x_1 q y_1 \Delta\cdots\Delta x_k q y_k$，且有 $|x_i q y_i| = 2L + 1$. 整个瞬时描述长为 $2k(L + 1) - 1$. 设在计算过程中，瞬时描述每一步的变化为:

$$I_0 \to I_1 \to I_2 \to \cdots \to I_L. \tag{2}$$

考虑其中的 $I_r \to I_{r+s}$，它是 $\mathscr{D}$ 中的一个部分推演式. 设 $x_i q y_i$ 为 I_r 在第 i 条带上的描述字. 因为只经历了 s 步，故在 I_{r+s} 的相应描述字中，只有相应于 x_i 最右边 s 个位置、y_i 的最左边的 s 个位置以及 q 的位置上的符号可能有变化(一共 $2s + 1$ 个). 其余部分不会有变化. 所以我们可把不会有变化的部分从部分推演式的两端省去，得到一个缩短了的形式 $I'_r \to I'_{r+s}$. 它仍然属于 $\mathscr{D}$，我们将用 $P(I_r \to I_{r+s})$ 来表示它. 不难知道，它的长度满足

$$|P(I_r \to I_{r+s})| = 4k(s + 1) - 1 < 8ks. \tag{3}$$

引理 4. 对 $r, s \geqslant 0$，部分推演式 $P(I_r \to I_{r+2s})$ 可由 $P(I_r \to I_{r+s})$ 及 $P(I_{r+s} \to I_{r+2s})$ 在 N_2 中应用两次规则 3)和应用一次规则 2)得到.

证. 考虑 $I_r \to I_{r+s} \to I_{r+2s}$. 设它们在第 i 条带上的描述字分别为 $x_i q y_i$, $x'_i q' y'_i$, $x''_i q'' y''_i$. 我们把 q 为中心长为 $4s + 1$ 的区间记为 $\mathscr{Q}$，把 q 为中心长为 $2s + 1$ 的区间记为 $\mathscr{Q}_1$，把 q' 为中心长为 $2s + 1$ 的区间记为 $\mathscr{Q}_2$，则 $\mathscr{Q}_1$ 和 $\mathscr{Q}_2$ 都是 $\mathscr{Q}$ 的子区间. 我们把 $I_r \to I_{r+s}$ 两端的瞬时描述都限制在 $\mathscr{Q}_1$ 上，记为 $(I_r \to I_{r+s})|\mathscr{Q}_1$ (其实它就是 $P(I_r \to I_{r+s})$). 把 $I_r \to I_{r+s}$ 两端限制在 $\mathscr{Q}$ 上，记为 $(I_r \to I_{r+s})|\mathscr{Q}$. 显然，它可由 $(I_r \to I_{r+s})|\mathscr{Q}_1$ 经由 N_2 应用一次规则 3) 而得到. 同样，$(I_{r+s} \to I_{r+2s})|\mathscr{Q}$ 可由 $(I_{r+s} \to I_{r+2s})|\mathscr{Q}_2$ (即 $P(I_{r+s} \to I_{r+2s})$) 应用一次规则 3)得到. 最后，应用规则 2)，可由 $(I_r \to I_{r+s})|\mathscr{Q}$ 和 $(I_{r+s} \to I_{r+2s})|\mathscr{Q}$ 得到 $(I_r \to I_{r+2s})|\mathscr{Q}$ (即 $P(I_r \to I_{r+2s})$). 引理 4 证毕.

引理 5. 若输入 f 在时间 L 内接受，则 f 在 N_2 中有一个证明，其长度$\leqslant cL\log L$，深度$\leqslant c\log L$，这里 c 是一个与 f 无关的常数.

证. 不妨设 $L = 2^r$. 因为 f 在时间 L 内被 T 接受，所以存在一个瞬时描述串

$$I_0 \to I_1 \to I_2 \to \cdots \to I_L,$$

其中 I_L 的状态是一个接受状态，每个 I_{n+1} 是由 I_n 经过一步得到的. 考虑一串部分推演式

$$P(I_0 \to I_1),\ P(I_1 \to i_2),\ \cdots,\ P(I_{L-1} \to I_L).$$

它们都是基本推演式，每个的长度$<8k$，深度都是 1，总长$\leqslant 8k \cdot 2^r$. 根据引理 4，从它们出发，可应用规则 3) 和规则 2) 得到部分推演式

$$P(I_0 \to I_2),\ P(I_2 \to I_4),\ \cdots,\ P(I_{L-2} \to I_L).$$

它们每个深度为 3，长度$<2 \cdot 8k$，总长$\leqslant 8k \cdot 2^r$. 再由它们出发，可得部分推演式

$$P(I_0 \to I_4),\ P(I_4 \to I_8),\ \cdots,\ P(L_{L-4} \to I_L).$$

它们每个深度为 s，长度$<4 \cdot 8k$，总长$\leqslant 8k \cdot 2^r$. 如此等等. 最后一直得出 $P(I_0 \to I_L)$，它的深度为 $2r+1$. 再用第4)条规则，得到 f 作为输出. 把上面的过程写下来，就得到 f 在 N_2 中的一个证明，其总长$=O(L\log L)$，深度$=O(\log L)$. 引理 5 证毕.

五、定理的证明

我们将在本节中逐步证明前面提到过的三个定理.

引理 6. 如果在一个正规系统中，可证公式 f 的深度为 D，则在同一个系统中，它的证明的长度不超过 c^D；同样，如果可证公式 f 相对于某检验系统的宽度为 W，则它的证明的长度不超过 c^W，这里 c 是一个与 f 无关的常数.

证. 由引理 1 和定义 6 直接可得.

于是，定理 1 和定理 2 都已经被证明了一半. 剩下的另一半在证明了下面的定理 4 之后，也可自然推出.

定理 4. 设 N_1 是一个正规系统，那末存在一个与之等价的正规系统 N_2 和 N_2 的一个检验系统 M，使得对任何可证公式 f 而言，若 f 在 N_1 中的证明长度为 L，则在 N_2 中存在 f 的一个证明，其长度为 $O(L^2\log L)$，深度为 $O(\log L)$，且该证明可在 $O(\log L)$ 的空间中被 M 接受.

引理 7. 对任何正规系统 N_1，都存在一个非确定图灵机 T，使得

1) T 接受的语言恰为 N_1 的可证公式集.

2) 若 f 的证明长度为 L，则 T 接受 f 的时间为 $O(L^2)$.

证. T 非确定地猜测长度 L 和 f 的一个长度为 L 的证明，所需时间是 $O(L)$. 设所猜出的证明为 $f_0, f_1, f_2, \cdots, f_n(f_n = f)$，并且标明了那些是辅助公式，那些是可证公式. T 可以逐个验证每个 $f_i(i = 0, 1, 2, \cdots, n)$ 是否可由前面的公式作为前提而推出. 为此，非确定地选取不超过 k 个前提和 k 个辅助前提，并且记录在 $2k$ 条工作带上，所需时间为 $O(L)$. 然后，T 模拟 N_1 的一步推理，检验是否可以从这些前提得出 f_i 作为结论或辅助结论. 根据引理 1，完成这一步的时间不超过前提总长的一个常数倍，因而等于 $O(L)$. 故整个接受 f 的时间为 $O(nL) = O(L^2)$. 引理 7 证毕.

定理 4 的证明. 对任何正规系统 N_1，可根据引理 7 构造出一个非确定图灵机 T，使得 T 接受的语言恰为 N_1 中的可证公式的集合. 根据上一节的办法，对于 T 又可以构造一个正规系统 N_2，使 N_2 中的可证公式集恰为 T 所接受的语言. 因此 N_1 和 N_2 是等价的. 设 f 是 N_1 中的一个可证公式，证明长度为 L. 那么，T 接受 f 的时间为 $O(L^2)$. 根据引理 5，f 在 N_2 中有一个长度为 $O(L^2\log(L^2)) = O(L^2\log L)$ 的证明. 其深度为 $O(\log(L^2)) = O(\log L)$. 根据引理 3，这个证明可在对数空间中检验. 也即存在一个检验系统 M，M 接变该证明的空间为 $O(\log(L^2)) = O(\log L)$. 定理 4 证毕.

根据定理 4 和引理 6 可得定理 1 及定理 2. 为了能使其中常数 c_1 取为 1，我们需要两个加速定理. 关于空间的加速定理可参见文献 [3]，关于深度的加速定理也不难证明，但不在此赘述. 从定理 1 和定理 2 (取 $c_1 = 1$) 可以立刻得到定理 3.

参 考 文 献

[1] Cook, S., & Sethi, R., *J. Comput. System Sci.*, **13** (1976), 25—37.

[2] Hong, J. W., *Proc. of 21st Symp. on Foundations of Computer Science*, 1980, 348—359.

[3] Hopcroft, J. & Ullman, J., *Introduction to Automata Theory*, Languages and Computation, Addison-Wesley, 1979.