对角线、悖论、真与可证

哲学系逻辑教研室

简介数理逻辑史上的几个重大结果：

康托尔定理
罗素悖论
塔斯基定理
哥德尔定理

展示其背后一以贯之的简单对角线直观。

一　对角线直观

随便取两个东西，用*0*和*1*代表它们。

取*0*与*1*组成的无穷序列（无穷多）。将它们随便排为：

表1

1 0 0 1 0 0 1 1 …

1 1 1 0 1 1 1 0 …

0 0 0 0 1 1 1 1 …

…

（标红序列称对角线。）

观察：

1）对角线— *1 1 0* …
和它的“反转”— *0 0 1* …，（*0*，*1*互换）
都构成*0-1*序列。

2）每一行都与对角线有一“交点”：

第n行的第n个 = 对角线的第n个。

基本原理

表1中不存在一行，恰好构成对角线的反转。

——否则在交点上，$0 = 1$。矛盾。

这个原理“一望而知”，可称为一种“理性直观”。

我们仅假设$0 \neq 1$，二者不必为自然数。

二　无穷的大小——康托尔定理

记自然数集为**N**。

偶数集为**E**（$= \{0, 2, 4, \ldots\}$）。

二者孰大孰小？

既然**E** $\subset$ **N**，似乎前小后大。

但是，二者之间却有一一对应（**N**到**E**的双射）：

$$f(n) = 2n$$

按一一对应的标准，二者一样大——无穷集可以与自己的真子集一样大。

回忆希尔伯特旅馆：可数集并上可数集……甚至可数多个可数集的并，都是可数集——**N**与有理数集一样大。

那么，有更大的无穷集吗？

考虑从**N**到集合{0, 1}的函数。

这是一种“染色函数”，把每个自然数对应到0或1。（染成红或绿色）。

每个染色函数从**N**中挑出独一的绿数组成的集合，而**N**的每个子集也可染绿，对应独一的函数。所以，这些染色函数与**N**的子集之间有一一对应。

问题：

N有多少子集？就是说，有多少这样的染色函数？

试把这些函数尽量数出来（即用自然数给它们编号），列出其值：

表2

$$
\begin{array}{llllll}
f_0: & f_0(0) & f_0(1) & f_0(2) & \cdots \\
f_1: & f_1(0) & f_1(1) & f_1(2) & \cdots \\
f_2: & f_2(0) & f_2(1) & f_2(2) & \cdots \\
\cdots & & & &
\end{array}
$$

这实际上是一个*0*-*1*序列表，即表1。

对角线：$f_0(0)$ $f_1(1)$ $f_2(2)$ …
对应的函数是$f_n(n)$，仍然是一个染色函数。

反转函数可表为$1 - f_n(n)$，也是染色函数。

根据“基本原理”，反转函数不在表2中，就是说，用光了自然数也没数到它。

<u>定理</u> 上面的染色函数多于自然数。

因此，**N**的子集比自然数多。

N的幂集*P*(**N**)比**N**大——不存在**N**到*P*(**N**)的满射。

就是说，*P*(**N**)是不可数集。

这种对角线直观可进一步抽象：

任给集合A（可以是不可数的）。

1）考虑从A到{0, 1}的染色函数——A-函数。

2）用A中元素“数”A函数，即建立从A到A-函数的映射，形成抽象的函数表：

$F = \{f_x: x \in A\}$

（F不一定能如上那样画出来。）

3）F中的对角线函数$f_x(x)$是一个A-函数，反转函数$1 - f_x(x)$也是。

4）可证：$1 - f_x(x)$不在F中。

（留为思考题，注意“交点”）。

<u>康托尔定理</u>：

对任意集合A，A-函数（或A的子集）多于A中元素。

即P(A)比A大。

因此，从**N**出发，重复取幂集，就得到越来越大的无穷集合：

N，*P*(**N**)，*P*(*P*(**N**))，… （可以超穷次）

“没有最大，只有更大”！

但它们穷尽了无穷集的大小了吗？

连续统问题——

有没有一个集合，其大小介于自然数集**N**与实数集**R**之间？

（康托尔已证明，P(**N**)与**R**一样大。）

这是希尔伯特第一问题。已知ZFC不能判定它。是否需要以及如何判定它，成为哲学问题，推动了集合论的发展。

三　概念问题——罗素悖论

现在令0与1分别代表“假”、“真”二值。

从一类东西到$\{0, 1\}$的函数，弗雷格称为一个概念。

如概念“白”为个体集到$\{0, 1\}$的函数：

白(这只粉笔) = 1
人(那面红旗) = 0
……

还有概念的概念，如“颜色”：

颜色(白) = *1*
颜色(马) = *0*
……

概念f挑出的独一类，称为f的外延，记为ex(f)。于是有：

对任何x，$x \in ex(f)$ iff $f(x) = 1$.

假定**所有**概念组成集合C。

考虑C到{*0*，*1*}的函数：它们仍然是概念（概念的概念），因此应该都属于C。

另一方面，据康托尔定理，它们比C中元素多，因此不会都属于C。矛盾。

这就是罗素悖论的思路。

具体而言，如果强行把这些概念放入C中，那么——

第一，可以用每个概念f为其自身“编号”，即令$f = f_f$，从而把它们“数”完。得到概念表$\{f_f: f \in C\}$，它包含了全部概念，包括：

对角线概念：$f_f(f)$，即$f(f)$——输入为自身；
反转概念：$g(f) = 1 - f(f)$.

第二，g输入g自身（“交点”），结果为：

$$g(g) = 1 - g(g),$$

即

$$g(g) = 1 \quad \text{iff} \quad g(g) = 0.$$

命题g(g)为真 iff 它为假。

罗素悖论1（内涵形式）：

概念g能谓述自身 iff 它不能谓述自身。

（概念f能谓述自身，定义为： $f(f) = 1$ ）

换用外延叙述：

罗素悖论2（外延形式）：

$ex(g) \in ex(g)$ iff $ex(g) \notin ex(g)$.

哥德尔：

“[这些悖论]昭显了一个令人惊异的事实——我们的逻辑直觉（就是说，关于真、概念、是、类等等的直觉）是自相矛盾的。”

——1944，“罗素的数理逻辑”

考虑ex(g)。如果它是某个集合R，则满足：对任何集合X，X ∈ R，当且仅当X ∉ X（R是所有不属于自身的集合的集合）。特别地，

罗素悖论3（集合形式）：R ∈ R，当且仅当R ∉ R。

哥德尔：集合不同于类（概念的外延）。

集合：从下到上，迭次使用“…的集合”运算而得到。这样无法得到R。

概念：从上到下，把某类东西一分为二（如染色，或分为外延与“反外延”）。R是把全体集合一分为二得到的。

解决方案——

1）限制大小：有些聚合太大，因此不是集合。一个概念只能从一个集合中“抓出”一个集合——ZFC.

2）区分集合与类——BG.

3）类型论：概念及外延分为不同的类型，谓述或属于关系只对不同类型的东西有意义——简单类型论。

罗素进一步认为，对角线“概念”f(f)是由全体概念定义的，因此不能再成为一个概念，否则其定义将指涉本身，而导致恶性循环。一般而言，任何一个全体都不能包含只有通过这个全体才能定义的成员——the vicious circle principle.

因此，概念及外延不但有类型，还有阶的区分。

这导致《数学原理》（第一版）中的分支类型论。

四、形式语言中的真——塔斯基定理

继续令0与1代表“假”、“真”二值（合称真值）。我们考察有关自然数的概念。

选择形式算术语言$(0, S, +, \times)$，建立形式算术PA（一阶逻辑 + 皮亚诺公理）。

关于自然数的概念被表为含有自由变元的公式（输入自然数，输出真值$0, 1$）。

如公式$\exists y(x = y + y)$表达概念“…是偶数”。还可以表达“…是素数”等更复杂的概念，包括多元概念（关系）。

哥德尔为每个符号、公式或公式序列α配了唯一的自然数[α]，可称α的名字（哥德尔编码）。

于是，一些关于自然数的概念，同时在谈论公式、证明等，从而表达PA的语法概念。如：

A(x)：x是一个公理（的名字）。

Prov(x, y)：x是公式y的一个证明（的名字）

这些概念是原始递归的，哥德尔证明，它们都能表达为公式。

$\exists y Prov(y, x)$是含有一个自由变元的公式，简记为$P(x)$。

对任何数x， $P(x)$为真 iff x是一个可证公式的名字。所以，

$P(x)$的外延 ＝ 所有可证公式（的名字）的集合。 $P(x)$表达：（在系统中）可证。

将公式名[A]代入$P(x)$：

$P([A])$：公式A可证。

问题：这个语言的语义概念“真”能否在这个语言中用一个公式表达（定义）？

即，语言中是否有（仅有一个自由变元的）公式T(x)，其外延 = 所有真语句（的名字）的集合？

即要求 T(x)满足：对任何语句A，

T([A])的真值 = A的真值。

这是著名的塔斯基“T-模式”。

含有一个自由变元的公式可全部列出，缀以其数值代入（语句），形成下表：

表3

$$F_0(x):\ F_0(0)\ \ F_0(1)\ \ F_0(2)\ \cdots$$
$$F_1(x):\ F_1(0)\ \ F_1(1)\ \ F_1(2)\ \cdots$$
$$F_2(x):\ F_2(0)\ \ F_2(1)\ \ F_2(2)\ \cdots$$
$$\cdots$$

（0, 1, 2, …都是语言中的项）

每个语句取真值，所以，这仍然是表1——每行是一个*0-1*序列。

根据基本原理，表3中没有对角线的反转序列。

即没有某个$F_n(x)$ “拷贝”了反转序列。

换言之，不存在n，使得：

公式$F_n(x)$的值 = $1 - F_x(x)$的值。

所以，也没有某个$F_m(x)$“拷贝”了对角线序列。

否则公式$\neg F_m(x)$（含有一个自由变元）将在表中，它“拷贝”了反转序列。

换言之，不存在m，使得：

公式$F_m(x)$的值 = $F_x(x)$的值。

<u>塔斯基定理：</u>（若PA是一致的，则）算术语言中没有公式T(x)，使得

（T-模式） T([A])的值 = A的值。

否则，T(x)中代入项$[F_x(x)]$，得到$T([F_x(x)])$，它也是有一个自由变元的公式，因此在表3中。但是，根据T-模式，对任何数x，

$T([F_x(x)])$的值 = $F_x(x)$的值。

$T([F_x(x)])$“拷贝”了对角线。矛盾。

【问题：既然对角线$F_x(x)$不是公式（不在表中），那么，它的真值是什么意思？$[F_x(x)]$又是什么？

答： 这里的$F_x(x)$是**N**到$\{0, 1\}$的一个函数：

输入数x——找到公式F_x——代入x——输出代入句的真值。

这是关于自然数的一个概念。塔斯基定理说，这个概念不可定义（不在表中）。

而$[F_x(x)]$是**N**到**N**的 一个函数：

输入数x——找到公式F_x——代入x——输出代入句的名字。

这是一个能行（递归）过程，哥德尔证明，它能表为一个公式，可处理为项。】

总之，算术语言的真概念（谓词）不能在算术语言中定义。

包含算术的形式理论，也不能定义其真概念。

塔斯基的语言分层观点：一个语言的真概念，只表达在其元语言中。

最后回到“交点”：

如果$T([F_x(x)])$——因此$\neg T([F_x(x)])$——在表3中，那么，对某个数n，

$$F_n(x) = \neg T([F_x(x)]).$$

因此“交点”处，$F_n(n) = \neg T([F_n(n)])$

语句$F_n(n)$为真 iff 它为假。或者，
它说自己为假——这就是所谓的说谎者悖论。

五、真与可证——哥德尔定理

现在令*1*与*0*分别代表系统中“可证”与“不可证”二值。则表3成为一个“可证值表”。

考虑可证性概念。如前所述，它在算术语言中表达为可证性谓词：

$$P(x) = \exists y \mathrm{Prov}(y, x)$$

其外延 = 所有可证公式（的名字）的集合。

仿照T-模式，制造以下的P-模式：对任何公式A，

P([A])的（蓝）值 = A的（蓝）值。

问题：能否仿塔斯基定理思路，由P-模式推出一种可证性悖论：

交点句$F_n(n)$ 可证 iff 它不可证？

仿上可得：$P([F_x(x)])$产生了对角线，$\neg P([F_x(x)])$也在表中。

但不能说：$\neg P([F_x(x)])$产生了对角线的反转。

因为，$\neg$表达的是*1*、*0*间的反转运算，而这不必是*1*、*0*间的反转，除非蓝的就是黑的——真与可证重合。

但此时仍有：

交点句$\neg P([F_n(n)]) = F_n(n)$。

它为**真** iff 它不可证。
——它说自身不可证。

如果它的确为真而又不可证，或为假而可证，则这个等值式就成立，而非悖论。

P-模式对系统提出要求：

对任何公式A,

1）若P([A])为真（即A可证），则P([A])可证。

——系统是P-完备的

2）若P([A])为假（即A不可证），则P([A])不可证。

——系统是P-可靠的

假定系统一致，且满足P-模式。有下面推论：

第一，

交点句$F_n(n)$可证
$\Rightarrow$ $P([F_n(n)])$可证（P-完备）
$\Rightarrow$ $\neg P([F_n(n)])$不可证 （系统一致）
$\Rightarrow$ $F_n(n)$ 不可证。

$F_n(n)$不可证。因此它为真（它说它不可证）。真$\neq$可证。

第二，

$\neg F_n(n)$可证

$\Rightarrow$ $\neg\neg P([F_n(n)])$可证

$\Rightarrow$ $P([F_n(n)])$可证（双否定消去）

$\Rightarrow$ $P([F_n(n)])$为真（P-可靠）

与“第一”矛盾。$\neg F_n(n)$也不可证。

记交点句$F_n(n)$为G（哥德尔句）。

由前面推论得：

<u>定理</u>：对于一个一致的形式算术系统,

1）如果它P-完备，则它不能证明G；

2）如果它P-可靠，则它不能证明¬G。

一个形式算术系统是否具有P-完备性，取决于系统的强弱，即它能否证出所有真的P-型句。

可验证，PA是P-完备的。甚至，比PA弱的一些系统，如Robinson算术Q（大致上是PA去掉归纳公理），也是P-完备的。

而P-可靠性，则是某种强的“一致性”：如果假的P-型句不可证，则系统显然是一致的。

文献中，称这里的“P-可靠性”为“1-一致性”（哥德尔用的是更强的“ω-一致性”）。

所以，以上定理可改述为：

哥德尔第一不完全性定理：

对于包含Q的形式算术系统（因此P-完备，比如PA），可以构造语句G，使得：

1）如果系统一致，则它不能证明G；

2）如果系统1-一致，则它不能证明¬G。

简言之，如果系统1-一致（因此一致），则它不完全——有真语句它不能证明。

罗瑟构造了另一个语句R，改进了以上结果，得到通行版本的

哥德尔-罗瑟定理：

包含Q的形式算术系统，如果是一致的，则是不完全的。