COMS10003

Name: Andreas Georgiou
Username: ag14774

Question 1:

a) i) $\{\Rightarrow\}$ It is <u>not</u> functionally complete
Every formula can be expressed in DNF. Therefore $\{\vee, \wedge, \neg\}$ is functionally complete. We have to express every connective in the set using $\Rightarrow$.

$p \vee q \equiv \neg p \Rightarrow q$. '$\vee$' cannot be expressed using '$\Rightarrow$' because we also need '$\neg$'.

$p \wedge q \equiv \neg(\neg p \vee \neg q)$ (De morgan law)
$\equiv \neg(p \Rightarrow \neg q)$
'$\wedge$' cannot be expressed using '$\Rightarrow$' because we also need '$\neg$'

$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$
$\equiv \neg(\neg(p \Rightarrow q) \vee \neg(q \Rightarrow p))$ (De morgan)
$\equiv \neg((p \Rightarrow q) \Rightarrow \neg(q \Rightarrow p))$
$\Leftrightarrow$ cannot be expressed using '$\Rightarrow$' because we need '$\neg$'

ii) $\{\Rightarrow, \neg\}$ We know that $\{\wedge, \vee, \neg\}$ is functionally complete.
$p \vee q \equiv \neg p \Rightarrow q$ ✓
$p \wedge q \equiv \neg(p \Rightarrow \neg q)$ ✓
$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$
$\equiv \neg(\neg(p \Rightarrow q) \vee \neg(q \Rightarrow p))$ (De morgan)
$\equiv \neg((p \Rightarrow q) \Rightarrow \neg(q \Rightarrow p))$ ✓

$\{\Rightarrow, \neg\}$ is <u>functionally complete</u> because we've expressed $\{\wedge, \vee, \neg\}$ using just $\{\Rightarrow, \neg\}$

Question 1

b)

A	B	C	¬A	¬B	¬C	¬A ⇒ B	A∧¬C	(A∧¬C) ⇔¬B	(¬A ⇒ B)∧((A∧¬C) ⇔¬B)
T	T	T	F	F	F	T	F	T	T ←
T	T	F	F	F	T	T	T	F	F
T	F	T	F	T	F	T	F	F	F
T	F	F	F	T	T	T	T	T	T ←
F	T	T	T	F	F	T	F	T	T ←
F	T	F	T	F	T	T	F	T	T ←
F	F	T	T	T	F	F	F	F	F
F	F	F	T	T	T	F	F	F	F

DNF: We find in the last column all entries with the value T. Those are called the minterms

DNF is the disjunction of the minterms:

$(A \wedge B \wedge C) \vee (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge C) \vee (\neg A \wedge B \wedge \neg C)$

Since this is not in minimised form yet, is called principal disjunctive normal form.

C \ AB	$\bar{A}\bar{B}$	$\bar{A}B$	AB	$A\bar{B}$
C	F	T	T	F
$\bar{C}$	F	T	F	T

$(B \wedge C) \vee (\neg A \wedge B) \vee (A \wedge \neg B \wedge \neg C)$

We use Karnaugh map to find the minimised form, by observing which variables stay the same

CNF: We find in the last column all entries with the value F. Those are called maxterms.

CNF is the conjuction of the maxterms (conjuction of disjunctions)

$\neg[(A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge C) \vee (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge \neg B \wedge \neg C)]$

$(\neg A \vee \neg B \vee C) \wedge (\neg A \vee B \vee \neg C) \wedge (A \vee B \vee \neg C) \wedge (A \vee B \vee C)$

C \ AB	$\bar{A}\bar{B}$	$\bar{A}B$	AB	$A\bar{B}$
C	F	T	T	F
$\bar{C}$	F	T	F	T

$\neg[(\neg A \wedge \neg B) \vee (\neg B \wedge C) \vee (A \wedge B \wedge \neg C)]$

$\neg(\neg A \wedge \neg B) \wedge \neg(\neg B \wedge C) \wedge \neg(A \wedge B \wedge \neg C)$

$(A \vee B) \wedge (B \vee \neg C) \wedge (\neg A \vee \neg B \vee C)$

Question 2

a) Proof by exhaustion

$n = 5k+1 \quad n^4 - 1$

$= (5k+1)^4 - 1$

$= 25(5k^2+2k)^2 + 10(5k^2+2k) \cancel{+1} \cancel{-1}$ Divisible by 5 by direct proof

$= 5\left[5(5k^2+2k)^2 + 2(5k^2+2k)\right]$

$n = 5k+2 \quad n^4 - 1$

$= (5k+2)^4 - 1$

$= 25(5k^2+4k)^2 + 40(5k^2+4k) + 16 - 1$

$= 25(5k^2+4k)^2 + 40(5k^2+4k) + 15$ Divisible by 5 by direct proof

$= 5\left[5(5k^2+4k)^2 + 8(5k^2+4k) + 3\right]$

$n = 5k+3$

$n^4 - 1$

$= (5k+3)^4 - 1$

$= 25(5k^2+6k)^2 + 90(5k^2+6k) + 81 - 1$

$= 25(5k^2+6k)^2 + 90(5k^2+6k) + 80$ Divisible by 5 by direct proof

$= 5\left[5(5k^2+6k)^2 + 18(5k^2+6k) + 16\right]$

$n = 5k+4$

$n^4 - 1$

$= (5k+4)^4 - 1$

$= 25(5k^2+8k)^2 + 160(5k^2+8k) + 256 - 1$ Divisible by 5 by direct proof

$= 25(5k^2+8k)^2 + 160(5k^2+8k) + 255$

$= 5\left[5(5k^2+8k)^2 + 32(5k^2+8k) + 51\right]$

Question 2

b) P: $x+y$ is even

Q: x and y have the same parity

$P \to Q \equiv \neg Q \to \neg P$

If x and y have different parity, $x+y$ is odd

Case 1: x: odd $\quad y$: even

$x: 2k+1 \quad y: 2j$

$$2k+1+2j = 2(k+j)+1$$

$x+y$ is odd by direct proof

Case 2: x: even $\quad y$: odd

$x: 2k \quad y: 2j+1$

$$2k+2j+1 = 2(k+j)+1$$

$x+y$ is odd by direct proof

Since we've proved that $\neg Q \to \neg P$ and $\neg Q \to \neg P \equiv P \to Q$, we've proved that $P \to Q$ hold using proof by contrapositive

This paper is recycled.

Question 3

a) Because $(40, 11) = 1$ there exists an inverse

$40 = 3 \cdot 11 + 7$

$11 = 1 \cdot 7 + 4$

$7 = 1 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1$

$1 = 4 - 3$

$1 = 4 - (7 - 4)$

$1 = 2 \cdot 4 - 7$

$1 = 2(11 - 7) - 7$

$1 = 2 \cdot 11 - 3 \cdot 7$

$1 = 2 \cdot 11 - 3 \cdot 40 + 9 \cdot 11$

$1 = \boxed{11} \cdot 11 - 3 \cdot 40$

$11^{-1} \equiv 11 \pmod{40}$

b) $x^{11} \bmod 41 = 10$ $\quad e = 11 \quad p = 41$

$d \equiv e^{-1} \pmod{p-1}$

$d \equiv 11^{-1} \pmod{40}$

From part a) $d \equiv 11 \pmod{40}$

$11 \cdot 11 \equiv 1 \pmod{40}$

$11 \cdot 11 = 1 + 40k$

$(x^{11})^{11} \equiv x^{1+40k} \equiv x \cdot x^{40k} \equiv x \pmod{41}$

Using Fermat's Little Theorem

$a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$

$x = 10^{11} \bmod 41$

$10^{11} = 10^{1+2+8} = 10 \cdot 10^2 \cdot 10^8$

$10^2 = 100 \equiv 18 \pmod{41}$

$10^4 \equiv 18^2 \equiv -4 \pmod{41}$

$10^8 \equiv (-4)^2 \equiv 16 \pmod{41}$

$10^{11} = 10 \cdot 10^2 \cdot 10^8 \equiv 10 \cdot 18 \cdot 16 \equiv 10 \pmod{41}$

$\boxed{x = 10}$

Question 4

$e=5$ $\qquad \phi(n)=\phi(pq)=\phi(p)\cdot\phi(q)=(p-1)(q-1)$

$n=111=3\cdot 37$ $\qquad \phi(111)=\phi(3)\cdot\phi(37)=2\cdot 36=72$

$d\equiv e^{-1} \pmod{\phi(n)}$ $\quad ed\equiv 1 \pmod{\phi(n)}$ $\quad ed=1+k\phi(n)$

$C(M)^d=M^{ed}=M\cdot(M^{\phi(n)})^k\equiv M \pmod n$

Because $(5,72)=1$ there is an inverse of e

$72=14\cdot 5+2$ $\qquad 29=(11101)_2$

$5=2\cdot 2+1$

$1=5-2\cdot 2$

$1=5-2\cdot(72-14\cdot 5)$

$1=5-2\cdot 72+28\cdot 5$

$1=29\cdot 5-2\cdot 72$

$d\equiv 29 \pmod{72}$

$101^2\equiv 100 \pmod{111}$

$101^4\equiv 100^2\equiv 10 \pmod{111}$

$101^8\equiv 10^2\equiv 100 \pmod{111}$

$101^{16}\equiv 100^2\equiv 10 \pmod{111}$

$101^{29}\equiv 101\cdot 10\cdot 100\cdot 10\equiv 11 \pmod{111}$

$81^2\equiv 12 \pmod{111}$

$81^4\equiv 12^2\equiv 33 \pmod{111}$

$81^8\equiv 33^2\equiv 90\equiv -21 \pmod{111}$

$81^{16}\equiv (-21)^2\equiv -3 \pmod{111}$

$81^{29}\equiv 81\cdot 33\cdot(-21)\cdot(-3)\equiv 12 \pmod{111}$

$25^2\equiv -41 \pmod{111}$

$25^4\equiv (-41)^2\equiv 16 \pmod{111}$

$25^8\equiv 16^2\equiv 34 \pmod{111}$

$25^{16}\equiv 34^2\equiv 46 \pmod{111}$

$25^{29}\equiv 25\cdot 16\cdot 34\cdot 46\equiv 4 \pmod{111}$

$32^2\equiv 25 \pmod{111}$

$32^4\equiv 25^2\equiv -41 \pmod{111}$

$32^8\equiv (-41)^2\equiv 16 \pmod{111}$

$32^{16}\equiv 16^2\equiv 34 \pmod{111}$

$32^{29}\equiv 32\cdot 34\cdot 16\cdot(-41)\equiv 2 \pmod{111}$

$001^{29} \bmod 111 = 001$ B

$101^{29} \bmod 111 = 011$ L

$000^{29} \bmod 111 = 000$ A

$081^{29} \bmod 111 = 012$ M

$025^{29} \bmod 111 = 004$ E

$032^{29} \bmod 111 = 002$ C

$000^{29} \bmod 111 = 000$ A

$101^{29} \bmod 111 = 011$ L

$013^{29} \bmod 111 = 022$ W

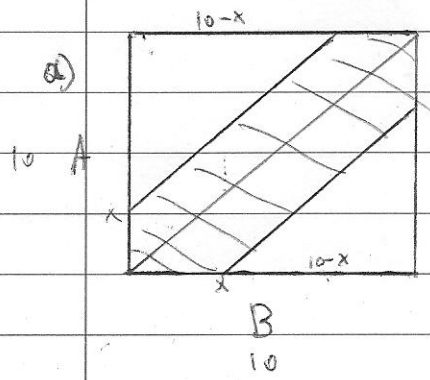
$000^{29} \bmod 111 = 000$ A

$067^{29} \bmod 111 = 025$ Z

The key $n=111$ is a 3-digit number, therefore the block size is 3.
Also in the encoded message there are 33 digits and $3 \mid 33$.
Everything greater than a 3-digit number would be greater than our key which is not possible.

Question 5

a)



$$0.5 = \frac{(10.10) - \frac{(10-x)^2}{\cancel{2}} \cdot \cancel{2}}{(10.10)}$$

$$50 = 100 - (100 - 20x + x^2)$$

$A = B + x$

$A = B - x$

$$50 = \cancel{100} - \cancel{100} + 20x - x^2$$

$$0 = -x^2 + 20x - 50$$

$$0 = x^2 - 20x + 50$$

$$x_{1,2} = \frac{20 \pm \sqrt{20^2 - 4.1.50}}{2}$$

$$= \frac{20 \pm 10\sqrt{2}}{2} = 5.(2 \pm \sqrt{2})$$

$$\cancel{x_1 = 5(2+\sqrt{2}) = 17.07}$$

$$\boxed{x_2 = 5(2-\sqrt{2}) = 2.929}$$

b) $P(128|A) = 0.25$ $\quad P(A) = \frac{1}{2}$

$P(256|A) = 0.75$ $\quad P(B) = \frac{1}{2}$

$P(128|B) = 0.36$ $\quad P(256) = 0.75 \cdot \frac{1}{2} + 0.64 \cdot \frac{1}{2} = 0.695$

$P(256|B) = 0.64$ $\quad P(128) = 0.25 \cdot \frac{1}{2} + 0.36 \cdot \frac{1}{2} = 0.305$

E_1: 256 followed by 128

$P(E_1) = (0.695).(0.305) = 0.211975$

$$P(AB|E_1) = \frac{P(E_1|AB)P(AB)}{P(E_1)} = \frac{(0.75)(0.36).(\frac{1}{2})(\frac{1}{2})}{0.211975} = \frac{2700}{8479} = 0.318$$