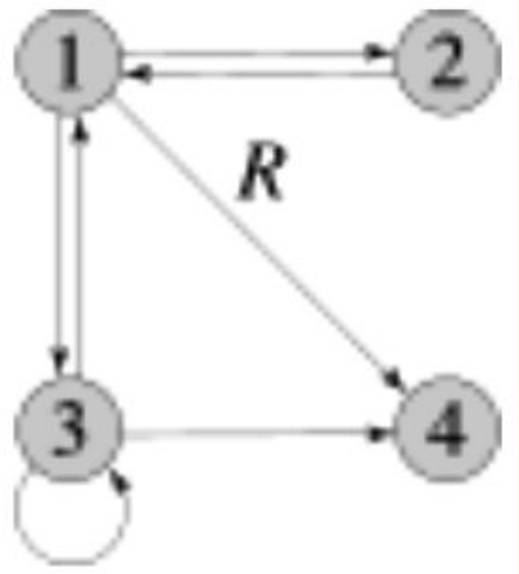
Discrete Structures

Tutorial 2

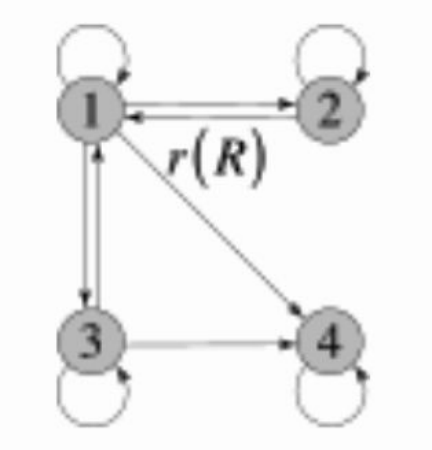
Question 1:

Let A={1,2,3,4}. A binary relation R on the set A is given by the digraph as shown in the figure. Find the reflexive closure of R.



Solution 1:

To build the reflexive closure of R, we just add the missing self-loops to all nodes of the digraph:



In roster form, the reflexive closure r(R) is given by
r(R) = {(1,1),(1,2),(1,3),(1,4),(2,1),(2,2),(3,1),(3,3),(3,4),(4,4)}.

Question 2:

Determine whether the relation R on the set of all integers is reflexive, symmetric, antisymmetric, and/or transitive, where $(x, y) \in R$ if and only if

a. $xy \geq 1$
b. $x = y+1$ or $x = y-1$

Solution 2:

$xy \geq 1$

- Not reflexive because we can't have (0,0).
- Is symmetric because we have $xy = yx$.
- Not antisymmetric because we have $xy = yx$.
- Is transitive because if we have $(a, b) \in R$ and that $(b, c) \in R$, it follows that $(a, c) \in R$.

Note that in order for the relation to be true, a, b, and c will have to be all positive or all negative.

$x = y+1$ or $x = y-1$

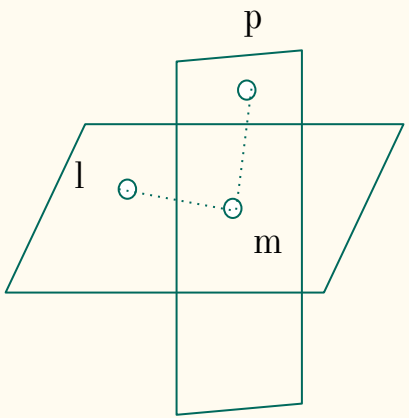
- Not reflexive because we can't have (1,1)
- Is symmetric because we have $x=y+1$ and $y=x-1$. They are equivalent equations.
- Not antisymmetric because of the same reason above.
- Not transitive because if we have (1,2) and (2,1) in the relation, (1,1) is not in relation.

Question 3:

Let S be the set of all lines in 3 dimensional space. A relation ρ is defined on S by “lρm if and only if l lies on the plane of m” for l, m $\in$ S. Is ρ an equivalence relation on S?

Solution 3:

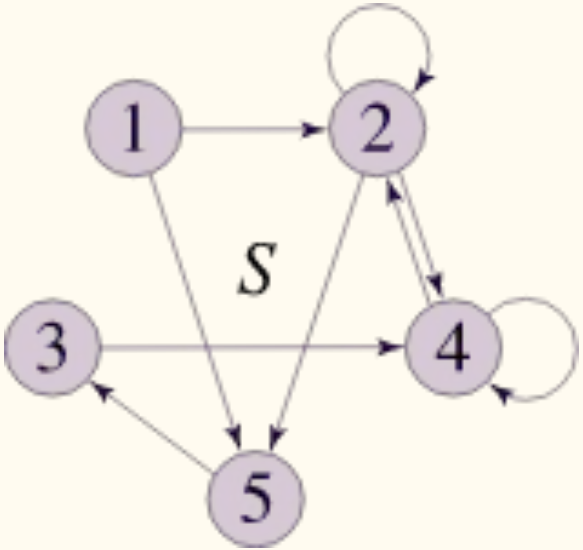
- Reflexive: Let l ∈ S. Then l is coplanar with itself. Therefore, lρl holds for all l in S. Hence, ρ is **reflexive**.
- Symmetric: Let l, m ∈ S and lρm holds. Then l lies on the plane of m. Therefore, m lies on the plane of l. Thus, lρm ⇒ mρl and therefore ρ is **symmetric**.
- Transitive: Let l, m, p ∈ S and lρm, mρp both hold. Then l lies on the plane of m and m lies on the plane of p. This does not always implies that l lies on the plane of p. That is, lρm and mρp do not necessarily imply lρp. Therefore, ρ is **not transitive**.



Since, R is reflexive and symmetric but not transitive so, R is not an equivalence relation on set S.

Question 4:

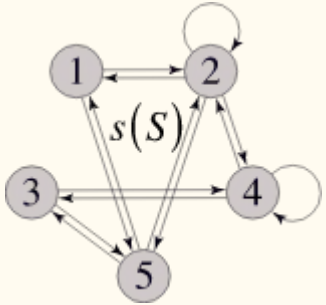
Let B=$\{1,2,3,4,5\}$. A binary relation S on the set B is given by the digraph.



Find the symmetric closure of S.

Solution 4:

To form the digraph of the symmetric closure, we simply add a new edge in the reverse direction (if none already exists) for each edge in the original digraph:



The symmetric closure of S contains the following ordered pairs:
s(S)=
{(1,2),(1,5),(2,1),(2,2),(2,4),(2,5),(3,4),(3,5),(4,2),(4,3),(4,4),(5,1),(5,2),(5,3)}.

Question 5:

Let S be a set of n>0 elements. Let be the number B_r of binary relations on S and let B_f be the number of functions from S to S. The expression for B_r and B_f , in terms of n should be:

Solution 5:

B_r = 2^(n*n) and B_f = n^n .

The number of elements in the Cartesian Product S X S = n * n
Binary relations over R are a subset of S X S. Therefore, number of binary relations B_r = 2^(n*n).

For every element in set S, function f can map it to one of the elements in S. There are n such possibilities for each element. Therefore, the number of functions is n^n.

Question 6:

Show that the closure with respect to the property P of the relation $R = \{(0, 0), (0, 1), (1, 1), (2, 2)\}$ on the set $\{0, 1, 2\}$ does not exist if P is the property

a) “is not reflexive.”

b) “has an odd number of elements.”

Solution 6:

a) No relation that contains R = {(0, 0), (0, 1), (1, 1), (2, 2)} is not reflexive, since R already contains all the pairs (0, 0), (1, 1), and (2, 2). Therefore there is no "non-reflexive" closure of R.

b) Suppose S were the closure of R with respect to this property. Since R does not have an odd number of elements, S != R, so S must be a proper superset of R.

Clearly S cannot have more than 5 elements, for if it did, then any subset of S consisting of R and one element of S - R would be a proper subset of S with the property; this would violate the requirement that S be a subset of every superset of R with the property. Thus S must have exactly 5 elements.

Let T be another superset of R with 5 elements (there are 9 - 4 = 5 such sets in all). Thus T has the property, but S is not a subset of T. This contradicts the definition. Therefore, our original assumption was faulty, and the closure does not exist.

Question 7

Find roots of the cubic equation using Cardano's method:

$$2x^3 + 12x^2 + 34x + 38 = 0$$

Solution 7

Step 1: reduce the equation to remove the x^2.

$$2x^3 + 12x^2 + 34x + 38 = 0$$
$$\Rightarrow \quad x^3 + 6x^2 + 17x + 19 = 0$$

replace $x = y - 2$

$$\Rightarrow \quad (y^3 - 6y^2 + 12y - 8) + (6y^2 - 24y + 24) + 17(y - 2) + 19 = 0$$
$$\Rightarrow \quad y^3 + 5y + 1 = 0$$

Solution 7

Step 2: replace $y = u - v$

$$y^3 + 5y + 1 = 0$$
$$\Rightarrow \; u^3 - v^3 - 3uv(u - v) + 5(u - v) + 1 = 0$$

by comparing, we have $3uv = 5$ and $v^3 - u^3 = 1$
$$\Rightarrow \; u^3v^3 = (5/3)^3 = 125/27$$

$$a + b = \sqrt{((a - b)^2 + 4ab)}$$
$$\Rightarrow \; v^3 + u^3 = \sqrt{(1 + 500/27)}$$

Solution 7

Step 3: solve for x

$v^3 - u^3 = 1$
$v^3 + u^3 = \sqrt{(527/27)}$
$y = u - v$
$x = y - 2$

$\Rightarrow x = u - v - 2$
$\Rightarrow x = \sqrt[3]{((\sqrt{(527/27)} - 1)/2)} - \sqrt[3]{((\sqrt{(527/27)} + 1)/2)} - 2$

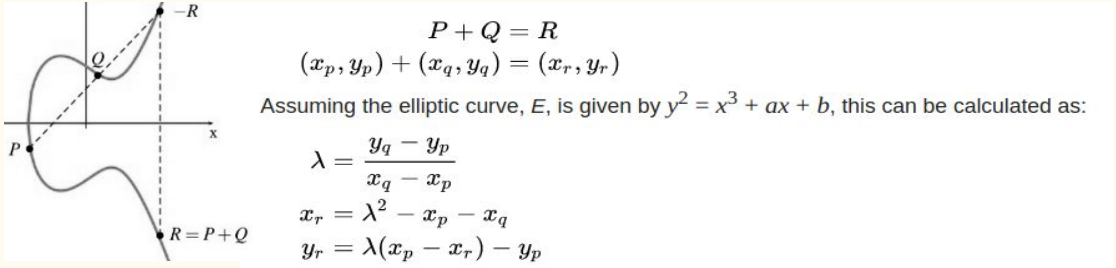
Question 8

Let P = (3 , 5) be a point on elliptic curve $y^2 = x^3 + 35 \pmod{37}$.

(i) Suppose each elliptic curve point addition and multiplication has 3 operations, for computing the slope, x coordinate and y coordinate. How many operations will it take to compute 41P ?

(ii) Compute 13P.

(iii) Find the order of the point P.



Solution 8 (i)

represent it in binary form

$41_{10} = 101001_2$

$\Rightarrow 41 = 1 + 8 + 32$

$\Rightarrow 41\text{P} = \text{P} + 8\text{P} + 32\text{P}$, so addition is done 2 times

$\Rightarrow 32\text{P} = 2^5\,\text{P}$, which means we need to perform doubling 5 times

Thus, total 7 * 3 = 21 operations are required here.

Solution 8 (ii)

$P = (3, 5)$

$2P = (32, 24)$

$4P = (36, 16)$

$8P = (29, 2)$

$5P = 4P + P = (31, 35)$

$13P = 8P + 5P = (18, 13)$

Solution 8 (iii)

$48P = -P$

thus $49P = 0$

Hence order of P is 49.

or,

see $24P = -25P$

so $49P = 0$

Extra Practice Problems

1. Let R={(a,b),(b,c),(c,a)} be a relation defined on the set A={a,b,c}. Find the reflexive closure of R^2

2. Determine whether the relation R on the set of all integers is reflexive, symmetric, antisymmetric, and/or transitive, where (x, y) $\in$ R if and only if

   a. x = y^2

   b. x>=y^2

3. Let R = { (a, b):|a-b| is even }. Prove that R is an equivalence relation in the set A = { 1, 2, 3, 4, 5 }.

4. Consider the binary relation, A = {(a,b) | b = a – 1 and a, b belong to {1, 2, 3}}. The reflexive transitive closure of A is?

5. Determine the characteristics of the relation aRb if a^2 = b^2 .

   a. a) Transitive and symmetric
   b. b) Reflexive and asymmetry
   c. c) Trichotomy, antisymmetry, and irreflexive
   d. d) Symmetric, Reflexive, and transitive

6. Let S={(k,ℓ),(k,n),(m,k),(m,m),(n,ℓ)} be a relation defined on the set B={k,ℓ,m,n}. Find the symmetric closure of S.

7. Let R be the relation on the set of all colorings of the 2×2 checkerboard where each of the four squares is colored either red or blue so that (C1 , C2), where C1 and C2 are 2×2 checkerboards with each of their four squares colored blue or red, belongs to R if and only if C2 can be obtained from C1 either by rotating the checkerboard or by rotating it and then reflecting it.

a) Show that R is an equivalence relation.
b) What are the equivalence classes of R?

Solutions to Practice Problems

1. $R = \{(a,b),(b,c),(c,a),(a,a),(b,b),(c,c)\}$

2. $x = y^2$

- Not reflexive because (2,2) does not satisfy.
- Not symmetric because although we can have (9,3), we can't have (3,9).
- Is antisymmetric because each integer will map to another integer but not in reverse (besides 0 and 1).
- Not transitive because if we have (16,4) and (4,2), it's not the case that $16 = 2^2$

$x \geq y^2$

- Not reflexive because we can't have (2,2).
- Not symmetric because if we have (9,3), we can't have (3,9).
- Is antisymmetric, because each integer will map to another integer but not in reverse (besides 0 and 1).
- Is transitive because if $x \geq y^2$ and $y \geq z^2$, then $x \geq z^2$

3. Here, R = { (a, b):|a-b| is even } and a, b ∈ A.

- Reflexive Property : From the given relation, |a – a| = | 0 |=0 and 0 is always even. Thus, |a-a| is even. Therefore, (a, a) ∈ R. Hence, R is Reflexive.
- Symmetric Property : From the given relation, |a – b| = |b – a|. We know that |a – b| = |-(b – a)|= |b – a|. Hence |a – b| is even. Then |b – a| is also even. Therefore, if (a, b) ∈ R, then (b, a) belongs to R. Hence, R is symmetric.
- Transitive Property : If |a-b| is even, then (a-b) is even. In the same way, if |b-c| is even, then (b-c) is also even. Sum of even number is also even. So, we can write it as a-b + b-c is even. Then, a – c is also even.

  So, |a – b| and |b – c| is even, then |a-c| is even. Therefore, if (a, b) ∈ R and (b, c) ∈ R, then (a, c) also belongs to R. Hence, R is transitive.

4. {(a,b) | a >= b and a, b belong to {1, 2, 3}}

By definition of Transitive closure we have that a is related to all smaller b (as every a is related to b – 1) and from the reflexive property a is related to a.

5. d) Symmetric, Reflexive, and transitive

Since, x 2 = y 2 is just a special case of equality, so all properties that apply to x = y also apply to this case. Hence, the relation satisfies symmetric, reflexive and transitive closure.

6. S = {(k,ℓ),(k,n),(m,k),(m,m),(n,ℓ),(ℓ,k),(n,k),(k,m),(ℓ,n)}

7. Symbols r0, r90, rl80, r270, fv, fh, fp, and fn for these operations, respectively. (The mnemonic is that r stands for "rotation," f stands for "flip," and v, h, p, and n stand for "vertical," "horizontal", "positive-sloping,'' and ''negative-sloping,'' respectively.)

Operation 'o' meaning ''followed by."

$\circ$	$r0$	$r90$	$r180$	$r270$	fv	fh	fp	fn
$r0$	$r0$	$r90$	$r180$	$r270$	fv	fh	fp	fn
$r90$	$r90$	$r180$	$r270$	$r0$	fn	fp	fv	fh
$r180$	$r180$	$r270$	$r0$	$r90$	fh	fv	fn	fp
$r270$	$r270$	$r0$	$r90$	$r180$	fp	fn	fh	fv
fv	fv	fp	fh	fn	$r0$	$r180$	$r90$	$r270$
fh	fh	fn	fv	fp	$r180$	$r0$	$r270$	$r90$
fp	fp	fh	fn	fv	$r270$	$r90$	$r0$	$r180$
fn	fn	fv	fp	fh	$r90$	$r270$	$r180$	$r0$

a) To show reflexivity, we note that every coloring can be obtained from itself via a 0° rotation. To show symmetry, we need to observe that rotations and reflections have inverses: If C1 comes from C2 via a rotation of n° clockwise, then C2 comes from C1 via a rotation of n° counterclockwise (or equivalently, via a rotation of (360 - n) 0 clockwise); and every reflection applied twice brings us back to the position (and therefore coloring) we began with. And transitivity follows from the fact that the composition of two of these operations is again one of these operations.

7. b) The equivalence classes are represented by colorings that are truly distinct, in the sense of not being obtainable from each other via these operations. Let us list them. Clearly there is just one coloring using four red squares, and so just one equivalence class, [rrrr]. Similarly there is only one using four blues, [bbbb].

There is also just one equivalence class of colorings using three reds and one blue, since no matter which corner the single blue occupies in such a coloring, we can rotate to put the blue in any other corner. Thus our third and fourth equivalence classes are [rrrb] and [bbbr]. Note that each of them contains four colorings. (For example, [rrrb] = {rrrb, rrbr, rbrr, brrr} .) This leaves only the colorings with two reds and two blues to consider. In every such coloring, either the red squares are adjacent (i.e., share a common edge), such as in bbrr, or they are not (e.g., brrb).

Clearly the red squares are adjacent if and only if the blue ones are, since the only pairs of nonadjacent squares are (lower-left,upper-right) and (upper-left,lower-right). It is equally clear that there are only two colorings in which the red squares are not adjacent, namely rbbr and brrb, and they are equivalent via a 90° rotation (among other transformations). So our fifth equivalence class is [rbbr] = {rbbr,brrb}.

Finally, there is only one more equivalence class, and it contains the remaining four colorings (in which the two red squares are adjacent and the two blue squares are adjacent), namely { rrbb, brbr, bbrr, rbrb}, since each of these can be obtained from each of the others by a rotation. In summary we have partitioned the set of 2^4 = 16 colorings (i.e., r-b strings of length four) into six equivalence classes, two of which have cardinality one, three of which have cardinality four, and one of which has cardinality two.