2.15 平面几何定理为什么可以机器证明

数学定理的机器证明是现代数学的重要成就，我国在这方面已有很突出的贡献，例如吴文俊教授、张景中教授和杨路教授等著名数学家在用计算机作平面几何定理的证明等项目上已取得了世界领先的成绩。下面用实例说明平面几何定理何时可以用计算机证明。

例如，已知锐角$\triangle ABC$，向$\triangle ABC$外作正方形$ACDF$，$BCEG$，求

证$BD \perp AE$。

(1) 适当安装直角平面坐标系，把平面几何定理的已知和求证化成代数问题

图 2-49 中 C 点取为原点，B 点坐标不妨设其为$(1,0)$，A 点在上半平面，于是 E 点坐标是$(0,-1)$，记 D 点坐标为(x_1, y_1)，则已知条件可写成

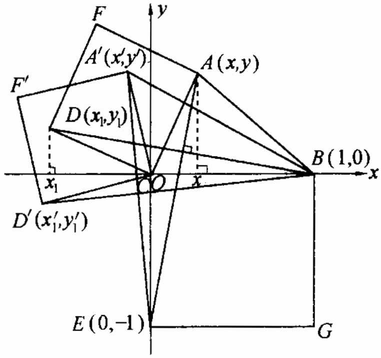

图 2-49

$$\begin{cases} x_1^2 = y^2 & (2.7) \\ x_1 x + y y_1 = 0 & (2.8) \end{cases}$$

求证

$$\frac{y_1 - 0}{x_1 - 1} \cdot \frac{y+1}{x} = -1$$

即求证

$$y_1(y+1) + x(x_1 - 1) = 0 \tag{2.9}$$

是恒等式。

(2) (2.7)、(2.8)、(2.9)方程联立，消去 x_1, y_1 化成只含 x 与 y 两个变元的恒等式

由方程(2.8)和(2.9)得

$$y_1 - x = 0, \; y_1 = x$$

由方程(2.9)得 $y_1 = \dfrac{-x_1 x}{y}$，代入 $y_1 = x$ 得

$$-x_1 x = xy$$

两边平方得

$$x_1^2 x^2 = x^2 y^2$$

由方程(2.7)得

$$y^2x^2=x^2y^2$$

这是一个恒等式，故不论 A 点如何运动，都有 $AE\perp BD$。

方程(2.7)、(2.8)、(2.9)联立消去 x_1, y_1 等参数的过程可用计算机来完成。

一般地，把几何问题化成代数问题之后，如果消元法得到的多项式 $f(x_1,x_2,x_3,\cdots,x_k)=0$ 不明显为恒等式，可用“数值实验”的方法来验证它是否恒等式。

例如 $x^3-1=(x-1)(x^2+x+1)$是恒等式，当时我们是直接进行 $x-1$ 与 x^2+x+1 的多项式乘法便算出了 x^3-1，其实还有比此妙得多的办法：

令 $x=0$，则得 $x^3-1=0^3-1=-1$，$(x-1)(x^2+x+1)=(0-1)(0^2+0+1)=-1$，左＝右。

令 $x=1$，则得 $x^3-1=1^3-1=0$，$(x-1)(x^2+x+1)=0$，左＝右。

令 $x=-1$，则得 $x^3-1=(-1)^3-1=-2$，$(x-1)(x^2+x+1)=(-1-1)((-1)^2-1+1)=-2$，左＝右。

令 $x=2$，则得 $x^3-1=2^3-1=7$，$(x-1)(x^2+x+1)=(2-1)(2^2+2+1)=7$，左＝右。

至此已经证出 $x^3-1=(x-1)(x^2+x+1)$是恒等式。

事实上，如果它不是恒等式而是三次方程，由代数基本定理，它至多有三个实根，而今有四个两两相异的实数都满足它，可见它不是方程，而是恒等式。

对于两个变元的等式 $f(x,y)=0$，其中 $f(x,y)$是 x 最高次数为 m 次，y 的最高次数为 n 次的多项式，m，n 为自然数，则取 x 的 $m+1$ 个特殊值，例如 $x=0,1,2,\cdots,m$，取 y 的 $n+1$ 个特殊值，例如 $y=0$,

$1, 2, \cdots, n$,组成$(m+1)(n+1)$组(x, y)的数组

$$(0,0),(1,0),(2,0),\cdots,(m,0)$$
$$(0,1),(1,1),(2,1),\cdots,(m,1)$$
$$\cdots$$
$$(0,n),(1,n),(2,n),\cdots,(m,n)$$

如果对这些特殊的 x, y 之取值, $f(x, y)$ 皆取零值, 则可判定 $f(x, y)=0$是恒等式。

事实上, $f(x, y)=0$ 可以写成

$$a_0(y)x^m + a_1(y)x^{m-1} + \cdots + a_{m-1}(y)x + a_m(y) = 0 \qquad (2.10)$$

其中 $a_0, a_1, \cdots, a_m$ 是y 的多项式, 次数最高者为 n 次多项式。

由于用$(0,0),(1,0),\cdots,(m,0)$代入(2.10)得出

$$a_0(0)x^m + a_1(0)x^{m-1} + \cdots + a_m(0) = 0$$

所以 $a_0(0)x^m + a_1(0)x^{m-1} + \cdots + a_m(0) \equiv 0$, 同理得

$$a_0(1)x^m + a_1(1)x^{m-1} + \cdots + a_m(1) \equiv 0$$
$$a_0(2)x^m + a_1(2)x^{m-1} + \cdots + a_m(2) \equiv 0$$
$$\cdots\cdots$$
$$a_0(n)x^m + a_1(n)x^{m-1} + \cdots + a_m(n) \equiv 0$$

于是 $a_0(y) \equiv a_1(y) \equiv \cdots \equiv a_m(y) \equiv 0$, 进而 $f(x, y) \equiv 0$。

对于多个变量的等式 $F(x_1, x_2, \cdots, x_n) = 0$, 其中 F 是 $x_1, x_2, \cdots, x_n$的多项式, 对它们的最高次数分别为 x_1 为 m_1 次, x_2 为 m_2 次, $\cdots$, x_n 为 m_n 次, 令 x_1 取值 $0, 1, 2, \cdots, m_1$, x_2 取值 $0, 1, 2, \cdots, m_2$, $\cdots$, x_n 取值 $0, 1, 2, \cdots, m_n$, 把每个数组$(x_1, x_2, \cdots, x_n) = (a_1, a_2, \cdots, a_n)$代入$F=0$后得 $F(a_1, a_2, \cdots, a_n) = 0$, $a_i \in \{0, 1, 2, \cdots, m_i\}$, $i = 1, 2, \cdots, n$, 则可判 $F(x_1, x_2, \cdots, x_n) \equiv 0$。上述数组有$(m_1+1)(m_2+1)\cdots(m_n+1)$个。

下面用著名的“西摩松线”来说明机器证明的步骤。

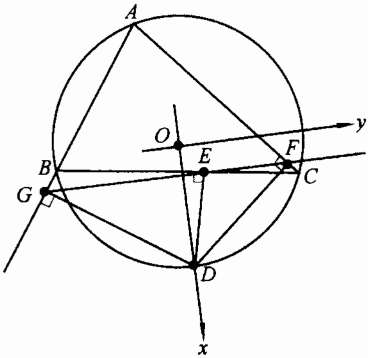

图 2-50

西摩松定理 在$\triangle ABC$的外接圆上(图 2-50)任取一点 D,自 D 向BC, CA, AB 引垂线,垂足依次为 E, F, G,则 E, F, G 三点共线(此直线称为西摩松线)。

取坐标系:外接圆圆心 O 为原点,D 点坐标为$(1,0)$,此外,还有六个点 $A(x_1, y_1)$, $B(x_2, y_2)$, $C(x_3, y_3)$, $E(x_5, y_5)$, $F(x_6, y_6)$, $G(x_7, y_7)$。由已知条件,E, F, G 分别在 BC, AC, AB 上,于是有

$$\begin{cases} x_5 = \lambda x_2 + (1-\lambda)x_3 \\ y_5 = \lambda y_2 + (1-\lambda)y_3 \end{cases}$$

$$\begin{cases} x_6 = \mu x_3 + (1-\mu)x_1 \\ y_6 = \mu y_3 + (1-\mu)y_1 \end{cases}$$

$$\begin{cases} x_7 = \rho x_1 + (1-\rho)x_2 \\ y_7 = \rho y_1 + (1-\rho)y_2 \end{cases}$$

再由已知条件,A, B, C 在单位圆上,故有

$$x_1^2 + y_1^2 = 1,\ x_2^2 + y_2^2 = 1,\ x_3^2 + y_3^2 = 1$$

又已知 $DE \perp BC$, $DF \perp AC$, $DG \perp AB$ 得

$$\begin{cases} [\lambda x_2 + (1-\lambda)x_3 - 1](x_2 - x_3) + \\ [\lambda y_2 + (1-\lambda)y_3](y_2 - y_3) = 0 \\ [\mu x_3 + (1-\mu)x_1 - 1](x_3 - x_1) + \\ [\mu y_3 + (1-\mu)y_1](y_3 - y_1) = 0 \\ [\rho x_1 + (1-\rho)x_2 - 1](x_1 - x_2) + \\ [\rho y_1 + (1-\rho)y_2](y_1 - y_2) = 0 \end{cases}$$

欲证 E, F, G 共线,即求证

$$\frac{y_5 - y_6}{y_5 - y_6} = \frac{y_5 - y_7}{x_5 - x_7}$$

等价于求证

$$(x_5 - x_6)(y_5 - y_7) - (x_5 - x_7)(y_5 - y_6) = 0$$

上面的已知和求证的各代数式(多项式)中有 $x_1, y_1, x_2, y_2, x_3, y_3, x_5, y_5, x_6, y_6, x_7, y_7, \lambda, \mu, \rho$ 15 个变量，有 13 个方程，可以用消去法从中消去 12 个变量，只留下 x_1, x_2, x_3 这三个自由变量组成的等式 $f(x_1, x_2, x_3) = 0$。

这一消元过程由计算机去做。

接下去的工作是用计算机求 $f(x_1, x_2, x_3)$在一些指定点上的值，如果这些指定点上的 f 值皆零，则 $f(x_1, x_2, x_3) \equiv 0$，从而西摩松定理证毕；这些指定点可如下指定：

设 x_1 在 f 中最高次数为 n_1，则取 $x_1 \in \{0, 1, 2, \cdots, n_1\}$，$x_2$ 在 f 中最高次数为 n_2，则取 $x_2 \in \{0, 1, 2, \cdots, n_2\}$，$x_3$ 在 f 中最高次数为 n_3，则取 $x_3 \in \{0, 1, 2, \cdots, n_3\}$，进而取指定点为

$$\begin{cases} (0,0,0), (0,0,1), (0,0,2), \cdots \\ (0,0,n_3-1), (0,0,n_3) \\ (0,1,0), (0,1,1), (0,1,2), \cdots \\ (0,1,n_3-1), (0,1,n_3) \\ \qquad \cdots \\ (0,n_2,0), (0,n_2,1), (0,n_2,2), \cdots \\ (0,n_2,n_3-1), (0,n_2,n_3) \end{cases}$$

$$\begin{cases} (1,0,0), (1,0,1), (1,0,2), \cdots \\ (1,0,n_3-1), (1,0,n_3) \\ \qquad \cdots\cdots \\ (1,n_2,0), (1,n_2,1), (1,n_2,2), \cdots \\ (1,n_2,n_3-1), (1,n_2,n_3) \end{cases}$$

$$\cdots\cdots$$

$$\begin{cases}(n_1,0,0),(n_1,0,1),(n_1,0,2),\cdots \\ (n_1,0,n_3-1),(n_1,0,n_3) \\ \qquad\cdots\cdots \\ (n_1,n_2,0),(n_1,n_2,1),(n_1,n_2,2),\cdots \\ (n_1,n_2,n_3-1),(n_1,n_2,n_3)\end{cases}$$

共计$(n_1+1)(n_2+1)(n_3+1)$个点需要用计算机(器)代入$f(x_1,x_2,x_3)$来求值,如果皆等于零,则证毕。

上面这些“活儿”用手来干当然烦人,但用计算机来干只需几秒钟即可完成。目前已有代数方程组消元的现成软件,用以得到一个单个的欲证其为恒等式的等式;也有现成软件来求多项式在指定点的值。

数学上已有理论(例如代数基本定理)的思想性与现代计算机的运算技术相结合,正在把数学家们从繁琐的证明书写和无味的数字或符号运算的桎梏中解救出来,并能用机器证明各种难以证明的数学定理和解决众多数学难题。例如1997年人造机器IBM公司的“深蓝计算机”在国际象棋盘上运筹博弈,战胜了国际天王级象棋大师卡斯帕罗夫,使人们为之瞠目结舌,叹为观止。

已知与求证中不涉及不等式的初等几何问题,总可以如上面西摩松定理那样,把它用机器化成一个多项式等于零的问题,再用机器证明该多项式是零多项式,即恒等于零,从而完成几何问题的证明。