

On a Theorem Proved by Dijkstra in EWD 967

Jayadev Misra

November 9, 2003

Let S be a finite set over which there is an operation $+$, satisfying:

1. S is closed under $+$; i.e., if $x \in S$ and $y \in S$, then $x + y \in S$.
2. $+$ is commutative and associative.
3. (involution) For any x and y , $x + x + y = y$

It is required to show that the size of S is a power of 2.

Let V be a subset of S , and V^* the closure of V , i.e., V^* is the smallest set containing V so that

$$x \in V^* \wedge y \in V^* \Rightarrow x + y \in V^*$$

We show that the size of V^* is a power of 2. Every closed set is V^* , for some V (in particular, $S^* = (S^*)^*$). So the size of a closed set is a power of 2.

Proof is by induction on the size of V .

• $|V| = 1$: Then V has a single element x . If $x = x^2$, then $x^i = x$, for all i , where $i \geq 1$, by induction on i . So $V^* = \{x\}$, which means its size is 2^0 . If $x \neq x^2$, then $x^{2 \times i} = x^2$, and $x^{2 \times i + 1} = x$, for all i , by induction on i . So, V^* is $\{x, x^2\}$, which means its size is 2^1 .

• $|V| = n + 1$: Let U be a subset of size n of V and y be the remaining element of V outside U . By the induction hypothesis, size of U^* is a power of 2. If $y \in U^*$, then $V^* = U^*$; so, the size of V^* is a power of 2. If $y \notin U^*$, then we show that V^* has exactly twice as many elements as U^* , thus establishing the required result.

Consider the set, $W = \{y + x \mid x \in U^*\}$. We claim that $V^* = U^* \cup W$, U^* and W are disjoint, and there is a 1-1 correspondence between the elements of U^* and W , so their sizes are equal.

1. $V^* = U^* \cup W$: It is easy to see that any element of $U^* \cup W$ is in V^* . We show the converse, that any expression over the elements of V has a value which is in U^* or W . This holds if the expression is over the terms from U .

For $n \geq 0$, $y^{2^n} + e = e$, where e is an expression over the elements of V , from the involution property of $+$; and e is in U^* . And, $y^{2^{n+1}} + e = y \times e$. Since the value of e is in U^* , $y \times e$ is in W , from the definition of W .

2. U^* and W are disjoint: similar to (1), above.
3. There is a 1-1 correspondence between the elements of U^* and W : x in one set maps to $y + x$ in the other set. This mapping is a bijection, because $y + y + x = x$.

Further Thoughts First, observe that $x+x = y+y$, for all x and y , because $(x+x) + (y+y) = y+y$, and also, $(x+x) + (y+y) = (y+y) + (x+x) = x+x$. We write 0 for $x+x$.

Note: A good example of $+$ is the exclusive-or operation over equal length binary strings.

Theorem: Let S be a closed set with more than 2 elements. $+$ applied to all elements of S yields 0.

Proof: Let V be a smallest set such that $S = V^*$. Clearly, V is non-empty, since S has more than 2 elements. So, $V = U \cup \{y\}$, for some U and y . Then, from the previous proof, either $S = U^*$ or $S = U^* \cup W$, where $W = \{y+x \mid x \in U^*\}$. In the first case, the choice of V as the smallest set such that $S = V^*$ is contradicted. So, we may assume that $S = U^* \cup W$, where $W = \{y+x \mid x \in U^*\}$. Let s, u, w be the results of $+$ applied to all elements of S, U^*, W , respectively.

Note that the size of U^* is even. This is because, U^* has half as many elements as S , And S , from the last proof, has 2^k elements, and it is given that $k > 1$.

$$\begin{aligned}
& s \\
= & \{\text{definition of } s\} \\
& (+x : x \in S : x) \\
= & \{S = U^* \cup W; \text{ from the last proof } U^* \text{ and } W \text{ are disjoint}\} \\
& (+x : x \in U^* : x) + (+x : x \in W : x) \\
= & \{\text{definition of } u\} \\
& u + (+x : x \in W : x) \\
= & \{W = \{y+x \mid x \in U^*\}\} \\
& u + (+x : x \in U^* : y+x) \\
= & \{\text{Number of occurrences of } y \text{ in } (+x : x \in U^* : y+x) \text{ is even, from } |U^*| \text{ even}\} \\
& \text{And } y+y=0\} \\
& u + (+x : x \in U^* : x) \\
= & \{\text{definition of } u\} \\
& u + u \\
= & \{\text{definition of } 0\} \\
& 0
\end{aligned}$$