Lemma 1 (Induktionsschritt)

Wir nehmen an, dass Lemma 1 für ein beliebiges w wahr ist. Zu zeigen ist: Wenn Lemma 1 für w wahr ist, dann ist es auch für $w+1$ wahr. Im Induktionsschritt betrachten wir also 2^{w+1} Elemente. Diese 2^{w+1} Elemente betrachten wir in zwei Hälften mit jeweils 2^w Elementen unterteilt, eine linke und eine rechte Teilmenge.
Folgendes ist zu beobachten:

(1) *Ein Scan der linken Teilmenge geschieht genau 2^w Schritte vor einem Scan der rechten Teilmenge.* Bei einem Scan der linken Teilmenge wird zunächst das linkste Element in B oder C aktiv. Nach Lemma 0.2 werden dann nacheinander alle darauffolgenden Elemente in B oder C aktiv, bis nach genau 2^w Schritten das linkste Element der rechten Teilmenge in B oder C aktiv ist, also ein Scan der rechten Teilmenge stattfindet.

(2) *Die Scans der beiden Teilmengen alternieren und der Scan der linken Teilmenge geschieht zuerst.* Da nach Lemma 0.1 zuerst das linkste Element in B oder C aktiv wird, geschieht der Scan der linken Teilmenge zuerst. Wie in Beobachtung (1) begründet, geschieht nach einem Scan der linken Teilmenge immer zuerst ein Scan der rechten Teilmenge. Es bleibt zu begründen, dass nach einem Scan der rechten Teilmenge immer auch zuerst ein Scan der linken Teilmenge erfolgen muss. Hierfür schauen wir uns System 3 nochmal genauer an: Nach 2^{w+1} Schritten ist das rechteste Element der Menge in B oder C aktiv. Ab hier läuft das System so lange weiter nach rechts, bis die erste 0 gelesen wird. Dann gibt es vier Fälle:[1] (i) $-_B10 \to -1_B0$, (ii) $-_C20 \to -1_B0$, (iii) $-_C10 \to -0_A0$ und (iv) $-_B20 \to -0_A0$. Zu beobachten ist hier, dass die ersten beiden Fälle und die letzten beiden Fälle zusammenfallen und wir es im nächsten Schritt nur noch mit zwei Fällen zu tun haben. Wenn man die Regeln für System 3 weiter ausführt (was ich hier nicht explizit machen werde), gelangen wir in beiden Fällen in einen Zustand, wo eine 1 oder eine 2 in Zustand A aktiv wird und das System im Zustand A nach links über die Menge hinwegläuft, bis links neben der Menge die erste 0 gelesen wird. Dann läuft das System wieder nach rechts und ein Scan der linken Teilmenge erfolgt. Nach einem Scan der rechten Teilmenge erfolgt also immer zuerst ein Scan der linken Teilmenge.

Aus den beiden Beobachtungen schließen wir: Der n-te Scan der linken Teilmenge geschieht genau 2^w Schritte vor dem n-ten Scan der rechten Teilmenge.
Wir definieren anschließend $sl(n)$ und $sr(n)$ als die Zustandsparität der linken bzw. rechten Teilmenge beim n-ten Scan und $pl(n)$ und $pr(n)$ als Parität der linken bzw. rechten Teilmenge beim n-ten Scan.
Wir beginnen mit Sublemma 1. Nach *I.V.* wissen wir:

$pl(n-2^w) = pl(n-2\cdot 2^w) + sl(n-2\cdot 2^w) \mod 2$ und
$pl(n) = pl(n-2^w) + sl(n-2^w) \mod 2$

$pl(n-2^w)$ setzen wir in $pl(n)$ ein:

$pl(n) = pl(n-2\cdot 2^w) + sl(n-2\cdot 2^w) + sl(n-2^w) \mod 2$

Das gleiche machen wir mit der rechten Teilmenge.
Wir beobachten, dass nach Sublemma 2 $sr(x) = pl(x) + sl(x) \mod 2$ gilt. $sr(x) = 0$ gilt, wenn die rechte Teilmenge beim Scan x in Zustand B ist. $pl(x) + sl(x) \mod 2 = 0$ gilt, wenn das Element rechts neben der linken Teilmenge, also das erste Element der rechten Teilmenge, das nächste Mal, dass es aktiv wird, in Zustand B aktiv wird. $sr(x) = 1$ gilt, wenn die rechte Teilmenge beim Scan x in Zustand C ist. $pl(x) + sl(x) \mod 2 = 1$ gilt, wenn das Element rechts neben der linken Teilmenge, also das erste Element der rechten Teilmenge, das nächste Mal, dass es aktiv wird, in Zustand C aktiv wird. (In Zustand A kann es nicht aktiv werden, weil das erste Element der rechten Teilmenge keine 0 sein kann.)
Smith stellt anschließend folgende Summe auf:[2]

$pl(n) + pr(n) \mod 2$ (einsetzen, was wir oben umgeformt haben)
$= pl(n-2\cdot 2^w) + sl(n-2\cdot 2^w) + sl(n-2^w) + pr(n-2\cdot 2^w) + sr(n-2\cdot 2^w) + sr(n-2^w)$
$\mod 2$ (Beobachtung $sr(x) = pl(x) + sl(x) \mod 2$)
$= pl(n-2\cdot 2^w) + sl(n-2\cdot 2^w) + sl(n-2^w) + pr(n-2\cdot 2^w) + pl(n-2\cdot 2^w) +$
$sl(n-2\cdot 2^w) + pl(n-2^w) + pl(n-2^w) \mod 2$ (doppelte Summanden rausstreichen)
$= pr(n-2\cdot 2^w) + pl(n-2^w) \mod 2$ ($pl(n-2^w)$ einsetzen)
$= pr(n-2\cdot 2^w) + pl(n-2\cdot 2^w) + pl(n-2\cdot 2^w) \mod 2$

Anmerkung: Die doppelten Summanden konnten wir deshalb herausstreichen, da entweder beide 0 oder beide 1 sind und für die Summe mod 2 damit keinen Unterschied machen.

[1] Notation: Die nach unten gestellten Buchstaben bezeichnen den Zustand, in dem die darauffolgende 1 oder 2 aktiv ist.
[2] Notation: Die grauen Anmerkungen bezeichnen die Umformungen, die im nächsten Schritt erfolgen.

Es folgen vier weitere Beobachtungen:

(1) *Die Parität der rechten Teilmenge bei ihrem n-ten Scan entspricht der Parität, die sie zum Zeitpunkt des n-ten Scans der linken Teilmenge hatte.* Dies ist der Fall, da während des n-ten Scans der linken Teilmenge nur die Elemente der linken Teilmenge aktiv sind. Da die Elemente der rechten Teilmenge biem n-ten Scan der linken Teilmenge nicht aktiv sind, bleiben sie bis zum Beginn des n-ten Scans der rechten Teilmenge unverändert.

(2) *Der n-ten Scan der gesamten Menge entspricht dem n-ten Scan der linken Teilmenge.* Beim Scan der gesamtem Menge sowie der linken Teilmenge wird dasselbe Element in B oder C aktiv, und zwar das linkste Element. Außerdem braucht es nach dem Scan der gesamtem Menge sowie nach dem Scan der linken Teilmenge genau die gleichen Schritte, bis das linkste Element wieder in B oder C aktiv ist, da nach einem Scan der linken Teilmenge immer zuerst ein Scan der rechten Teilmenge stattfinden muss.

(3) *Die Parität der gesamten Menge (also aller 2^{w+1} Elemente) beim n-ten Scan entspricht der Summe der Paritäten der linken und rechten Teilmenge beim jeweils n-ten Scan, also $p(n) = pl(n) + pr(n)$ mod 2.* Die Beobachtung folgt aus den vorherigen beiden Beobachtungen: Der n-te Scan der gesamten Menge entspricht dem n-ten Scan der linken Teilmenge und die Parität der rechten Teilmenge bei ihrem n-ten Scan entspricht der Parität, die sie zum Zeitpunkt des n-ten Scans der linken Teilmenge hatte.

(4) *$s(x) = sl(x)$ gilt für alle x.* Da der n-te Scan der gesamten Menge dem n-ten Scan der linken Teilmenge entspricht, beginnen die beiden Scans auch im gleichen Zustand - haben also die gleiche Zustandsparität.

Mit den Beobachtungen formen wir die oben aufgestellte Gleichung
$pl(n) + pr(n) \text{ mod } 2 = pr(n - 2 \cdot 2^w) + pl(n - 2 \cdot 2^w) + pl(n - 2 \cdot 2^w) \text{ mod } 2$
zu folgender Gleichung um:
$p(n) = p(n - 2 \cdot 2^w) + s(n - 2 \cdot 2^w) \text{ mod } 2$
Damit ist Sublemma 1 gezeigt.
Nun zeigen wir Sublemma 2 im Induktionsschritt. Wir stellen folgende Beobachtung an:

$p(n) + s(n) \text{ mod } 2$ (mit Beobachtung (3) und (4))
$= pl(n) + pr(n) + sl(n) \text{ mod } 2$ (mit obiger Beobachtung, $sr(n) = pl(n) + sl(n) \text{ mod } 2$)
$= sr(n) + pr(n) \text{ mod } 2$

Nach *I.V.* gilt Sublemma 2 für die rechte Teilmenge. Also gilt: Wenn $pr(n)+sr(n) \text{ mod } 2 = 0$, dann wird das Element rechts neben der rechten Teilmenge das nächste Mal, dass es aktiv wird, in B aktiv, und wenn $pr(n) + sr(n) \text{ mod } 2 = 1$, dann wird das Element rechts neben der rechten Teilmenge das nächste Mal, dass es aktiv wird, in A aktiv, wenn das Element eine 0 ist, und in C aktiv, wenn das Element eine 1 oder eine 2 ist. Das gleiche gilt nun auch für die gesamte Menge, weil das Element rechts neben der rechten Teilmenge dem Element rechts neben der gesamten Menge entspricht und weil $pr(n) + sr(n) \text{ mod } 2 = p(n) + s(n) \text{ mod } 2$ gilt. Damit ist Sublemma 2 gezeigt.
Nun zeigen wir Sublemma 3 im Induktionsschritt. Wir stellen fest, dass Sublemma 3 ein Spezialfall von Lemma 0.9 ist. Nach Lemmate 0.3 und 0.4 wissen wir, dass nur das rechteste Element der Menge eine 0 sein kann. Lemma 0.9 besagt, dass wenn das rechteste Element aktiv wird und zu einer 0 wird, es dann zu einer 2 wird, sobald es das nächste Mal aktiv wird, was sein wird, bevor das linkste Element das nächste Mal in B oder C aktiv wird, also bevor der nächste Scan stattfindet. Lemma 0.9 besagt auch, dass wenn das rechteste Element aktiv wird und nicht zu einer 0 wird, es so lange keine 0 bleibt, bis das linkste Element das nächste Mal in B oder C aktiv wird, also bis der nächste Scan stattfindet. Wenn ein Scan stattfindet, sind also alle Elemente der Menge eine 1 oder eine 2. Damit ist Sublemma 3 gezeigt.
Da wir alle drei Sublemmata gezeigt haben, ist nun Lemma 1 gezeigt.

Korollar 0

Korollar 0 besagt: Gegeben eine Menge an insgesamt 2^w zusammenhängenden Elementen, die entweder 1 oder 2 sind. Die Parität dieser Menge bei ihren ersten 2^w Scans ist unabhängig von der Zustandsparität bei diesen Scans.
Dies ist der Fall, da die Parität und die Zustandsparität bei jedem Scan nur davon abhängig sind, welche Parität und welche Zustandsparität beim ersten Scan gewählt wurden.

Korollar 1

Korollar 1 besagt: Angenommen wir legen für die ersten n Scans eine gewünschte Parität fest. Dann existiert eine Menge an zusammenhängenden 1en und 2en, die bei jedem der ersten n Scans die gewünschte Parität hat, unabhängig von der Zustandsparität bei diesen Scans.
Es folgen zwei Methoden, mithilfe derer wir eine solche Menge erzeugen können.

Methode 1

Bei Methode 1 legen wir eine beliebige Menge an zusammenhängenden 1en und 2en fest. Die Menge soll $2^w > n$ viele Elemente haben. Das Element rechts neben den 2^w Elementen soll eine 1 oder eine 2 sein. Danach folgen nur 0en. Wir wählen B als Zustand für das erste Element, wenn die Parität der Menge der gewünschten Parität für diesen Scan entspricht, und C sonst. Wir führen anschließend 2^w Scans durch. Nach 2^w Scans haben wir eine Menge an 2^w 1en und 2en, die für die ersten n Scans die jeweils gewünschte Parität hat.
Beispiel:
$2^2 = 4$ Elemente, $n = 3$ Scans, gewünschte Pariät bei den ersten n Scans ist 1
Beliebige Anfangsmenge, erster Scan: $|_C 1122|20$
Zweiter Scan: $|_B 2212|$
Dritter Scan: $|_C 2112|$
Vierter Scan: $|_B 1112|$
Nach dem vierten Scan erhalten wir die Menge 1112, die für die ersten 3 Scans die gewünschte Parität hat.

Methode 2 (Induktionsanfang)

Wir definieren die Paritätsmenge einer Folge an insgesamt 2^w zusammenhängenden 1en und 2en als die Menge der Scans, bei denen die Parität dieser Folge ungerade ist.
Für Methode 2 gibt Smith einen zellulären Automaten an, mit denen wir Folgen an 2^w zusammenhängenden 1en und 2en generieren können, die den Paritätsmengen $\{0\}, \{1\}, \{2\}, ..., \{2^w - 1\}$ entsprechen. Um zu zeigen, dass die Strings, die der zelluläre Automat generiert, tatsächlich den jeweiligen Paritätsmengen entsprechen, führt er einen Induktionsbeweis über die Zeilen in der Liste an generierten Strings.
Induktionsanfang:
Zu zeigen ist, dass ein String, der aus einer 2 und 2^w 1en besteht, also der erste String der Liste, der Paritätsmenge $\{0\}$ entspricht.
Für einen String, der aus 2^w 1en besteht, gilt:

- Wenn der Scan dieses Strings in B beginnt, bleibt der String unverändert.
  Mit der Regel $-_B 1- \to -1_B-$ laufen wir nämlich über alle 1en hinweg.
- Wenn der Scan dieses Strings in C beginnt, erhalten wir nach dem Scan einen String mit 2^w 2en.
  Mit der Regel $-_C 11 \to -2_C 1$ wandeln wir nämlich alle 1en zu 2en um.

Ein String bestehend aus 2^w 1en entspricht der leeren Paritätsmenge, weil wir bei allen 2^w Scans gerade Parität haben. Für einen String, der aus einer 2 und $2^w - 1$ 1en besteht, gilt:

- Wenn der Scan dieses Strings in B beginnt, erhalten wir nach dem Scan 2^w 2en.
  Denn: $_B 2111 \to 2_C 111 \to 22_C 11 \to 222_C 1 \to 2222_C$ usw.
- Wenn der Scan dieses Strings in C beginnt, erhalten wir nach dem Scan 2^w 1en.
  Denn: $_C 2111 \to 1_B 111 \to 11_B 11 \to 111_B 1 \to 1111_B$ usw.

Für den String aus einer 2 und $2^w - 1$ 1en gilt also, dass er sich nur im ersten Scan vom String bestehend aus 2^w 1en unterscheidet. Da hat der String aus einer 2 und $2^w - 1$ 1en nämlich ungerade Parität. Damit entspricht der erste String der Liste der Paritätsmenge $\{0\}$.