Números Inteiros e Criptografia, PLE 2020 Lista de Exercícios 2
Aluno: Luiz Rodrigo Lacé Rodrigues
DRE: 118049873

Questão 1. Sejam X e Y conjuntos. Prove as seguintes afirmações.

c. Temos $X \subseteq Y$ sse $X \cup (Y \cap Z) = (X \cup Z) \cap Y$.

$X \subseteq Y$ <--> $X \cup (Y \cap Z) = (X \cup Z) \cap Y$

$X \subseteq Y = \forall a(a \in X \text{ -> } a \in Y)$ temos aqui que todo elemento que pertence a X, pertence a Y.

Podemos dizer que $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$:
$\forall a(a \in X \vee (Y \wedge Z) = \forall a(a \in (X \vee Y) \wedge (X \vee Z)$

Como também $(X \cup Z) \cap Y = (Y \cap X) \cup (Y \cap Z)$:
$(X \cup Z) \cap Y = \forall a(a \in (X \vee Z) \wedge Y)$

Chegamos em:
$X \subseteq Y$ <--> $(X \cup Y) \cap (X \cup Z) = (Y \cap X) \cup (Y \cap Z)$:

Voltando ao fato que se o X está contido em Y, temos que sua união é igual ao próprio Y:
$(X \cup Y) = Y$
Substituindo:
$X \subseteq Y$ <--> $Y \cap (X \cup Z) = (Y \cap X) \cup (Y \cap Z)$:

E como a intersecção é o que temos em comum entre dois conjuntos, temos que $(Y \cap X) = X$
Substituindo:
$X \subseteq Y$ <--> $Y \cap (X \cup Z) = X \cup (Y \cap Z)$.

Assim provamos a igualdade $(Y \cap Z) = (X \cup Z) \cap Y$ se somente se os elementos de X estiverem contidos em Y.

Questão 2.
Se $A, B, C \subseteq X$ são conjuntos tais que $A \cap B = A \cap C$ e $(X \setminus A) \cap B = (X \setminus A) \cap C$, então $B = C$.

$A \cap B = A \cap C \wedge (X \setminus A) \cap B = (X \setminus A) \cap C \dashrightarrow B = C$.

$A, B, C \subseteq X : \forall a(a \in (A,B,C) \rightarrow a \in X)$

$A \cap B = \forall a(a \in A \wedge B)$
$A \cap C = \forall a(a \in A \wedge C)$

$(X \setminus A) \cap B = \forall a(a \in (X \wedge \notin A) \wedge B$
Então podemos dizer que ‘a’ está na intersecção de B com a diferença de X e A, o que também pode ser $(X \cap B) \setminus A$
$(X \setminus A) \cap C = \forall a(a \in (X \wedge \notin A) \wedge C$
A mesma coisa nesse caso: $(X \cap C) \setminus A$

Como A,B e C estão contidos em X, temos a intersecção de X com qualquer um desses outros conjuntos serão eles mesmos.

Chegando em:
$B \setminus A = C \setminus A$
Chamando os elementos de B de x e os elementos de A de y temos que:
$B \setminus A = B - A = x - y$
Chamando os elementos de C de w e os elementos de A de y novamente temos que:
$C \setminus A = C - A = w - y$
Assim chegamos que os elementos de B e de C são iguais:
$x - y = w - y$
$x = w$

Questão 5. Sejam X, Y e Z conjuntos. Prove cada uma das afirmações abaixo.
a. $X \subseteq Y \cap Z$ sse ($X \subseteq Y$ e $X \subseteq Z$).

$X \subseteq Y \cap Z \dashleftarrow\dashrightarrow (X \subseteq Y$ e $X \subseteq Z)$

$X \subseteq Y \cap Z \dashrightarrow (X \subseteq Y$ e $X \subseteq Z)$
$X \subseteq Y \cap Z = \forall a(a \in X \rightarrow a \in (Y \wedge Z))$
$X \subseteq Y = \forall a(a \in X \rightarrow a \in Y)$
$X \subseteq Z = \forall a(a \in X \rightarrow a \in Z)$
Se X está contido na intersecção de Y e Z, logo X está contido em Y e também em Z.

$(X \subseteq Y$ e $X \subseteq Z) \dashrightarrow X \subseteq Y \cap Z$
$X \subseteq Y = \forall a(a \in X \rightarrow a \in Y)$

$X \subseteq Z = \forall a(a \in X \rightarrow a \in Z)$
$X \subseteq Y \cap Z = \forall a(a \in X \rightarrow a \in (Y \wedge Z))$
Se X está contido em Y e também em Z, logo X está contido na intersecção de Y e Z..

c. $X \subseteq Y$ sse $X \cup Y = Y$ sse $X \cap Y = X$ (Atenção! Aqui temos duas afirmações separadas, uma para cada sse.)

$X \subseteq Y \leftrightarrow X \cup Y = Y \leftrightarrow X \cap Y = X$

$X \subseteq Y \rightarrow X \cup Y = Y$
$X \subseteq Y$: $\forall a(a \in X \rightarrow a \in Y)$
$X \cup Y = Y$: $\forall a(a \in X \vee a \in Y) = \forall a(a \in Y)$
Se todo elemento 'a' está contido em X, logo ele está contido em Y. Então se X está contido em Y, então a união de X e Y é igual a Y.

$X \subseteq Y \leftarrow X \cup Y = Y$
$X \cup Y = Y$: $\forall a(a \in X \vee a \in Y) = \forall a(a \in Y)$
$X \subseteq Y$: $\forall a(a \in X \rightarrow a \in Y)$
Se a união de X e Y é igual a Y, então X está contido em Y.

$X \cup Y = Y \rightarrow X \cap Y = X$
$X \cup Y = Y$: $\forall a(a \in X \vee a \in Y) = \forall a(a \in Y)$
$X \cap Y = X$: $\forall a(a \in X \vee a \in Y) = va(a \in X)$
Se todo elemento 'a' está contido na união de X e Y, logo ele está contido em Y.
Se a união de X e Y é igual a Y, então a intersecção de X e Y é igual a X.

$X \cup Y = Y \leftarrow X \cap Y = X$
$X \cap Y = X$: $\forall a(a \in X \vee a \in Y) = va(a \in X)$
$X \cup Y = Y$: $\forall a(a \in X \vee a \in Y) = \forall a(a \in Y)$
Se todo elemento 'a' está contido na intersecção de X e Y, logo ele está contido em X.
Se a intersecção X e Y é igual a X, então a união de X e Y é igual a Y.

Questão 6. Dê um exemplo de uma relação não-vazia no conjunto {a, b, c, d, e} que tenha as seguintes propriedades (ou informe se não for possível):

reflexiva: $\forall a \in A(aRa)$

simétrica: $\forall a1,a2 \in A(a1Ra2 \leftrightarrow a2Ra1)$

transitiva: $\forall a,b,c \in A(aRb \wedge bRc) \rightarrow aRc$

e. reflexiva, simétrica e não-transitiva
R:{(a,a),(a,b),(b,b),(b,a),(c,c),(e,e),(b,c)}

Sendo:
(a,a),(b,b),(c,c) e (e,e) as relações reflexivas;
(a,b),(b,a) a relação simétrica e

(a,b),(b,c) e (a,c) seria a relação transitiva, mas como se pede uma relação "não-transitiva", o (a,c) não está presente no conjunto de relações R.

Questão 11. Diremos que dois números inteiros "estão próximos" entre si sse o valor absoluto da diferença entre eles for menor ou igual a 2. Por exemplo, 3 está próximo de 5, 10 está próximo de 9, mas 8 não está próximo de 4. Representemos por R esta relação.

a. Dê a definição de R em notação de construção de conjuntos {. . . | . . .}.

R= {(x,x),(x,y),(x,y), (y,y)}

b. Prove ou refute: R é reflexiva.

Pela definição:(∀a∈A)(aRa)

Para todo 'a' contido em um conjunto A, temos que a relação de a com a é reflexiva.

Ex: R(x,x),

x-x = 0

c. Prove ou refute: R é simétrica.

Pela definição: (∀a1,a2∈A)(a1Ra2 <--> a2Ra1)

Para todo a1,a2 contidos em um conjunto A, temos que a1 está relacionado com a2 e " vice-versa".

Ex:R{(x,y),(y,x)}, x=2,y=4

x-y = |-2| = 2

y-x = 2

d. Prove ou refute: R é transitiva.

Pela definição: ∀a1,a2,a3∈A(a1Ra2 e a2Ra3) -> a1Ra3

R não é transitiva, pois se 'a1' se relacionar com 'a3' pode ser que não encontremos o mesmo resultado obtido quando relacionamos 'a1' com 'a2' e 'a2' com 'a3'

contraexemplo:

a1=2, a2=4, a3=6

a1-a2 = |-2| =2

a2-a3 = |-2| =2

a1-a3 = |-4| = 4

Podemos ver que a relação de a1Ra2 e de a2Ra3 , nós achamos números "próximos", mas em a1Ra3 não.

Questão 13. Sejam x1, x2, x3 e x4 números naturais. Prove o seguinte teorema: se $x1 + x2 + x3 + x4 \leq 4$, então $x1 \leq 1$ ou $x2 \leq 1$ ou $x3 \leq 1$ ou $x4 \leq 1$.

Através do enunciado podemos tirar uma informação do tipo p-->q, sendo a contrapositiva, por definição, igual a ¬q->¬p

$$(x1 + x2 + x3 + x4 \leq 4) \rightarrow (x1 \leq 1) v(x2 \leq 1) v (x3 \leq 1) v (x4 \leq 1)$$

A contrapositiva do teorema sendo:

$$\neg((x1 \leq 1) v (x2 \leq 1) v (x3 \leq 1) v (x4 \leq 1)) \text{->} \neg(x1 + x2 + x3 + x4 \leq 4)$$

Por algebrismo chegamos em:

$$((x1 > 1) \wedge (x2 > 1) \wedge (x3 > 1) \wedge (x4 > 1)) \text{->} (x1 + x2 + x3 + x4 > 4)$$

Portanto, se x1,x2,x3 e x4 forem maiores que 1, então a soma deles é maior que 4. Assim provamos através da contrapositiva que para que a soma tenha resultado igual ou menor que 4, todos os números devem ser iguais ou menores que 1.

Questão 20. Considere a função f : Z +(números inteiros positivos)→ Z definida abaixo:
f(x) = x/2 se x for par
f(x) = −(x−1)/2 se x for ímpar

a. Prove que f é injetiva. (Dica: faça uma prova em quatro casos considerando as possíveis paridades dos elementos do domínio).

Pela definição, para que f seja injetiva, temos que $\forall x,y \in A(f(x) = f(y) \rightarrow x=y)$

Caso x e y sejam pares:
x/2 = y/2
2x=2y
x=y
Provamos que é injetiva

Caso sejam ímpares:
−(x−1)/2 = −(y−1)/2
-x+1 = -y+1
-x = -y
x = y
Provamos que é injetiva

Caso x seja par e y seja ímpar ou vice-versa:
x/2 = −(y−1)/2
x = - y + 1
x + y = 1

Como são situação envolve números inteiros, não há como x ser par e y ser ímpar e a soma entre eles dar 1. Logo, pela definição $f(x) = f(y) \rightarrow x = y$. Provando que f é injetiva.

b. Prove que f é sobrejetiva. (Dica: faça uma prova por casos, considerando os sinais do elemento do contradomínio)

Pela definição, para que f seja sobrejetiva temos que:
$\forall y \in B \exists x \in A(f(x) = y)$

Caso o $y>=0$:
Para que isso aconteça, x deve ser par, logo:
$x/2 = y$
Então, para todo y existe pelo menos um x inteiro par que é seu dobro, satisfazendo $f(x) = y$ e provando ser sobrejetiva

Caso $y<0$:
Para que isso aconteça, x deve ser ímpar:
$-(x-1)/2 = y$

Então, para todo y existe pelo menos um x inteiro ímpar que que satisfaz
$-(x-1)/2$.

Em ambos os casos a função não apresenta descontinuidade, o que também ajuda a ser sobrejetiva.