Discrete Mathematics and Proof Unit 1 worksheet: Exclusive or and logic circuits (answer key)

ANSWERS AT A GLANCE

1. (a) $\neg P$ (b) T (c) F (d) Q
2. (a) $C = 10101111$ (b) in each position $(m \oplus k) \oplus k \equiv m \oplus (k \oplus k) \equiv m \oplus \mathrm{F} \equiv m$ (c) $M \oplus C = K = 11000110$, so the message is 01011010
3. (a) Each switch that is up has been flipped once since all were down, and each flip changes the light, so the light is on exactly when an odd number of switches are up; by the parity theorem that is when $A \oplus B \oplus C$ is true. (b) Two XOR gates: A and B feed one, and its output and C feed the other. (c) $(A \wedge B \wedge C) \vee (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$; 3 NOT, 8 AND and 3 OR gates, 14 in all.
4. (a) $Y = (P \oplus Q) \vee (P \wedge R)$ (b) Y is false on rows 2, 7 and 8 (c) the new output is $(P \oplus Q) \vee (Q \wedge R)$, and it agrees with Y on every row: when P and Q differ both are T, and when they agree $P \wedge R$ and $Q \wedge R$ have the same value.
5. (a) $(A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge C)$; 3 NOT, 8 AND and 3 OR gates, 14 in all (b) $Z \equiv A \oplus (B \wedge C)$: an AND gate on B and C, and an XOR gate fed by its output and A.
6. (a) The inputs are on the list, and the exclusive or of any two statements on the list is on the list again. (b) Those four are true on 0, 2, 2 and 2 of the 4 rows, but $P \wedge Q$ is true on 1 row and $P \vee Q$ on 3. (c) 8 of the 16: F, T, P, $\neg P$, Q, $\neg Q$, $P \oplus Q$, $\neg(P \oplus Q)$.

WORKED SOLUTIONS

1. Use the laws of exclusive or to simplify each statement to a single letter, its negation, T or F.

(a) $Q \oplus (\neg P \oplus Q)$

(b) $(P \oplus \mathrm{T}) \oplus (\neg P \oplus \mathrm{T})$

(c) $\neg P \oplus \neg(Q \oplus P) \oplus Q$

(d) $(P \oplus \neg Q) \oplus (\neg Q \oplus R) \oplus (R \oplus P \oplus Q)$

ANSWER

(a) $\neg P$ (b) T (c) F (d) Q

SOLUTION

Each time, regroup and reorder the chain (associative and commutative laws), then use $X \oplus X \equiv \mathrm{F}$, $X \oplus \mathrm{F} \equiv X$ and $X \oplus \mathrm{T} \equiv \neg X$. A negation can be written $\neg X \equiv X \oplus \mathrm{T}$.

(a) $Q \oplus \neg P \oplus Q \equiv (Q \oplus Q) \oplus \neg P \equiv \mathrm{F} \oplus \neg P \equiv \neg P$.

(b) $P \oplus \mathrm{T} \equiv \neg P$ and $\neg P \oplus \mathrm{T} \equiv P$, so the statement is $\neg P \oplus P$. A statement always differs from its negation, so this is T. (Or: $(P \oplus \neg P) \oplus (\mathrm{T} \oplus \mathrm{T}) \equiv \mathrm{T} \oplus \mathrm{F} \equiv \mathrm{T}$.)

(c) Write $\neg P$ as $P \oplus \mathrm{T}$ and $\neg(Q \oplus P)$ as $Q \oplus P \oplus \mathrm{T}$. The chain is $P \oplus \mathrm{T} \oplus Q \oplus P \oplus \mathrm{T} \oplus Q \equiv (P \oplus P) \oplus (Q \oplus Q) \oplus (\mathrm{T} \oplus \mathrm{T}) \equiv \mathrm{F}$.

(d) The chain is $P \oplus \neg Q \oplus \neg Q \oplus R \oplus R \oplus P \oplus Q$. The two copies of $\neg Q$, of R and of P each cancel to F, leaving Q. Check at P, Q, R all T: the parts are T, T and T, and $\mathrm{T} \oplus \mathrm{T} \oplus \mathrm{T}$ is T, which is Q.

2. Yuna and Andre share a secret key $K = 11000110$. To send an 8-bit message M, Yuna sends $C = M \oplus K$, where $\oplus$ is taken position by position: the first bit of C is the exclusive or of the first bits of M and K, and so on.

(a) Find C when $M = 01101001$.

(b) Andre receives C and works out $C \oplus K$, position by position. Use the laws of exclusive or to explain why this always gives back M.

(c) An eavesdropper learns both M and C from part (a). The next day the same key is used, and the eavesdropper sees $C' = 10011100$. Find the next day's message, and explain how the eavesdropper can.

ANSWER

(a) $C = 10101111$ (b) in each position $(m \oplus k) \oplus k \equiv m \oplus (k \oplus k) \equiv m \oplus \mathrm{F} \equiv m$ (c) $M \oplus C = K = 11000110$, so the message is 01011010

Free sample from math.wiki for classroom use. Do not post. math.wiki

SOLUTION

(a) Line the strings up. A bit of C is 1 exactly where M and K differ:

$M = 01101001$, $K = 11000110$, so $C = 10101111$.

(b) Take one position, with message bit m and key bit k. The bit sent is $m \oplus k$, and Andre computes $(m \oplus k) \oplus k$. By the associative law this is $m \oplus (k \oplus k)$; a statement exclusive-or'ed with itself is F, so it is $m \oplus$ F, which is m. This holds in every position whatever the bits are, so $C \oplus K = M$.

(c) The same laws give $M \oplus C = M \oplus (M \oplus K) \equiv (M \oplus M) \oplus K \equiv K$, position by position. So the eavesdropper computes $01101001 \oplus 10101111 = 11000110$, which is the key. Then the next day's message is $C' \oplus K = 10011100 \oplus 11000110 = 01011010$, just as Andre would decode it. This is why such a key must never be used twice.

3. A long hallway has one light and three switches, one at each door. Let A, B and C be "switch A is up", "switch B is up" and "switch C is up". The electrician's rules: the light is off when all three switches are down, and flipping any one switch, from any position, changes the light.

(a) Explain why the light L must be $A \oplus B \oplus C$.

(b) Describe a circuit for L made of XOR gates only, and count its gates.

(c) Suppose only AND, OR and NOT gates are available. Write the statement the table method gives for L (rows in the order A, B, C). Count its two-input gates, building each term separately and using one NOT gate for each letter that is negated.

ANSWER

(a) Each switch that is up has been flipped once since all were down, and each flip changes the light, so the light is on exactly when an odd number of switches are up; by the parity theorem that is when $A \oplus B \oplus C$ is true. (b) Two XOR gates: A and B feed one, and its output and C feed the other. (c) $(A \wedge B \wedge C) \vee (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge \neg C) \vee (\neg A \wedge \neg B \wedge C)$; 3 NOT, 8 AND and 3 OR gates, 14 in all.

SOLUTION

(a) Start with all three switches down: the light is off. Any position can be reached from there by flipping up, one at a time, the switches that are up in it. Each flip changes the light, so after an even number of flips it is off and after an odd number it is on. So the light is on exactly when an odd number of A, B, C are true. By the parity theorem, $A \oplus B \oplus C$ is true exactly then, so $L = A \oplus B \oplus C$. (It also obeys the rule directly: flipping switch A replaces A by $A \oplus$ T, and T in a chain negates the whole chain.)

(b) A and B feed an XOR gate, which outputs $A \oplus B$. That output and C feed a second XOR gate, which outputs $(A \oplus B) \oplus C$. Two gates.

(c) L is true on the rows with an odd number of T's: rows 1 (T, T, T), 4 (T, F, F), 6 (F, T, F) and 7 (F, F, T). One term for each:

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

Each of A, B, C is negated somewhere, so 3 NOT gates. Each term joins three letters, 2 AND gates, so 8 AND gates. Joining four terms takes 3 OR gates. That is 14 gates against 2, which is why circuits that test parity are built from XOR gates.

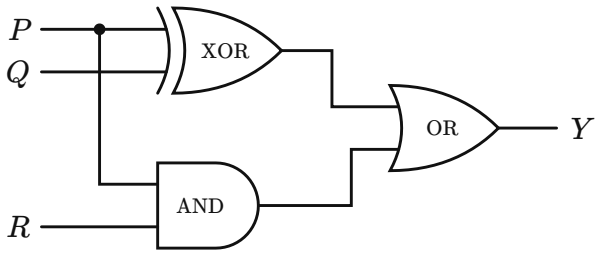
4. The circuit has inputs P, Q, R and output Y. The dot shows where P's wire branches; the branch crosses Q's wire without connecting to it.

(a) Write Y as a statement in P, Q and R.

(b) Make the truth table of Y, rows in the order P, Q, R, and list the rows on which Y is false.

Free sample from math.wiki for classroom use. Do not post. math.wiki

(c) The branch from P is moved so that it carries Q into the AND gate instead. Show that this does not change the output on any row.



ANSWER

(a) $Y = (P \oplus Q) \vee (P \wedge R)$ (b) Y is false on rows 2, 7 and 8 (c) the new output is $(P \oplus Q) \vee (Q \wedge R)$, and it agrees with Y on every row: when P and Q differ both are T, and when they agree $P \wedge R$ and $Q \wedge R$ have the same value.

SOLUTION

(a) Work from the inputs. The XOR gate carries $P \oplus Q$. The AND gate is fed by the branch of P and by R, so it carries $P \wedge R$. Both feed the OR gate: $Y = (P \oplus Q) \vee (P \wedge R)$.

(b)

Row	P	Q	R	$P \oplus Q$	$P \wedge R$	$(P \oplus Q) \vee (P \wedge R)$
1	T	T	T	F	T	T
2	T	T	F	F	F	F
3	T	F	T	T	T	T
4	T	F	F	T	F	T
5	F	T	T	T	F	T
6	F	T	F	T	F	T
7	F	F	T	F	F	F
8	F	F	F	F	F	F

Y is false on rows 2, 7 and 8.

(c) The new circuit outputs $(P \oplus Q) \vee (Q \wedge R)$. Split on whether P and Q differ. If they differ, $P \oplus Q$ is T, so both outputs are T. If they agree, P and Q have the same value, so $P \wedge R$ and $Q \wedge R$ have the same value, and both outputs are F$\vee$ that value. Every row falls in one case, so the outputs agree on every row.

5. An engineer is handed this table for the output Z of a circuit with inputs A, B and C.

Row	A	B	C	Z
1	T	T	T	F
2	T	T	F	T
3	T	F	T	T
4	T	F	F	T
5	F	T	T	T
6	F	T	F	F
7	F	F	T	F
8	F	F	F	F

(a) Write the statement the table method gives for Z. Count its two-input gates, building each term separately and using one NOT gate for each letter that is negated.

(b) Find a circuit for Z with only two gates, one of them an XOR gate, and explain why it has the column above.

Free sample from math.wiki for classroom use. Do not post. math.wiki

ANSWER

(a) $(A \wedge B \wedge \neg C) \vee (A \wedge \neg B \wedge C) \vee (A \wedge \neg B \wedge \neg C) \vee (\neg A \wedge B \wedge C)$; 3 NOT, 8 AND and 3 OR gates, 14 in all (b) $Z \equiv A \oplus (B \wedge C)$: an AND gate on B and C, and an XOR gate fed by its output and A.

SOLUTION

(a) Z is T on rows 2, 3, 4 and 5. Each row gives a term that is true on that row only:

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

NOT gates for $\neg A$, $\neg B$ and $\neg C$: 3. Each term joins three letters: 2 AND gates each, 8 in all. Four terms take 3 OR gates. Total 14. (Sharing one wire for $A \wedge \neg B$, which starts two terms, would save an AND gate.)

(b) Look at the two halves of the table. When A is T (rows 1 to 4), Z is F only where B and C are both T, so there Z has the value of $\neg(B \wedge C)$. When A is F (rows 5 to 8), Z is T only where B and C are both T, so there Z has the value of $B \wedge C$. So Z is $B \wedge C$, flipped exactly when A is T: $Z \equiv A \oplus (B \wedge C)$, since $X \oplus \mathrm{F} \equiv X$ and $X \oplus \mathrm{T} \equiv \neg X$. The circuit: B and C feed an AND gate, and its output and A feed an XOR gate. Two gates against fourteen.

6. A circuit has two inputs, P and Q, and is made of XOR gates only (as many as you like, wired any way without loops; a wire may branch).

(a) Explain why every wire in the circuit carries a statement equivalent to one of F, P, Q, $P \oplus Q$.

(b) Conclude that no such circuit computes $P \wedge Q$, and none computes $P \vee Q$.

(c) Now a wire that is always T may also be used. How many of the 16 possible columns of a two-letter truth table can such circuits compute? List the statements.

ANSWER

(a) The inputs are on the list, and the exclusive or of any two statements on the list is on the list again. (b) Those four are true on 0, 2, 2 and 2 of the 4 rows, but $P \wedge Q$ is true on 1 row and $P \vee Q$ on 3. (c) 8 of the 16: F, T, P, $\neg P$, Q, $\neg Q$, $P \oplus Q$, $\neg(P \oplus Q)$.

SOLUTION

(a) The two input wires carry P and Q, which are on the list. Since there are no loops, the gates can be taken in an order in which each gate's inputs come from the inputs or from earlier gates. So it is enough to see that the output of a gate fed by two statements from the list is again on the list. By the laws: $X \oplus X \equiv \mathrm{F}$ (a branched wire feeding both inputs), $\mathrm{F} \oplus X \equiv X$, $P \oplus Q$ is on the list, $P \oplus (P \oplus Q) \equiv Q$ and $Q \oplus (P \oplus Q) \equiv P$, and the commutative law covers the other orders.

(b) Count true rows in the four-row table. F is true on none; P, Q and $P \oplus Q$ are each true on 2 (the last by the parity theorem: rows TF and FT). $P \wedge Q$ is true on 1 row only (TT), and $P \vee Q$ on 3, so neither is equivalent to anything on the list.

(c) Now every wire is an exclusive or of some of P, Q, T, each used at most once, since two copies cancel. There are $2^3 = 8$ such choices: F (none), T, P, $P \oplus \mathrm{T} \equiv \neg P$, Q, $\neg Q$, $P \oplus Q$ and $P \oplus Q \oplus \mathrm{T} \equiv \neg(P \oplus Q)$. Their columns are all different, so the circuits compute 8 of the 16 columns: exactly those true on an even number of rows. The other 8, true on 1 or 3 rows, include $P \wedge Q$ and $P \vee Q$; an XOR gate needs an AND gate beside it, as in the half adder.

Free sample from math.wiki for classroom use. Do not post. math.wiki