1. [8 points] For each of these relations, decide whether it is reflexive, whether it is symmetric, whether it is antisymmetric, and whether it is transitive.

每问 2 分，每问包含 4 个结果，错一个扣 0.5 分；本题最终扣分向下取整。

a) "divides" relation on the set of nonnegative integers.

Not Reflexive, not symmetric, antisymmeytic, transitive.

b) The inverse relation of R={(2, 5), (5, 2),(2,2),(5,5)} on the set {1,2,3,4,5}.

Not Reflexive, symmetric, not antisymmeytic, transitive.

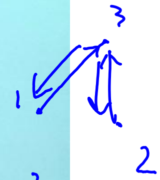
c) The complementary relation of R={(1,3) , (2, 3), (3, 1), (3,2) } on the set {1,2,3}.

补集

Reflexive, symmetric, not antisymmeytic, transitive.

d) The composite of "less than" relation on the set of intergers and "greater than" relation on the set of intergers.

Reflexive, symmetric, not antisymmeytic, transitive.



3

Example: Let S={1,2,3,…}, then R1°R2= $\begin{matrix}0&1&1\\0&0&1\\0&0&0\end{matrix} \cdot \begin{matrix}0&0&0\\1&0&0\\1&1&0\end{matrix} = \begin{matrix}1&1&0\\1&1&0\\0&0&0\end{matrix}$

2. [8 points] Use Warshall's algorithm to find the transitive closure of R on {1,2,3,4,5 } where R={(1, 2),(1,3),(2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4),(3,5),(4,5) ,(5,1) }.

$W_0 = [\ \cdots\ ]$

$$w0=\begin{bmatrix}0&1&1&0&0\\0&1&1&1&0\\0&1&1&1&1\\0&0&0&0&1\\1&0&0&0&0\end{bmatrix}, w1=\begin{bmatrix}0&1&1&0&0\\0&1&1&1&0\\0&1&1&1&1\\0&0&0&0&1\\1&1&1&0&0\end{bmatrix}, w2=\begin{bmatrix}0&1&1&1&0\\0&1&1&1&0\\0&1&1&1&1\\0&0&0&0&1\\1&1&1&1&0\end{bmatrix},$$

$$w3=\begin{bmatrix}0&1&1&1&1\\0&1&1&1&1\\0&1&1&1&1\\0&0&0&0&1\\1&1&1&1&1\end{bmatrix}, w4=w3,\ w5=\begin{bmatrix}1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\\1&1&1&1&1\end{bmatrix}$$

按 walshall 算法写出过程，w0 对得 2 分，w1 对得 2 分；最终结果 w5 全对得 4 分，w5 中错 2 个元素扣 1 分,扣完 4 分为止。

3. [8 points] Let R_1 is an equivalence relation produced by the partition A_1={a,b}, A_2={c,d},and A_3={e,f} of S={a,b,c,d,e,f}, R_2 is another equivalence relation produced by the partition A_1={a, c}, A_2={ b,d}, A_3={e},and A_4={ f} of S={a,b,c,d,e,f}.
List the ordered pairs of relation (1) $R_1 \cap R_2$ and (2) $R_1 \oplus R_2$.

(1) R1 ∩R2 ={ (a,a), (b,b), (c,c), (d,d), (e,e), (f,f) }

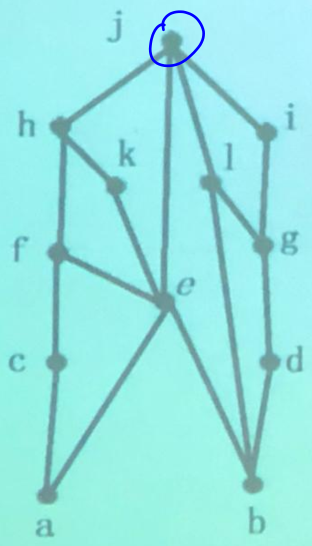
(2) R1 ⊕R2 = { (a,b), (b,a), (c,d), (d,c), (e,f), (f,e), (a,c), (c,a), (b,d), (d,b) }.

每问4分，错2个元素扣1分,扣完4分为止。

R_1= (a,a) (a,b) (b,a) (c,c) (c,d) (d,c) (e,e) (e,f) (f,e)

$R_1 \oplus R_2 = R_1 - R_2 \cup R_2 - R_1$

[12 points] Answer these questions for the partial order represented by this Hasse diagram.



(1) Find all maximal elements.

{ j } 正确得 1 分　{j}

(2) Find all minimal elements.

{a , b}　正确得 1 分　{a, b}

(3) Is there a greatest element?　Yes

Yes　正确得 1 分

(4) Is there a least element?

No　正确得 1 分

(5) Find all upper bounds of {a, b, c}.

{ f , h, j }　　正确得 2 分,写错或漏一个扣 1 分

(6) Find the least upper bound of {e, f, g}, if it exists.

j　　正确得 2 分,答不存在的扣 2 分，写错元素的扣 1 分。

(7) Find all lower bounds of {h, j, k}.

{ k , e, a, b }　正确得 2 分，写错或漏一个扣 1 分.

(8) Find the greatest lower bound of {i, j,l}, if it exists.

g　　正确得 2 分,答不存在的扣 2 分，写错元素的扣 1 分。

5. [10 points] Let Q be the set of rational numbers and define a*b=a+b-ab

有理数

(a) Is (Q,*) a monoid? Justify your answer.

(b) If (Q,*) a monoid, which elements of Q have an inverse?

幺半群

答:（1）

由于 a,b 是实数，所以 $ab=a+b-ab$ 也是实数，运算闭合。（1 分）

$a * (b* c) = a * (b+c-b\times c) = a+(b+c-b\times c) - a\times(b+c-b\times c)$

$= a+b+c-bc-ab-ac+abc$

群可结合

$a*(b*c)$

$(a*b)*c$

$(a * b)* c = (a+b-a\times b) * c = a+b-a\times b + c - (a+b-a\times b)\times c$

$= a+b+c-ab-ac-bc+abc$

$a*0=0*a=a$

因此 *是可结合的。（3 分）

由于 $a * 0 = 0 * a = a$，所以 0 是单位元，(Q, *)是独异点。（1 分）　0则单位元

（2）

如果 $a\neq 1$，

$a*a^{-1}=a+a^{-1}-aa^{-1}=0$

$a * \frac{-a}{1-a} = a + \frac{-a}{1-a} + a\times \frac{-a}{1-a} = 0$　（3 分）

$a^{-1}=\frac{a}{a-1}$　$a\neq 1$

所以，Q 中除 1 以外都有逆元。（2 分）

6. [10 points] Let G be a group and K is a subgroup of G. Show that for any element a,b in G, either aK=bK or aK∩bK=Φ.

解法 1--

证明：思路是构造一个等价关系，使得 K 的每个左陪集都是其中的等价类。

1、构造一个二元关系 $R=\{aRb \mid a^{-1}*b\in K\}$。 （2 分）

下面证明它是一个等价关系。

自反性：$\forall x\in G,\ x^{-1}*x=e\in K \Rightarrow xRx$.（1 分）

对称性：$\forall x,y\in G,\ xRy \Rightarrow x^{-1}*y\in H$, so $y^{-1}*x=(x^{-1}*y)^{-1}\in K$, yRx. （1 分）

传递性：$\forall x,y,z\in G$, (xRy and yRz)$\Rightarrow x^{-1}*y\in K$ and $y^{-1}*z\in K$.

$x^{-1}*z=x^{-1}*y*y^{-1}*z\in K$, xRz. （1 分）

$ak=bk$ or $ak\cap bk=\phi$

2、证明 R 的等价类是 K 的左陪集。

在关系 $R=\{aRb \mid a^{-1}*b\in K\}$基础上

$\forall a\in G$ 其等价类为$\{b\}$ （包含a自身）

左陪集是 $a*K=a*(a^{-1}*b)$

$=a*a^{-1}*b$

$=e*b=\{b\}$

∵ R的等价类是K的左陪集

假设 $ak\cap bk\neq\phi$

则设 $x\in ak\cap bk$

则 $x\in ak$ 且 $x\in bk$

则 $\exists k_1,k_2\in K$,

$x=ak_1=bk_2$.

$y\in ak \rightarrow y=ak_3$

则 $y\in bK$.

解法 2--

证明：

$\Rightarrow a=bk_2k_1^{-1}$ $\quad y=bk_2k_1^{-1}k_3$

假设 aK∩bK≠Φ，设 x∈aK∩bK 则 $\exists k_1,k_2\in K, x=ak_1=bk_2$,由此可得 $a=b\,k_2\,k_1^{-1}$（3 分）

对$\forall y\in aK, \exists k_3\in K, y=a\,k_3=b\,k_2\,k_1^{-1}\,k_3$. 因 K 为 G 的子群，所以$k_2\,k_1^{-1}\,k_3\in K$

即$\exists h=k_2\,k_1^{-1}\,k_3\in K$， y=bh,所以 y∈bK.即 aK⊆bK。（4 分）

同理可证，bK⊆aK.（2 分）

所以 aK=bK.（1 分）

$\exists k_1,k_2\in k$,使得 $x=ak_1=bk_2$.

$\Rightarrow a=bk_2k_1^{-1}$.

封闭的

$k_2k_1^{-1}k_3\in K$.

所以 $y=bk'$

则 $y\in bK$

故 $ak\subseteq bk$

同理 $bk\subseteq ak$

故 $ak=bk$

7. [8 points] Let (G,*) be a group. Show that If $(a*b)^2=a^2*b^2$ for all a and b in G then G is Abelian.

$y\in ak$, $\exists k_3\in K$, $y=ak_3$

$=bk_2k_1^{-1}k_3$

proof:

$(a*b)^2=(a*b)*(a*b)=a*(b*a)*b$, for G is associative. （2 分）

$a^2*b^2=(a*a)*(b*b)=a*(a*b)*b$, for G is associative. （2 分）

based left/right cancellation, $b*a=a*b$. （4 分）

$y=bh$

Hence, G is Abelian.

可结合

所以 $y\in bK$

即 $ak\subseteq bK$.

$\boxed{ak\subseteq bK}$

$(a*b)^2=a^2*b^2$

$(a*b)*(a*b)$

$=a*(b*a)*b$

$=a*a)*(b*b)$

$=a^2*b^2$

$\boxed{\begin{array}{l}a^2=a*a\\ b^2=b*b\end{array}}$

8. [12 points] Let Z be the set of all integers and let + be the binary operation of addition on Z. Let $B = \{0, 1\}$, and let $+_2$ be the operation defined on B as follows:

$+_2$	0	1
0	0	1
1	1	0

. Let f be a function from group $(Z, +)$ to $(B, +_2)$.

$a * e = e * a = 0$

(a) Prove that f defined by $f(x)=x \pmod 2$ is homomorphism from Z to B.

回忆 $f(a*b) = f(a) *' f(b)$　　$a \pmod 2$

证：（4 分）

$f(x+y)= (x+y) \pmod 2 = (x \pmod 2 + y \pmod 2) \bmod 2 = (f(x)+ f(y)) \bmod 2$

$= f(x) +_2 f(y)$

$f(x+y) = (x+y) \pmod 2 = f(x) +_2 f(y)$

所以 f defined by $f(x)=x \pmod 2$ is homomorphism from Z to B

$a \in \ker f)$

$f(a) = 0$

(b) Find ker(f). （4 分）

$\ker(f)=\{2x \mid x \in Z\}$

(b) $\ker(f) = \{2x \mid x \in Z\}$　　$f(a) = e'$

(c) Write the operation table of quotient group Z/ker(f). （4 分）

⊕	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

(c) $Z/\ker(f)$　　$\Downarrow$ [0] [1]　　$(Z/\ker(f))$ 商集

Z/R 所有等价类的集合

（4 分，运算表正确可得分，错一个扣 1 分，扣完为止） 什么东西.

9. [8 points] Let $H = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$ be a parity check matrix.

$e_H: B^3 \to B^7$

(a) Determine the (3,7) group code $e_H: B^3 \to B^7$.　$e(000) = 000$

（6分， 8个结果错一个扣 1分，扣完为止）

$$B^3 * H = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} * \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 \end{bmatrix}$$

或者写成如下形式:

e(000)=0000000 ，e(001)=0011011，
e(010)=0101101 ，e(011)=0110110，
e(100)=1001110 ，e(101)=1010101，
e(110)=1100011 ，e(111)=1111000.

$e(000) = 0000000$
$e(001) = 0011011$
$e(010) = 0101101$
$e(011) = 0110110$
. . . .

(b) How many errors will e detect ?

Because the minimal distance of e is 4， so e can detect 3 errors.

(2分,答对结果数即可得分,结果错但最小距离算对了可得1分)

最小距离, 4　能检测出3个错误.

9. [8 points] Consider the (3,6) group encoding function e: $B^3 \to B^6$ defined by

e(000)=000000, e(001)=001011, e(010)=010101,
e(011)=011110, e(100)=100110, e(101)=101101,
e(110)=110011, e(111)=111000.

(a) How many errors will (e, d) correct? $3 \geq 2k+1 \Rightarrow k \leq 1$

Because the minimal distance of e is 3，(e, d) can correct 1 error.

(2分,答对结果数即可得分,结果错但最小距离算对了可得1分)

(b) Determine the coset leaders for $N = e_H(B^3)$.

陪集头

000000	001011	010101	011110	100110	101101	110011	111000
000001	001010	010100	011111	100111	101100	110010	111001
000010	001001	010111	011100	100100	101111	110001	111010
000100	001111	010001	011010	100010	101001	110111	111100
001000	000011	011101	010110	101110	100101	111011	110000
010000	011011	000101	001110	110110	111101	100011	101000
100000	101011	110101	111110	000110	001101	010011	011000
001100	000111	011001	010010	101010	100001	111111	110100

（6分， 8个结果错一个扣 1分，扣完为止）

The coset leaders for N is {000000， 000001, 000010, 000100, 001000, 010000, 100000, 001100 / 010010 / 100001 }. 注意最后一个陪集头有3种写法都对

N is {000000, 000001, 000010, ... 100000, 001100}

10. [8 points] Let m=3, n=6, H=$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ be a parity check matrix.

(a) Compute the syndrome for the coset leaders { 000000，000001, 000010, 000100, 001000, 010000, 100000, 000110} for N=$e_H(B^3)$.

（5分， 8对结果错一个扣 0.5分，最终扣分若有小数则向下取整）

Syndrome	Coset leader
000	000000
001	000001
010	000010
100	000100
011	001000
101	010000
111	100000
110	000110

000000	000
000001	001
000010	010
000100	100
001000	011
010000	101
100000	111
000110	110

(a) Decode the following words relative to a maximum likelihood decoding function associated with e_H by using the coset leaders and their syndromes from (a).

a)100110 b) 011011 c) 110001

（3分，错一个结果扣1分。）

d(100110)=100, d(011011)=001, d(110001)=111.

100110 * H = 001

000001 ⊕ 100110

= 100111

100

Because 100110*H=001, so coset leader is 000001,
100110⊕000001=100111, so b=100.
Similar, 011011*H=101, so coset leader is 010000,
011011⊕010000=001011, so b=001. 001
110001*H=011, so coset leader is 001000, 110001⊕001000=111001, so b=111.

111