

HW 3

S-Box, section BC's:

BC's - 4:

Proposition: If n is an even number then $n-1$ is an odd number.

Proof:

Assume $n-1$ is not odd. So $n-1$ is even.

By def'n, if $n-1$ is even then $n-1 = 2k$ for some $k \in \mathbb{Z}$.

So, $n-1 = 2k$ can be re-written as $n = 2k+1 = 2(k+1)-1$,
 $= 2m-1$, where $m = (k+1) \in \mathbb{Z}$.

So, $n = 2m-1$

We see that n is an odd number by def'n.

Therefore, if $n-1$ is not an odd number, then n is not an even number. $\square$

BC's - 5:

Proposition: If m^2 is an odd number, then m is an odd number.

Proof:

Assume m^2 is odd.

So $m^2 = 2l+1$, for some $l \in \mathbb{Z}$.

Assuming that m is odd we can write $m = 2kr$ for some $k \in \mathbb{Z}$ and r is either 0 or 1.

So we can re-write $m^2 = 2l+1$ as $(2kr)^2 = 2l+1$. Rearranging we get $4k^2 + 4kr + r^2 = 2l+1$.

So $4k^2 + 4kr + (r^2 - 1) = 2l$

Since the left side of the equation is even then the right must also be even.

But $2l$ is even so $r^2 - 1$ must also be even as well.

We consider two cases:

1.) If $r=0$, then $r^2 - 1 = 0^2 - 1 = -1$, which is not an even number.

2.) If $r=1$, then $r^2 - 1 = 1^2 - 1 = 0$, which is even.

Therefore we can conclude that $r=1$. So $m = 2k$. So if m^2 is odd then m is odd. $\square$

HW 3 cont.

BCI)-6:

Theorem: If n is not divisible by 4, then n is not divisible by 12.

Proof:

Assume n is divisible by 12.

Then by def'n, $n = 12x$ for some $x \in \mathbb{Z}$.

Let n be divisible by 4.

Then by def'n $n = 4k$ for some $k \in \mathbb{Z}$.

So, $12x = 4k$, which can be re-written as $3x = k$.

So, $n = 4k = 4(3x)$

So $n = 12x$.

Therefore, if n is divisible by 12 then n is divisible by 4.

So, if n is not divisible by 4, then n is not divisible by 12. $\square$

BCI)-7:

If x is odd, then x is not divisible by 3.

False: $x=5$ is odd by 5 is not divisible by 3 as it leaves a remainder of 2.

BCI)-8:

If $a|(b+c)$, then $a|b$ and $a|c$.

False: Let $a=5$, $b=1$, and $c=4$. $a|(b+c)$ because $25=5k$ for some $k \in \mathbb{Z}$. If $k=5$ then $25=25$. However $b+c=25$ but $b=1$ and $1 \neq 5k$ and $c=4$ and $4 \neq 5k$, where $k \in \mathbb{Z}$.

BCI)-9:

Theorem: An integer n is divisible by 6 iff n is both even and divisible by 3.

Proof:

$\Rightarrow$ Assume n is divisible by 6.

Then $n = 6m$ for some $m \in \mathbb{Z}$.

If n is even then m is also be even, so $m = 2k$ for some $k \in \mathbb{Z}$.

So $n = 6m = 6(2k) = 12k$.

By the contraposition
of exercise BCI)-1(b)

HWk 3 cont.

BL1-a (Continued):

$n = 12k$ can also be expressed as $n = 2l$, where $l = 6k$ and $l \in \mathbb{Z}$.

By def'n $n = 2l$ is even.

n is also divisible by 3 because it is divisible by 3.
So $\Rightarrow$ Assume n is both even and divisible by 3.

Then if n is divisible by 3, $n = 3k$ for some $k \in \mathbb{Z}$.

Moreover, if n is also an even number then k must be divisible by 2 meaning k must be even.

So $k = 2w$ for some $w \in \mathbb{Z}$.

So $n = 3k$ can be re-written as $n = 3(2w) = 6w$, which by def'n is even.

So if $n = 6w$ then n is also divisible by 6.

So n is divisible by 6 iff n is both even and divisible by 3. $\square$

BL1-10:

Theorem: $x^2 = 1$ iff $x = -1$ or $x = 1$.

Proof:

Assume x is a real number.

$x^2 = 1$ iff $x^2 - 1 = 0$.

We can factor $x^2 - 1 = (x-1)(x+1)$.

$x^2 - 1 = 0$ iff $(x-1)(x+1) = 0$ iff $x-1 = 0$ or $x+1 = 0$.

Therefore, $x = 1$ or $x = -1$.

So $x^2 = 1$ iff $x = -1$ or $x = 1$. $\square$

HWk 3 cont.

BCIS-5:

Theorem: $\mathbb{Z} = 3\mathbb{Z} \cup 3\mathbb{Z} + 1 \cup 3\mathbb{Z} + 2$

Proof:

Let $x \in \mathbb{Z}$, by the division algorithm, we can express x as $x = 3q + r$ for some $q, r \in \mathbb{Z}$ and $0 \leq r < 3$.

If $r = 0$, then $x = 3q$, which means $x \in 3\mathbb{Z}$.

If $r = 1$, then $x = 3q + 1$, which means $x \in (3\mathbb{Z} + 1)$.

If $r = 2$, then $x = 3q + 2$, which means $x \in (3\mathbb{Z} + 2)$.

In each case $x \in 3\mathbb{Z} \cup (3\mathbb{Z} + 1) \cup (3\mathbb{Z} + 2)$.

So $\mathbb{Z} \subseteq 3\mathbb{Z} \cup (3\mathbb{Z} + 1) \cup (3\mathbb{Z} + 2)$.

Let $x \in 3\mathbb{Z} \cup (3\mathbb{Z} + 1) \cup (3\mathbb{Z} + 2)$.

x can be expressed as $3q + r$ for some $q, r \in \mathbb{Z}$ and such that $0 \leq r < 3$.

Since $q \in \mathbb{Z} \Rightarrow 3q \in \mathbb{Z}$.

Therefore, $x \in \mathbb{Z}$.

So $3\mathbb{Z} \cup (3\mathbb{Z} + 1) \cup (3\mathbb{Z} + 2) \subseteq \mathbb{Z}$.

Therefore, $\mathbb{Z} \subseteq 3\mathbb{Z} \cup (3\mathbb{Z} + 1) \cup (3\mathbb{Z} + 2)$ and $3\mathbb{Z} \cup (3\mathbb{Z} + 1) \cup (3\mathbb{Z} + 2) \subseteq \mathbb{Z}$.

So $\mathbb{Z} = 3\mathbb{Z} \cup (3\mathbb{Z} + 1) \cup (3\mathbb{Z} + 2)$. $\square$

BCIS-6:

No the sets are not disjoint.

BCIS-7:

Theorem: $x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$

Proof:

Let x, y , and z be sets.

1) Assume $k \in x \cup (y \cap z)$.

Then, by def'n of union $k \in x$ or $k \in (y \cap z)$.

Then, by def'n of intersection $k \in y$ and $k \in z$.

We consider two cases:

HWK 3 cont.

BCIS - 7 (continued):

(a) $k \in Y$. Then, since $k \in X$ we have $k \in (X \cup Y)$, by def'n of union.

so $k \in (X \cup Y) \cap (X \cup Z)$ by def'n of Intersection.

(b) $k \in Z$. Then, since $k \in X$ we have $k \in (X \cup Z)$, by def'n of union.

Therefore, $X \cup (Y \cap Z) \subseteq (X \cup Y) \cap (X \cup Z)$.

2) Assume that $k \in (X \cup Y) \cap (X \cup Z)$.

Then $k \in (X \cup Y)$ and $k \in (X \cup Z)$ by def'n of Intersection.

In either case, $k \in X$ by def'n of union.

Moreover, in the first case $k \in Y$ by def'n of union while

in the second case $k \in Z$ by def'n of union.

So in either case, $k \in Y \cap Z$ by def'n of Intersection.

so in both cases $k \in X \cup (Y \cap Z)$ by def'n of union

so $(X \cup Y) \cap (X \cup Z) \subseteq X \cup (Y \cap Z)$.

Therefore, $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$. $\square$

T-BoP chapter 5:

(14) Theorem: If A, B , and C are sets, then $(A \cup B) - C = (A - C) \cup (B - C)$.
proof:

Let A, B , and C be sets.

Assume $x \in (A \cup B) - C$.

so $x \in A \cup B$ by def'n of union and $x \notin C$ by def'n of minus.

Since $x \in A \cup B$, either $x \in A$ or $x \in B$.

If $x \in A$, then $x \in A - C$ by def'n of minus.

If $x \in B$, then $x \in B - C$ by def'n of minus.

In either case, $x \in (A - C) \cup (B - C)$.

so $(A \cup B) - C \subseteq (A - C) \cup (B - C)$.

Next, assume $x \in (A - C) \cup (B - C)$.

so $x \in A - C$ or $x \in B - C$ by def'n of union.

→

HWK3 cont.

14 continued:

If $x \in A - C$, then $x \in A$ and $x \notin C$ by def'n of minus.
If $x \in B - C$, then $x \in B$ and $x \notin C$ by def'n of minus.
Since $x \in A$ and $x \in B$ then $x \in A \cup B$ by def'n of union.
Since $x \notin C$ then $x \in A \cup B - C$.

So $(A - C) \cup (B - C) \subseteq (A \cup B) - C$.

Since $(A \cup B) - C \subseteq (A - C) \cup (B - C)$ and $(A - C) \cup (B - C) \subseteq (A \cup B) - C$
then $(A \cup B) - C = (A - C) \cup (B - C)$. $\square$

(16) Theorem: If A, B , and C are sets, then $A \times (B \cup C) = (A \times B) \cup (A \times C)$.

Proof:

Let A, B , and C be sets.

Assume $(a, b) \in A \times (B \cup C)$.

By def'n of cartesian product $a \in A$ and $b \in B \cup C$.

By def'n of union, $b \in B$ or $b \in C$.

Since, $a \in A$ and $b \in B$ it follows that $(a, b) \in A \times B$ by def'n of cartesian product.

Since $a \in A$ and $b \in C$ it follows that $(a, b) \in A \times C$ by def'n of cartesian product.

So $(a, b) \in A \times B$ and $(a, b) \in A \times C$, so $(a, b) \in (A \times B) \cup (A \times C)$ by def'n of union.

Therefore, $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$.

Next, suppose $(a, b) \in (A \times B) \cup (A \times C)$.

By def'n of union, $(a, b) \in A \times B$ and $(a, b) \in A \times C$.

By def'n of cartesian product $(a, b) \in A \times B$ so $a \in A$ and $b \in B$.

By def'n of cartesian product $(a, b) \in A \times C$ so $a \in A$ and $b \in C$.

Since, $b \in B$ and $b \in C$ then $b \in B \cup C$ by def'n of union.

So $a \in A$ and $b \in B \cup C$ so $(a, b) \in A \times (B \cup C)$.

Therefore, $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$.

Since $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$ and $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$

then $A \times (B \cup C) = (A \times B) \cup (A \times C)$. $\square$