離散數學 - 筆記

1. 基礎：邏輯與證明

1.1 邏輯命題

Introduce - 命題

命題通常都是一個明確的陳述句，只會有True或者False兩種結果，不會有兩種結果同時出現的可能。

Example 1

1. Washington, D.C., is the capital of the United States of America.
2. Toronto is the capital of Canada.
3. 1 + 1 = 2.
4. 2 + 2 = 3.

命題 1 和 3 是 True，而命題 2 和 4 是 False

Example 2

1. What time is it?
2. Read this carefully.
3. x + 1 = 2.
4. x + y = z.

1 和 2 不是命題，因為他們並不是陳述句

3 和 4 不是命題，因為他們並沒辦法用True或者False回答

我們習慣用一些英文字母來當作命題變數(例如$p, q, r, s...$)，也就是用英文字母當作命題，就像數字的代數一樣。

如果命題是true，我們習慣用T來表示這個命題是true，而如果命題是false，則會使用F來表示這個命題是false。

Definition - 邏輯非

令p為一命題，p的邏輯非，我們表示為$\neg p$，或者也可以表示為$\overline{p}$，表示在p的條件下，結論不成立。

通常來說，$\neg p$讀做"not p"，而$\neg p$的值與p的值互為反相，也就是若p是true，則$\neg p$就是false，反之亦然。

Example 1

Find the negation of the proposition

"Michael’s PC runs Linux."

and express this in simple English.

The negation of "Michael's PC runs Linux" is "It's not the case that Michael's PC runs Linux."

This negation can be more simply expressed as "Michael's PC doesn't run Linux."

Example 2

Find the negation of the proposition

"Vandana’s smartphone has at least 32GB of memory"

and express this in simple English.

The negation of "Vandana’s smartphone has at least 32GB of memory" is "It's not the case that Vandana’s smartphone has at least 32GB of memory".

The negation can be more simply expressed as "Vandana’s smartphone does not have at least 32GB of memory"

or even more simply as "Vandana’s smartphone has less then 32GB of memory"

Table - 邏輯非的真值表

TABLE 1 The Truth Table for the Negation of a Proposition.

p	$\neg p$
T	F
F	T

Definition - 邏輯與

令p與q為命題，p與q的邏輯與，我們表示為$p \wedge q$，念作"p and q"。

當p與q都為True時，$p \wedge q$才會true，反之為false。

Example

Find the conjunction of the propositions p and q where p is the proposition “Rebecca’s PC has more than 16 GB free hard disk space” and q is the proposition “The processor in Rebecca’s PC runs faster than 1 GHz.”

The conjunction of the propositions p and q is

"Rebecca’s PC has more than 16 GB free hard disk space, and the processor in Rebecca’s PC runs faster than 1 GHz."

Table - 邏輯與的真值表

TABLE 2 The Truth Table for the Conjunction of Two Propositions.		
p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

Definition - 邏輯或

令p與q為命題，p與q的邏輯或，我們表示為$p \vee q$，念作"p or q"。

當p與q都為false時，$p \vee q$為false，反之為true。

Example

What is the disjunction of the propositions p and q where p and q are the same propositions as in Example 5?

The disjunction of the propositions p and q is

"Rebecca’s PC has more than 16 GB free hard disk space, or the processor in Rebecca’s PC runs faster than 1 GHz."

Table - 邏輯或的真值表

TABLE 3 The Truth Table for the Disjunction of Two Propositions.		
p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

Definition - 邏輯異或

令p與q為命題，p與q的邏輯異或，我們表示為$p \oplus q$。

當p或q都同為true或同為false時，$p \oplus q$為false，反之為true。

Definition - 實質蘊涵

令p與q為命題，p與q的 實質蘊涵，我們表示為$p \to q$，表示若p則q。

當p為true且q為false時，則$p \to q$為false，否則為true。

在實質蘊涵中的p，我們稱作前件，而q我們稱作後件

Table - 實質蘊涵的真值表

TABLE 5 The Truth Table for the Conditional Statement $p \to q$.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Example

若期末考考100分，那你就會拿到A。

合理(T)

P：若期末考考100分(T)，則Q：你會拿到A(T)

P：若期末考沒考100分(F)，則Q：你不會拿到A(F)

P：若期末考沒考100分(F)，則Q：你依然可能拿到A(T)

不合理(F)

P：若期末考考了100分(T)，則Q：沒拿到A(F)

Definition - 換位命題

令p與q為命題，p與q的換位命題，我們表示為$q \to p$。

當p為false且q為true時，$q \to p$為false，否則為true。

Example

若期末考考100分，那你就會拿到A。

合理(T)

Q：拿到A，則P：期末考考了100分

Q：沒有拿到A，則P：期末考沒有考100分

Q：拿到A，則P：期末考沒有考100分

不合理(F)

Q：沒有拿到A，則P：期末考考100分

Table - 換位命題的真值表

P	Q	Q → P
0	0	1
0	1	0
1	0	1
1	1	1

Definition - 換質換位命題

令 p 與 q 為一個命題

則一條件敘述 $\neg q \to \neg p$ 稱作換質換位命題

質位互換命題與假設邏輯等價(也就是，$(\neg q \to \neg p) \leftrightarrow (p \to q)$)，可以窮舉真值表來證明。

Table - 換質換位命題的真值表

p	q	$\neg q \to \neg p$	$p \to q$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Definition - 換質命題

令 p 與 q 為一個命題

則一條件敘述 $\neg p \to \neg q$ 稱作換質命題，與換位命題(也就是，$(q \to p) \leftrightarrow (\neg p \to \neg q)$)邏輯等價，可以窮舉真值表來證明。

Table - 換質命題的真值表

p	q	$\neg p \to \neg q$
0	0	1
0	1	0
1	0	1
1	1	1

Definition - 若且為若

令 p 與 q 為一個命題

則一條件敘述$p \leftrightarrow q$稱作若且為若

若p與q皆True，或p與q皆False，則$p \leftrightarrow q$為True，否則為False。

Table - 若為且若的真值表

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

1.2 邏輯命題應用

Example

How can this English sentence be translated into a logical expression?

"You can access the Internet from campus only if you are a computer science major or you are not a freshman."

Let A can access the internet from compus, B are a computer science major, and C are a freshman.

So that the English sentence be translated into $A \to (B \vee \neg C)$

1.3 命題等價

Introduce - 恆真式

恆真式代表複合命題恆為true。

Example

$(p \vee \neg p)$

無論p是True或者False，他都恆為True，稱為tautology(恆真式)

Introduce - 矛盾式

矛盾式代表負和命題恆為false。

Example

$(p \land \neg p)$

無論p是True或者False，他都恆為False，稱為contradiction

Definition - 邏輯等價

令p和q為複合命題，邏輯等價的定義為$p \leftrightarrow q$為恆等式，寫作$p \equiv q$

Example

證明$p \to q$和$\neg p \lor q$為邏輯等價。

我們可以窮舉真值表，來證明兩者為邏輯等價

令$A = p \to q$，$B = \neg p \lor q$，則

p	q	$A = p \to q$	$B = \neg p \lor q$	$A \leftrightarrow B$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	1
1	1	1	1	1

Recall - 德摩根定律

$\neg(p \land q) \equiv \neg p \lor \neg q$

$\neg(p \lor q) \equiv \neg p \land \neg q$

Example 2

證明 $\neg(p \lor q)$ 與 $\neg p \land \neg q$ 邏輯等價。

設$A = \neg(p \lor q)$，$B = \neg p \land \neg q$

我們可以窮舉真值表，來證明兩者為邏輯等價

p	q	$A = \neg(p \lor q)$	$B = \neg p \land \neg q$	$A \leftrightarrow B$
0	0	1	1	1
0	1	0	0	1
1	0	0	0	1
1	1	0	0	1

Example 3

證明 $p \rightarrow q$ 和 $\neg p \vee q$ 邏輯等價。

設$A = p \rightarrow q$，$B = \neg p \vee q$

我們可以窮舉真值表，來證明兩者為邏輯等價。

p	q	$A = p \rightarrow q$	$B = \neg p \vee q$	$A \leftrightarrow B$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	1
1	1	1	1	1

Example 4

證明 $p \vee (q \wedge r)$ 和 $(p \vee q) \wedge (p \wedge r)$ 邏輯等價。

我們可以窮舉真值表，來證明兩者為邏輯等價。

p	q	r	$(q \wedge r)$	$(p \vee q)$	$(p \wedge r)$	$p \wedge (q \vee r)$	$(p \wedge q) \wedge (p \wedge r)$	$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \wedge (p \wedge r)$
0	0	0	0	0	0	0	0	1
0	0	1	0	0	0	0	0	1
0	1	0	0	1	0	0	0	1
0	1	1	1	1	0	0	0	1
1	0	0	0	1	0	0	0	1
1	0	1	0	1	0	0	0	1
1	1	0	0	1	0	0	0	1
1	1	1	1	1	1	1	1	1

Recall - 衡等律

$p \wedge T \equiv p$

$p \vee F \equiv p$

Recall - 支配律

$p \wedge F \equiv F$

$p \vee T \equiv T$

Recall - 冪等律

$p \wedge p \equiv p$

$p \vee p \equiv p$

Recall - 雙非律

$\neg(\neg p) \equiv p$

Recall - 交換律

$p \wedge q \equiv q \wedge p$

$p \vee q \equiv q \vee p$

Recall - 結合律

$(p \vee q) \vee r \equiv p \vee (q \vee r)$

$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$

Recall - 分配律

$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$

Recall - 吸收律

$p \vee (p \wedge q) \equiv p$

$p \wedge (p \vee q) \equiv p$

Recall - 否定律

$p \wedge \neg p \equiv F$

$p \vee \neg p \equiv T$

Recall - 一些有關實質蘊含的邏輯等價

$p \rightarrow q \equiv \neg p \vee q$

$p \rightarrow q \equiv \neg q \rightarrow \neg p$

$p \vee q \equiv \neg p \rightarrow q$

$p \wedge q \equiv \neg(p \rightarrow \neg q)$

$\neg(p \rightarrow q) \equiv p \wedge \neg q$

$(p \rightarrow q) \wedge (p \rightarrow r) \equiv p \rightarrow (q \wedge r)$

$(p \rightarrow r) \wedge (q \rightarrow r) \equiv (p \vee q) \rightarrow r$

$(p \rightarrow q) \wedge (p \rightarrow r) \wedge p \rightarrow (q \vee r)$

$(p \rightarrow r) \vee (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

Recall - 一些有關若為且若的邏輯等價

$p \leftrightarrow q \equiv (p \to q) \land (q \to p)$

$p \leftrightarrow q \equiv \neg p \leftrightarrow \neg q$

$p \leftrightarrow q \equiv (p \land q) \lor (\neg p \land \neg q)$

$\neg(p \leftrightarrow q) \equiv p \leftrightarrow \neg q$

Introduce - 建構新的邏輯等價

如果p與q邏輯等價，且q與r邏輯等價，那麼我們就可以說p與r邏輯等價。

Example 1

證明 $\neg(p \to q) \equiv p \land \neg q$ 邏輯等價

首先，$p \to q \equiv \neg p \lor q$，所以$\neg(p \to q) \equiv \neg(\neg p \lor q) \equiv p \land \neg q$

因此$\neg(p \to q) \equiv p \land \neg q$，證畢

Example 2

利用一連串的邏輯等價，證明 $\neg(p \lor (\neg p \land q)) \equiv \neg p \land \neg q$

利用德摩根定律，得到$\neg(p \lor (\neg p \land q)) \equiv \neg p \land \neg(\neg p \land q)$

再次利用德摩根定律，得到$\neg p \land \neg(\neg p \land q) \equiv \neg p \land (p \lor \neg q)$

利用分配律，$\neg p \land (p \lor \neg q) \equiv (p \land \neg p) \lor (\neg p \land \neg q) \equiv F \lor (\neg p \land \neg q) \equiv (\neg p \land \neg q)$

因此，$\neg(p \lor (\neg p \land q)) \equiv \neg p \land \neg q$，證畢

Example 3

證明 $(p \land q) \to (p \lor q)$為恆等式

利用$p \to q \equiv \neg p \lor q$的特性，改寫為$(p \land q) \to (p \lor q) \equiv \neg(p \land q) \lor (p \lor q)$

利用德摩根定律，改寫為$\neg(p \land q) \lor (p \land q) \equiv (\neg p \lor \neg q) \lor (p \lor q)$

利用交換律，$(\neg p \lor p) \lor (\neg q \lor q) \equiv T \lor T \equiv T$

故$(p \land q) \to (p \lor q)$為恆等式，證畢。

Introduce - 滿足命題

滿足命題的定義是，若有一個複合命題P，若能找到一組變數能夠使P為true，則P能夠被滿足。

Example

判斷以下三個複合命題P是否能夠被滿足。

1. $(p \wedge \neg q) \vee (q \wedge \neg r) \wedge (r \vee \ \neg p)$
2. $(p \wedge q \wedge r) \vee (\neg p \wedge \neg q \wedge \neg r)$
3. $(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$

第一個命題：若p, q, r其中有一個是true，則可以滿足命題：。

第二個命題：若p, q, r都為true或者都為false，則可以滿足命題。

第三個命題：

考慮到

$(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p)$必須要是true，則$p, q, r$都必須要是true，或者$p, q, r$都必須要是false。

$(p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$必須要是true，則$p, q, r$都不能是true，或者都不能是false。

因此，兩者矛盾，故$(p \vee \neg q) \wedge (q \vee \neg r) \wedge (r \vee \neg p) \wedge (p \vee q \vee r) \wedge (\neg p \vee \neg q \vee \neg r)$不能被滿足。

1.4 謂語和限定詞

Introduce - 謂語

命題是具有真假意義的陳述句，而陳述句是由主語與謂語所組成的。

例如我們可以說

1. 阿軒是北科大的學生
2. 阿哲不是北科大的學生

則我們假設$P(x)$為：x是北科大的學生

在這個範例中，$P(x)$為謂語，x為主語，當x被賦予值，則$P(x)$則成為一個命題。

因此則上面兩句分別可以寫成P(阿軒)與P(阿哲)，所得到的結果分別為true與false。

Example 1

若$P(x)$代表$x > 3$，求真值$P(2)$與$P(4)$

$P(2)$等於$2 > 3$，則$P(2)$的真值為false。

$P(4)$等於$4 > 3$，則$P(4)$的真值為true。

Example 2

若$A(x)$代表「電腦x正在被入侵者攻擊」，且我們假設正在被入侵者攻擊的電腦為$CS2$與$MATH1$

則求真值$A(CS1)$與$A(CS2)$，以及$A(MATH1)$

我們可以很清楚的知道，$CS2$與$MATH1$正在被攻擊，因此我們可以知道$A(CS2) = T$，$A(MATH1) = T$

而$CS1$沒有被攻擊，故$A(CS1) = F$

Example 3

若$Q(x,y)$代表敘述$x=y+3$，則求真值$Q(1,2)$與$Q(3,0)$

$Q(1,2) \Rightarrow 1 \neq 2+3 \Rightarrow Q(1,2)=F$

$Q(3,0) \Rightarrow 3=0+3 \Rightarrow Q(3,0)=T$

Example 4

令$A(c,n)$代表「電腦c連接著網路n」，其中c代表電腦而n代表著網路，假設$MATH1$正在連接著網路$CAMPUS2$而不是$CAMPUS1$，求$A(MATH1, CAMPUS1)$與$A(MATH1, CAMPUS2)$的真值。

因為$MATH1$沒有連接著網路$CAMPUS1$，因此$A(MATH1, CAMPUS1)$為false

而$MATH1$連接著網路$CAMPUS2$因此$A(MATH1, CAMPUS2)$為true

Example 5

令$R(x,y,z)$代表$x+y=z$，求真值$R(1,2,3)$與$R(0,0,1)$

因為$R(1,2,3)$代表$1+2=3$，因此$R(1,2,3)$為true。

因為$R(0,0,1)$代表$0+0=1$，因此$R(0,0,1)$為false。

Introduce - 量化

量化用來決定一個謂詞，在一定的事物上成立的程度。

產生量化的語言叫作量詞。

舉個例子，「我**所有**的玻璃都破了」，「**大量**的人是聰明的」。

通常來說，有兩種量化的類型：全稱量化、存在量化

Definition - 全稱量化

對於$P(x)$來說，全稱量化的代表對於所有在P的定義域內的x，我們可以寫作$\forall x P(x)$

$\forall$符號代表全域量詞，我們把$\forall x P(x)$讀作"for all $x, P(x)$" 或者"for every $x, P(x)$"。

若存在一個x，使得$P(x)$為false，則我們把他稱作$\forall x P(x)$的反例。

Table - 量化類別

敘述	什麼時候為true	什麼時候為false
$\forall x P(x)$	對於所有在$P(x)$定義域中的x，$P(x)$都為true。	存在一個x使得$P(x)$為false
$\exists x P(x)$	存在一個x使得$P(x)$為true	對於所有在$P(x)$定義域中的x，$P(x)$都為false。

Example 1

令$P(x)$代表$x+1>x$，對於所有實數域中的x，$\forall xP(x)$的真值為何

我們可以清楚知道，對於所有實數域中的x，$x+1$都大於x，找不到一個反例使的$x+1<x$，因此$\forall xP(x)$的真值為true。

Example 2

令$Q(x)$代表$x<2$，對於所有實數域中的x，$\forall xP(x)$的真值為何

當$Q(0),Q(1)$的時候$Q(x)$為true，但$Q(2)$為false，故$\forall xP(x)$為false。

Example 3

令$P(x)$代表$x^2<10$，求所有不超過4的正整數中，$\forall xP(x)$的真值為何

我們可以把真值表達成$P(1)\wedge P(2)\wedge P(3)\wedge P(4)$

但是$P(4)$為false，因為$4^2<10$

所以$\forall xP(x)$為false。

Example 4

令$P(x)$代表$x^2\geq x$，若x的定義域為所有實數，則$\forall xP(x)$的真值為何？

若x的定義域為所有整數，那麼$\forall xP(x)$的真值又為何？

我們可以找到一個反例，若$x=0.5$，則$0.5^2<0.5$。

故若x的定義域為所有實數，則$\forall xP(x)$的真值為false。

但若x的定義域為所有整數，我們找不到任何一個反例能夠證明$\forall xP(x)$的真值為false。

故若x的定義域為所有整數，$\forall xP(x)$的真值為true。

Definition - 存在量化

對於$P(x)$來說，存在量化的代表對於至少一個在P的定義域內的x，我們可以寫作$\exists xP(x)$，$\exists$符號代表存在量詞

若不存在一個x，使得$P(x)$為true，則我們把他稱作$\exists xP(x)$的反例。

Example 1

令$P(x)$代表$x>3$，若x的定義域為所有實數，則$\exists xP(x)$的真值為何？

我們可以找到$x=4$使得$x>3$成立，故$\exists xP(x)$的真值為true。

Example 2

令$Q(x)$代表$x = x + 1$，若x的定義域為所有實數，則$\exists xQ(x)$的真值為何？

我們找不到任何一個實數，使得$x = x + 1$，故$\exists xQ(x)$為false。

Example 3

令$P(x)$代表$x^2 > 10$，若x的定義域為不超過4的正整數，則$\exists xP(x)$的真值為何？

我們可以知道$x \in \{1, 2, 3, 4\}$

所以我們可以寫成$P(1) \vee P(2) \vee P(3) \vee P(4)$

由於我們可以知道，$4^2 = 16 > 10$ ，因此$P(4)$為true

故$P(1) \vee P(2) \vee P(3) \vee P(4)$為true

因此$\exists xP(x)$為true

Introduce - 唯一量化

我們可以使用$\exists !xP(x)$，用來表示「唯一一個」、「正好一個」、「剛好一個」x使得$P(x)$為真。

例如，令$P(x)$代表$x - 2 = 4$，則$\exists !xP(x)$成立，因為我們可以找到$x = 6$，使得$P(6)$為true

除此之外我們找不到任何的x，使得$P(x)$為true，故$\exists !xP(x)$為true。

Introduce - 限定定義域的量詞

通常來說， 我們可以透過縮寫，來表示定義域所需要符合的條件。

例如說$\forall x > 0(x^2 > x)$，且定義域為所有實數，則代表說，對於所有大於0的實數，使得$x^2 > x$。

Example

若下列敘述的定義域皆為$x \in \mathbb{R}$，求$\forall x < 0(x^2 > 0)$，$\forall y \neq 0(y^3 \neq 0)$，還有$\exists z > 0(z^2 = 2)$的意義。

第一個例子，若$x < 0$，則$x^2 > 0$，則我們可以寫成$(x < 0) \rightarrow (x^2 > 0)$

且所有的實數x都要符合這個敘述，因此$\forall x[(x < 0) \rightarrow (x^2 > 0)]$

第二個例子，若$y \neq 0$，則$y^3 \neq 0$，則我們可以寫成$(y \neq 0) \rightarrow (y^3 \neq 0)$

且所有的實數y都要符合這個敘述，因此$\forall y[(y \neq 0) \rightarrow (y^3 \neq 0)]$

第三個例子，若$z > 0$，則$z^2 = 2$，則我們可以寫成$(z > 0) \wedge (z^2 = 2)$

且至少一個z都要符合這個敘述，因此$\exists z[(z > 0) \wedge (z^2 = 2)]$

Introduce - 量詞的優先級

$\forall$與$\exists$是所有邏輯符號中優先級最高的，也就是若$\forall xP(x) \vee Q(x)$，他代表著$(\forall xP(x)) \vee Q(x)$，而非$\forall x(P(x) \vee Q(x))$

Introduce - 綑綁變數

如果量詞用在變數x上，則我們說變數x為一個綑綁變數，否則他就是自由變數。

一個命題函數所有變數都必須為綑綁變數，則這個命題變數才會變成一命題。

無論是存在量化、全稱量化都可以使用

Example 1

在敘述$\exists x(x+y=1)$中，我們可以知道x是綑綁變數，因為前面的存在量詞是對x的

但是沒有任何對y的量化，因此y為一個自由變數。

Example 2

在敘述$\exists x(P(x) \wedge Q(x)) \vee \forall x R(x)$，所有的變數都是綑綁變數

第一個存在量詞對括號內所有的x進行綑綁，而第二個存在量詞對命題函數R的變數x進行綑綁。

Example 3

在敘述$\exists x(P(x) \wedge Q(x)) \vee \forall y R(y)$，所有變數都是綑綁變數

第一個存在量詞對括號內所有的x進行綑綁，而第二個存在量詞對命題函數R的變數y進行綑綁。

Introduce - 關於量化的邏輯等價

Definition - 量化的邏輯等價

關於量詞與謂語的邏輯等價，若兩邊敘述若為且若擁有相同的真值，則我們稱他為邏輯等價。

不用考慮謂語如何替代敘述，或者在命題函數中的定義域為何。

Example

證明$\forall x(P(x) \wedge Q(x))$與$\forall P(x) \wedge \forall Q(x)$邏輯等價。

若要證明$\forall x(P(x) \wedge Q(x))$與$\forall P(x) \wedge \forall Q(x)$邏輯等價

則我們假設$a \in D(x)$，其中$D(x)$代表x的定義域，那麼如果$\forall x(P(x) \wedge Q(x))$是true，則$P(a) \wedge Q(a)$都為true。

達成與邏輯為正的條件即為$P(a)$與$Q(a)$皆為true，則與邏輯才會成立。

接著，假設$\forall x P(x) \wedge \forall x Q(x)$為true，且$a \in D(x)$

那麼為了達成與邏輯的條件，$P(a)$應為true，$Q(a)$也應為true。

故$P(a) \wedge Q(a)$應為true，而$a \in D(x)$，則代表所有在$D(x)$的變數a都可以使得$P(a) \wedge Q(a)$為true

故我們可以把a改寫成$\forall x(P(x) \wedge Q(x))$

因此，我們可以得知，$\forall x(P(x) \wedge Q(x))$與$\forall x P(x) \wedge \forall x Q(x)$邏輯等價。

Introduce - 邏輯非的量化表達式

Introduce - 全稱量化的邏輯非

思考以下的敘述

「在這間教室所有人都修過微積分」

若我們利用謂語取代敘述的部分，則我們可以令$P(x)$為「x修過微積分」，而x的定義域限定為在這間教室的人

故敘述可以表達成$\forall x P(x)$

而若不是所有人都修過微積分，則必定在教室有一個人x使得$P(x)$為false。

因此，我們可以表達成，若不是所有人都修過微積分，則我們可以用存在量化來表示

也就是$\exists x \neg P(x)$

因此，我們可以知道，$\neg(\exists x \neg P(x)) \equiv \forall x P(x)$

兩邊邏輯等價同取邏輯非，則$\neg\neg(\exists x \neg P(x)) \equiv \neg \forall x P(x)$

也就是$\exists x \neg P(x) \equiv \neg \forall x P(x)$

Introduce - 存在量化的邏輯非

思考以下敘述

「在這間教室，至少有一個人修過微積分」

若我們利用謂語取代敘述的部分，則我們可以令$P(x)$為「x修過微積分」，而x的定義域限定為在這間教室的人

故敘述可以表達成$\exists x P(x)$

而若不是至少有一個人修過微積分，則必定在定義域內所有的x都能使$\exists x P(x)$為false。

因此，我們可以表達成，若沒有人修過微積分，則我們可以用全稱量化來表示

也就是$\forall x \neg P(x)$

因此我們可以知道，$\neg(\forall x \neg P(x)) \equiv \exists x P(x)$

兩邊邏輯等價同取邏輯非，則$\neg\neg(\forall x \neg P(x)) \equiv \neg \exists x P(x)$

也就是$\forall x \neg P(x) \equiv \neg \exists x P(x)$

Table - 量化表達式的德摩根定律

量化表達式	取邏輯非後的量化表達式
$\forall x P(x)$	$\exists x \neg P(x)$
$\exists x P(x)$	$\forall x \neg P(x)$

Example

求$\forall x(x^2 > x)$與$\exists x(x^2 = 2)$的反邏輯。

對於所有的x，$x^2 > x$皆成立

而他的反邏輯即為存在一個x使得$x^2 > x$不成立

故我們可以寫成存在一個x使得$x^2 \leq x$

因此，$\neg\forall x(x^2 > x) \equiv \exists x(x^2 \leq x)$

存在一個x使得$x^2 = 2$成立

而他的反邏輯即為使所有的x讓$x^2 = 2$不成立

故我們可以寫成讓所有的x使得$x^2 \neq 2$

因此，$\neg\exists x(x^2 = 2) \equiv \forall x(x^2 \neq 2)$

x的值取決於定義域。

1.5 嵌套限定詞

Introduce - 嵌套量詞

在1.4的章節，我們通常都只會用到一個量詞，而量詞是可以被嵌套的。

舉個例子，就像這樣：$\forall x\exists y(x+y=0)$，一層一層套上的量詞

而我們也可以改個表達方式，令$Q(x)$為$\exists yP(x,y)$，而$P(x,y)$為$x+y=0$

則利用$\forall xQ(x)$，就能表達$\forall x\exists y(x+y=0)$

也就能表達在定義域$D(x)$內的所有x，都存在一個$y \in D(y)$使得$x+y=0$

Introduce - 嵌套量詞的順序

Example 1

若我們考慮$\forall x\forall y(x+y=y+x)$，則他唸起來會像

「對於每一對的(x,y)，$\forall x\forall y(x+y=y+x)$均成立。」

而若我們變換一下順序，寫作$\forall y\forall x(x+y=y+x)$，則他唸起來會像

「對於每一對的(y,x)，$\forall y\forall x(x+y=y+x)$均成立。」

因此，我們可以知道，兩個不同的全稱量詞對換是不會影響命題本身的。

Example 2

1. 若我們考慮$\exists x\forall y(x+y=0)$，且$x,y$的定義域為所有實數
   則他唸起來會像，存在一個x，使得每一種y都能符合$x+y=0$
   這個命題很明顯是false，因為不存在任何一個x，使得每一種y都能符合$x+y=0$。
2. 若我們考慮$\forall x\exists y(x+y=0)$，且$x,y$的定義域為所有實數
   則他唸起來會像，對於每一個屬於實數的x，存在一種y能符合$x+y=0$
   這個命題就會是true，因為只要使$y=-x$，就能使敘述成立。

因此，兩者對調是會影響命題本身的。

Example 3

令$Q(x, y, z)$代表敘述$x + y = z$，若x, y, z的定義域為所有實數，試求$\forall x \forall y \exists z Q(x, y, z)$和$\exists z \forall x \forall y Q(x, y, z)$的真值。

1. 若我們考慮$\forall x \forall y \exists z Q(x, y, z)$，則他唸起來會像，對於所有的$x$與所有的$y$，存在一個$z$，使得$x + y = z$
   這樣是合理的，無論x與y的值為多少，兩個實數相加必定為另一個實數，故$\forall x \forall y \exists z Q(x, y, z)$的真值為true
2. 若我們考慮$\exists z \forall x \forall y Q(x, y, z)$，則他唸起來會像，存在一個$z$使得對於所有的$(x, y)$，都能符合$x + y = z$
   這樣是不合理的，因為找不到一種z，使得任意的(x, y)對符合$x + y = z$，故$\exists z \forall x \forall y Q(x, y, z)$的真值為false

綜合上述，兩者的量詞互換，會影響到命題的結果。

Table - 兩個嵌套量詞的意義

Statement	*When True?*	*When False?*
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	$P(x, y)$ is true for every pair x, y.	There is a pair x, y for which $P(x, y)$ is false.
$\forall x \exists y P(x, y)$	For every x there is a y for which $P(x, y)$ is true.	There is an x such that $P(x, y)$ is false for every y.
$\exists x \forall y P(x, y)$	There is an x for which $P(x, y)$ is true for every y.	For every x there is a y for which $P(x, y)$ is false.
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	There is a pair x, y for which $P(x, y)$ is true.	$P(x, y)$ is false for every pair x, y.

Introduce - 嵌套量詞的負邏輯

負邏輯一樣可以用在嵌套量詞上。

Example

請找出$\forall x \exists y (xy = 1)$的負邏輯命題

命題翻譯會變成，對於所有的x，存在一個y使得$xy = 1$

那麼對於這個命題加上負邏輯，則變成了存在一個x，使得所有可能的y，讓$xy = 1$不成立。

故我們可以寫成$\exists x \forall y \neg (xy = 1)$

而$\neg (xy = 1)$又可以寫成$(xy \neq 1)$

故整個式子可以寫成$\exists x \forall y (xy \neq 1)$

1.6 推論規則

Introduce - 肯定前件

若$P \equiv T$，且$P \to Q \equiv T$，則$Q \equiv T$

Example

你考到了100分。

若你考到100分，就會得到A。

所以，你會得到A。

Introduce - 否定後件

若$\neg Q \equiv T$，且$P \to Q \equiv T$，則$\neg P \equiv T$

Example

你沒有得到A。

若你考到100分，就會得到A。

所以你沒有考到100分。

Introduce - 三段論證

若$P \to Q \equiv T$，且$Q \to R \equiv T$，則$P \to R \equiv T$

Example

若你難過，就吃東西

若你吃東西，就可能會變胖

所以你難過就可能會變胖。

Introduce - 選言三段論

若$P \vee Q \equiv T$，且$\neg P \equiv T$，則$Q \equiv T$

Example

我要嘛選擇睡覺，要嘛選擇讀書。

我沒在睡覺。

所以我在讀書。

Introduce - 添加律

若$P \equiv T$，則$P \vee Q \equiv T$

Example

若我在睡覺。

所以我可能在睡覺或者在讀書。

Introduce - 簡化律

若$P \wedge Q \equiv T$，則$P \equiv T$

Example

外面是晚上而且外面在下雨

所以外面是晚上。

Introduce - 連言

若$P \equiv T$，且$Q \equiv T$，則$P \wedge Q \equiv T$

Example

外面是晚上。

外面在下雨。

所以外面是晚上，而且外面在下雨。

Introduce - 預解律

若$P \vee Q \equiv T$，且$\neg P \vee R \equiv T$，則$Q \vee R \equiv T$

Example

外面是晚上或者外面在下雨。

且外面是白天或者外面在放晴。

則外面在下雨或者外面在放晴。

Introduce - 全稱實例化

若$\forall x P(x) \equiv T$，則若$c \in D(x)$，則$P(c) \equiv T$

Example

所有資工系的學生都修過微積分

若小碩是資工系的學生

則小碩修過微積分

Introduce - 全稱普遍化

若$c \in D(x)$，且$P(c)$ for an arbitrary c，則$\forall x P(x) \equiv T$

Example

若小碩是資工系的學生

所有資工系的學生都修過微積分

則小碩修過微積分

Introduce - 存在實例化

若$\exists x P(x) \equiv T$，則$P(c) \equiv T$ for some element c

Introduce - 存在普遍化

若$P(c) \equiv T$ for some element c，則$\exists x P(x) \equiv T$

1.7 Introduce to proof

Introduce - 定理

定理是一個可以被證明的敘述。

Introduce - 公理

公理是一個不需要證明，假設正確的敘述。

Example

$\forall x, y \in \mathbb{R}$，$x + y \in \mathbb{R}$是一個公理。

Introduce - 引理

引理是較不重要的敘述，用來協助證明其他的結果。

Introduce - 系理

系理是一個定理，由另一個定理推導出另一個顯而易見的定理。

Introduce - 猜想/假說

猜想(假說)是一個定理，被提出但沒有人能夠證明正確與否。

Example

費馬大定理：$x^n + y^n = z^n$

當$n \in \mathbb{Z}$且$n > 2$時，(x, y, z)沒有整數解。

Example

試證明，若$n \in odd$，則$n^2 \in odd$

我們可以寫成$\forall n(P(n) \rightarrow Q(n))$，$P(n)$代表$n$是奇數，而$Q(n)$代表$n^2$是奇數。

假設$n \in odd$，則$n = 2k + 1, k \in \mathbb{Z}$

則$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$

則我們可以知道$2k^2 + 2k$必定是某個整數

由於偶數乘以任何整數均為偶數，故偶數+1必為奇數

故n^2必為奇數。

Introduce - 反證法

若$P \rightarrow Q$證明較為困難，則證明與$P \rightarrow Q$等價的$\neg Q \rightarrow \neg P$。

Example

試證明，若$n \in \mathbb{Z}$，且$3n + 2$是奇數，則n是奇數。

我們可以寫成$\forall n(P(n) \rightarrow Q(n))$，$P(n)$代表$3n + 2$是奇數，$Q(n)$代表$n$是奇數。

則我們利用反證法，證明$\forall n(\neg Q(n) \rightarrow \neg P(n))$，也就是證明對於所有的整數$n$，若$n$是偶數，則$3n + 2$是偶數。

則n可以寫成$2k$的形式，因此$3n + 2 = 6k + 2$，$k \in \mathbb{Z}$

由於偶數乘以任何整數均為偶數，且偶數加上任何偶數均為偶數

故我們可以證明，若n是偶數，則$3n + 2$是偶數。

故若$n \in \mathbb{Z}$，且$3n + 2$是奇數，則n是奇數。

Introduce - 空泛證明

若$P \equiv F$，則證明完成。

Example

試證明，如果$0 > 1$，則$0^2 > 0$

我們可以寫成$P \rightarrow Q$，其中P為$0 > 1$，且Q為$0^2 > 0$

但$P \equiv F$，則Q不可能發生，證畢。

Introduce - 平庸證明

若$Q \equiv T$，則證明完成。

Example

設$a, b \in \mathbb{Z}$，若$a \geq b$，則$a^0 \geq b^0$

我們可以寫成$\forall a \forall b (P(a, b) \rightarrow Q(a, b))$，其中$P(a, b)$為$a \geq b$，且$Q(a, b)$為$a^0 \geq b^0$

則由於無論a, b為何，$a^0 = b^0$，故$\forall a \forall b Q(a, b) \equiv T$，故$\forall a \forall b (P(a, b) \rightarrow Q(a, b)) \equiv T$

Introduce - 歸謬證明法

有兩種用途

用途	假設	矛盾
P is true	$\neg P$ is true	$\neg P \rightarrow F$
$P \rightarrow Q$ is true	P is true, $\neg Q$ is true	$(P \wedge \neg Q) \rightarrow F$

1.8 Exhaustive Proof

Example 1

$(n+1)^3 \geq 3$，$n \in \mathbb{Z}^+, n \leq 4$

若$n = 1$，則$2^3 = 8 \geq 3$，

若$n = 2$，則$3^3 = 27 \geq 3$

若$n = 3$，則$4^3 = 64 \geq 3$

若$n = 4$，則$5^3 = 125 \geq 3$

故$(n+1)^3 \geq 3$成立。

Example 2

若$n \in \mathbb{Z}$，則$n^2 \geq n$

設$\forall n P(n)$代表對於所有實數n，$n^2 \geq n$

分成三個case分開做處理。

$n = 0$，$0 = 0$，故$P(0)$成立。

$n \geq 1$，已知$n \geq 1$，則兩邊同乘以$n^2 \geq n$，故$n^2 \geq n$成立。

$n \leq 1$，已知$n^2 \geq 0$，故$n^2 \geq n$

故$\forall n P(n)$成立

Introduce - 建構式證明

建構式證明可以分成存在證明或不存在證明。

Example 1

請證明可以找到一個整數，這個整數可以用兩個以上不同的立方和所組成。

我們可以找到一個數字1729，且$1729 = 10^3 + 9^3$且$1729 = 12^3 + 1^3$，故證明完畢。

Example 2

請證明可以找到一個無理數x與y，使得x^y為有理數。

分成兩個case

若$\sqrt{2}^{\sqrt{2}}$是有理數，則$x = \sqrt{2}, y = \sqrt{2}$

若$\sqrt{2}^{\sqrt{2}}$是無理數，則$x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$，$x^y = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$

則這兩者其中之一可以符合命題。

Introduce - 存在證明

存在一個x，使得$P(x)$為true，且除了x以外的y，使得$P(x)$為false。

$\exists x(P(x) \land \forall y(y \neq x \rightarrow \neg P(y)))$

Introduce - 反例

Example

試證明，每個正整數，是三個整數的平方和。

若正整數為1，則我們找不到任意一組$(x, y, z) \in \mathbb{Z}$，使得$x^2 + y^2 + z^2 = 1$，故假說錯誤。

2. 基礎結構: 集合、函數、序列、總和、與矩陣

2.1 集合

Definition - 集合

集合是一個不需按照順序排列，且集合內部所有元素均不相等的物件。

$a \in A, a$ 是集合 A 的元素之一。

$a \notin A, a$ 不是集合 A 的元素之一。

Example

$\{a, b\} = \{b, a\}$

$\{\text{a, a, b}\} = \{\text{a, b}\}$

$(a, b) \neq (b, a)$

Introduce - 窮舉法

如果窮舉出集合內的所有物件是可能的，我們可以窮舉出集合內的所有物件。

Example 1

所有母音的集合。

$V = \{a, e, i, o, u\}$

Example 2

所有小於100的正整數的集合。

$O = \{1,\ 2,\ 3,\ \ldots\ 99,\ 100\}$

Introduce - 集合建構式符號

$\{\text{x} \mid \text{x has property P}\}$，念作「所有符合條件$P$元素$x$的集合」。

Example 1

所有小於10的正整數奇數集合。

$O = \{1, 3, 5, 7, 9 \ldots\}$

$O = \{\text{x} \mid \text{x is an odd positive integers less than 10}\}$

$O = \{2x + 1 \mid 0 \leq x \leq 4\}$

Example 2

所有正的有理數，且為整數的集合$\mathbb{Q}^+$。

$\mathbb{Q}^+ = \{x \in \mathbb{R} \mid x = \dfrac{a}{b} \text{ for some positive integers p and q.}\}$

Example 3

所有自然數的整數集合。

$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$

Example 4

所有整數的集合。

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

Example 5

所有正整數的集合。

$\mathbb{Z}^+ = \{0, 1, 2, \dots\}$

Example 6

所有有理數的集合。

$\mathbb{Q} = \{\frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0\}$

Definition - 集合相等

若兩個集合的所有元素相等，則我們說這兩個集合相等。

$A = B \iff (x \in A \to x \in B)$

Example

$\{1, 3, 5\} = \{3, 5, 1\}$

$\{1, 3, 3, 3, 5, 5, 5, 5\} = \{1, 3, 5\}$

Definition - 空集合

空集合沒有任何元素，寫作 $\varnothing$。

Definition - 單元素集合

單元素集合只有一個元素。

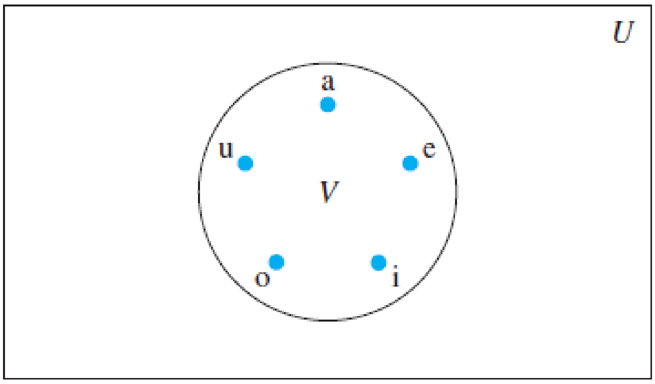
Example

$\{\varnothing\}$ 是一個單元素集合。

Introduce - 文氏圖

我們可以用文氏圖來表示一個集合。

Example



$U = \{\mathrm{a, b, c, d, e, f, g} \ldots\}$

$V = \{\mathrm{a, e, i, o, u}\}$

Definition - 子集合

若為且若集合A的每個元素都為集合B的元素，則我們說A是B的子集合，且B為A的父集合。

可以表示成$(A \subseteq B \wedge B \supseteq A) \iff \forall x(x \in A \rightarrow x \in B)$

Theorem - 1

對於每一個集合 $S, \varnothing \subseteq S, S \subseteq S$

$\{\} \subseteq \{\}$

$\{\} \subseteq \{a\}$

$\{a\} \subseteq \{a\}$

$\{\} \subseteq \{a, b\}$

$\{a\} \subseteq \{a, b\}$

$\{b\} \subseteq \{a, b\}$

$\{a, b\} \subseteq \{a, b\}$

如果一個集合有n個元素，則他會有$n!$種不同的子集合。

Introduce - 真子集

若A是B的真子集，則對於所有在集合A的x也都在集合B，且B存在一個元素不在集合A。

可以寫作，$A \subset B \iff \forall x(x \in A \rightarrow x \in B) \wedge \exists x(x \in B \wedge x \notin A)$。

Definition - 有限集合與無限集合

如果一個集合有剛好n個元素，且n存在，則我們說這個集合是有限的，否則這個集合是無限的。

Definition - 集合的勢

若有一個集合A，我們定義「集合的勢」為集合內部的元素數量，寫作$|A|$。

Example 1

$|\varnothing| = 0$

Example 2

令集合S為擁有所有字母的集合，則$|S| = 26$

Example 3

$|\{1, 2, 3\}| = 3$

Example 4

$|\{\varnothing\}| = 1$

Example 5

若S為所有整數的集合，則$|S|$為無限。

Introduce - 冪集

若存在一個集合有集合A的所有子集，我們寫作$\wp(A)$。

如果集合A有N個元素，則$|\wp(A)| = 2^N$。

Example

若$A = \{a, b\}$，則$\wp(A) = \{\{\varnothing\}, \{a\}, \{b\}, \{a, b\}\}$

Introduce - 多元組

- 一個有序且長度為n的多元組包含了元素$(a_1, a_2, a_3, \dots a_n)$，且$a_1$是第一個元素，$a_n$是最後一個元素。
- 兩個長度為n的多元組A, B，我們先用A_i表示多元組A的第i個元素。

  若兩個多元組的每一項都相同，也就是$A_1 = B_1, A_2 = B_2, \dots, A_n = B_n$，則兩個多元組就是相同的。
- 長度為2的多元組我們稱作有序對。
- 若有兩個有序對(a, b)與(c, d)，則若$a = c$且$b = d$，則兩個有序對才相同。

Example

若有兩個長度為n的多元組A, B。

$A = (1, 2, 3, 4, 5)$，$B = (5, 4, 3, 2, 1)$，則$A \neq B$

$A = (1, 2, 3, 4, 5)$，$B = (1, 2, 3, 4)$，則$A \neq B$

$A = (1, 2, 3, 4, 5)$，$B = (1, 2, 3, 4, 5)$，則$A = B$

Introduce - 笛卡兒積

兩個集合A, B相乘，我們稱作笛卡爾積，寫作$A \times B$。

$A \times B$是一個集合，包含了所有不同的有序對(a, b)，其中$a \in A$，$b \in B$

我們可以寫成這樣：$A \times B = \{(a, b) | a \in A \wedge b \in B\}$

Example

若集合$A = \{a, b\}$，集合$B = \{1, 2\}$

則$A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2)\}$

Introduce - 笛卡兒積的子集合

在笛卡爾積的子集合R，我們可以說與集合A和集合B都有關係。

Introduce - 多個集合的笛卡兒積

若我們有m個集合$A_1, A_2, A_3, \ldots, A_M$，則笛卡爾積寫作$A_1 \times A_2 \times \ldots \times A_M$。

則$A_1 \times A_2 \times \ldots \times A_M = (a_1, a_2, \ldots, a_n)$，為一個有序多元組的集合，其中$a_i \in A_i, i = 1, 2, \ldots, n$。

Example

若$A = \{0, 1\}$，$B = \{1, 2\}$，$C = \{0, 1, 2\}$，求$A \times B \times C$

$$A \times B \times C = \{(0,1,0), (0,1,1), (0,1,2), (0,2,0), (0,2,1), (0,2,2), (1,1,0), (1,1,1), (1,1,2), (1,2,0), (1,2,1), (1,2,2)\}$$

Introduce - 量詞的真值集

給定一個量詞P與定義域D，我們定義量詞P的真值集為所有使得P為true且在定義域D的元素。

我們可以把真值集寫作$\{x \in D | P(x)\}$。

Example

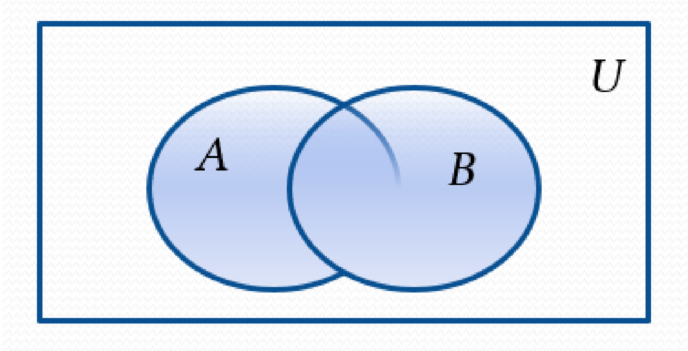
給定定義域D為所有整數與$P(x)$為$|x| = 1$，找出$P(x)$的真值集。

則$P(x)$的真值集為$\{-1, 1\}$。

2.2 集合運算子

Introduce - 聯集

A與B為集合，若A與B取聯集，則我們可以表示成$A \cup B = \{x | x \in A \vee x \in B\}$。

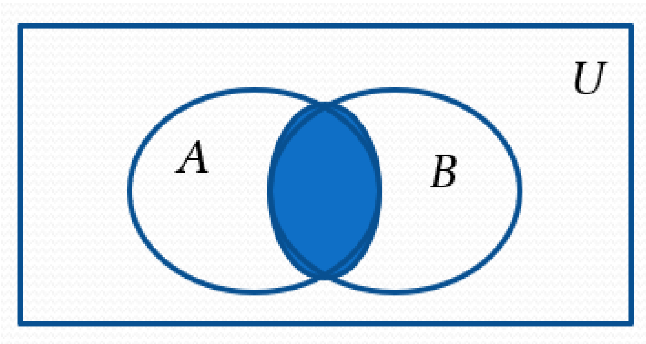


Example

若$A=\{1,2,3\}$，且$B=\{3,4,5\}$，則$A\cup B=\{1,2,3,4,5\}$

Introduce - 交集

A與B為集合，若A與B取交集，則我們可以表示成$A\cap B=\{x|x\in A\wedge x\in B\}$



如果$A\cap B=\varnothing$，則A與B的關係為互斥的。

Example 1

若$A=\{1,2,3\}$，且$B=\{3,4,5\}$，則$A\cap B=\{3\}$

Example 2

若$A=\{1,2,3\}$，且$B=\{4,5,6\}$，則$A\cap B=\varnothing$

Introduce - 補集

令A是一個集合，則A的補集(通常叫做宇集U)，寫作$\overline{A}$，為$U-\overline{A}$的集合。

定義為$\overline{A}=\{x\in U|x\notin A\}$

A的補集有時表示成A^c。

Example

如果宇集U代表小於100的正整數，則求$\{x|x>70\}$的補集。

$\{x|x\leq 70\}$

####

Introduce - 差集

令A與B為一個集合。

A與B的差集，可以表示成$A-B$，代表集合A不包含集合B的東西。

可以被定義為$A-B=\{x|x\in A\wedge x\notin B\}=A\cap\overline{B}$

Example

令$A=\{1,2,3\}$，$B=\{3,4,5\}$，求$A-B$

$A-B=\{1,2\}$

Introduce - 兩個集合交集的勢

利用排容原理。

$|A\cup B|=|A|+|B|-|A\cap B|$

Example

令$A=\{1,2,3\}$，$B=\{3,4,5\}$，求$|A\cup B|$

$|A\cup B|=|A|+|B|-|A\cap B|=|3|+|3|-|5|=1$

Introduce - 對稱差

若有兩個集合A與B，則A與B的對稱差寫作$A\oplus B$。

定義為$A\oplus B=(A-B)\cup(B-A)$

Example

若$U=\{0,1,2,3,4,5,6,7,8,9\}$，$A=\{1,2,3,4,5\}$，$B=\{3,4,5,6,7\}$，求$A\oplus B$

$A\oplus B=(A-B)\cup(B-A)=\{1,2\}\cup\{6,7\}=\{1,2,6,7\}$

Introduce - 集合特徵

- 恆等律
  - $A\cup\varnothing=A$，$A\cap U=A$
- 支配律
  - $A\cup U=U$，$A\cap\varnothing=\varnothing$
- 冪等律
  - $A\cup A=A$，$A\cap A=A$
- 補餘律
  - $\overline{(\overline{A})}=A$
- 交換律
  - $A\cup B=B\cup A$，$A\cap B=B\cap A$
- 連鎖律
  - $A\cup(B\cup C)=(A\cup B)\cup C$
  - $A\cap(B\cap C)=(A\cap B)\cap C$
- 分配律
  - $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$
  - $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$
- 德摩根定律
  - $\overline{A\cup B}=\overline{A}\cap\overline{B}$，$\overline{A\cap B}=\overline{A}\cup\overline{B}$
- 吸收律
  - $A\cap(A\cup B)=A$，$A\cap(A\cup B)=A$
- Complement laws
  - $A\cup\overline{A}=U$，$A\cap\overline{A}=\varnothing$

2.3 函數

Definition - 函數

令A與B為一個非空集合，一個函數從A映射B，寫作$A\to B$。

代表每一個集合A的元素都剛好指向一個集合B的元素，寫作$f(a)=b$。

其中b為集合B的相異元素，被集合A的元素所映射。

Introduce - 笛卡耳積的函數

一個$A\to B$，可以用來表示$A\times B$的子集合，寫作

$\forall x(x\in A\to\exists y(y\in B\land(x,y)\in f))$

以及

$\forall x,y_1,y_2[[(x,y_1)\in f\land(x,y_2)\in f]\to y_1=y_2]$

Introduce - 映射、像與原像

給你一個集合A與集合B，我們說f是由A映射B所組成，則

A被稱為f的定義域

B被稱為f的值域

如果$f(a)=b$，則b被稱為f在a的像，a被稱為b的像原

當兩個函數有相同的定義域，相同的域值，還有兩個函數的像與像原映射相同，則兩個函數相同。

Introduce - 單射

函數f被稱做一對一函數，或者稱做單射，也就是對於所有在定義域的a, b，若為且若$f(a) = f(b)$，則$a = b$。

函數f如果是一對一函數，則這個函數是個單射函數。

Introduce - 滿射

若有兩集合A, B，若為且若所有元素$b \in B$，存在一個$a \in A$，使得$f(a) = b$，則稱做這個函數為滿射函數。

Introduce - 對射

若一個函數是一對一函數，且函數滿射，則我們稱作這個函數是一對一對應函數或叫做對射函數。

Introduce - 反函數

令f是一個集合A對集合B的對射函數，f的反函數寫作f^{-1}。

反函數f^{-1}代表集合B對集合A的函數，定義為若為且若$f^{-1}(y) = x$則$f(x) = y$。

Introduce - 複合函數

令f為集合B對集合C的函數，且g為集合A對集合B的函數，f與g的複合函數，寫作$f \circ g$，代表一個集合A對集合C的函數，定義為$(f \circ g)(x) = f(g(x))$。

Introduce - 函數的圖形

令f為一個集合A對集合B函數，函數f的圖形即為每一對的(a, b)，即為

$\{(a, b) | a \in A \wedge f(a) = b\}$

Introduce - 一些重要的函數

底函數代表將小於等於x之最大整數指派給實數x，記為$\lfloor x \rfloor$

頂函數代表將大於等於x之最小整數指派給實數x，記為$\lfloor x \rfloor$

階乘函數$f : \mathbb{N} \to \mathbb{Z}^+$，記為$f(n) = n! = 1 \times 2 \times .... \times n$，其中$n \in \mathbb{Z}^+$。

Table - 頂函數與升函數

TABLE 1 Useful Properties of the Floor and Ceiling Functions.
(n is an integer, x is a real number)

(1a)	$\lfloor x \rfloor = n$ if and only if $n \leq x < n+1$
(1b)	$\lceil x \rceil = n$ if and only if $n-1 < x \leq n$
(1c)	$\lfloor x \rfloor = n$ if and only if $x-1 < n \leq x$
(1d)	$\lceil x \rceil = n$ if and only if $x \leq n < x+1$
(2)	$x-1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x+1$
(3a)	$\lfloor -x \rfloor = -\lceil x \rceil$
(3b)	$\lceil -x \rceil = -\lfloor x \rfloor$
(4a)	$\lfloor x+n \rfloor = \lfloor x \rfloor + n$
(4b)	$\lceil x+n \rceil = \lceil x \rceil + n$

Introduce - 部分函數

令f為一個集合A對集合B函數。

若f的定義域$D(f) \subseteq A$，且f的值域$R(f) \subseteq B$，則我們稱f為一部分函數。

2.4 數列與總和

Definition - 序列

- 序列是有序的表列，例如$1, 3, 5, 7, 9$，或者$1, 4, 9, 16, 25$。
- 序列是一個整數子集的函數。
- 我們使用符號$\{a_n\}$來描述序列。

Example

考慮序列a_n，其中$a_n = \dfrac{1}{n}$

由a_1開始，可記為$a_1, a_2, a_3, a_4, \ldots$

前幾項為$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4} \ldots$

Introduce - 幾何數列

一個幾何數列可以表示成：$a, ar, ar^2, ar^3, \ldots, ar^n$，其中$a$為首項，$r$為公比。

Example

若有一序列$a_n = (-1)^n$，則我們說這是一個幾何數列，因為a_n的前幾項為$1, -1, 1, -1 \dots$，即為$a = 1$，$r = -1$。

Introduce - 算術數列

一個算術數列可以表示成：$a, a+d, a+2d, a+3d, \dots, a+nd$，其中$a$為首項，$d$為公差

Example

若有一序列$a_n = 1 + 3n$，則我們說這是一個算術數列，因為a_n的前幾項為$1, 4, 7, 10 ...$，即為$a = 1$，$r = 3$。

Definition - 字串

- 字串為有限字元數所組成的序列。
- 一個不含任何項的字串稱作空字串。

Introduce - 遞迴關係式

遞迴關係，也就是差分方程式，是一種遞推地定義一個序列的方程式：序列的每一項目是定義為前一項的函數。

Example - 斐波納契數列

一個Fibonacci Sequence可以由以下的性質定義

$F_0 = 0$

$F_1 = 1$

$F_n = F_{n-2} + F_{n-1}$

因此，斐波納契數列的序列為

$\{0, 1, 1, 2, 3, 5, 8, 13, 21 \dots\}$

2.5 集合的勢

Definition - 勢

- 令A與B為兩個集合，若為且若A與B對射，則集合A與集合B的勢是相同的，寫作$|A| = |B|$。
- 令A與B為兩個集合，若為且若A與B單射，則集合A的勢小於等於集合B的勢，寫作$|A| \leq |B|$。

  如果集合A的勢與集合B的勢不同，則$|A| < |B|$。
- 一個集合如果是有限的，或者與正整數集合的勢相同，則我們說這個集合是可數的，否則就是不可數的。

  例如一個實數集合是個不可數的集合。
- 如果一個無限的集合是可數的，他的勢為$\aleph_0$，寫作$|S| = \aleph_0$，且唸做"aleph null"。
- 一個無限集合的勢，若為且若可以將所有的元素列成一個數列，則我們說這個無限集合的勢是可數的。

  原因是一個無限集合的勢，可以寫作一個對射函數，且函數的index是正整數，故我們可以寫成這樣的形式：

  $f(1) = a_1, f(2) = a_2, \dots f(n) = a_n$

  故根據「一個集合如果是有限的，或者與正整數集合的勢相同，則我們說這個集合是可數的」，我們可以知道無限集合的勢，若為且若可以將所有的元素列成一個數列，則我們說這個集合是無限的。

Introduce - 希爾伯特旅館悖論

一個有無限間房間的旅館，每一個房間均住滿人，我們要怎麼樣能夠再容納一個旅客？

假設我們有無限多個客人，我們將每個客人j編號成a_j，新的客人我們表示成a_0，則我們可以寫成這樣的形式

$f(1)=a_1, f(2)=a_2, f(3)=a_3, f(4)=a_4, \ldots, f(n)=a_n, \ldots$

我們可以將第i房的人，請他移駕至第$i+1$房，這樣就會使第一間房間空出來。

$g(1)=a_0, g(2)=a_1, g(3)=a_2, g(4)=a_3, \ldots, g(n)=a_{n-1}, \ldots$

可以顯而易見的知道這樣分配不會使房間編號撞號。

Example - 證明集合是可數的(1)

證明正偶數整數集合E是可數的。

令$f(x)=2x$，則我們可以將其列成序列，也就是

$f(1)=2, f(2)=4, f(3)=6, f(4)=8, \ldots, f(n)=2n$

我們可以證明這個函數是對射，假設t為偶正整數，則它可以寫成$2k$的形式，故每一個t存在唯一一個k，使得$f(k)=t$

我們可以證明這個函數是一對一函數，假設存在$f(n)=f(m)$，必定存在$2n=2m$，也就是存在$n=m$

故若$n=m$，才能使得$f(n)=f(m)$

根據勢的定義，「一個無限集合的勢，若為且若可以將所有的元素列成一個數列，則我們說這個無限集合的勢是可數的。」

因此$f(x)=2x$是可數的。

Example - 證明集合是可數的(2)

證明整數集合Z是可數的。

將集合Z列成：$0,1,-1,2,-2,3,-3...$

我們可以寫成以下的部分函數：$f(x)=\begin{cases} f(x)=-(x-1)/2 & x\in \text{odd} \\ f(x)=x/2 & x\in \text{even}\end{cases}$

4. 數論與密碼學

4.1 可除性與模算術

Definition - 除法

- 如果a與b是整數，且$a \neq 0$，則我們說b能夠被a整除，如果存在一個整數c，使得$b = ac$。
- 如果b能夠被a整除，則我們說a是b的因數或者被除數，且b為a的倍數。
- 我們用$a|b$來表示b能夠被a整除。
- 如果$a|b$，則b/a為一個整數。
- 如果a沒辦法整除b，則我們表示為$a \not| \ b$

Theorem 1

令a, b, c為整數，且$a \neq 0$，則如果$a|b$和$a|c$，則$a|(b + c)$

Proof

如果$a|b$，則我們可以說存在一個整數s，使得$as = b$

如果$a|c$，則我們可以說存在一個整數t，使得$at = c$

因此$b + c = as + at = a(s + t)$，因為$s + t$為整數，由此可證如果$a|b$和$a|c$，則$a|(b + c)$

Theorem 2

令a, b, c為整數，且$a \neq 0$，則如果$a|b$，那麼對於任意c，符合$a|bc$

Proof

如果$a|b$，則我們可以說存在一個整數s，使得$as = b$

將等號兩邊同乘以c，得到$asc = bc$

由於兩個整數相乘為整數，故我們依然可以找到一個整數$d = sc$，使得$ad = bc$

由此可證如果$a|b$，那麼對於任意c，符合$a|bc$。

Theorem 3

令a, b, c為整數，且$a \neq 0$，則如果$a|b$且$b|c$，那麼$a|c$

Proof

如果$a|b$，則我們可以說存在一個整數s，使得$as = b$

如果$b|c$，則我們可以說存在一個整數t，使得$bt = c$，也就是$ast = c$

由於兩個整數相乘為整數，故我們依然可以找到一個整數$d = st$，使得$ad = c$

由此可證如果如果$a|b$且$b|c$，那麼$a|c$。

Corollary 1

如果a, b, c為整數，且$a \neq 0$，$a|b$和$a|c$，那麼$a|mb + nc$，其中$n, m \in \mathbb{Z}$

Introduce - 除法算法

如果$a \in \mathbb{Z}$，且$d \in \mathbb{Z}^+$，那麼存在唯一$q, r \in \mathbb{Z}$，其中$0 \le r < d$，使得$a = dq + r$。

其中a被稱為被除數，d被稱為除數，q被稱做商，r被稱做餘數。

我們可以用mod與div來取得商與餘數，定義

$q = \mathrm{a\ div\ d}$

$r = \mathrm{a\ mod\ d}$

Introduce - 同餘關係

如果a, b為整數，且m為一正整數，則如果m可以整除$a - b$，我們說a與b同餘模m，可以用$a \equiv b \pmod{m}$來表示。

兩個整數a, b能夠同餘模m，若為且若a除以m與b除以m的餘數相同。

如果a除以m與b除以m的餘數不同，那麼我們表示為$a \not\equiv b \pmod{m}$

Theorem 4

令m為一正整數，整數a, b能夠同餘於m，若為且若存在一個k使得$a = b + km$

Proof

若$a \equiv b \pmod{m}$，那麼$m|(a - b)$

因此，會存在一個k，使得$mk = a - b$，因此$a = mk + b$

反之，若存在一個k使得$a = b + km$，那麼$km = a - b$，因此可以得知$m|(a - b)$和$a \equiv b \pmod{m}$

Introduce - 兩個不同的表示法(mod m) 與 mod m

- $a \equiv b \pmod{m}$與$a \bmod m = b$是不同的東西
  - $a \bmod m = b$, 代表函數的關係。
  - $a \equiv b \pmod{m}$, 代表一個整數集合的關係。

Theorem 5

令a, b為整數，令m為正整數，則$a \equiv b \pmod{m}$ 若為且若 $a \bmod m = b \bmod m$。

Proof

如果$a \equiv b \pmod{m}$，則我們可以說$a - b = me, e \in \mathbb{Z}$，因此$a = me + b$

那麼令$d = b \bmod m$，我們可以表示成$b = mr + d, r \in \mathbb{Z}, , 0 \le d < m$

因此$a = me + mr + d = m(e + r) + d$

我們可以說$(e + r)$是a/m的商，d為a/m的餘。

故$a \mod m = d = b \mod m$

Theorem 6

令m為正整數，如果$a \equiv b \pmod{m}$和$c \equiv d \pmod{m}$，那麼$(a+c) \equiv (b+d) \pmod{m}$且$ac \equiv bd \pmod{m}$

Proof

如果$a \equiv b \pmod{m}, c \equiv d \pmod{m}$，那麼存在$s, t \in \mathbb{Z}$，使得$a = sm + b$，且$c = tm + d$

故$a + c = (s+t)m + (b+d)$，且$ac = stm^2 + sdm + tbm + bd = m(stm + sd + tb) + bd$

因此$(a+c) \equiv (b+d) \pmod{m}$，$ac \equiv bd \pmod{m}$

Introduce - 同餘的代數運算

- 令a, b為整數，若$a \equiv b \pmod{m}$，則$ac \equiv bc \pmod{m}$
  ※可以根據Theorem 6，令$d = c$。
- 令a, b為整數，若$a \equiv b \pmod{m}$，則$a + c \equiv b + c \pmod{m}$
  ※可以根據Theorem 6，令$d = c$。
- 除法並不保證能夠用在同餘上。

Corollary 2

令m為正整數，令a, b為整數，則

$(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

$(ab) \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

Proof

根據模的定義，則$a \equiv (a \bmod m) \pmod{m}$，$b \equiv (b \bmod m) \pmod{m}$

By Theorem 6，可知$a + b \equiv (a \bmod m) + (b \bmod m) \pmod{m}$

以及$ab \equiv (a \bmod m)(b \bmod m) \pmod{m}$

Definition - 模的算術運算元

令$\mathbb{Z}_m$為所有小於m的非負整數集合，則

- $a +_m b$，用來表示$(a+b) \bmod m$
- $a \cdot_m b$，用來表示$(ab) \bmod m$
- 模的算術運算元有許多性質
  - 封閉性：如果$a, b \in \mathbb{Z}_\mathrm{m}$，則$a +_m b \in \mathbb{Z}_m$和$a \cdot_m b \in \mathbb{Z}_m$。
  - 結合律：如果$a, b, c, \in \mathbb{Z}_m$，則$(a +_m b) +_m c = a +_m (b +_m c)$，且$(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$
  - 交換律：如果$a, b \in \mathbb{Z}_m$，則$a +_m b = b +_m a$，且$a \cdot_m b = b \cdot_m a$
  - 單位元素：如果$a \in \mathbb{Z}_m$，則$a +_m 0 = a$，且$a \cdot_m 1 = a$
  - 加法反元素：如果$a \neq 0$且$a \in \mathbb{Z}_m$，則$a +_m (m-a) = 0$，且$0 +_m 0 = 0$
  - 分配律：如果$a, b, c, \in \mathbb{Z}_m$，那麼$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$，$(a +_m b) \cdot_m c = (a \cdot_m c) + (b \cdot_m c)$

4.2 整數表示與演算法

Theorem 1

令b為一個大於1的正整數，如果n為一正整數，則他可以表示成$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0 b^0$

其中k為非負整數，$a_0, a_1 ...$為一非負整數，且小於b，且$a_k \neq 0$。

a_j，$j = 0, 1, ..., k$為以b為底數的各個位數。

4.3 質數與最大公因數

Definition - 質數

一個正整數$p > 1$，若p的因數只有它自己與1，則我們說這個數字p是質數。

若$p > 1$，且p的因數不只有它自己與1即為合數。

Theorem 1

任何大於1的正整數都可以用質數的乘積來分解，且分解的結果為唯一。

且結果我們通常會用非遞減的形式呈現。

Example

$100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$

$641 = 641$

$999 = 3 \times 3 \times 3 \times 37 = 3^3 \times 37$

$1024 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^{10}$

Introduce - 厄拉托西尼篩法

厄拉托西尼篩法可以在一定的範圍內找到所有質數，舉個例子，我們可以用厄拉托西尼篩法找1~100的所有質數。

1. 刪除所有2的倍數的數字，除了2。
2. 刪除所有3的倍數的數字，除了3。
3. 刪除所有5的倍數的數字，除了5。
4. 刪除所有7的倍數的數字，除了7。
5. 這樣一來，所有剩下的數字都不能被2、3、5、7給整除，因此質數為
   $\{2, 3, 5, 7, 11, 15, 1719, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}$

Theorem 2

質數的個數是無限的。

Proof

令$P = p_1p_2p_3p_4...p_n$，且$q = P + 1$，則q是質數或不是質數，兩者必居其一。

如果q是質數，那麼至少有一個質數不在有限質數集$p1, p2, p3...p_n$中。

如果q是合數，那麼存在一個質數因子p整除q，如果p在我們的質數集合P中，則p必然整除P。

但是，已知p整除$P+1$，如果p同時整除P和q，則P必然整除P與q之差，也就是$(P+1) - P = 1$

但是沒有質數能整除1，即有p整除q，就不存在p整除P，因此p不在有限質數集合P中。

這就證明了：對於任何一個有限的質數集，總有一個質數不在其中，所以質數一定是無限的。

Theorem 3

定義$\pi(x) = \frac{x}{\ln(x)}$為質數計數函數，也就是小於$x$的質數個數。

則若$x \to \infty$，$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} \approx 1$

這個定理告訴我們，若要尋找所有不超過x的質數，則他的數量會趨近於$\frac{x}{\ln(x)}$

若我們要從所有小於x的正整數中挑中質數，則他的機率為$\frac{x}{\ln(x)} \div x = \frac{1}{\ln(x)}$

Definition - 最大公因數

令a, b為兩整數，且$a, b \neq 0$，若存在一個最大的整數d使得$d|a$且$d|b$，則d被稱做a, b的最大公因數。

最大公因數a, b被寫作$gcd(a, b)$。

Definition - 互質

令a, b為兩整數，若$gcd(a, b) = 1$，則我們說a, b互質。

Definition - 兩兩互質

若有一整數數列$a_1, a_2, a_3, a_4, \ldots, a_n$，若$gcd(a_i, a_j) = 1, 1 <= i < j <= n$，則我們說這個數列兩兩互質。

Introduce - 利用質因數分解尋找最大公因數

假設$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots p_n^{a_n}$，且$b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \ldots p_n^{b_n}$

則兩數的$gcd(a, b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} p_3^{\min(a_3,b_3)} \ldots p_n^{\min(a_n,b_n)}$

Definition - 最小公倍數

令a, b為兩正整數，若存在一個d使得$a|d$且$b|d$，則我們說d為a, b的最小公倍數。

最小公倍數a, b被寫作$lcm(a, b)$

我們可以用質因數分解來尋找最小公倍數，也就是

假設$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots p_n^{a_n}$，且$b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \ldots p_n^{b_n}$

則兩數的$lcm(a, b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} p_3^{\max(a_3,b_3)} \ldots p_n^{\max(a_n,b_n)}$

Theorem 4

令a, b為正整數，則$ab = gcd(a, b) \times lcm(a, b)$

Proof

待補

Introduce - 歐幾里得演算法

我們可以用歐幾里得演算法來計算a, b的最大公因數

論點建立在$gcd(a, b) = gcd(b, c), a > b$，其中$c$為$a$除以$b$的餘數。

Introduce - 歐幾里得演算法的正確性

引理1

令$a = bq + r$，其中$a, b, q, r \in \mathbb{Z}$，則$gcd(a, b) = gcd(b, r)$。

證明

假設d能夠整除a, b，則d也可以整除$a - bq = r$，因此，若$gcd(a, b) = d_1$，則$gcd(b, r) = d_1$

假設d能夠整除b, r，則d也可以整除$bq + r = a$，因此，若$gcd(b, r) = d_2$，則$gcd(a, b) = d_2$

因此，$gcd(a, b) = gcd(b, r)$。

Introduce - 歐幾里得演算法

歐幾里得演算法可以用來計算兩個整數(a, b)的最大公因數。

概念建立在$\gcd(a, b) = \gcd(b, c)$，其中$a > b$且c為a除b的餘數。

Example

Find $\gcd(91, 287)$

$287 = 91 \times 3 + 14$

$91 = 14 \times 6 + 7$

$14 = 7 \times 2 + 0$

因此$\gcd(91, 287) = \gcd(91, 14) = \gcd(14, 7) = 7$

Introduce - 引理 1

令$a = bq + r$，其中$a, b, q, r \in \mathbb{R}$，則$\gcd(a, b) = \gcd(b, r)$

Proof

假設d可以整除a, b，則d也可以整除$a - bq = r$。

因此若a, b存在一公因數，則此公因數也是b, r的公因數。

假設d可以整除b, r，則d也可以整除$bq + r = a$。

因此若a, b存在一公因數，則此公因數也是b, r的公因數。

因此，$\gcd(a, b) = \gcd(b, r)$

Introduce - 歐幾里得演算法的正確

假設a, b為正整數，且$a \geq b$，令$r_0 = a, r_1 = b$，則我們可以透過除法定理得到以下步驟。

$r_0 = r_1 q_1 + r_2$

$r_1 = r_2 q_2 + r_3$

$r_2 = r_3 q_3 + r_4$

重複多次後

$r_{n-2} = r_{n-1} q_{n-1} + r_n$

$r_{n-1} = r_n q_n$

則我們可以知道，餘數隨著步驟越來越多，得到以下結果：

$r_0 > r_1 > r_2 > r_3 \ldots \geq 0$

則根據引理1，得到

$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$

因此最大公因數發生在最後一個非零的餘數。

Introduce - 貝祖定理

如果a, b為正整數，則存在一組s, t使得$gcd(a, b) = as + bt$

Example

$\gcd(6, 14) = 2 = 6 \times (-2) + 14 \times 1$

Example

利用歐幾里得演算法，將$\gcd(252, 198) = 18$利用線性組合找出s, t，使得$252s + 198t = \gcd(252, 198) = 18$

$252 = 198 \times 1 + 54$

$198 = 54 \times 3 + 36$

$54 = 36 \times 1 + 18$

$36 = 18 \times 2 + 0$

又

$18 = 54 - 36$

$= 54 - (198 - 54 \times 3) = 54 \times 4 - 198$

$= (252 - 198) \times 4 - 198 = 4 \times 252 - 5 \times 198$

故我們可以找到$s = 4, t = -5$，使得$\gcd(252, 198) = 4 \times 252 - 5 \times 198$

我們可以整理成以下的表格

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	252	198	1	54
1	198	54	3	36
2	54	36	1	18
3	36	18	2	0

Introduce - 歐幾里得擴展演算法

若我們已經找到足夠的q，則我們可以將s, t擴展成以下的遞迴式。

$s_j = s_{j-2} - q_{j-1}s_{j-1}$和$t_j = t_{j-2} - q_{j-1}t_{j-1}, j \geq 2$

其中$s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$

Example

利用歐幾里得擴展，尋找出s, t使得$\gcd(252, 198) = 252 \times s + 198 \times t$

$s_2 = s_0 - q_1 s_1 = 1 - 1 \times 0 = 1$

$t_2 = t_0 - q_1 t_1 = 0 - 1 \times 1 = -1$

$s_3 = s_1 - q_2 s_2 = 0 - 3 \times 1 = -3$

$t_3 = t_1 - q_2 t_2 = 1 - 3 \times (-1) = 4$

$s_4 = s_2 - q_3 s_3 = 1 - 1 \times (-3) = 4$

$t_4 = t_2 - q_3 t_3 = -1 - 1 \times 4 = -5$

因此，我們可以知道$s = 4, t = -5$時符合$\gcd(252, 198) = 4 \times 252 - 5 \times 198 = 18$

Introduce - 引理 2

如果a, b, c為正整數，且$\gcd(a, b) = 1$而且$a|bc$，則$a|c$

Proof

假設$\gcd(a,b)=1$，且$a|bc$，則

根據貝祖定理，存在一組(s,t)使得$\gcd(a,b)=as+bt=1$

將等號兩邊同乘以c，則得到$asc+btc=c$

已知$a|bc$，代表存在一個r使得$bc=ar$，將等號兩邊同乘t，可以得到$btc=art \iff btc=a(rt)$，故$a|btc$

又已知asc可被a整除($asc/a=sc, sc\in\mathbb{R}$)，故$a|asc, a|btc \Rightarrow a|c$

Introduce - 引理3

假設p是質數，且$p|a_1a_2a_3\ldots a_n$，則對於某些i，$p|a_i$

Introduce - 質數分解的唯一性

若一個數字可被質數分解，且分解的結果為非遞增的方式排列，則這個結果為唯一。

Proof

假設有些大於1的自然數可以用多種方式寫成多個質數的乘積

則假設n為最小可以用多種方式寫成多個質數的乘積的數字。

因此我們可以將n寫成$n=p_1p_2p_3p_4\ldots p_s=q_1q_2q_3q_4\ldots q_t$，$p,q$為質數。

根據引理3，假設p是質數，且$p|a_1a_2a_3\ldots a_n$，則對於某些i，$p|a_i$

因此$q_1q_2q_3\ldots q_t$存在一個數字使得p_1可以整除，假設為q_1

又若要使得$p_1|q_1$，只存在於$p_1=q_1$。

所以$n'=p_2p_3p_4p_5\ldots p_s=q_2q_3q_4q_5\ldots q_t$

但n是最小的一個，不應該存在比n更小的數字n'能夠用多種方式寫成多個質數的乘積

故與n的最小性矛盾，因此唯一性得證。

Theorem 5

在先前有介紹過同餘的除法代數運算並不適用於每一種結果，在這邊會介紹同餘的除法代數運算。

令m為一正整數，且a,b,c為整數，則若$ac\equiv bc \pmod m$和$\gcd(c,m)=1$，則$a\equiv b \pmod m$。

Proof

若$ac\equiv bc \pmod m$，則$ac=mr+bc$，$ac-bc=mr$，$r=\dfrac{(ac-bc)}{m}=\dfrac{ac}{m}-\dfrac{bc}{m}$

利用引理2可知

若$m|ac$且$\gcd(m,c)$，則$m|a$

若$m|bc$且$\gcd(m,c)$，則$m|b$

又因$m|a,m|b$，則$a\equiv b \pmod m$

4.4 求解同餘方程式

Introduce - 線性同餘

當m為正整數，a, b為整數，而x為變數時，$ax \equiv b \pmod{m}$稱為線性同餘。

Definition - 反元素

若存在一個整數$\overline{a}$，使得$\overline{a}a \equiv 1$，則我們說$\overline{a}$為模m的反元素。

Theorem 1

若a與m為互質整數，且$m > 1$，則a在模m下的反元素存在，此外，在模m下，此反元素是唯一的。

Proof (存在性)

利用定理：若$\gcd(a, m) = 1$，則存在兩整數s, t使得$as + mt = 1$，也可以看成$as + mt \equiv 1 \pmod{m}$

由於$mt \equiv 0 \pmod{m}$，因此$as \equiv 1 \pmod{m}$

因此，s是a在模m的反元素。

Introduce - 找出反元素

我們可以用歐幾里得演算法與貝祖定理來找出反元素。

首先我們必須要證明$\gcd(a, b) = 1$，再利用貝祖定理做回推。

Example 1

尋找3模7的反元素。

根據歐幾里得演算法：

$7 = 3 \times 2 + 1$

$3 = 1 \times 3 + 0$

因此我們能夠證明$\gcd(7, 3) = 1$

接著利用貝祖定理進行回推，可得$-2 \times 3 + 1 \times 7 = 1$

因此可以得到貝祖係數$s = -2, t = 1$

因此，-2是3模7的反元素，而所有結果為-2模7同餘的整數皆為3模7的反元素。

Example 2

尋找101模4620的反元素。

根據歐幾里得演算法：

$4620 = 101 \times 45 + 75$

$101 = 75 \times 1 + 26$

$75 = 26 \times 2 + 23$

$26 = 23 \times 1 + 3$

$23 = 3 \times 7 + 2$

$3 = 2 \times 1 + 1$

$2 = 1 \times 2 + 0$

故我們可以證明$\gcd(101, 4620) = 1$

利用這個來反推貝祖係數

$1 = 3 - 2 \times 1$

$= 3 - (23 - 3 \times 7) = 3 \times 8 - 23$

$= (26 - 23) \times 8 - 23 = 8 \times 26 - 9 \times 23$

$= 8 \times 26 - 9 \times (75 - 26 \times 2) = 26 \times 26 - 9 \times 75$

$= (101 - 75) \times 26 - 9 \times 75 = 101 \times 26 - 35 \times 75$

$= 101 \times 26 - 35 \times (4620 - 101 \times 45)$

$= 101 \times 1601 - 35 \times 4620$

故我們可以得到$s = 1601, t = -35$

故我們說1601為101模4620的反元素。

Introduce - 中國剩餘定理

令$m_1, m_2, m_3, \ldots, m_n$為兩兩互質的正整數，而$a_1, a_2, a_3, \ldots, a_n$為任意正整數，則下列系統

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \\ . \\ . \\ . \\ x \equiv a_n \pmod{m_n} \end{cases}$$

在$m = m_1 m_2 m_3 m_4 \ldots m_n$有唯一解，其中$0 \le x < m$，而其他解都在$x$模$m$的情況下同餘。

Proof

我們設$M_k = m/m_k$，其中$k = 1, 2, 3 \ldots n$，也就是說M_k為除了m_k以外的所有兩兩互質正整數乘積。

當$i \neq k$時，M_k與m_k沒有公因數，故$\gcd(M_k, m_k) = 1$

根據Theorem 1，可知存在一個反元素使得$M_k y_k \equiv 1 \pmod{m_k}$

令$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \ldots + a_n M_n y_n$，因為$M_j \equiv 0 \pmod{m_k}$，其中$j \neq k$

因此，對所有的$k = 1, 2, 3, \ldots, n$，得到$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$，因此$x$即為方程式系統的解。

Example

求解下列同餘方程式系統。

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

$m = 3 \times 5 \times 7$

則

$M_1 = 5 \times 7 = 35$，$35y_1 \equiv 1 \pmod 3$，得到$y_1 = 2$

$M_2 = 3 \times 7 = 21$，$21y_2 \equiv 1 \pmod 5$，得到$y_2 = 1$

$M_3 = 3 \times 5 = 15$，$15y_3 \equiv 1 \pmod 7$，得到$y_3 = 1$

因此$x = 35 \times 2 \times 2 + 21 \times 1 \times 3 + 15 \times 1 \times 2 = 233 \equiv 23 \pmod{105}$

故$x = 23$為這個系統的最小正整數解。