Administrativia: no discussions, no extra material consulted

Problem

Let S denote all subsets of some set of elements U.

For $A, B \in S$, define $A\Delta B = \{x \in U \,|\, (x \in A) \text{ XOR } (x \in B)\}$.

Note that δ is commutative and associative since XOR is commutative and associative.

Let $n \in \mathbb{Z}^+$ and let $A_1, \ldots, A_n \in S$.

Formally prove (using induction) that, for all $x \in U$, $x \in A_1 \Delta A_2 \Delta \cdots \Delta A_n$ if and only if $\#\{i \in \{1, \ldots, n\} \,|\, x \in A_i\}$ is odd.

Solution

For any $i \in \mathbb{N}$, let T_i be the set of all sets consisting of i subsets in S.

Let A_i be the i^{th} element in each $Q_i \in T_i$.

For $n \in \mathbb{N}$, let

$P(n) =$ "$\forall \tau_n \in T_n . \forall x \in U . (x \in A_1 \Delta \cdots \Delta A_n \text{ IFF } \#\{i \in \{1, \ldots, n\} \,|\, x \in A_i\} \text{ is odd}$".

(1)	$P(1)$	Base Case for all $x \in U$, if $x \in A_1$, then, $\#\{i \in \{1, \dots, n\} \mid x \in A_i\} = 1$, which is odd
(2)	$\boxed{\forall i \in [1,k] \cap \mathbb{N}. P(i) \text{ for some } k \in \mathbb{N}}$	Inductive Step Assumption
(3)	$P(k)$	Specialisation, (2)
(4)	$\forall Q'_k \in T_k. \forall x \in U.$ $(x \in A_1 \Delta \cdots \Delta A_k \text{ IFF } \#\{i \in \{1, \dots, k\} \mid x \in A_i\} \text{ is odd})$	Definition of P, (3)
(5)	$\boxed{\text{Let } S_k \in T_k \text{ be arbitrary.}}$	
(6)	$\boxed{\text{Let } x \in U \text{ be arbitrary.}}$	
(7)	Let $A_1, \dots, A_k$ be distinct elements in S_k.	
(8)	$x \in A_1 \Delta \cdots \Delta A_k \text{ IFF } \#\{i \in \{1, \dots, k\} \mid x \in A_i\} \text{ is odd}$	Specialisation, (4)
(9)	$\boxed{\text{Let } A_{k+1} \in S \text{ be arbitrary.}}$	
(10)	$A_k \Delta A_{k+1} \in S$	Definition of S
(11)	$\{A_1, \dots, A_{k-1}, A_k \Delta A_{k+1}\}$ is a set of k subsets in S	(5), (10)
(12)	$\boxed{\text{Let } Q_k = A_k \Delta A_{k+1} \text{ and } Q_i = A_i \text{ for } i \in [1, k-1] \cap \mathbb{N}.}$	

(13)	$Q = \{Q_1, \ldots, Q_k\}$ is a set of k subsets in S	Substitution; (11), (13)
(14)	$Q \in T_k$	Definition of Q, (13)
(15)	$\forall y \in U.$ $(y \in Q_1 \Delta \cdots \Delta Q_k$ IFF $\#\{i \in \{1, \ldots, k\} \mid y \in Q_i\}$ is odd)	Specialisation for Q, (14)
(16)	$(x \in Q_1 \Delta \cdots \Delta Q_k$ IFF $\#\{i \in \{1, \ldots, k\} \mid x \in Q_i\}$ is odd)	Specialisation for x, (15)
(17)	$Q_1 \Delta \cdots \Delta Q_k = A_1 \Delta \cdots \Delta A_k \Delta A_{k+1}$	Definition of Q_i for $i \in [1, k+1] \cap \mathbb{N}$; (12)
(18)	$(x \in A_1 \Delta \cdots \Delta A_k \Delta A_{k+1}$ IFF $\#\{i \in \{1, \ldots, k\} \mid x \in Q_i\}$ is odd)	Substitution, (17)
(19)	$\#\{i \in \{1, \ldots, k\} \mid x \in Q_i\} =$ $\#\{i \in \{1, \ldots, k-1\} \mid x \in Q_i\} + \#\{i \in \{k\} \mid x \in Q_i\}$	Definition of $\#\{i \in \{1, \ldots, k\} \mid x \in Q_i\}$
(20)	Let $R = \{A_k, A_{k+1}\}$.	
(21)	$R \in T_2$	Definition of T_2 and R,(20)
(22)	$\boxed{P(2)}$	Specialisation, (2)
(23)	$\forall w \in U.(w \in A_k \Delta A_{k+1}$ IFF $\#\{i \in \{k, k+1\} \mid w \in A_i\}$ is odd)	Specialisation for R, (20), (22)
(24)	$(x \in A_k \Delta A_{k+1}$ IFF $\#\{i \in \{k, k+1\} \mid x \in A_i\}$ is odd)	Specialisation for x, (23)
(25)	$(x \in Q_k$ IFF $\#\{i \in \{k, k+1\} \mid x \in A_i\}$ is odd)	Substitution, (9), (24)

(26)	$\boxed{P(1)}$	Specialisation, (2)
(27)	$Q_k \in T_1$	Definition of T_1 and Q_k, (12)
(28)	$(x \in Q_k$ IFF $\#\{i \in \{k\} \mid x \in Q_i\}$ is odd$)$	Specialisation for Q_k and x, (26)
(29)	Let A, B, C be arbitrary propositional variables.	
(30)	((A IFF B) AND (A IFF C)) IMPLIES (B IFF C)	Tautology
(31)	$\#\{i \in \{k\} \mid x \in Q_i\}$ is odd IFF $\#\{i \in \{k, k+1\} \mid x \in A_i\}$ is odd	Use of Tautology (Modus Ponens), (25), (28), (30)
(32)	$\forall A \in \mathbb{N} \cup \{0\}. \forall B \in \mathbb{N} \cup \{0\}. \forall C \in \mathbb{N} \cup \{0\}.$ $[(A$ is odd IFF B is odd$)$ IFF $(A + C$ is odd IFF $B + C$ is odd$)]$	Tautology: Parity Equivalence is Conserved Under Addition
(33)	$(\#\{i \in \{k\} \mid x \in Q_i\}$ is odd IFF $\#\{i \in \{k, k+1\} \mid x \in A_i\}$ is odd$)$ IFF $(\#\{i \in \{k\} \mid x \in Q_i\} +$ $\#\{i \in \{1, \ldots, k-1\} \mid x \in Q_i\}$ is odd IFF $\#\{i \in \{k, k+1\} \mid x \in A_i\}$ $+ \#\{i \in \{1, \ldots, k-1\} \mid x \in Q_i\}$ is odd$)$	Specialisation, (32)
(34)	$\#\{i \in \{k\} \mid x \in Q_i\} +$ $\#\{i \in \{1, \ldots, k-1\} \mid x \in Q_i\}$ is odd IFF $\#\{i \in \{k, k+1\} \mid x \in A_i\}$ $+ \#\{i \in \{1, \ldots, k-1\} \mid x \in Q_i\}$ is odd	Modus Ponens, (31), (35)
(35)	$\#\{i \in \{1, \ldots, k\} \mid x \in Q_i\}$ is odd IFF $\#\{i \in \{k, k+1\} \mid x \in A_i\}$ $+ \#\{i \in \{1, \ldots, k-1\} \mid x \in A_i\}$ is odd	Substitution, (19)

(36)	$\#\{i \in \{k, k+1\} \mid x \in A_i\}$ $+\#\{i \in \{1, \ldots, k-1\} \mid x \in A_i\}$ $= \#\{i \in \{1, \ldots, k+1\} \mid x \in A_i\}$	Definition of $\#\{i \in \{1, \ldots, k+1\} \mid x \in A_i\}$
(37)	$\#\{i \in \{1, \ldots, k\} \mid x \in Q_i\}$ is odd IFF $\#\{i \in \{1, \ldots, k+1\} \mid x \in A_i\}$ is odd	Substitution, (35)
(38)	$x \in A_1 \Delta \cdots \Delta A_k \Delta A_{k+1}$ IFF $\#\{i \in \{1, \ldots, k+1\} \mid x \in A_i\}$ is odd	Use of Tautology (Modus Ponens), (18), (30), (37)
(39)	$\forall x \in U.(x \in A_1 \Delta \cdots \Delta A_k \Delta A_{k+1}$ IFF $\#\{i \in \{1, \ldots, k+1\} \mid x \in A_i\}$ is odd)	Generalisation, (6)
(40)	$\forall S \in T_k . \forall x \in U.(x \in A_1 \Delta \cdots \Delta A_k \Delta A_{k+1}$ IFF $\#\{i \in \{1, \ldots, k+1\} \mid x \in A_i\}$ is odd)	Generalisation, (5)
(41)	$P(k+1)$	Direct Proof; (2)-(40)
(42)	$\forall n \in \mathbb{N}.P(n)$	Induction; (1)-(41)