Further Musings on the Wang *et al.* MD5 Collision: Improvements and Corrections on the Work of Hawkes, Paddon, and Rose

Gregory Hirshman

La Jolla Country Day School, 9490 Genesee Ave., La Jolla, CA 92037, U.S.A
ghirshman@yahoo.com
858-457-3073

Abstract. The recent successful attack on the widely used hash function, the MD5 Message Digest Algorithm, was a breakthrough in cryptanalysis. The original paper, published in 2004 by Wang *et al.*, described this attack in an obscure and elliptical manner. Hawkes, Paddon, and Rose subsequently presented the attack in more detail, but even their paper contained numerous unproven statements and several significant errors. In a seven-step process, this paper will explicate their work, prove many of their assertions, and provide original corrections and illustrations to make the differential attack on MD5 more accessible to the mathematically literate reader. First, this paper will augment their introductory material by comparing their unorthodox description of MD5 to the original notation of Ron Rivest. Second, it will provide original examples for conditions that they present for the T_t. Third, it will elaborate on the description of the first block of the differential, showing why and how the conditions on the T_t are determined. Fourth, it will develop a step by step analysis of the description of the second block of the differential based only on the table that Hawkes, Paddon, and Rose provide. Fifth, it will supply original proofs of their assertions regarding the conditions for the propagation of the differences through the f_t functions for the first block. Sixth, it will give both assertions and proofs for the propagation of the differences through the f_t functions for the second block. Finally, it will correct two significant errors in the work of Hawkes, Paddon, and Rose. It will demonstrate that the complexity of the attack is only about half as great as they believed, and it will show that their *Case Two* does not succeed in fulfilling the conditions required for the collision differential to hold.
Keywords: MD5, Collision, Hash function, Differential cryptanalysis.

1 Introduction

For thirteen years, no one was able to find a collision for the cryptographic hash function MD5 [1]. The successful attack demonstrated by X. Wang, D. Feng, X. Lai, and H. Yu in 2004 [2] represented a significant achievement in cryptanalysis. After their paper was published, cryptographers struggled to comprehend the elusive attack. A year later, Hawkes, Paddon, and Rose [3] developed a method to explicate the collision that Wang *et al.* had found, yet even their paper was terse and schematic, and it contained several important errors. This paper utilizes a step-wise approach and employs a variety of original techniques to make the differential attack on MD5 more comprehensible to a wider audience.

The two-iteration attack on MD5 consists of finding two messages, each two blocks (1024 bits) in length, that produce identical 128-bit message digests. Processing the first block of each message produces a small difference, which is eliminated in processing the second block. The vast majority of the conditions that Wang et al. set for the attack occur in round 1 of each iteration. These conditions preclude a second pre-image attack. Using single-message modification, however, two messages can be created in such a way as to fulfill every condition in the first round of each iteration. Thus, in calculating the complexity of the attack, only conditions for rounds 2 to 4 need to be considered. We will show that the complexity of the attack is 2^{42}.

This paper is organized as follows. Section 2 presents a brief history of the cryptanalysis on MD5. Section 3 presents the notation that Hawkes, Paddon, and Rose used in explaining the attack. Section 4 provides the new description of MD5 introduced in [3] and then compares this description of the algorithm to the original description in [1]. Section 5 discusses the message construction necessary for the attack to succeed. Section 6 supplies original examples for the conditions on the T_t presented in [3] and describes the differential for both the first and second blocks, demonstrating how a collision is obtained at the end of the attack. It also specifies the probabilities that the T_t will hold in each step. Section 7 presents the conditions for the propagation of the differences through the f_t functions for both the first and second blocks. Section 8 provides proofs for all of the assertions made in section 7. Finally, section 9 describes various errors in [3], some trivial, some minor, and two quite significant.

The original papers on the cryptanalysis of MD5 are only accessible to experts in the field. This paper provides necessary explanations and fills in the gaps to make the attack more comprehensible to a larger audience and to answer many questions which might naturally occur to educated readers. Many original examples, explanations, illustrations, and corrections are provided. It is hoped that this paper will foster understanding of a major mathematical achievement and facilitate further advances in the field.

2 Brief History of the Cryptanalysis on MD5

MD5 was designed by Ron Rivest in 1991 after it became apparent that MD5's predecessor, MD4 [4], was no longer secure. Rivest amended his earlier hash function by implementing a fourth round, by adding a unique additive constant to each step, by changing G function in round 2 to make it less symmetric, by ensuring that each step adds in the result of the previous step, by altering the order in which the input words are accessed in rounds 2 and 3, and by attempting to optimize the magnitude of the shift function in order to increase the avalanche effect. With these improvements, MD5 became one of the most widespread hash functions ever created, yet it also became the target of much cryptanalytic research.

The first major accomplishment in the cryptanalysis of MD5 came in 1993 when B. den Boer and A. Bosselaers [5] discovered the first pseudo-collision. Three years later, H. Dobbertin [6] found a collision for MD5 using predetermined initial values and input words. It was not until 2004, however, that Wang et al. discovered the first real collision for MD5. This paper sparked great excitement in the cryptographic community, and many of the leading cryptanalyst sought to understand and expand on the collision attack. Later in 2004, P. Hawkes, M. Paddon, and G. Rose presented one of the most comprehensive analyses into how the collision in [2] was actually obtained. Early in the following year, X. Wang and H. Yu [7] presented their method to find collisions in reasonable time. Also in 2005, J. Liang and X. Lai [8] improved on [7] by removing unnecessary conditions and by discovering more efficient pathways, speeding up the attack about 30-fold. The following year, J. Black, M. Cochran, and T. Highland [9] further improved on [7] by providing insight into both single and multi-message modification and by presenting new multi-message modification techniques to make Wang and Yu's attack even faster. Probably the best known cryptanalyst on MD5 after Wang and Yu is V. Klima, whose 2005 publication [10] combined with a 2006 publication by M. Stevens [11] to find an attack which succeeded in finding collisions in a matter of minutes. Then, in April of 2006, Klima developed the fastest known attack on MD5 using a method known as tunneling [12]. His algorithm can find collisions in an average of 17 seconds.

3 Notation

MD5 is based on processing 32-bit words. We denote the i^{th} bit of a 32-bit word, a, as a_i. Then, "$\wedge$" represents the bitwise AND operation with $(a \wedge b)[i] = a[i] \wedge b[i]$, $0 \leq i \leq 31$, "$\vee$" represents the bitwise OR operation with $(a \vee b)[i] = a[i] \vee b[i]$, $0 \leq i \leq 31$, and "$\oplus$" represents the bitwise exclusive-OR operation with $(a \oplus b)[i] = a[i] \oplus b[i]$, $0 \leq i \leq 31$. Also, addition and subtraction modulo 2^{32} are represented by "+" AND "-", respectively. In addition, we denote the bitwise complement of x as $\neg x$, so that $\neg x = 2^{32}$ - 1 - x. The $ROTL^r(X)$ function denotes the rotation of the bits in X by r positions to the left.

We also employ some shorthand techniques. When we consider several bit conditions, say, $X[a]$, $X[b]$, $X[c]$, and $X[d]$, we denote is as follows:

$$X[a,\ b,\ c,\ d] = (X[a],\ X[b],\ X[c],\ X[d]).$$

We write the bits in descending order, and if bits are adjacent to one another, we may combine them. For example,

$$X[a\ \text{-}\ b,\ c] = (X[a],\ X[a\ \text{-}\ 1],\ \dots\ ,\ X[b+1],\ X[b],\ X[c]).$$

If we want to set individual bits in a set to a specific value, then, for example, we may write:

$$X[a\ \text{-}\ b,\ c] = 1\ X[a] = 1,\ X[a\ \text{-}\ 1] = 1,\ \dots,\ X[b+1] = 1,\ X[b] = 1,\ X[c], = 1.$$

4 Description of MD5

We will now present how MD5 is described in [3] and demonstrate how the unorthodox description is essentially the same as that of [1].

4.1 Padding

A message of arbitrary length is padded so that its length will be congruent to 0 mod 512.

4.2 Parsing

The padded message is divided into 512-bit blocks M_0, M_1, ..., M_n. Then each block, M_i is divided into 16, 32-bit words $M_0^{(i)}$, $M_1^{(i)}$, ..., $M_n^{(i)}$,

4.3 Message Expansion

Each iteration of MD5 processes one, 512-bit message block, and the 64 steps of one iteration process each of the 16, 32-bit words, W_t, exactly 4 times. The order in which the message words are processed for a single iteration of MD5 is described below:

$$f_t(X,Y,Z) = \begin{cases} F(X,Y,Z) = (X \wedge Y) \oplus (\overline{X} \wedge Z), & 0 \leq t \leq 15; \\ G(X,Y,Z) = (Z \wedge X) \oplus (\overline{Z} \wedge Y), & 16 \leq t \leq 31; \\ H(X,Y,Z) = X \oplus Y \oplus Z, & 32 \leq t \leq 47; \\ I(X,Y,Z) = Y \oplus (X \vee \overline{Z}), & 48 \leq t \leq 63. \end{cases}$$

Note that for each r, $0 \leq r \leq 3$, the values of W_{16r+0}, W_{16r+1}, ..., W_{16r+15} form a permutation in the words of the message block.

This notation means that, for each iteration, the message words are applied in the following manner. In the first round (steps 0 to 15), the message words are inputted into MD5 "in order," so that M_0 is the input word into step 0, M_1 is the input word into step 1, M_2 is the input word into step 2, and so on until M_{15} is the input word into step 15. In the second round (steps 16 to 31), the message words are inputted into MD5, so that $M_{1+5\times16(mod16)} = M_{81(mod16)} = M_1$ is the input word into step 16, $M_{1+5\times17(mod16)} = M_{86(mod16)} = M_6$ is the input word into step 17, $M_{1+5\times18(mod16)} = M_{91(mod16)} = M_{11}$ is the input word into step 18, and so on until $M_{1+5\times31(mod16)} = M_{156(mod16)} = M_{12}$ is the input word into step 31. In the third round (steps 32 to 47), the message words are inputted into MD5, so that $M_{5+3\times32(mod16)} = M_{101(mod16)} = M_5$ is the input word into step 32, that $M_{5+3\times33(mod16)} = M_{104(mod16)} = M_8$ is the input word into step 33, that $M_{5+3\times34(mod16)} = M_{107(mod16)} = M_{11}$ is the input word into step 34, and so on until that $M_{5+3\times47(mod16)} = M_{146(mod16)} = M_2$ is the input word into step 47. In the fourth round (steps 48 to 63), the message words are inputted into MD5, so that $M_{7\times48(mod16)} = M_{336(mod16)} = M_0$ is the input word into step 48, $M_{7\times49(mod16)} = M_{343(mod16)} = M_7$ is the input word into step 49, $M_{7\times50(mod16)} = M_{350(mod16)} = M_{14}$ is the input word into step 50, and so on until $M_{7\times63(mod16)} = M_{441(mod16)} = M_9$ is the input word into step 63.

4.4 Register Update

After each iteration of MD5, the intermediate hash values, $IHV^{(i)}[0]$, $IHV^{(i)}[1]$, $IHV^{(i)}[2]$, and $IHV^{(i)}[3]$, are updated, where each $IHV^{(i)}$ denotes the intermediate hash value before hashing the ith 512-bit block. The four words, $IHV^{(0)}[j]$, are initialized to predetermined constants. We denote Q_{4t-3}, Q_{4t-2}, Q_{4t-1}, Q_{4t}, $1 \leq t \leq 16$, to be our chaining variables. They are initialized after the first iteration as

$$Q_0 = IHV^{(i)}[1],\ Q_{-1} = IHV^{(i)}[2],\ Q_{-2} = IHV^{(i)}[3],\ Q_{-3} = IHV^{(i)}[0].$$

Then, each $IHV^{(i)}[j]$ are calculated as follows:

$$\begin{aligned} IHV^{(i)}[0] &= IHV^{(i-1)}[0] + Q_{61},\ IHV^{(i)}[3] = IHV^{(i-1)}[3] + Q_{62}, \\ IHV^{(i)}[2] &= IHV^{(i-1)}[2] + Q_{63},\ IHV^{(i)}[1] = IHV^{(i-1)}[1] + Q_{64}. \end{aligned}$$

In other words, each $IHV^{(i)}[j]$ is the value of one of the four, 32-bit registers after i-1 iterations of the compression function. Relating this notation to that of [1], we find that $IHV^{(i)}[0]$ is equivalent to the chaining variable a, $IHV^{(i)}[3]$ is equivalent to the chaining variable d, $IHV^{(i)}[2]$ is equivalent to the chaining variable c, $IHV^{(i)}[1]$ is equivalent to the chaining variable b since MD5 operates on a, b, c, and d in the order a, d, c, b. Consequently, each Q_{4t-3} is equivalent to a_t, each Q_{4t-2} is equivalent to d_t, each Q_{4t-1} is equivalent to c_t, each Q_{4t} is equivalent to b_t. This means that, for example, $Q_{17} = Q_{4\times5-3} = a_5$, $Q_{54} = Q_{4\times14-2} = d_{14}$, $Q_{31} = Q_{4\times8-1} = c_8$, and $Q_{44} = Q_{4\times11} = b_{11}$. Thus, our calculations for the intermediate hash values,

$$\begin{aligned} IHV^{(i)}[0] &= IHV^{(i-1)}[0] + Q_{61},\ IHV^{(i)}[3] = IHV^{(i-1)}[3] + Q_{62}, \\ IHV^{(i)}[2] &= IHV^{(i-1)}[2] + Q_{63},\ IHV^{(i)}[1] = IHV^{(i-1)}[1] + Q_{64}, \end{aligned}$$

could be expressed as

$$IHV^{(i)}[0] = IHV^{(i-1)}[0] + a_{16},\ IHV^{(i)}[3] = IHV^{(i-1)}[3] + d_{16},$$
$$IHV^{(i)}[2] = IHV^{(i-1)}[2] + c_{16},\ IHV^{(i)}[1] = IHV^{(i-1)}[1] + c_{16}.$$

We denote our calculations in the former way, however, because it facilitates our later presentation of Wang and Yu's attack.

Each round of MD5 consists of a 32-bit input word, W_t, a left rotation by $S(t) \in [0{,}31]$, a predetermined 32-bit constant, AC_t, addition modulo 2^{32}, and a non-linear function, f_t, which is defined as

$$f_t(X,Y,Z) = \begin{cases} F(X,Y,Z) = (X \wedge Y) \oplus (\overline{X} \wedge Z), & 0 \leq t \leq 15; \\ G(X,Y,Z) = (Z \wedge X) \oplus (\overline{Z} \wedge Y), & 16 \leq t \leq 31; \\ H(X,Y,Z) = X \oplus Y \oplus Z, & 32 \leq t \leq 47; \\ I(X,Y,Z) = Y \oplus (X \vee \overline{Z}), & 48 \leq t \leq 63. \end{cases}$$

where each f_t takes three, 32-bit words as input and yields one, 32-bit word as output. The compression function modifies the register as follows:

$$T_t = f_t(Q_t, Q_{t-1}, Q_{t-2}) + Q_{t-3} + AC_t + W_t;$$
$$R_t = ROTL^{S(t)}(T_t); \quad Q_{t+1} = Q_t + R_t.$$

After all 64 steps of an iteration are complete, the resulting values, Q_{61}, Q_{62}, Q_{63}, and Q_{64} are added to $IHV[0]$, $IHV[3]$, $IHV[2]$, and $IHV[1]$ of the previous round, respectively. These four sums comprise the new intermediate hash value. When the last message block is processed, the new intermediate hash value becomes the message digest. Up until the last message block, the algorithm proceeds to update the registers using the next message block.

Relating this to [1], each W_t represents $X[k]$, each $S(t)$ represents $\lll s$, each AC_t represents $T[i]$, and each f_t represents either F, G, H, or I, where the order in which the input words are used is described above and values for the left rotation and the constants are predetermined. Furthermore, the value of Q_{t+1}, which is expressed in [3] as

$$Q_{t+1} = Q_t + ROTL^{S(T)}(f_t(Q_t, Q_{t-1}, Q_{t-2}) + Q_{t-3} + AC_t + W_t)$$

is more familiarly represented as

$$a_{i+1} = b_i + ((a_i + \phi(b_i, c_i, d_i) + X[k] + T[i]) \lll s),$$
$$d_{i+1} = c_i + ((b_i + \phi(c_i, d_i, a_{i+1}) + X[k] + T[i]) \lll s),$$
$$c_{i+1} = d_i + ((c_i + \phi(d_i, a_{i+1}, b_{i+1}) + X[k] + T[i]) \lll s),$$
$$b_{i+1} = a_{i+1} + ((d_i + \phi(a_{i+1}, b_{i+1}, c_{i+1}) + X[k] + T[i]) \lll s).$$

where could be the F, G, H, or I function. The values of Q_{61}, Q_{62}, Q_{63}, and Q_{64} are equivalent to a_{16}, d_{16}, c_{16}, b_{16}, respectively, They are added to the intermediate hash value of the previous round to obtain the new intermediate hash value.

5 Message Construction

The collision found in [7] consists of two message blocks of data where the first message is comprised of $(M \mid N)$ and the second message is comprised of $(M' \mid N')$. When split into 32-bit words, $(M_0, M_1, ..., M_{15} \mid N_0, N_1, ..., N_{15})$ and $(M'_0, M'_1, ..., M'_{15} \mid N'_0, N'_1, ..., N'_{15})$, the following conditions must be satisfied according to [7]:

$$\begin{gathered} M_4 \text{ - } M_4 = \pm 2^{31},\ M'_{11} \text{ - } M_{11} = +2^{15},\ M'_{14} \text{ - } M_{14} = \pm 2^{31},\ M'_i = M_i \text{ otherwise}, \\ N'_4 \text{ - } N_4 = \pm 2^{31},\ N'_{11} \text{ - } N_{11} = -2^{15},\ N'_{14} \text{ - } N_{14} = \pm 2^{31},\ N'_i = N_i \text{ otherwise}. \end{gathered}$$

The message expansion transforms the message block into the input word sequence W_t, $0 \leq t \leq 63$. For the first message blocks M and M', we have:

$$\begin{gathered} W'_4 \text{ - } W_4 = W'_{23} \text{ - } W_{23} = W'_{37} \text{ - } W_{37} = W'_{60} \text{ - } W_{60} = \pm 2^{31}, \\ W'_{11} \text{ - } W_{11} = W'_{18} \text{ - } W_{18} = W'_{34} \text{ - } W_{34} = W'_{61} \text{ - } W_{61} = +2^{15}, \\ W'_{14} \text{ - } W_{14} = W'_{25} \text{ - } W_{25} = W'_{35} \text{ - } W_{35} = W'_{50} \text{ - } W_{50} = \pm 2^{31}, \end{gathered}$$

and $W_i = W_i$. For the second message blocks N' and N, we have:

$$\begin{gathered} W'_4 \text{ - } W_4 = W'_{23} \text{ - } W_{23} = W'_{37} \text{ - } W_{37} = W'_{60} \text{ - } W_{60} = \pm 2^{31}, \\ W'_{11} \text{ - } W_{11} = W'_{18} \text{ - } W_{18} = W'_{34} \text{ - } W_{34} = W'_{61} \text{ - } W_{61} = -2^{15}, \\ W'_{14} \text{ - } W_{14} = W'_{25} \text{ - } W_{25} = W'_{35} \text{ - } W_{35} = W'_{50} \text{ - } W_{50} = \pm 2^{31}, \end{gathered}$$

and $W'_i = W_i$. Note that for all four of the ΔW_i which are equal to $\pm 2^{31}$, Wang and Yu asserted that these ΔW_i are equal to $+2^{31}$. This is not an inconsistency, however, since $\pm 2^{31} \equiv +2^{31} \pmod{2^{32}}$.

To verify that the only non-zero differences occur with W_4, W_{23}, W_{37}, W_{60}, W_{11}, W_{18}, W_{34}, W_{61}, W_{14}, W_{25}, W_{35}, and W_{50} for both blocks, we note the following. From [7], we know that the only differences in the original message are in M_4, M_{11}, and M_{14}. Because we have that

$$f_t(X,Y,Z) = \begin{cases} F(X,Y,Z) = (X \wedge Y) \oplus (\overline{X} \wedge Z), & 0 \leq t \leq 15; \\ G(X,Y,Z) = (Z \wedge X) \oplus (\overline{Z} \wedge Y), & 16 \leq t \leq 31; \\ H(X,Y,Z) = X \oplus Y \oplus Z, & 32 \leq t \leq 47; \\ I(X,Y,Z) = Y \oplus (X \vee \overline{Z}), & 48 \leq t \leq 63. \end{cases}$$

we must find three values of t for each round such that the result of the addition and reduction modulo 16 is equal to 4, 11, or 14. For the first round, it is obvious that t = 4, 11, 14. Thus, the only differences are in W_4, W_{11}, and W_{14}. For the second round, we find that t = 23, 18, 25 since

$$\begin{gathered} 1{+}5 \times 23 \pmod{16} = 116 \pmod{16} = 4, \\ 1{+}5 \times 18 \pmod{16} = 91 \pmod{16} = 11, \\ 1{+}5 \times 25 \pmod{16} = 126 \pmod{16} = 14. \end{gathered}$$

Thus, the only differences are in W_{23}, W_{18}, and W_{25}. For the third round, we find that t = 37, 34, 35 since

$$\begin{gathered} 5{+}3 \times 37 \pmod{16} = 116 \pmod{16} = 4, \\ 5{+}3 \times 34 \pmod{16} = 107 \pmod{16} = 11, \\ 5{+}3 \times 35 \pmod{16} = 110 \pmod{16} = 14. \end{gathered}$$

Thus, the only differences are in W_{37}, W_{34}, and W_{35}. For the fourth round, we find that $t = 60, 61, 50$ since

$$\begin{aligned}7 \times 60 \pmod{16} &= 420 \pmod{16} = 4,\\ 7 \times 61 \pmod{16} &= 427 \pmod{16} = 11,\\ 7 \times 50 \pmod{16} &= 350 \pmod{16} = 14.\end{aligned}$$

Thus, the only differences are in W_{60}, W_{61}, and W_{50}.

6 Description of the Differential

In describing the first and second blocks of the differential, we use the following equations:

$$\begin{aligned}\delta T_t &= \delta f_t(Q_t, Q_{t-1}, Q_{t-2}) + \delta Q_{t-3} + \delta W_t,\\ \delta Q_{t+1} &= \delta Q_t + \delta R_t.\end{aligned}$$

Note that since the AC_t are predetermined constants, $\Delta AC_t = 0$, so we have not inserted ΔAC_t in our calculation of ΔT_t.

Tables 1 and 2 on the following two pages summarize the differential in [7] for the first and second blocks, listing the values of ΔQ_t, Δf_t, ΔQ_{t-3}, ΔW_t, $S(t)$, and ΔR_t. The columns of ΔQ_t, Δf_t, ΔQ_{t-3}, ΔW_t, and ΔR_t give the result of the appropriate add-difference. For example, $\Delta Q_t = Q'_t$ - $Q_t \pmod{2^{32}}$. To save space,

- a difference of the form $+2^j$ is denoted $\overset{+}{j}$, and
- a difference of the form -2^j is denoted $\overset{-}{j}$.

Note that since $-2^{31} \equiv +2^{31} \equiv \pm 2^{31}$, we usually input "±" in front of bit 31. The only time that the congruency does not hold is when bit 31 is rotated to some other bit position. In this case, we must distinguish between -2^{31} and -2^{31} by setting a condition. Also note that the propagation of the differences through the f_t functions will be discussed in section 7.

6.1 Conditions on T_t

In creating table 1, it is necessary that we place restrictions on T_t to ensure that the rotation of T_t, i.e., R_t, will produce the correct add-difference. We impose three restrictions on T_t and provide examples to explain them.

Condition I:

- A given add-difference usually must not propagate past the bit position for T_t which is rotated to bit $R_t[31]$. Otherwise, the rotation will carry that add-difference to low order bits, which will result in the wrong add-difference for R_t.

To understand what this means, consider the following example. Suppose that $T_t = +2^8$. Also, suppose that $S(t) = 22$, so upon rotation, we should have $R_t = +2^{8+22=30} = 2^{30}$. T_t could be written as

$$\Delta T_t = 00000000000000000000000 + 00000000.$$

t	δQ_t	δf_t	δQ_{t-3}	δW_t	δT_t	$S(t)$	δR_t
0-3	-	-	-	-	-	.	-
4	-	-	-	$\overset{-}{31}$	$\overset{-}{31}$	7	$\overset{-}{6}$
5	$\overset{-}{6}$	$\overset{+}{19}, \overset{+}{11}$	-	-	$\overset{+}{19}, \overset{+}{11}$	12	$\overset{+}{31}, \overset{+}{23}$
6	$\overset{\pm}{31}, \overset{+}{23}, \overset{-}{6}$	$\overset{-}{14}, \overset{-}{10}$	-	-	$\overset{-}{15}, \overset{+}{14}, \overset{-}{10}$	17	$\overset{+}{31}, \overset{-}{27}, \overset{-}{0}$
7	$\overset{-}{27}, \overset{+}{23}, \overset{-}{6}, \overset{-}{0}$	$\overset{-}{27}, \overset{-}{25}, \overset{+}{16}, \overset{+}{10}, \overset{+}{5}, \overset{-}{2}$	-	-	$\overset{-}{27}, \overset{-}{25}, \overset{+}{16}, \overset{+}{10}, \overset{+}{5}, \overset{-}{2}$	22	$\overset{+}{27}, \overset{-}{24}, \overset{-}{17}, \overset{-}{15}, \overset{+}{6}, \overset{+}{1}$
8	$\overset{-}{23}, \overset{-}{17}, \overset{-}{15}, \overset{+}{0}$	$\overset{\pm}{31}, \overset{-}{24}, \overset{+}{16}, \overset{+}{10}, \overset{+}{8}, \overset{+}{6}$	$\overset{-}{6}$	-	$\overset{-}{31}, \overset{-}{24}, \overset{+}{16}, \overset{+}{10}, \overset{+}{8}$	7	$\overset{-}{31}, \overset{+}{23}, \overset{+}{17}, \overset{+}{15}, \overset{-}{6}$
9	$\overset{\pm}{31}, \overset{-}{6}, \overset{+}{0}$	$\overset{\pm}{31}, \overset{+}{26}, \overset{-}{23}, \overset{-}{20}, \overset{+}{6}, \overset{+}{0}$	$\overset{\pm}{31}, \overset{+}{23}, \overset{-}{6}$	-	$\overset{+}{26}, \overset{-}{20}, \overset{+}{0}$	12	$\overset{+}{12}, \overset{+}{6}, \overset{-}{0}$
10	$\overset{+}{31}, \overset{+}{12}$	$\overset{-}{23}, \overset{+}{13}, \overset{+}{6}, \overset{+}{0}$	$\overset{-}{27}, \overset{+}{23}, \overset{-}{6}, \overset{-}{0}$	-	$\overset{-}{27}, \overset{+}{13}$	17	$\overset{+}{30}, \overset{-}{12}$
11	$\overset{+}{31}, \overset{+}{30}$	$\overset{-}{8}, \overset{-}{0}$	$\overset{-}{23}, \overset{-}{17}, \overset{-}{15}, \overset{+}{0}$	$\overset{+}{15}$	$\overset{-}{23}, \overset{-}{17}, \overset{-}{8}$	22	$\overset{-}{30}, \overset{-}{13}, \overset{-}{7}$
12	$\overset{+}{31}, \overset{-}{13}, \overset{-}{7}$	$\overset{+}{31}, \overset{+}{17}, \overset{+}{7}$	$\overset{-}{31}, \overset{-}{6}, \overset{+}{0}$	-	$\overset{+}{17}, \overset{+}{6}, \overset{+}{0}$	7	$\overset{+}{24}, \overset{+}{13}, \overset{+}{7}$
13	$\overset{+}{31}, \overset{+}{24}$	$\overset{+}{31}, \overset{-}{13}$	$\overset{+}{31}, \overset{+}{12}$	-	$\overset{-}{12}$	12	$\overset{-}{24}$
14	$\overset{+}{31}$	$\overset{+}{31}, \overset{+}{18}$	$\overset{+}{31}, \overset{+}{30}$	$\overset{-}{31}$	$\overset{-}{30}, \overset{+}{18}$	17	$\overset{-}{15}, \overset{+}{3}$
15	$\overset{+}{31}, \overset{-}{15}, \overset{+}{3}$	$\overset{+}{31}, \overset{+}{25}$	$\overset{+}{31}, \overset{-}{13}, \overset{-}{7}$	-	$\overset{+}{25}, \overset{-}{13}, \overset{-}{7}$	22	$\overset{-}{29}, \overset{+}{15}, \overset{-}{3}$
16	$\overset{+}{31}, \overset{-}{29}$	$\overset{+}{31}$	$\overset{+}{31}, \overset{+}{24}$	-	$\overset{+}{24}$	5	$\overset{+}{29}$
17	$\overset{+}{31}$	$\overset{+}{31}$	$\overset{+}{31}$	-	-	9	-
18	$\overset{+}{31}$	$\overset{+}{31}$	$\overset{+}{31}, \overset{-}{15}, \overset{+}{3}$	$\overset{+}{15}$	$\overset{+}{3}$	14	$\overset{+}{17}$
19	$\overset{+}{31}, \overset{+}{17}$	$\overset{+}{31}$	$\overset{+}{31}, \overset{-}{29}$	-	$\overset{-}{29}$	20	$\overset{-}{17}$
20-21	$\overset{+}{31}$	$\overset{+}{31}$	$\overset{+}{31}$	-	-	.	-
22	$\overset{+}{31}$	$\overset{+}{31}$	$\overset{+}{31}, \overset{+}{17}$	-	$\overset{+}{17}$	14	$\overset{+}{31}$
23	-	-	$\overset{+}{31}$	$\overset{-}{31}$	-	20	-
24	-	$\overset{+}{31}$	$\overset{+}{31}$	-	-	5	-
25	-	-	$\overset{+}{31}$	$\overset{-}{31}$	-	9	-
26-33	-	-	-	-	-	.	-
34	-	-	-	$\overset{+}{15}$	$\overset{+}{15}$	16	$\overset{+}{31}$
35	$\overset{+}{31}$	$\overset{-}{31}$	-	$\overset{-}{31}$	-	23	-
36	$\overset{+}{31}$	-	-	-	-	4	-
37	$\overset{+}{31}$	$\overset{+}{31}$		$\overset{-}{31}$	-	11	-
38-49	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$	-	-	.	-
50	$\overset{-}{31}$		$\overset{-}{31}$	$\overset{-}{31}$	-	15	-
51-59	$\overset{-}{31}$	$\overset{+}{31}$	$\overset{\pm}{31}$	-	-	.	-
60	$\overset{+}{31}$		$\overset{-}{31}$	$\overset{-}{31}$	-	6	-
61	$\overset{-}{31}$	$\overset{-}{31}$	$\overset{-}{31}$	$\overset{+}{15}$	$\overset{+}{15}$	10	$\overset{+}{25}$
62-63	$\overset{\pm}{31}, \overset{+}{25}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$	-	-	.	-

Table 1. The first block of the differential. Recall that $\Delta Q_t = \Delta Q_{t-1} + \Delta R_{t-1}$, $\Delta T_t = \Delta f_t + \Delta Q_{t-3} + \Delta W_t$, and (most of the time) $\Delta R_t = ROTL^{S(t)}(\Delta T_t)$.

t	δQ_t	δf_t	δQ_{t-3}	δW_t	δT_t	$S(t)$	δR_t
0	$\overset{\pm}{31},\overset{+}{25}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$			7	
1	$\overset{\pm}{31},\overset{+}{25}$	$\overset{\pm}{31}$	$\overset{\pm}{31},\overset{+}{25}$		$\overset{+}{25}$	12	$\overset{+}{5}$
2	$\overset{\pm}{31},\overset{+}{25},\overset{+}{5}$	$\overset{+}{25}$	$\overset{\pm}{31},\overset{+}{25}$		$\overset{+}{31},\overset{+}{26}$	17	$\overset{+}{16},\overset{+}{11}$
3	$\overset{\pm}{31},\overset{+}{25},\overset{+}{16},\overset{+}{11},\overset{+}{5}$	$\overset{\pm}{31},\overset{-}{27},\overset{+}{25},\overset{-}{21},\overset{-}{11}$	$\overset{\pm}{31},\overset{+}{25}$		$\overset{-}{26},\overset{-}{21},\overset{-}{11}$	22	$\overset{-}{16},\overset{-}{11},\overset{-}{1}$
4	$\overset{\pm}{31},\overset{+}{25},\overset{+}{5},\overset{-}{1}$	$\overset{+}{30},\overset{+}{26},\overset{-}{18},\overset{-}{3},\overset{+}{1}$	$\overset{\pm}{31},\overset{+}{25}$	$\overset{\pm}{31}$	$\overset{+}{30},\overset{+}{26},\overset{+}{25},\overset{-}{18},\overset{+}{2},\overset{+}{1}$	7	$\overset{-}{25},\overset{+}{10},\overset{-}{8},\overset{+}{5},\overset{+}{1},\overset{+}{0}$
5	$\overset{\pm}{31},\overset{+}{10},\overset{-}{8},\overset{+}{6},\overset{+}{0}$	$\overset{+}{30},\overset{+}{28},\overset{-}{26},\overset{-}{25},\overset{-}{20},\overset{-}{8},\overset{-}{5},\overset{-}{4}$	$\overset{\pm}{31},\overset{+}{25},\overset{+}{5}$		$\overset{-}{30},\overset{+}{28},\overset{-}{26},\overset{-}{20},\overset{-}{8},\overset{-}{4}$	12	$\overset{-}{20},\overset{-}{16},\overset{-}{10},\overset{+}{8},\overset{-}{6},\overset{-}{0}$
6	$\overset{\pm}{31},\overset{-}{20},\overset{-}{16}$	$\overset{-}{25},\overset{-}{21},\overset{-}{16},\overset{-}{11},\overset{-}{10},\overset{-}{5},\overset{+}{3}$	$\overset{\pm}{31},\overset{+}{25},\overset{+}{16},\overset{+}{11},\overset{+}{5}$		$\overset{-}{31},\overset{-}{21},\overset{-}{10},\overset{+}{3}$	17	$\overset{-}{27},\overset{+}{20},\overset{+}{16},\overset{-}{6}$
7	$\overset{\pm}{31},\overset{-}{27},\overset{-}{6}$	$\overset{\pm}{31},\overset{-}{27},\overset{+}{16}$	$\overset{\pm}{31},\overset{+}{25},\overset{+}{5},\overset{-}{1}$		$\overset{-}{27},\overset{+}{25},\overset{+}{16},\overset{+}{5},\overset{-}{1}$	22	$\overset{+}{27},\overset{-}{23},\overset{-}{17},\overset{+}{15},\overset{+}{6}$
8	$\overset{\pm}{31},\overset{-}{23},\overset{-}{17},\overset{+}{15}$	$\overset{+}{25},\overset{+}{16},\overset{-}{6}$	$\overset{\pm}{31},\overset{+}{10},\overset{-}{7},\overset{-}{6},\overset{+}{0}$		$\overset{-}{31},\overset{+}{25},\overset{+}{16},\overset{+}{9},\overset{+}{8},\overset{+}{0}$	7	$\overset{+}{23},\overset{+}{16},\overset{+}{15},\overset{+}{6},\overset{+}{0}$
9	$\overset{\pm}{31},\overset{+}{6},\overset{+}{0}$	$\overset{\pm}{31},\overset{-}{26},\overset{+}{16},\overset{+}{0}$	$\overset{\pm}{31},\overset{-}{20},\overset{-}{16}$		$\overset{-}{26},\overset{-}{20},\overset{+}{0}$	12	$\overset{+}{12},\overset{-}{6},\overset{-}{0}$
10	$\overset{\pm}{31},\overset{+}{12}$	$\overset{\pm}{31},\overset{+}{6}$	$\overset{\pm}{31},\overset{-}{27},\overset{-}{6}$		$\overset{-}{27}$	17	$\overset{-}{12}$
11	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31},\overset{-}{23},\overset{-}{17},\overset{+}{15}$	$\overset{-}{15}$	$\overset{-}{23},\overset{-}{17}$	22	$\overset{-}{13},\overset{-}{7}$
12	$\overset{\pm}{31},\overset{-}{13},\overset{-}{7}$	$\overset{\pm}{31},\overset{+}{17}$	$\overset{\pm}{31},\overset{+}{6},\overset{+}{0}$		$\overset{+}{17},\overset{+}{6},\overset{+}{0}$	7	$\overset{+}{24},\overset{+}{13},\overset{+}{7}$
13	$\overset{\pm}{31},\overset{+}{24}$	$\overset{\pm}{31},\overset{-}{13}$	$\overset{\pm}{31},\overset{+}{12}$		$\overset{-}{12}$	12	$\overset{-}{24}$
14	$\overset{\pm}{31}$	$\overset{+}{30},\overset{+}{18}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{+}{30},\overset{+}{18}$	17	$\overset{+}{15},\overset{+}{3}$
15	$\overset{\pm}{31},\overset{+}{15},\overset{+}{3}$	$\overset{\pm}{31},\overset{-}{25}$	$\overset{\pm}{31},\overset{-}{13},\overset{-}{7}$		$\overset{-}{25},\overset{-}{13},\overset{-}{7}$	22	$\overset{-}{29},\overset{-}{15},\overset{-}{3}$
16	$\overset{\pm}{31},\overset{-}{29}$	$\overset{\pm}{31}$	$\overset{\pm}{31},\overset{+}{24}$		$\overset{+}{24}$	5	$\overset{+}{29}$
17	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$			9	
18	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31},\overset{+}{15},\overset{+}{3}$	$\overset{-}{15}$	$\overset{+}{3}$	14	$\overset{+}{17}$
19	$\overset{\pm}{31},\overset{+}{17}$	$\overset{\pm}{31}$	$\overset{\pm}{31},\overset{-}{29}$		$\overset{-}{29}$	20	$\overset{-}{17}$
20-21	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$			.	
22	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31},\overset{+}{17}$		$\overset{+}{17}$	14	$\overset{\pm}{31}$
23			$\overset{\pm}{31}$	$\overset{\pm}{31}$		20	
24		$\overset{\pm}{31}$	$\overset{\pm}{31}$			5	
25			$\overset{\pm}{31}$	$\overset{\pm}{31}$		9	
26-33						.	
34				$\overset{-}{15}$	$\overset{-}{15}$	16	$\overset{\pm}{31}$
35	$\overset{\pm}{31}$	$\overset{\pm}{31}$		$\overset{\pm}{31}$		23	
36	$\overset{\pm}{31}$					4	
37	$\overset{\pm}{31}$	$\overset{\pm}{31}$		$\overset{\pm}{31}$		11	
38-49	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$			.	
50	$\overset{\pm}{31}$		$\overset{\pm}{31}$	$\overset{\pm}{31}$		15	
51-59	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$			.	
60	$\overset{\pm}{31}$		$\overset{\pm}{31}$	$\overset{\pm}{31}$		6	
61	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$	$\overset{-}{15}$	$\overset{-}{15}$	10	$\overset{-}{25}$
62-63	$\overset{\pm}{31},\overset{-}{25}$	$\overset{\pm}{31}$	$\overset{\pm}{31}$				

Table 2. Sequence of add-differences for rounds 16 to 63 of the second block. Recall that $\Delta Q_t = \Delta Q_{t-1} + \Delta R_{t-1}$, $\Delta T_t = \Delta f_t + \Delta Q_{t-3} + \Delta W_t$, and (most of the time) $\Delta R_t = ROTL^{S(t)}(\Delta T_t)$.

Upon applying $S(t)$, we have

$$\Delta R_t = 0 + 000000000000000000000000000000.$$

This is desired since $\Delta R_t = +2^{8+22=30} = +2^{30}$. T_t could also be written as

$$\Delta T_t = 0000000000000000000000 + -00000000$$

since $\Delta T_t = +2^9$ - $2^8 = +2^8$. Upon applying $S(t)$, we have

$$\Delta R_t = + - 000000000000000000000000000000.$$

This would also suffice since $\Delta R_t = +2^{31}$ - $2^{30} = +2^{30}$. But T_t could be written as

$$\Delta T_t = 000000000000000000000 + - - 00000000$$

since $\Delta T_t = +2^{10}$ - 2^9 - $2^8 = +2^8$. However, upon applying $S(t)$, we have

$$\Delta R_t = - - 00000000000000000000000000000+.$$

But this is equal to -2^{31} - $2^{30} + 2^0 \equiv 2^{30} + 2^0 \pmod{2^{32}}$, which is not what we wanted. As we stated earlier, the add-difference must not propagate past the bit position for T_t which is rotated to bit $R_t[31]$ since the rotation would carry that add-difference to low order bits. That is exactly what happened during the last part of the example. For the first two parts, the add-difference did not propagate past the bit position for T_t which is rotated to bit $R_t[31]$, so there was no problem. For the last part, however, the add-difference propagated past the bit position for T_t which is rotated to bit $R_t[31]$, so there was a carry to a low order bit, which resulted in the wrong add-difference for $R_t[31]$.

Condition II:

- A given add-difference may sometimes have to propagate past a certain bit position in T_t to ensure that the rotation will carry to low order bits in order to obtain the correct add-difference for R_t.

This means is that sometimes it is useful for a bit to be rotated so that it carries to a low order bit in order to cancel out another low order bit. Suppose, for example, that we would like to cancel out the -2^0 term of Q_t in our calculation of

$$\Delta T_t = +2^{12} + 2^4 + 2^2$$

and a shift of magnitude 19 for step t. If we apply the shift function, we would get

$$\Delta R_t = +2^{12+19=31} + 2^{4+19=23} + 2^{2+19=21} = +2^{31} + 2^{23} + 2^{21},$$

which clearly cannot cancel out -2^0. However, suppose we write our add-difference of ΔT_t as

$$\Delta T_t = +2^{13} \text{ - } 2^{12} + 2^4 + 2^2.$$

This is, of course, the same value for ΔT_t since

$$\Delta T_t = (+2^{13} \text{ - } 2^{12}) + 2^4 + 2^2 = +2^{12} + 2^4 + 2^2.$$

But, expressing ΔT_t in this manner will give us

$$\Delta R_t = +2^{13+19=32\equiv 0 (mod 32)} \text{ - } 2^{12+19=31} + 2^{4+19=23} + 2^{2+19=21} = -2^{31} + 2^{23} + 2^{21} + 2^0.$$

Since $\Delta Q_{t+1} = \Delta Q_t + \Delta R_t$, the -2^0 term of ΔQ_t will be cancelled out by the $+2^0$ term of ΔR_t.

Condition III:

- An add-difference must not propagate past bit 31 before rotation since this will yield in an undesirable result.

For example, suppose that the desired add-difference is $\Delta T_t = -2^{25}$ and that $T_t[j] = 0$, $25 \le j \le 31$. Then, the second message will have $T'_t[j] = 1$, $25 \le j \le 31$, since

$$\Delta T_t = T'_t \text{ - } T_t = 2^{25} + 2^{26} + 2^{27} + 2^{28} + 2^{29} + 2^{30} + 2^{31} \equiv -2^{25} \pmod{2^{32}}.$$

Now suppose that $S(t) = 12$. Applying the rotation, we should have $\Delta R_t = -2^{25+12=37\equiv 5(mod 32)}$ = -2^5. However, for our example, we have

$$\Delta R_t = \sum_{j=25}^{31} +2^{j+12 \pmod{32}} = \sum_{j=5}^{11} +2^j.$$

But this is not the desired add-difference since

$$\Delta R_t = +2^5 + 2^6 + 2^7 + 2^8 + 2^9 + 2^{10} + 2^{11} = +2^{12} \text{ - } 2^5 \not\equiv -2^5.$$

Thus, we must ensure that that this add-difference does not propagate past bit 31, so we must have that at least one bit of $T_t[j]$, $25 \le j \le 31$, be equal to 1. Consider the following example. Suppose for our add-difference $\Delta T_t = -2^{25}$ that $T_t[j] = 0$, $25 \le j \le 30$, and that $T_t[31] = 1$. Then, the second message will have $T'_t[j] = 1$, $25 \le j \le 30$, and $T'_t[31] = 0$ since

$$\Delta T_t = T'_t \text{ - } T_t = +2^{25} + 2^{26} + 2^{27} + 2^{28} + 2^{29} + 2^{30} \text{ - } 2^{31} = -2^{25}.$$

Suppose again $S(t) = 12$. Applying the rotation, we should have $R_t = -2^{25+12=37\equiv 5(mod 32)}$ = -2^5, and, for our example, we have

$$\Delta R_t = \sum_{j=25}^{31} +2^{j+12 \pmod{32}} - 2^{31+12 (mod 32)} = \sum_{j=5}^{10} +2^j - 2^{11} = -2^5.$$

which is exactly what we wanted since

$$\Delta R_t = 2^5 + 2^6 + 2^7 + 2^8 + 2^9 + 2^{10} + 2^{11} = -2^5.$$

6.2 Description of the First Block of the Differential

Steps 0 to 3:

- $\Delta Q_t = 0$.
- $\Delta f_t = \Delta Q_{t-3} = 0$, $\Delta W_t = 0$.
- $\Delta T_t = \Delta f_t + \Delta Q_{t-3} + \Delta W_t = 0 + 0 + 0 = 0$.
- Condition(s) on ΔT_t: none
- $\Delta T_t = 0 \Rightarrow \Delta R_t = 0$.

- $\Delta Q_{t+1} = \Delta Q_t + \Delta R_t = 0 + 0 = 0$.

Step 4:

- $\Delta Q_4 = 0$.
- $\Delta f_4 = 0$, $\Delta Q_1 = 0$, and $\Delta W_4 = -2^{31}$.
- $\Delta T_4 = \Delta f_4 + \Delta Q_1 + \Delta W_4 = 0 + 0 + (-2^{31}) = -2^{31}$.
- Condition(s) on ΔT_4:
- $\Delta T_4[31] = 1$ ensures that the add difference is -2^{31} (condition III). The probability that this condition holds is (2^{-1}) since $\Delta T_4[31] = 1$ rather than $\Delta T_4[31] = (0, 1)$.
- $S(4) = 7$, so $\Delta T_4 = -2^{31} \Rightarrow \Delta R_4 = -2^{31+7=38\equiv 6(mod 32)} = -2^6$.
- $\Delta Q_5 = \Delta Q_4 + \Delta R_4 = 0 + (-2^6) = -2^6$.

Step 5:

- $\Delta Q_5 = -2^6$.
- $\Delta f_5 = +2^{19} + 2^{11}$, $\Delta Q_2 = 0$, and ΔW_5.
- $\Delta T_5 = \Delta f_5 + \Delta Q_2 + \Delta W_5 = (+2^{19} + 2^{11}) + 0 + 0 = +2^{19} + 2^{11}$.
- Condition(s) on ΔT_5:
  - $\Delta = (+2^{19} + 2^{11})$ must not propagate past bit 19 since we do not want to affect low order bits upon rotation (condition I). The probability that this condition holds is $2^{-1} \times (1 - 2^{-8})$ since $T_5[19] = 0$ and $0 \in T_5[18 - 11]$ to ensure there is no propagation past bit 19.
  - $S(5) = 12$, so $\Delta T_5 = +2^{19} + 2^{11} \Rightarrow \Delta R_5 = +2^{19+12=31} + 2^{11+12=23} = +2^{31} + 2^{23}$.
  - $\Delta Q_6 = \Delta Q_5 + \Delta R_5 = (-2^6) + (+2^{31} + 2^{23}) = \pm 2^{31} + 2^{23} - 2^6$.

Step 6:

- $\Delta Q_6 = \pm 2^{31} + 2^{23} - 2^6$.
- $\Delta f_6 = -2^{14} - 2^{10}$, $\Delta Q_3 = 0$, and $\Delta W_6 = 0$.
- $\Delta T_6 = \Delta f_6 + \Delta Q_3 + \Delta W_6 = (-2^{14} - 2^{10}) + 0 + 0 = -2^{14} - 2^{10}$.
- Condition(s) on ΔT_6:
  - $\Delta = (-2^{14})$ must propagate to bit 15 since we want to affect bit 0 upon rotation (condition II). Thus, -2^{14} is rewritten as $-2^{15} + 2^{14}$. The probability that this condition holds is 2^{-1} since having $T_6[14] = 0$ will ensure the appropriate propagation.
  - $\Delta = (-2^{10})$ must not propagate past bit 13 (bit 14 has already been specified) since we do not want to affect any more low order bits upon rotation (condition I). The probability that this condition holds is $(1 - 2^{-4})$ since $1 \in T_6[13 - 10]$ to ensure there is no propagation past bit 13.
- $S(6) = 17$, so $\Delta T_6 = -2^{15} + 2^{14} - 2^{10} \Rightarrow \Delta R_6 = -2^{15+17=32\equiv 0(mod 32)} + 2^{14+17=31} - 2^{10+17=27} = +2^{31} - 2^{27} - 2^0$.
- $\Delta Q_7 = \Delta Q_6 + \Delta R_6 = (\pm 2^{31} + 2^{23} - 2^6) + (+2^{31} - 2^{27} - 2^0) = -2^{27} + 2^{23} - 2^6 - 2^0$.

- the add-differences ($\pm 2^{31}$) and ($+2^{31}$) cancel each other out modulo 2^{32}.

Step 7:

- ΔQ_7 = -2^{27} + 2^{23} - 2^6 - 2^0.
- Δf_7 = -2^{27} - 2^{25} + 2^{16} + 2^{10} + 2^5 - 2^2, $\Delta Q_4 = 0$, and $\Delta W_7 = 0$.
- $\Delta T_7 = \Delta f_7 + \Delta Q_4 + \Delta W_7$ = (-2^{27} - 2^{25} + 2^{16} + 2^{10} + 2^5 - 2^2) + 0 + 0 = -2^{27} - 2^{25} + 2^{16} + 2^{10} + 2^5 - 2^2.
- Condition(s) on ΔT_7:
  - Δ = (-2^{27} - 2^{25} + 2^{16}) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-5}) × (1 - 2^{-2}) × (1 - 2^{-9}) since 1 ∈ T_7[31 - 27], 1 ∈ T_7[2^6, 25], and 0 ∈ T_7[24 - 16] to ensure there is no propagation past bit 31.
  - Δ = (+2^{10} + 2^5) must propagate to bit 11 since we want to affect bit 1 upon rotation (condition II). Thus, +2^{10} + 2^5 is written as +2^{11} - 2^9 - 2^8 - 2^7 - 2^6 - 2^5. The probability that this condition is 2^{-5} since T_7[9 - 5] = 1, where each of the five bits contains a 2^{-1} chance of being a 1.
  - Δ = (-2^2) must not propagate past bit 9 since we do not want to affect any more low order bits upon rotation (condition I). The probability that this condition holds is (1 - 2^{-8}) since 1 ∈ T_7[9 - 2] to ensure there is no propagation past bit 9.
- $S(7) = 22$, so ΔT_7 = -2^{27} - 2^{25} + 2^{16} + 2^{11} - 2^9 - 2^8 - 2^7 - 2^6 - 2^5 - 2^2 ⇒

$$
\begin{aligned}
\Delta R_7 = &-2^{27+22=49\equiv 17} - 2^{25+22=47\equiv 15} + 2^{16+22=38\equiv 6} + 2^{11+22=33\equiv 1} - 2^{2+22=24} \\
&+ \underbrace{(-2^{9+22=31} - 2^{8+22=30} - 2^{7+22=29} - 2^{6+22=28} - 2^{5+22=27})}_{=+2^{27}} \\
= &+2^{27} - 2^{24} - 2^{17} - 2^{15} + 2^6 + 2^1.
\end{aligned}
$$

- $\Delta Q_8 = \Delta Q_7 + \Delta R_7$ = (-2^{27} + 2^{23} - 2^6 - 2^0) + (+2^{27} - 2^{24} - 2^{17} - 2^{15} + 2^6 + 2^1) = -2^{23} - 2^{17} - 2^{15} + 2^0.
  - the add-differences (-2^{27}) and (+2^{27}) cancel each other out,
  - the add-differences (+2^{23}) and (-2^{24}) combine to yield (-2^{23}),
  - the add-differences (-2^6) and (+2^6) cancel each other out, and
  - the add-differences (-2^0) and (+2^1) combine to yield (+2^0).

Step 8:

- ΔQ_8 = -2^{23} - 2^{17} - 2^{15} + 2^0.
- Δf_8 = ±2^{31} - 2^{24} + 2^{16} + 2^{10} + 2^8 + 2^6, ΔQ_5 = -2^6, and $\Delta W_8 = 0$.
- $\Delta T_8 = \Delta f_8 + \Delta Q_5 + \Delta W_8$ = (±2^{31} - 2^{24} + 2^{16} + 2^{10} + 28 + 2^6) + (-2^6) + 0 = ±2^{31} - 2^{24} + 2^{16} + 2^{10} + 2^8.
  - the add-differences (+2^6) and (-2^6) cancel each other out.
- Condition(s) on ΔT_8:
  - $\Delta T_8[31] = 1$ ensures that the add difference is -2^{31} (condition III). The probability that this condition holds is (2^{-1}) since $\Delta T_8[31] = 1$ rather than $\Delta T_8[31]$ = (0, 1).

- Δ = (-2^{24} + 2^{16} + 2^{10} + 2^8) must not propagate past bit 24 since we do not want to affect low order bits upon rotation (condition I). The probability that this condition holds is $(2^{-1}) \times (1 - 2^{-8}) \times (1 - 2^{-6}) \times (1 - 2^{-2})$ since $T_8[24] = 1$, $0 \in T_8[23 - 16]$, $0 \in T_8[15 - 10]$, and $0 \in T_8[9, 8]$ to ensure there is no propagation past bit 24.

– $S(8) = 7$, so ΔT_8 = -2^{31} - 2^{24} + 2^{16} + 2^{10} + 2^8 $\Rightarrow$ ΔR_8 = -$2^{31+7=38\equiv6(mod32)}$ - $2^{24+7=31}$ + $2^{16+7=23}$ + $2^{10+7=17}$ + $2^{8+7=15}$ = -2^{31} + 2^{23} + 2^{17} + 2^{15} - 2^6.

– $\Delta Q_9 = \Delta Q_8 + \Delta R_8$ = (-2^{23} - 2^{17} - 2^{15} + 2^0) + (-2^{31} + 2^{23} + 2^{17} + 2^{15} - 2^6) = $\pm2^{31}$ - 2^6 + 2^0.
  - the add-differences (-2^{23}) and (+2^{23}) cancel each other out,
  - the add-differences (-2^{17}) and (+2^{17}) cancel each other out, and
  - the add-differences (-2^{15}) and (+2^{15}) cancel each other out.

Step 9:

– $\Delta Q_9 = \pm2^{31}$ - 2^6 + 2^0.

– $\Delta f_9 = \pm2^{31}$ + 2^{26} - 2^{23} - 2^{20} + 2^6 + 2^0, $\Delta Q_6 = \pm2^{31}$ + 2^{23} - 2^6, and $\Delta W_9 = 0$.

– $\Delta T_9 = \Delta f_9 + \Delta Q_6 + \Delta W_9$ = ($\pm2^{31}$ + 2^{26} - 2^{23} - 2^{20} + 2^6 + 20) + ($\pm2^{31}$ + 2^{23} - 2^6) + 0 = +2^{26} - 2^{20} + 2^0.
  - the add-differences ($\pm2^{31}$) and ($\pm2^{31}$) cancel each other out modulo 2^{32},
  - the add-differences (-2^{23}) and (+2^{23}) cancel each other out, and
  - the add-differences (+2^6) and (-2^6) cancel each other out.

– Condition(s) on ΔT_9:
  - Δ = (+2^{26} - 2^{20}) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-6}) $\times$ (1 - 2^{-6}) since $0 \in T_9[31 - 26]$ and $1 \in T_9[25 - 20]$ to ensure there is no propagation past bit 31.
  - Δ = (+2^0) must not propagate past bit 19 since we do not want to affect any more low order bits upon rotation (condition I). The probability that this condition holds is (1 - 2^{-20}) since $0 \in T_9[19 - 0]$ to ensure there is no propagation past bit 19.

– $S(9) = 12$, so ΔT_9 = +2^{26} - 2^{20} + 2^0 $\Rightarrow$ ΔR_9 = +$2^{26+12=38\equiv6(mod32)}$ - $2^{20+12=32\equiv0(mod32)}$ + $2^{0+12=12}$ = +2^{12} + 2^6 - 2^0.

– $\Delta Q_{10} = \Delta Q_9 + \Delta R_9$ = ($\pm2^{31}$ - 2^6 + 2^0) + (+2^{12} + 2^6 - 2^0) = $\pm2^{31}$ + 2^{12}.
  - the add-differences (-2^6) and (+2^6) cancel each other out.
  - the add-differences (+2^0) and (-2^0) cancel each other out.

Step 10:

– $\Delta Q_{10} = \pm2^{31}$ + 2^{12}.

– Δf_{10} = -2^{23} + 2^{13} + 2^6 + 2^0, ΔQ_7 = -2^{27} + 2^{23} - 2^6 - 2^0, and $\Delta W_{10} = 0$.

– $\Delta T_{10} = \Delta f_{10} + \Delta Q_7 + \Delta W_{10}$ = (-2^{23} + 2^{13} + 2^6 + 2^0) + (-2^{27} + 2^{23} - 2^6 - 20) + 0 = -2^{27} + 2^{13}.
  - the add-differences (-2^{23}) and (+2^{23}) cancel each other out,
  - the add-differences (+2^6) and (-2^6) cancel each other out, and
  - the add-differences (+2^0) and (-2^0) cancel each other out.

– Condition(s) on ΔT_{10}:

- Δ = (-2^{27}) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-5}) since $1 \in T_{10}[31 - 27]$ to ensure there is no propagation past bit 31.
- Δ = (+2^{13}) must not propagate past bit 14 since we do not want to affect any more low order bits upon rotation (condition I). The probability that this condition holds is (1 - 2^{-2}) since $0 \in T_{10}[14, 13]$ to ensure there is no propagation past bit 14.

– $S(10) = 17$, so ΔT_{10} = -2^{27} + 2^{13} $\Rightarrow$ ΔR_{10} = -$2^{27+17=44\equiv 12(mod 32)}$ + $2^{13+17=30}$ = +2^{30} - 2^{12}.
– $\Delta Q_{11} = \Delta Q_{10} + \Delta R_{10}$ = ($\pm 2^{31}$ + 2^{12}) + (+2^{30} - 2^{12}) = $\pm 2^{31}$ + 2^{30}.

- the add-differences (+2^{12}) and (-2^{12}) cancel each other out.

Step 11:

– ΔQ_{11} = $\pm 2^{31}$ + 2^{30}.
– Δf_{11} = -2^{8} - 2^{0}, ΔQ_{8} = -2^{23} - 2^{17} - 2^{15} + 2^{0}, and ΔW_{11} = +2^{15}.
– $\Delta T_{11} = \Delta f_{11} + \Delta Q_8 + \Delta W_{11}$ = (-2^{8} - 2^{0}) + (-2^{23} - 2^{17} - 2^{15} + 2^{0}) + (+2^{15}) = -2^{23} - 2^{17} - 2^{8}.

- the add-differences (-2^{15}) and (+2^{15}) cancel each other out, and
- the add-differences (-2^{0}) and (+2^{0}) cancel each other out, and

– Condition(s) on ΔT_{11}:

- Δ = (-2^{23} - 2^{17}) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-9}) $\times$ (1 - 2^{-6}) since $1 \in T_{11}[31 - 23]$ and $1 \in T_{11}[22 - 17]$ to ensure there is no propagation past bit 31.
- Δ = (-2^{8}) must not propagate past bit 9 since we do not want to affect any more low order bits upon rotation (condition I). The probability that this condition holds is (1 - 2^{-2}) since $1 \in T_{11}[9, 8]$ to ensure there is no propagation past bit 9.

– $S(11) = 22$, so ΔT_{11} = -2^{23} - 2^{17} - 2^{8} $\Rightarrow$ ΔR_{11} = -$2^{23+22=45\equiv 13(mod 32)}$ - $2^{17+22=39\equiv 7(mod 32)}$ - $2^{8+22=30}$ = -2^{30} - 2^{13} - 2^{7}.
– $\Delta Q_{12} = \Delta Q_{11} + \Delta R_{11}$ = ($\pm 2^{31}$ + 2^{30}) + (-2^{30} - 2^{13} - 2^{7}) = $\pm 2^{31}$ - 2^{13} - 2^{7}.

- the add-differences (+2^{30}) and (-2^{30}) cancel each other out.

Step 12:

– ΔQ_{12} = $\pm 2^{31}$ - 2^{13} - 2^{7}.
– Δf_{12} = $\pm 2^{31}$ + 2^{17} + 2^{7}, ΔQ_{9} = $\pm 2^{31}$ - 2^{6} + 2^{0}, and ΔW_{12} = 0.
– $\Delta T_{12} = \Delta f_{12} + \Delta Q_9 + \Delta W_{12}$ = ($\pm 2^{31}$ + 2^{17} + 2^{7}) + ($\pm 2^{31}$ - 2^{6} + 20) + 0 = +2^{17} + 2^{6} + 2^{0}.

- the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}, and
- the add-differences (+2^{7}) and (-2^{6}) combine to yield (+2^{6}).

– Condition(s) on ΔT_{12}:

- Δ = (+2^{17} + 2^{6} + 2^{0}) must not propagate past bit 24 since we do not want to affect any more low order bits upon rotation (condition I). The probability that this condition holds is $(1 - 2^{-8}) \times (1 - 2^{-11}) \times (1 - 2^{-6})$ since $0 \in T_{12}[24 - 17]$, $0 \in T_{12}[16 - 6]$, and $0 \in T_{12}[5 - 0]$ to ensure there is no propagation past bit 24.

- $S(12) = 7$, so Delta$T_{12} = +2^{17} + 2^6 + 2^0 \Rightarrow \Delta R_{12} = +2^{17+7=24} + 2^{6+7=13} + 2^{0+7=7} = +2^{24} + 2^{13} + 2^7$.
- $\Delta Q_{13} = \Delta Q_{12} + \Delta R_{12} = (\pm 2^{31}$ - 2^{13} - 27) + $(+2^{24} + 2^{13} + 2^7) = \pm 2^{31} + 2^{24}$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32},
  - the add-differences (-2^{13}) and (+2^{13}) cancel each other out, and
  - the add-differences (-2^7) and (+2^7) cancel each other out.

Step 13:

- $\Delta Q_{13} = \pm 2^{31} + 2^{24}$.
- $\Delta f_{13} = \pm 2^{31}$ - 2^{13}, $\Delta Q_{10} = \pm 2^{31} + 2^{12}$, and $\Delta W_{13} = 0$.
- $\Delta T_{13} = \Delta f_{13} + \Delta Q_{10} + \Delta W_{13} = (\pm 2^{31}$ - $2^{13}) + (\pm 2^{31} + 2^{12}) + 0 =$ -2^{12}.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}, and
  - the add-differences (-2^{13}) and (+2^{12}) combine to yield (-2^{12}).
- Condition(s) on ΔT_{13}:
  - Δ = (-2^{12}) must not propagate past bit 19 since we do not want to affect any more low order bits upon rotation (condition I). The probability that this condition holds is (1 - 2^{-8}) since $1 \in T_{13}[19$ - $12]$ to ensure there is no propagation past bit 19.
- $S(13) = 12$, so ΔT_{13} = -$2^{12} \Rightarrow \Delta R_{13}$ = -$2^{12+12=24}$ = -2^{24}. $\Delta Q_{14} = \Delta Q_{13} + \Delta R_{13} = (\pm 2^{31} + 2^{24})$ + (-$2^{24}) = \pm 2^{31}$.
  - the add-differences (+2^{24}) and (-2^{24}) cancel each other out.

Step 14:

- $\Delta Q_{14} = \pm 2^{31}$.
- $\Delta f_{14} = \pm 2^{31} + 2^{18}$, $\Delta Q_{11} = \pm 2^{31} + 2^{30}$, and $\Delta W_{14} = \pm 2^{31}$.
- $\Delta T_{14} = \Delta f_{14} + \Delta Q_{11} + \Delta W_{14} = (\pm 2^{31} + 2^{18}) + (\pm 2^{31} + 2^{30}) + (\pm 2^{31})$ = -$2^{30} + 2^{18}$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}, and
  - the add-differences (+2^{30}) and ($\pm 2^{31}$) combine to yield (-2^{30}) modulo 2^{32}.
- Condition(s) on ΔT_{14}:
  - Δ = (-$2^{30} + 2^{18}$) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-2}) $\times$ (1 - 2^{-12}) since $1 \in T_{14}[31, 30]$ and $0 \in T_{14}[29$ - $18]$ to ensure there is no propagation past bit 31.
- $S(14) = 17$, so ΔT_{14} = -$2^{30} + 2^{18} \Rightarrow \Delta R_{14}$ = -$2^{30+17=47\equiv 15 (mod 32)} + 2^{18+17=35\equiv 3 (mod 32)}$ = -$2^{15} + 2^3$.
- $\Delta Q_{15} = \Delta Q_{14} + \Delta R_{14} = (\pm 2^{31})$ + (-$2^{15} + 2^3) = \pm 2^{31}$ - $2^{15} + 2^3$.

Step 15:

- $\Delta Q_{15} = \pm 2^{31}$ - $2^{15} + 2^3$.
- $\Delta f_{15} = \pm 2^{31} + 2^{25}$, $\Delta Q_{12} = \pm 2^{31}$ - 2^{13} - 2^7, and $\Delta W_{15} = 0$.
- $\Delta T_{15} = \Delta f_{15} + \Delta Q_{12} + \Delta W_{15} = (\pm 2^{31} + 2^{25}) + (\pm 2^{31}$ - 2^{13} - $2^7) + 0 = +2^{25}$ - 2^{13} - 2^7.

  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{15}:
  - Δ = ($+2^{25}$ - 2^{13}) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-7}) $\times$ (1 - 2^{-12}) since $0 \in T_{15}[31 - 25]$ and $1 \in T_{15}[24 - 13]$ to ensure there is no propagation past bit 31.
  - Δ = (-2^7) must not propagate past bit 9 since we do not want to affect any more low order bits upon rotation (condition I). The probability that this condition holds is (1 - 2^{-3}) since $1 \in T_{15}[9 - 7]$ to ensure there is no propagation past bit 9.
- $S(15) = 22$, so $\Delta T_{15} = +2^{25} - 2^{13} - 2^7 \Rightarrow \Delta R_{15} = +2^{25+22=47\equiv 15(mod 32)} - 2^{13+22=35\equiv 3(mod 32)} - 2^{7+22=29} = -2^{29} + 2^{15} - 2^3$.
- $\Delta Q_{16} = \Delta Q_{15} + \Delta R_{15} = (\pm 2^{31} - 2^{15} + 2^3) + (-2^{29} + 2^{15} - 2^3) = \pm 2^{31} - 2^{29}$.
  - the add-differences (-2^{15}) and ($+2^{15}$) cancel each other out, and
  - the add-differences ($+2^3$) and (-2^3) cancel each other out.

Step 16:

- $\Delta Q_{16} = \pm 2^{31} - 2^{29}$.
- $\Delta f_{16} = \pm 2^{31}$, $\Delta Q_{13} = \pm 2^{31} + 2^{24}$, and $\Delta W_{16} = 0$.
- $\Delta T_{16} = \Delta f_{16} + \Delta Q_{13} + \Delta W_{16} = (\pm 2^{31}) + (\pm 2^{31} + 2^{24}) + 0 = +2^{24}$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{16}:
  - Δ = ($+2^{24}$) must not propagate past bit 26 since we do not want to affect any more low order bits upon rotation (condition I). The probability that this condition holds is (1 - 2^{-3}) since $0 \in T_{16}[26 - 24]$ to ensure there is no propagation past bit 26.
- $S(16) = 5$, so $\Delta T_{16} = +2^{24} \Rightarrow \Delta R_{16} = +2^{24+5=29} = +2^{29}$.
- $\Delta Q_{17} = \Delta Q_{16} + \Delta R_{16} = (\pm 2^{31} - 2^{29}) + (+2^{29}) = \pm 2^{31}$.
  - the add-differences (-2^{29}) and ($+2^{29}$) cancel each other out.

Step 17:

- $\Delta Q_{17} = \pm 2^{31}$.
- $\Delta f_{17} = \pm 2^{31}$, $\Delta Q_{14} = \pm 2^{31}$, and $\Delta W_{17} = 0$.
- $\Delta T_{17} = \Delta f_{17} + \Delta Q_{14} + \Delta W_{17} = (\pm 2^{31}) + (\pm 2^{31}) + 0 = 0$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{17}: none
- $\Delta T_{17} = 0 \Rightarrow \Delta R_{17} = 0$.
- $\Delta Q_{18} = \Delta Q_{17} + \Delta R_{17} = (\pm 2^{31}) + (0) = \pm 2^{31}$.

Step 18:

- $\Delta Q_{18} = \pm 2^{31}$.

- $\Delta f_{18} = \pm 2^{31}$, $\Delta Q_{15} = \pm 2^{31}$ - 2^{15} + 2^3, and $\Delta W_{18} = +2^{15}$.
- $\Delta T_{18} = \Delta f_{18} + \Delta Q_{15} + \Delta W_{18} = (\pm 2^{31}) + (\pm 2^{31}$ - $2^{15} + 2^3) + (+2^{15}) = +2^3$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}, and
  - the add-differences (-2^{15}) and (+2^{15}) cancel each other out.
- Condition(s) on ΔT_{18}:
  - Δ = (+2^3) must not propagate past bit 17 since we do not want to affect any more low order bits upon rotation (condition I). The probability that this condition holds is (1 - 2^{-15}) since $0 \in T_{18}$[17 - 3] to ensure there is no propagation past bit 17.
- $S(18) = 14$, so $\Delta T_{18} = +2^3 \Rightarrow \Delta R_{18} = +2^{3+14}$ =17 = $+2^{17}$. $\Delta Q_{19} = \Delta Q_{18} + \Delta R_{18} = (\pm 2^{31}) + (+2^{17})$ = $\pm 2^{31} + 2^{17}$.

Step 19:

- $\Delta Q_{19} = \pm 2^{31} + 2^{17}$.
- $\Delta f_{19} = \pm 2^{31}$, $\Delta Q_{16} = \pm 2^{31}$ - 2^{29}, and $\Delta W_{19} = 0$.
- $\Delta T_{19} = \Delta f_{19} + \Delta Q_{16} + \Delta W_{19} = (\pm 2^{31}) + (\pm 2^{31}$ - $2^{29}) + 0$ = -2^{29}.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{19}:
  - Δ = (-2^{29}) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-3}) since $1 \in T_{19}$[31 - 29] to ensure there is no propagation past bit 31.
- $S(19) = 20$, so ΔT_{19} = -$2^{29} \Rightarrow \Delta R_{19}$ = -$2^{29+20=49\equiv 17 (mod 32)}$ = -2^{17}.
- $\Delta Q_{20} = \Delta Q_{19} + \Delta R_{19} = (\pm 2^{31} + 2^{17})$ + (-2^{17}) = $\pm 2^{31}$.
  - the add-differences (+2^{17}) and (-2^{17}) cancel each other out.

Steps 20 and 21:

- $\Delta Q_t = \pm 2^{31}$.
- $\Delta f_t = \pm 2^{31}$, $\Delta Q_{t-3} = \pm 2^{31}$, and $\Delta W_t = 0$.
- $\Delta T_t = \Delta f_t + \Delta Q_{t-3} + \Delta W_t = (\pm 2^{31}) + (\pm 2^{31}) + 0 = 0$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_t: none
- $\Delta T_t = 0 \Rightarrow \Delta R_t$ 0.
- $\Delta Q_{t+1} = \Delta Q_t + \Delta R_t = (\pm 2^{31}) + 0 = \pm 2^{31}$.

Step 22:

- $\Delta Q_{22} = \pm 2^{31}$.
- $\Delta f_{22} = \pm 2^{31}$, $\Delta Q_{19} = \pm 2^{31} + 2^{17}$, and $\Delta W_{22} = 0$.
- $\Delta T_{22} = \Delta f_{22} + \Delta Q_{19} + \Delta W_{22} = (\pm 2^{31}) + (\pm 2^{31} + 2^{17}) + 0 = +2^{17}$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.

- Condition(s) on ΔT_{22}:
  - $\Delta = (+2^{17})$ must not propagate past bit 17 since we do not want to affect lower order bits (condition I). The probability that this condition holds is (2^{-1}) since $T_{22}[17] = 0$ to ensure there is no propagation past bit 17.
- $S(22) = 14$, so $\Delta T_{22} = +2^{17} \Rightarrow \Delta R_{22} = +2^{17+14=31} = +2^{31}$.
- $\Delta Q_{23} = \Delta Q_{22} + \Delta R_{22} = (\pm 2^{31}) + (\pm 2^{31}) = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.

Step 23:

- $\Delta Q_{23} = 0$.
- $\Delta f_{23} = 0$, $\Delta Q_{20} = \pm 2^{31}$, and $\Delta W_{23} = \pm 2^{31}$.
- $\Delta T_{23} = \Delta f_{23} + \Delta Q_{20} + \Delta W_{23} = 0 + (\pm 2^{31}) + (\pm 2^{31}) = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{23}: none
- $\Delta T_{23} = 0 \Rightarrow \Delta R_{23} = 0$.
- $\Delta Q_{24} = \Delta Q_{23} + \Delta R_{23} = 0 + 0 = 0$.

Step 24:

- $\Delta Q_{24} = 0$.
- $\Delta f_{24} = \pm 2^{31}$, $\Delta Q_{21} = \pm 2^{31}$, and $\Delta W_{24} = 0$.
- $\Delta T_{24} = \Delta f_{24} + \Delta Q_{21} + \Delta W_{24} = (\pm 2^{31}) + (\pm 2^{31}) + 0 = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{24}: none
- $\Delta T_{24} = 0 \Rightarrow \Delta R_{24} = 0$.
- $\Delta Q_{25} = \Delta Q_{24} + \Delta R_{24} = 0 + 0 = 0$.

Step 25:

- $\Delta Q_{25} = 0$.
- $\Delta f_{25} = 0$, $\Delta Q_{22} = \pm 2^{31}$, and $\Delta W_{25} = \pm 2^{31}$.
- $\Delta T_{25} = \Delta f_{25} + \Delta Q_{22} + \Delta W_{25} = 0 + (\pm 2^{31}) + (\pm 2^{31}) = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{25}: none
- $\Delta T_{25} = 0 \Rightarrow \Delta R_{25} = 0$.
- $\Delta Q_{26} = \Delta Q_{25} + \Delta R_{25} = 0 + 0 = 0$.

Steps 26 to 33:

- $\Delta Q_t = 0$.
- $\Delta f_t = \Delta Q_{t-3} = \Delta W_t = 0$.
- $\Delta T_t = \Delta f_t + \Delta Q_{t-3} + \Delta W_t = 0 + 0 + 0 = 0$.
- Condition(s) on ΔT_t: none
- $\Delta T_t = 0 \Rightarrow \Delta R_t = 0$.
- $\Delta Q_{t+1} = \Delta Q_t + \Delta R_t = 0 + 0 = 0$.

Step 34:

- $\Delta Q_{34} = 0$.
- $\Delta f_{34} = 0$, $\Delta Q_{31} = 0$, and $\Delta W_{34} = +2^{15}$.
- $\Delta T_{34} = \Delta f_{34} + \Delta Q_{31} + \Delta W_{34} = 0 + 0 + (+2^{15}) = +2^{15}$.
- Condition(s) on ΔT_{34}:
  - $\Delta = (+2^{15})$ must not propagate past bit 15 since we do not want to affect lower order bits (condition I). The probability that this condition holds is (2^{-1}) since $T^{34}[15] = 0$ to ensure there is no propagation past bit 15.
- $S(34) = 16$, so $\Delta T_{34} = +2^{15} \Rightarrow \Delta R_{34} = +2^{15+16=31} = +2^{31}$.
- $\Delta Q_{35} = \Delta Q_{34} + \Delta R_{34} = 0 + (\pm 2^{31}) = \pm 2^{31}$.

Step 35:

- $\Delta Q_{35} = \pm 2^{31}$.
- $\Delta f_{35} = \pm 2^{31}$, $\Delta Q_{32} = 0$, and $\Delta W_{35} = \pm 2^{31}$.
- $\Delta T_{35} = \Delta f_{35} + \Delta Q_{32} + \Delta W_{35} = (\pm 2^{31}) + 0 + (\pm 2^{31}) = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{35}: none
- $\Delta T_{35} = 0 \Rightarrow \Delta R_{35} = 0$.
- $\Delta Q_{36} = \Delta Q_{35} + \Delta R_{35} = (\pm 2^{31}) + 0 = \pm 2^{31}$.

Step 36:

- $\Delta Q_{36} = \pm 2^{31}$.
- $\Delta f_{36} = 0$, $\Delta Q_{33} = 0$, and $\Delta W_{36} = 0$.
- $\Delta T_{36} = \Delta f_{36} + \Delta Q_{33} + \Delta W_{36} = 0 + 0 + 0 = 0$.
- Condition(s) on ΔT_{36}: none
- $\Delta T_{36} = 0 \Rightarrow \Delta R_{36} = 0$.
- $\Delta Q_{37} = \Delta Q_{36} + \Delta R_{36} = (\pm 2^{31}) + 0 = \pm 2^{31}$.

Step 37:

- $\Delta Q_{37} = \pm 2^{31}$.
- $\Delta f_{37} = \pm 2^{31}$, $\Delta Q_{34} = 0$, and $\Delta W_{37} = \pm 2^{31}$.
- $\Delta T_{37} = \Delta f_{37} + \Delta Q_{34} + \Delta W_{37} = (\pm 2^{31}) + 0 + (\pm 2^{31}) = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{37}: none
- $\Delta T_{37} = 0 \Rightarrow \Delta R_{37} = 0$.
- $\Delta Q_{38} = \Delta Q_{37} + \Delta R_{37} = (\pm 2^{31}) + 0 = \pm 2^{31}$.

Steps 38 to 49:

- $\Delta Q_t = \pm 2^{31}$.
- $\Delta f_t = \pm 2^{31}$, $\Delta Q_{t-3} = \pm 2^{31}$, and $\Delta W_t = 0$.
- $\Delta T_t = \Delta f_t + \Delta Q_{t-3} + \Delta W_t = (\pm 2^{31}) + (\pm 2^{31}) + 0 = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_t: none
- $\Delta T_t = 0 \Rightarrow \Delta R_t = 0$.
- $\Delta Q_{t+1} = \Delta Q_t + \Delta R_t = (\pm 2^{31}) + 0 = 0$.

Step 50:

- $\Delta Q_{50} = \pm 2^{31}$.
- $\Delta f_{50} = 0$, $\Delta Q_{47} = \pm 2^{31}$, and $\Delta W_{50} = \pm 2^{31}$.
- $\Delta T_{50} = \Delta f_{50} + \Delta Q_{47} + \Delta W_{50} = 0 + (\pm 2^{31}) + (\pm 2^{31}) = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{50}: none
- $\Delta T_{50} = 0 \Rightarrow \Delta R_{50} = 0$.
- $\Delta Q_{51} = \Delta Q_{50} + \Delta R_{50} = (\pm 2^{31}) + 0 = \pm 2^{31}$.

Steps 51 to 59:

- $\Delta Q_t = \pm 2^{31}$.
- $\Delta f_t = \pm 2^{31}$, $\Delta Q_{t-3} = \pm 2^{31}$, and $\Delta W_t = 0$.
- $\Delta T_t = \Delta f_t + \Delta Q_{t-3} + \Delta W_t = (\pm 2^{31}) + (\pm 2^{31}) + 0 = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_t: none
- $\Delta T_t = 0 \Rightarrow \Delta R_t = 0$.
- $\Delta Q_{t+1} = \Delta Q_t + \Delta R_t = (\pm 2^{31}) + 0 = 0$.

Step 60:

- $\Delta Q_{60} = \pm 2^{31}$.
- $\Delta f_{60} = 0$, $\Delta Q_{58} = \pm 2^{31}$, and $\Delta W_{60} = \pm 2^{31}$.
- $\Delta T_{60} = \Delta f_{60} + \Delta Q_{58} + \Delta W_{60} = 0 + (\pm 2^{31}) + (\pm 2^{31}) = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{60}: none
- $\Delta T_{60} = 0 \Rightarrow \Delta R_{60} = 0$.
- $\Delta Q_{61} = \Delta Q_{60} + \Delta R_{60} = (\pm 2^{31}) + 0 = \pm 2^{31}$.

Step 61:

- $\Delta Q_{61} = \pm 2^{31}$.
- $\Delta f_{61} = \pm 2^{31}$, $\Delta Q_{58} = \pm 2^{31}$, and $\Delta W_{61} = +2^{15}$.
- $\Delta T_{61} = \Delta f_{61} + \Delta Q_{58} + \Delta W_{61} = (\pm 2^{31}) + (\pm 2^{31}) + (+2^{15}) = +2^{15}$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{61}:
  - $\Delta = (+2^{15})$ must not propagate past bit 21 since we do not want to affect lower order bits (condition I). The probability that this condition holds is (1 - 2^{-7}) since $0 \in \Delta T_{61}[21 - 15]$ to ensure there is no propagation past bit 21.
- $S(61) = 10$, so $\Delta T_{61} = +2^{15} \Rightarrow \Delta R_{61} = +2^{15+10=25} = +2^{25}$.
- $\Delta Q_{62} = \Delta Q_{61} + \Delta R_{61} = (\pm 2^{31}) + (+2^{25}) = \pm 2^{31} + 2^{25}$.

Steps 62 to 63:

- $\Delta Q_t = \pm 2^{31} + 2^{25}$.
- $\Delta f_t = \pm 2^{31}$, $\Delta Q_{t-3} = \pm 2^{31}$, and $\Delta W_t = 0$.
- $\Delta T_t = \Delta f_t + \Delta Q_{t-3} + \Delta W_t = (\pm 2^{31}) + (\pm 2^{31}) + 0 = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_t: none
- $\Delta T_t = 0 \Rightarrow \Delta R_t = 0$.
- $\Delta Q_{t+1} = \Delta Q_t + \Delta R_t = (\pm 2^{31} + 2^{25}) + 0 = \pm 2^{31} + 2^{25}$.

Assuming that all of our conditions are met, the final result of the differential for the first block is

$$\begin{aligned}
\Delta Q_{61} &= \Delta IHV^{(1)}[0] = \pm 2^{31}, \\
\Delta Q_{62} &= \Delta IHV^{(1)}[3] = \pm 2^{31} + 2^{25}, \\
\Delta Q_{63} &= \Delta IHV^{(1)}[2] = \pm 2^{31} + 2^{25}, \\
\Delta Q_{64} &= \Delta IHV^{(1)}[1] = \pm 2^{31} + 2^{25}.
\end{aligned}$$

Thus, we have:

$$\begin{aligned}
\Delta IHV^{(1)}[0] &= \Delta IHV^{(0)}[0] + \Delta Q_{61} = (0) + (\pm 2^{31}) = \pm 2^{31},\\
\Delta IHV^{(1)}[3] &= \Delta IHV^{(0)}[3] + \Delta Q_{62} = (0) + (\pm 2^{31} + 2^{25}) = \pm 2^{31} + 2^{25},\\
\Delta IHV^{(1)}[2] &= \Delta IHV^{(0)}[2] + \Delta Q_{63} = (0) + (\pm 2^{31} + 2^{25}) = \pm 2^{31} + 2^{25},\\
\Delta IHV^{(1)}[1] &= \Delta IHV^{(0)}[1] + \Delta Q_{64} = (0) + (\pm 2^{31} + 2^{25}) = \pm 2^{31} + 2^{25}.
\end{aligned}$$

The second block begins with

$$\begin{aligned}
\Delta IHV^{(1)}[0] &= (0) + (\pm 2^{31}) = \pm 2^{31},\\
\Delta IHV^{(1)}[3] &= (0) + (\pm 2^{31} + 2^{25}) = \pm 2^{31} + 2^{25},\\
\Delta IHV^{(1)}[2] &= (0) + (\pm 2^{31} + 2^{25}) = \pm 2^{31} + 2^{25},\\
\Delta IHV^{(1)}[1] &= (0) + (\pm 2^{31} + 2^{25}) = \pm 2^{31} + 2^{25}.
\end{aligned}$$

6.3 Description of the Second Block of the Differential

Step 0:

- $\Delta Q_0 = \Delta IHV^{(1)}[1] = \pm 2^{31} + 2^{25}$.
- $\Delta f_0 = \pm 2^{31}$, $\Delta Q_{-3} = \Delta IHV^{(1)}[0] = \pm 2^{31}$, and $\Delta W_0 = 0$.
- $\Delta T_0 = \Delta f_0 + \Delta Q_{-3} + \Delta W_0 = (\pm 2^{31}) + (\pm 2^{31}) + 0 = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_0: none
- $\Delta T_0 = 0 \Rightarrow \Delta R_0 = 0$.
- $\Delta Q_1 = \Delta Q_0 + \Delta R_0 = (\pm 2^{31} + 2^{25}) + 0 = \pm 2^{31} + 2^{25}$.

Step 1:

- $\Delta Q_1 = \pm 2^{31} + 2^{25}$.
- $\Delta f_1 = \pm 2^{31}$, $\Delta Q_{-2} = \Delta IHV^{(1)}[3] = \pm 2^{31} + 2^{25}$, and $\Delta W_1 = 0$.
- $\Delta T_1 = \Delta f_1 + \Delta Q_{-2} + \Delta W_1 = (\pm 2^{31}) + (\pm 2^{31} + 2^{25}) + 0 = +2^{25}$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_1:
  - $\Delta = (+2^{25})$ must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-7}) since 0 $T_1[31 - 25]$ to ensure there is no propagation past bit 31.
- $S(1) = 12$, so $\Delta T_1 = +2^{25} \Rightarrow \Delta R_1 = +2^{25+12=37\equiv 5 (mod 32)} = +2^5$.
- $\Delta Q_2 = \Delta Q_1 + \Delta R_1 = (\pm 2^{31} + 2^{25}) + (+2^5) = \pm 2^{31} + 2^{25} + 2^5$.

Step 2:

- $\Delta Q_2 = \pm 2^{31} + 2^{25} + 2^5$.
- $\Delta f_2 = +2^{25}$, $\Delta Q_{-1} = \Delta IHV^{(1)}[2] = \pm 2^{31} + 2^{25}$, and $\Delta W_2 = 0$.
- $\Delta T_2 = \Delta f_2 + \Delta Q_{-1} + \Delta W_2 = (+2^{25}) + (\pm 2^{31} + 2^{25}) + 0 = \pm 2^{31} + 2^{26}$.

  - the add-differences $(+2^{25})$ and $(+2^{25})$ combine to yield $(+2^{26})$.
- Condition(s) on ΔT_2:
  - $\Delta T_2[31] = 0$ ensures that the add difference is $+2^{31}$ (condition III). The probability that this condition holds is (2^{-1}) since $\Delta T_2[31] = 0$ rather than $T_2[31] = (0, 1)$.
  - $\Delta = (+2^{26})$ must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is $(1 - 2^{-6})$ since $0 \in T_2[31 - 26]$ to ensure there is no propagation past bit 31.
- $S(2) = 17$, so $\Delta T_2 = +2^{31} + 2^{26} \Rightarrow \Delta R_2 = +2^{31+17=48\equiv16(mod32)} + 2^{26+17=43\equiv11(mod32)} = +2^{16} + 2^{11}$.
- $\Delta Q_3 = \Delta Q_2 + \Delta R_2 = (\pm2^{31} + 2^{25} + 2^5) + (+2^{16} + 2^{11}) = \pm2^{31} + 2^{25} + 2^{16} + 2^{11} + 2^5$.

Step 3:

- $\Delta Q_3 = \pm2^{31} + 2^{25} + 2^{16} + 2^{11} + 2^5$.
- $\Delta f_3 = \pm2^{31} - 2^{27} + 2^{25} - 2^{21} - 2^{11}$, $\Delta Q_0 = \Delta IHV^{(1)}[1] = \pm2^{31} + 2^{25}$, and ΔW_3.
- $\Delta T_3 = \Delta f_3 + \Delta Q_0 + \Delta W_3 = (\pm2^{31} - 2^{27} + 2^{25} - 2^{21} - 2^{11}) + (\pm2^{31} + 2^{25}) + 0 = -2^{26} - 2^{21} - 2^{11}$.
  - the add-differences $(\pm2^{31})$ and $(\pm2^{31})$ cancel each other out modulo 2^{32}, and
  - the add-differences (-2^{27}), $(+2^{25})$, and $(+2^{25})$ combine to yield (-2^{26}).
- Condition(s) on ΔT_3:
  - $\Delta = (-2^{26} - 2^{21} - 2^{11})$ must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is $(1 - 2^{-6}) \times (1 - 2^{-5}) \times (1 - 2^{-10})$ since $1 \in T_3[31 - 26]$, $1 \in T_3[25 - 21]$, and $1 \in T_3[20 - 11]$ to ensure there is no propagation past bit 31.
- $S(3) = 22$, so $\Delta T_3 = -2^{26} - 2^{21} - 2^{11} \Rightarrow \Delta R_3 = -2^{26+22=48\equiv16(mod32)} - 2^{21+22=43\equiv11(mod32)} - 2^{11+22=33\equiv1(mod32)} = -2^{16} - 2^{11} - 2^1$.
- $\Delta Q_4 = \Delta Q_3 + \Delta R_3 = (\pm2^{31} + 2^{25} + 2^{16} + 2^{11} + 2^5) + (-2^{16} - 2^{11} - 2^1) = \pm2^{31} + 2^{25} + 2^5 - 2^1$.
  - the add-differences $(+2^{16})$ and (-2^{16}) cancel each other out, and
  - the add-differences $(+2^{11})$ and (-2^{11}) cancel each other out.

Step 4:

- $\Delta Q_4 = \pm2^{31} + 2^{25} + 2^5 - 2^1$.
- $\Delta f_4 = +2^{30} + 2^{26} - 2^{18} + 2^2 + 2^1$, $\Delta Q_1 = \pm2^{31} + 2^{25}$, and $\Delta W_4 = \pm2^{31}$.
- $\Delta T_4 = \Delta f_4 + \Delta Q_1 + \Delta W_4 = (+2^{30} + 2^{26} - 2^{18} + 2^2 + 2^1) + (\pm2^{31} + 2^{25}) + (\pm2^{31}) = +2^{30} + 2^{26} + 2^{25} - 2^{18} + 2^3 - 2^1$.
  - the add-differences $(\pm2^{31})$ and $(\pm2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_4:
  - $\Delta = (+2^{30} + 2^{26} + 2^{25})$ must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is $(1 - 2^{-2}) \times (1 - 2^{-4}) \times (2^{-1})$ since $0 \in T_4[31, 30]$, $0 \in T_4[29 - 2^6]$, and $T_4[25] = 0$ to ensure there is no propagation past bit 31.
  - $\Delta = (-2^{18} + 2^3 - 2^1)$ must not propagate past bit 24 since we do not want to affect lower order bits (condition I). The probability that this condition holds is $(1 - 2^{-7}) \times (1 - 2^{-15}) \times (1 - 2^{-2})$ since $1 \in T_4[24 - 18]$, $0 \in T_4[17 - 3]$, and $1 \in T_4[2, 1]$ to ensure there is no propagation past bit 24.

- $S(4) = 7$, so $\Delta T_4 = +2^{30} + 2^{26} + 2^{25} - 2^{18} + 2^3 - 2^1 \Rightarrow \Delta R_4 = +2^{30+7=37\equiv 5(mod32)} + 2^{26+7=33\equiv 1(mod32)} + 2^{25+7=32\equiv 0(mod32)} - 2^{18+7=25} + 2^{3+7=10} - 2^{1+7=8} = -2^{25} + 2^{10} - 2^8 + 2^5 + 2^1 + 2^0$.
- $\Delta Q_5 = \Delta Q_4 + \Delta R_4 = (\pm 2^{31} + 2^{25} + 2^5 - 2^1) + (-2^{25} + 2^{10} - 2^8 + 2^5 + 2^1 + 2^0) = \pm 2^{31} + 2^{10} - 2^8 + 2^6 + 2^0$.
  - the add-differences ($+2^{25}$) and (-2^{25}) cancel each other out,
  - the add-differences ($+2^5$) and ($+2^5$) combine to yield ($+2^6$), and
  - the add-differences (-2^1) and ($+2^1$) cancel each other out.

Step 5:

- $\Delta Q_5 = \pm 2^{31} + 2^{10} - 2^8 + 2^6 + 2^0$.
- $\Delta f_5 = +2^{30} + 2^{28} - 2^{26} - 2^{25} - 2^{20} - 2^8 - 2^5 - 2^4$, $\Delta Q_2 = \pm 2^{31} + 2^{25} + 2^5$, and ΔW_5.
- $\Delta T_5 = \Delta f_5 + \Delta Q_2 + \Delta W_5 = (+2^{30} + 2^{28} - 2^{26} - 2^{25} - 2^{20} - 2^8 - 2^5 - 2^4) + (\pm 2^{31} + 2^{25} + 2^5) + 0 = -2^{30} + 2^{28} - 2^{26} - 2^{20} - 2^8 - 2^4$.
  - the add-differences ($+2^{30}$) and ($\pm 2^{31}$) combine to yield (-2^{30}) modulo 2^{32},
  - the add-differences (-2^{25}) and ($+2^{25}$) cancel each other out, and
  - the add-differences (-2^5) and ($+2^5$) cancel each other out.
- Condition(s) on ΔT_5:
  - $\Delta = (-2^{30} + 2^{28} - 2^{26} - 2^{20})$ must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is $(1 - 2^{-2}) \times (1 - 2^{-2}) \times (1 - 2^{-2}) \times (1 - 2^{-6})$ since $1 \in T_5[31, 30]$, $0 \in T_5[29, 28]$, $1 \in T_5[27, 2^6]$, and $1 \in T_5[25 - 20]$ to ensure there is no propagation past bit 31.
  - $\Delta = (-2^8 - 2^4)$ must not propagate past bit 19 since we do not want to affect lower order bits (condition I). The probability that this condition holds is $(1 - 2^{-12}) \times (1 - 2^{-4})$ since $1 \in T_5[19 - 8]$ and $1 \in T_5[7 - 4]$ to ensure there is no propagation past bit 19.
- $S(5) = 12$, so $\Delta T_5 = -2^{30} + 2^{28} - 2^{26} - 2^{20} - 2^8 - 2^4 \Rightarrow \Delta R_5 = -2^{30+12=42\equiv 10(mod32)} + 2^{28+12=40\equiv 8(mod32)} - 2^{26+12=38\equiv 6(mod32)} - 2^{20+12=32\equiv 0(mod32)} - 2^{8+12=20} - 2^{4+12=16} = -2^{20} - 2^{16} - 2^{10} + 2^8 - 2^6 - 2^0$.
- $\Delta Q_6 = \Delta Q_5 + \Delta R_5 = (\pm 2^{31} + 2^{10} - 2^8 + 2^6 + 2^0) + (-2^{20} - 2^{16} - 2^{10} + 2^8 - 2^6 - 2^0) = \pm 2^{31} - 2^{20} - 2^{16}$.
  - the add-differences ($+2^{10}$) and (-2^{10}) cancel each other out,
  - the add-differences (-2^8) and ($+2^8$) cancel each other out, and
  - the add-differences ($+2^6$) and (-2^6) cancel each other out.
  - the add-differences ($+2^0$) and (-2^0) cancel each other out.

Step 6:

- $\Delta Q_6 = \pm 2^{31} - 2^{20} - 2^{16}$.
- $\Delta f_6 = -2^{25} - 2^{21} - 2^{16} - 2^{11} - 2^{10} - 2^5 + 2^3$, $\Delta Q_3 = \pm 2^{31} + 2^{25} + 2^{16} + 2^{11} + 2^5$, and $\Delta W_6 = 0$.
- $\Delta T_6 = \Delta f_6 + \Delta Q_3 + \Delta W_6 = (-2^{25} - 2^{21} - 2^{16} - 2^{11} - 2^{10} - 2^5 + 2^3) + (\pm 2^{31} + 2^{25} + 2^{16} + 2^{11} + 2^5) + 0 = \pm 2^{31} - 2^{21} - 2^{10} + 2^3$.
  - the add-differences (-2^{25}) and ($+2^{25}$) cancel each other out,
  - the add-differences (-2^{16}) and ($+2^{16}$) cancel each other out,
  - the add-differences (-2^{11}) and ($+2^{11}$) cancel each other out, and

- the add-differences (-2^5) and (+2^5) cancel each other out.

– Condition(s) on ΔT_6:
  - $\Delta T_6[31] = 0$ ensures that the add difference is +2^{31} (condition III). The probability that this condition holds is (2^{-1}) since $\Delta T_6[31] = 0$ rather than $T_6[31] = (0, 1)$.
  - Δ = (-2^{21}) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - $2^{-1}1$) since 1 $\in T_6$[31 - 21] to ensure there is no propagation past bit 31.
  - Δ = (-2^{10} + 2^3) must not propagate past bit 14 since we do not want to affect lower order bits (condition I). The probability that this condition holds is (1 - 2^{-5}) $\times$ (1 - 2^{-7}) since 1 $\in T_6$[14 - 10] and 0 $\in T_6$[9 - 3] to ensure there is no propagation past bit 14.

– $S(6)$ = 17, so ΔT_6 = +2^{31} - 2^{21} - 2^{10} + 2^3 $\Rightarrow$ ΔR_6 = +$2^{31+17=48\equiv 16(mod 32)}$ - $2^{21+17=38\equiv 6(mod 32)}$ - $2^{10+17=27}$ + $2^{3+17=20}$ = -2^{27} + 2^{20} + 2^{16} - 2^6.

– ΔQ_7 = ΔQ_6+ ΔR_6 = ($\pm 2^{31}$ - 2^{20} - 2^{16}) + (-2^{27} + 2^{20} + 2^{16} - 2^6) = $\pm 2^{31}$ - 2^{27} - 2^6.
  - the add-differences (-2^{20}) and (-2^{20}) cancel each other out, and
  - the add-differences (-2^{16}) and (+2^{16}) cancel each other out.

Step 7:

– ΔQ_7 = $\pm 2^{31}$ - 2^{27} - 2^6.

– Δf_7 = $\pm 2^{31}$ - 2^{27} + 2^{16}, ΔQ_4 = $\pm 2^{31}$ + 2^{25} + 2^5 - 2^1, and $\Delta W_7 = 0$.

– ΔT_7 = Δf_7 + ΔQ_4 + ΔW_7 = ($\pm 2^{31}$ - 2^{27} + 2^{16}) + ($\pm 2^{31}$ + 2^{25} + 2^5 - 2^1) + 0 = -2^{27} + 2^{25} + 2^{16} + 2^5 - 2^1.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.

– Condition(s) on ΔT_7:
  - Δ = (-2^{27} + 2^{25} +2^{16}) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-5}) $\times$ (1 - 2^{-2}) $\times$ (1 - 2^{-9}) since 1 $\in T_7$[31 - 27], 0 $\in T_7$[2^6, 25], and 0 $\in T_7$[24 - 16] to ensure there is no propagation past bit 31.
  - Δ = (+2^5 - 2^1) must not propagate past bit 9 since we do not want to affect lower order bits (condition I). The probability that this condition holds is (1 - 2^{-5}) $\times$ (1 - 2^{-4}) since 0 $\in T_7$[9 - 5] and 1 $\in T_7$[4 - 1] to ensure there is no propagation past bit 9.

– $S(7)$ = 22, so ΔT_7 = -2^{27} + 2^{25} + 2^{16} + 2^5 - 2^1 $\Rightarrow$ ΔR_7 = -$2^{27+22=49\equiv 17(mod 32)}$ + $2^{25+22=47\equiv 15(mod 32)}$ + $2^{16+22=38\equiv 6(mod 32)}$ + $2^{5+22=27}$ - $2^{1+22=23}$ = +2^{27} - 2^{23} - 2^{17} + 2^{15} + 2^6.

– ΔQ_8 = ΔQ_7 + ΔR_7 = ($\pm 2^{31}$ - 2^{27} - 2^6) + (+2^{27} - 2^{23} - 2^{17} + 2^{15} + 2^6) = $\pm 2^{31}$ - 2^{23} - 2^{17} + 2^{15}.
  - the add-differences (-2^{27}) and (+2^{27}) cancel each other out, and
  - the add-differences (-2^6) and (+2^6) cancel each other out.

Step 8:

– ΔQ_8 = $\pm 2^{31}$ - 2^{23} - 2^{17} + 2^{15}.

– Δf_8 = +2^{25} + 2^{16} - 2^6, ΔQ_5 = $\pm 2^{31}$ + 2^{10} - 2^8 + 2^6 + 2^0, and ΔW_8.

- $\Delta T_8 = \Delta f_8 + \Delta Q_5 + \Delta W_8 = (+2^{25} + 2^{16}$ - $2^6) + (\pm 2^{31} + 2^{10}$ - $2^8 + 2^6 + 2^0) + 0 = \pm 2^{31} + 2^{25} + 2^{16} + 2^{10}$ - $2^8 + 2^0$.
  - the add-differences (-2^6) and (+2^6) cancel each other out.
- Condition(s) on ΔT_8:
  - $\Delta T_8[31] = 1$ ensures that the add difference is -2^{31} (condition III). The probability that this condition holds is (2^{-1}) since $\Delta T_8[31] = 1$ rather than $T_8[31] = (0, 1)$.
  - $\Delta = (+2^{25})$ must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-7}) since $0 \in T_8[31$ - $25]$ to ensure there is no propagation past bit 31.
  - $\Delta = (+2^{16} + 2^{10}$ - $28 + 20)$ must not propagate past bit 24 since we do not want to affect lower order bits (condition I). The probability that this condition holds is (1 - 2^{-9}) $\times$ (1 - 2^{-6}) $\times$ (1 - 2^{-2}) $\times$ (1 - 2^{-8}) since $0 \in T_8[24$ - $16]$, $0 \in T_8[15$ - $10]$, $1 \in T_8[9, 8]$, and $0 \in T_8[7$ - $0]$ to ensure there is no propagation past bit 24.
- $S(8) = 7$, so $\Delta T_8 = \pm 2^{31} + 2^{25} + 2^{16} + 2^{10}$ - $2^8 + 2^0 \Rightarrow \Delta R_8 =$ -$2^{31+7=38\equiv 6 (mod 32)} + 2^{25+7=32\equiv 0 (mod 32)} + 2^{16+7=23} + 2^{10+7=17}$ - $2^{8+7=15} + 2^{0+7=7} = +2^{23} + 2^{17}$ - $2^{15} + (2^7$ - $2^6) + 2^0 = +2^{23} + 2^{17}$ - $2^{15} + 2^6 + 2^0$.
- $\Delta Q_9 = \Delta Q_8 + \Delta R_8 = (\pm 2^{31}$ - 2^{23} - $2^{17} + 2^{15}) + (+2^{23} + 2^{17}$ - 2^{15} - $2^6 + 2^0) = \pm 2^{31} + 2^6 + 2^0$.
  - the add-differences (-2^{23}) and (+2^{23}) cancel each other out,
  - the add-differences (-2^{17}) and (+2^{17}) cancel each other out, and
  - the add-differences (+2^{15}) and (-2^{15}) cancel each other out.

Step 9:

- $\Delta Q_9 = \pm 2^{31} + 2^6 + 2^0$.
- $\Delta f_9 = \pm 2^{31}$ - $2^{26} + 2^{16} + 2^0$, $\Delta Q_6 = \pm 2^{31}$ - 2^{20} - 2^{16}, and $\Delta W_9 = 0$.
- $\Delta T_9 = \Delta f_9 + \Delta Q_6 + \Delta W_9 = (\pm 2^{31}$ - $2^{26} + 2^{16} + 2^0) + (\pm 2^{31}$ - 2^{20} - $2^{16}) + 0 =$ -2^{26} - $2^{20} + 2^0$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}, and
  - the add-differences (+2^{16}) and (-2^{16}) cancel each other out.
- Condition(s) on ΔT_9:
  - $\Delta =$ (-2^{26} - 2^{20}) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-6}) $\times$ (1 - 2^{-6}) since $1 \in T_9[31$ - $26]$ and $1 \in T_9[25$ - $20]$ to ensure there is no propagation past bit 31.
  - $\Delta = (+2^0)$ must not propagate past bit 19 since we do not want to affect lower order bits (condition I). The probability that this condition holds is (1 - 2^{-20}) since $0 \in T_9[19$ - $0]$ to ensure there is no propagation past bit 19.
- $S(9) = 12$, so $\Delta T_9 =$ -2^{26} - $2^{20} + 2^0 \Rightarrow \Delta R_9 =$ -$2^{26+12=38\equiv 6 (mod 32)}$ - $2^{20+12=32\equiv 0 (mod 32)} + 2^{0+12=12} = +2^{12}$ - 2^6 - 2^0.
- $\Delta Q_{10} = \Delta Q_9 + \Delta R_9 = (\pm 2^{31} + 2^6 + 2^0) + (+2^{12}$ - 2^6 - $2^0) = \pm 2^{31} + 2^{12}$.
  - the add-differences (+2^6) and (-2^6) cancel each other out, and
  - the add-differences (+2^0) and (-2^0) cancel each other out.

Step 10:

- ΔQ_{10} = ±2^{31} + 2^{12}.
- Δf_{10} = ±2^{31} + 2^{6}, ΔQ_7 = ±2^{31} - 2^{27} - 2^{6}, and ΔW_{10} = 0.
- ΔT_{10} = Δf_{10} + ΔQ_7 + ΔW_{10} = (±2^{31} + 2^{6}) + (±2^{31} - 2^{27} - 2^{6}) + 0 = -2^{27}.
  - the add-differences (±2^{31}) and (±2^{31}) cancel each other out modulo 2^{32}, and
  - the add-differences (+2^{6}) and (-2^{6}) cancel each other out.
- Condition(s) on ΔT_{10}:
  - Δ = (-2^{27}) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-5}) since 1 $\in T_{10}$[31 - 27] to ensure there is no propagation past bit 31.
- $S(10)$ = 17, so ΔT_{10} = -2^{27} $\Rightarrow$ ΔR_{10} = -$2^{27+17=44\equiv12(mod32)}$ = -2^{12}.
- ΔQ_{11} = ΔQ_{10} + ΔR_{10} = (±2^{31} + 2^{12}) + (-2^{12}) = ±2^{31}.
  - the add-differences (+2^{12}) and (-2^{12}) cancel each other out.

Step 11:

- ΔQ_{11} = ±2^{31}.
- Δf_{11} = ±2^{31}, ΔQ_8 = ±2^{31} - 2^{23} - 2^{17} + 2^{15}, and ΔW_{11} = -2^{15}.
- ΔT_{11} = Δf_{11} + ΔQ_8 + ΔW_{11} = (±2^{31}) + (±2^{31} - 2^{23} - 2^{17} + 2^{15}) + (-2^{15}) = -2^{23} - 2^{17}.
  - the add-differences (±2^{31}) and (±2^{31}) cancel each other out modulo 2^{32}, and
  - the add-differences (+2^{15}) and (-2^{15}) cancel each other out.
- Condition(s) on ΔT_{11}:
  - Δ = (-2^{23} - 2^{17}) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-9}) × (1 - 2^{-6}) since 1 $\in T_{11}$[31 - 23] and 1 $\in T_{11}$[22 - 17] to ensure there is no propagation past bit 31.
- $S(11)$ = 22, so ΔT_{11} = -2^{23} - 2^{17} $\Rightarrow$ ΔR_{11} = -$2^{23+22=45\equiv13(mod32)}$ - $2^{17+22=39\equiv7(mod32)}$ = -2^{13} - 2^{7}.
- ΔQ_{12} = ΔQ_{11} + ΔR_{11} = (±2^{31}) + (-2^{13} - 2^{7}) = ±2^{31} - 2^{13} - 2^{7}.

Step 12:

- ΔQ_{12} = ±2^{31} - 2^{13} - 2^{7}.
- Δf_{12} = ±2^{31} + 2^{17}, ΔQ_9 = ±2^{31} + 2^{6} + 2^{0}, and ΔW_{12} = 0.
- ΔT_{12} = Δf_{12} + ΔQ_9 + ΔW_{12} = (±2^{31} + 2^{17}) + (±2^{31} + 2^{6} + 2^{0}) + 0 = +2^{17} + 2^{6} + 2^{0}.
  - the add-differences (±2^{31}) and (±2^{31}) cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{12}:
  - Δ = (+2^{17} + 2^{6} + 2^{0}) must not propagate past bit 24 since we do not want to affect lower order bits (condition I). The probability that this condition holds is (1 - 2^{-8}) × (1 - 2^{-11}) × (1 - 2^{-6}) since 0 $\in T_{12}$[24 - 17], 0 $\in T_{12}$[16 - 6], and 0 $\in T_{12}$[5 - 0] to ensure there is no propagation past bit 24.
- $S(12)$ = 7, so ΔT_{12} = +2^{17} + 2^{6} + 2^{0} $\Rightarrow$ ΔR_{12} = +$2^{17+7=24}$ + $2^{6+7=13}$ + $2^{0+7=7}$ = +2^{24} + 2^{13} + 2^{7}.
- ΔQ_{13} = ΔQ_{12} + ΔR_{12} = (±2^{31} - 2^{13} - 2^{7}) + (+2^{24} + 2^{13} + 27) = ±2^{31} + 2^{24}.
  - the add-differences (-2^{13}) and (+2^{13}) cancel each other out, and
  - the add-differences (-2^{7}) and (+2^{7}) cancel each other out.

Step 13:

- $\Delta Q_{13} = \pm 2^{31} + 2^{24}$.
- $\Delta f_{13} = \pm 2^{31}$ - 2^{13}, $\Delta Q_{10} = \pm 2^{31} + 2^{12}$, and $\Delta W_{13} = 0$.
- $\Delta T_{13} = \Delta f_{13} + \Delta Q_{10} + \Delta W_{13} = (\pm 2^{31}$ - $2^{13}) + (\pm 2^{31} + 2^{12}) + 0 =$ -2^{12}.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
  - the add-differences (-2^{13}) and (+2^{12}) combine to yield (-2^{12}).
- Condition(s) on ΔT_{13}:
  - Δ = (-2^{12}) must not propagate past bit 19 since we do not want to affect lower order bits (condition I). The probability that this condition holds is (1 - 2^{-8}) since $1 \in T_{13}[19$ - $12]$ to ensure there is no propagation past bit 19.
- $S(13) = 12$, so ΔT_{13} = -$2^{12} \Rightarrow \Delta R_{13}$ = -$2^{12+12=24}$ = -2^{24}.
- $\Delta Q_{14} = \Delta Q_{13} + \Delta R_{13} = (\pm 2^{31} + 2^{24}) + (-2^{24}) = \pm 2^{31}$.
  - the add-differences (+2^{24}) and (-2^{24}) cancel each other out.

Step 14:

- $\Delta Q_{14} = \pm 2^{31}$.
- $\Delta f_{14} = +2^{30} + 2^{18}$, $\Delta Q_{11} = \pm 2^{31}$, and $\Delta W_{14} = \pm 2^{31}$.
- $\Delta T_{14} = \Delta f_{12} + \Delta Q_{11} + \Delta W_{14} = (+2^{30} + 2^{18}) + (\pm 2^{31}) + (\pm 2^{31}) = +2^{30} + 2^{18}$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
  - Condition(s) on ΔT_{14}:
  - $\Delta = (+2^{30} + 2^{18})$ must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-2}) $\times$ (1 - 2^{-12}) since $0 \in T_{14}[31, 30]$ and $0 \in T_{14}[29$ - $18]$ to ensure there is no propagation past bit 31.
- $S(14) = 17$, so $\Delta T_{14} = +2^{30} + 2^{18} \Rightarrow \Delta R_{14} = +2^{30+17=47\equiv 15(mod 32)} + 2^{18+17=35\equiv 3(mod 32)} = +2^{15} + 2^{3}$.
- $\Delta Q_{15} = \Delta Q_{14} + \Delta R_{14} = (\pm 2^{31}) + (+2^{15} + 2^{3}) = \pm 2^{31} + 2^{15} + 2^{3}$.

Step 15:

- $\Delta Q_{15} = \pm 2^{31} + 2^{15} + 2^{3}$.
- $\Delta f_{15} = \pm 2^{31}$ - 2^{25}, $\Delta Q_{12} = \pm 2^{31}$ - 2^{13} - 27, and $\Delta W_{15} = 0$.
- $\Delta T_{15} = \Delta f_{15} + \Delta Q_{12} + \Delta W_{15} = (\pm 2^{31}$ - $2^{25}) + (\pm 2^{31}$ - 2^{13} - $27) + 0$ = -2^{25} - 2^{13} - 2^{7}.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{15}:
  - Δ = (-2^{25} - 2^{13}) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-7}) $\times$ (1 - 2^{-12}) since $1 \in T_{15}[31$ - $25]$ and $1 \in T_{15}[24$ - $13]$ to ensure there is no propagation past bit 31.
  - Δ = (-2^{7}) must not propagate past bit 9 since we do not want to affect any more low order bits upon rotation (condition I). The probability that this condition holds is (1 - 2^{-3}) since $1 \in T_{15}[9$ - $7]$ to ensure there is no propagation past bit 9.

- $S(15) = 22$, so ΔT_{15} = -2^{25} - 2^{13} - 2^7 $\Rightarrow$ ΔR_{15} = -$2^{25+22=47\equiv 15(mod32)}$ - $2^{13+22=35\equiv 3(mod32)}$ - $2^{7+22=29}$ = -2^{29} - 2^{15} - 2^3.
- $\Delta Q_{16} = \Delta Q_{15} + \Delta R_{15}$ = ($\pm 2^{31}$ + 2^{15} + 2^3) + (-2^{29} - 2^{15} - 2^3) = $\pm 2^{31}$ - 2^{29}.
  - the add-differences (+2^{15}) and (-2^{15}) cancel each other out, and
  - the add-differences (+2^3) and (-2^3) cancel each other out.

Step 16:

- ΔQ_{16} = $\pm 2^{31}$ - 2^{29}.
- $\Delta f_{16} = \pm 2^{31}$, $\Delta Q_{13} = \pm 2^{31} + 2^{24}$, and $\Delta W_{16} = 0$.
- $\Delta T_{16} = \Delta f_{16} + \Delta Q_{13} + \Delta W_{16} = (\pm 2^{31}) + (\pm 2^{31} + 2^{24}) + 0 = +2^{24}$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{16}:
  - Δ = (+2^{24}) must not propagate past bit 2^6 since we do not want to affect any more low order bits upon rotation (condition I). The probability that this condition holds is (1 - 2^{-3}) since $0 \in T_{16}[26 - 24]$ to ensure there is no propagation past bit 26.
- $S(16) = 5$, so $\Delta T_{16} = +2^{24} \Rightarrow \Delta R_{16} = +2^{24+5=29} = +2^{29}$.
- $\Delta Q_{17} = \Delta Q_{16} + \Delta R_{16}$ = ($\pm 2^{31}$ - 2^{29}) + (+2^{29}) = $\pm 2^{31}$.
  - the add-differences (-2^{29}) and (+2^{29}) cancel each other out.

Step 17:

- $\Delta Q_{17} = \pm 2^{31}$.
- $\Delta f_{17} = \pm 2^{31}$, $\Delta Q_{14} = \pm 2^{31}$, and $\Delta W_{17} = 0$.
- $\Delta T_{17} = \Delta f_{17} + \Delta Q_{14} + \Delta W_{17} = (\pm 2^{31}) + (\pm 2^{31}) + 0 = 0$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{17}: none
- $\Delta T_{17} = 0 \Rightarrow \Delta R_{17} = 0$.
- $\Delta Q_{18} = \Delta Q_{17} + \Delta R_{17} = (\pm 2^{31}) + (0) = \pm 2^{31}$.

Step 18:

- $\Delta Q_{18} = \pm 2^{31}$.
- $\Delta f_{18} = \pm 2^{31}$, $\Delta Q_{15} = \pm 2^{31} + 2^{15} + 2^3$, and ΔW_{18} = -2^{15}.
- $\Delta T_{18} = \Delta f_{18} + \Delta Q_{15} + \Delta W_{18}$ = ($\pm 2^{31}$) + ($\pm 2^{31}$ + 2^{15} + 2^3) + (-2^{15}) = +23.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}, and
  - the add-differences (+2^{15}) and (-2^{15}) cancel each other out.
- Condition(s) on ΔT_{18}:
  - Δ = (+23) must not propagate past bit 17 since we do not want to affect any more low order bits upon rotation (condition I). The probability that this condition holds is (1 - 2^{-15}) since $0 \in T_{18}[17 - 3]$ to ensure there is no propagation past bit 17.

- $S(18) = 14$, so $\Delta T_{18} = +2^3 \Rightarrow \Delta R_{18} = +2^{3+14=17} = +2^{17}$. $\Delta Q_{19} = \Delta Q_{18} + \Delta R_{18} = (\pm 2^{31}) + (+2^{17}) = \pm 2^{31} + 2^{17}$.

Step 19:

- $\Delta Q_{19} = \pm 2^{31} + 2^{17}$.
- $\Delta f_{19} = \pm 2^{31}$, $\Delta Q_{16} = \pm 2^{31}$ - 2^{29}, and $\Delta W_{19} = 0$.
- $\Delta T_{19} = \Delta f_{19} + \Delta Q_{16} + \Delta W_{19} = (\pm 2^{31}) + (\pm 2^{31}$ - $2^{29}) + 0 =$ -2^{29}.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{19}:
  - Δ = (-2^{29}) must not propagate past bit 31 since we do not want to affect lower order bits (condition III). The probability that this condition holds is (1 - 2^{-3}) since $1 \in T_{19}[31$ - $29]$ to ensure there is no propagation past bit 31.
- $S(19) = 20$, so $\Delta T_{19} =$ -$2^{29} \Rightarrow \Delta R_{19} =$ -$2^{29+20=4917 (mod 32)} =$ -2^{17}.
- $\Delta Q_{20} = \Delta Q_{19} + \Delta R_{19} = (\pm 2^{31} + 2^{17}) + (\text{-}2^{17}) = \pm 2^{31}$.
  - the add-differences ($+2^{17}$) and (-2^{17}) cancel each other out.

Steps 20 to 21:

- $\Delta Q_t = \pm 2^{31}$.
- $\Delta f_t = \pm 2^{31}$, $\Delta Q_{t-3} = \pm 2^{31}$, and $\Delta W_t = 0$.
- $\Delta T_t = \Delta f_t + \Delta Q_{t-3} + \Delta W_t = (\pm 2^{31}) + (\pm 2^{31}) + 0 = 0$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_t: none
- $\Delta T_t = 0 \Rightarrow \Delta R_t$ 0.
- $\Delta Q_{t+1} = \Delta Q_t + \Delta R_t = (\pm 2^{31}) + 0 = \pm 2^{31}$.

Step 22:

- $\Delta Q_{22} = \pm 2^{31}$.
- $\Delta f_{22} = \pm 2^{31}$, $\Delta Q_{19} = \pm 2^{31} + 2^{17}$, and $\Delta W_{22} = 0$.
- $\Delta T_{22} = \Delta f_{22} + \Delta Q_{19} + \Delta W_{22} = (\pm 2^{31}) + (\pm 2^{31} + 2^{17}) + 0 = +2^{17}$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{22}:
  - Δ = ($+2^{17}$) must not propagate past bit 17 since we do not want to affect lower order bits (condition I). The probability that this condition holds is (2^{-1}) since $T_{22}[17] = 0$ to ensure there is no propagation past bit 17.
- $S(22) = 14$, so $\Delta T_{22} = +2^{17} \Rightarrow \Delta R_{22} = +2^{17+14=31} = +2^{31}$.
- $\Delta Q_{23} = \Delta Q_{22} + \Delta R_{22} = (\pm 2^{31}) + (\pm 2^{31}) = 0$.
  - the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.

Step 23:

- $\Delta Q_{23} = 0$.
- $\Delta f_{23} = 0$, $\Delta Q_{20} = \pm 2^{31}$, and $\Delta W_{23} = \pm 2^{31}$.
- $\Delta T_{23} = \Delta f_{23} + \Delta Q_{20} + \Delta W_{23} = 0 + (\pm 2^{31}) + (\pm 2^{31}) = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{23}: none
- $\Delta T_{23} = 0 \Rightarrow \Delta R_{23} = 0$.
- $\Delta Q_{24} = \Delta Q_{23} + \Delta R_{23} = 0 + 0 = 0$.

Step 24:

- $\Delta Q_{24} = 0$.
- $\Delta f_{24} = \pm 2^{31}$, $\Delta Q_{21} = \pm 2^{31}$, and $\Delta W_{24} = 0$.
- $\Delta T_{24} = \Delta f_{24} + \Delta Q_{21} + \Delta W_{24} = (\pm 2^{31}) + (\pm 2^{31}) + 0 = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{24}: none
- $\Delta T_{24} = 0 \Rightarrow \Delta R_{24} = 0$.
- $\Delta Q_{25} = \Delta Q_{24} + \Delta R_{24} = 0 + 0 = 0$.

Step 25:

- $\Delta Q_{25} = 0$.
- $\Delta f_{25} = 0$, $\Delta Q_{22} = \pm 2^{31}$, and $\Delta W_{25} = \pm 2^{31}$.
- $\Delta T_{25} = \Delta f_{25} + \Delta Q_{22} + \Delta W_{25} = 0 + (\pm 2^{31}) + (\pm 2^{31}) = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{25}: none
- $\Delta T_{25} = 0 \Rightarrow \Delta R_{25} = 0$.
- $\Delta Q_{26} = \Delta Q_{25} + \Delta R_{25} = 0 + 0 = 0$.

Steps 26 to 33:

- $\Delta Q_t = 0$.
- $\Delta f_t = \Delta Q_{t-3} = \Delta W_t = 0$.
- $\Delta T_t = \Delta f_t + \Delta Q_{t-3} + \Delta W_t = 0 + 0 + 0 = 0$.
- Condition(s) on ΔT_t: none
- $\Delta T_t = 0 \Rightarrow \Delta R_t = 0$.
- $\Delta Q_{t+1} = \Delta Q_t + \Delta R_t = 0 + 0 = 0$.

Step 34:

- $\Delta Q_{34} = 0$.
- $\Delta f_{34} = 0$, $\Delta Q_{31} = 0$, and $\Delta W_{34} = +2^{15}$.
- $\Delta T_{34} = \Delta f_{34} + \Delta Q_{31} + \Delta W_{34} = 0 + 0 + (\text{-}2^{15}) = \text{-}2^{15}$.
- Condition(s) on ΔT_{34}:
  - $\Delta = (\text{-}2^{15})$ must not propagate past bit 15 since we do not want to affect lower order bits (condition I). The probability that this condition holds is (2^{-1}) since $T^{34}[15] = 1$ to ensure there is no propagation past bit 15.
- $S(34) = 16$, so $\Delta T_{34} = \text{-}2^{15} \Rightarrow \Delta R_{34} = \text{-}2^{15+16=31} = \text{-}2^{31}$.
- $\Delta Q_{35} = \Delta Q_{34} + \Delta R_{34} = 0 + (\pm 2^{31}) = \pm 2^{31}$.

Step 35:

- $\Delta Q_{35} = \pm 2^{31}$.
- $\Delta f_{35} = \pm 2^{31}$, $\Delta Q_{32} = 0$, and $\Delta W_{35} = \pm 2^{31}$.
- $\Delta T_{35} = \Delta f_{35} + \Delta Q_{32} + \Delta W_{35} = (\pm 2^{31}) + 0 + (\pm 2^{31}) = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{35}: none
- $\Delta T_{35} = 0 \Rightarrow \Delta R_{35} = 0$.
- $\Delta Q_{36} = \Delta Q_{35} + \Delta R_{35} = (\pm 2^{31}) + 0 = \pm 2^{31}$.

Step 36:

- $\Delta Q_{36} = \pm 2^{31}$.
- $\Delta f_{36} = 0$, $\Delta Q_{33} = 0$, and $\Delta W_{36} = 0$.
- $\Delta T_{36} = \Delta f_{36} + \Delta Q_{33} + \Delta W_{36} = 0 + 0 + 0 = 0$.
- Condition(s) on ΔT_{36}: none
- $\Delta T_{36} = 0 \Rightarrow \Delta R_{36} = 0$.
- $\Delta Q_{37} = \Delta Q_{36} + \Delta R_{36} = (\pm 2^{31}) + 0 = \pm 2^{31}$.

Step 37:

- $\Delta Q_{37} = \pm 2^{31}$.
- $\Delta f_{37} = \pm 2^{31}$, $\Delta Q_{34} = 0$, and $\Delta W_{37} = \pm 2^{31}$.
- $\Delta T_{37} = \Delta f_{37} + \Delta Q_{34} + \Delta W_{37} = (\pm 2^{31}) + 0 + (\pm 2^{31}) = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{37}: none
- $\Delta T_{37} = 0 \Rightarrow \Delta R_{37} = 0$.
- $\Delta Q_{38} = \Delta Q_{37} + \Delta R_{37} = (\pm 2^{31}) + 0 = \pm 2^{31}$.

Steps 38 to 49:

- $\Delta Q_t = \pm 2^{31}$.
- $\Delta f_t = \pm 2^{31}$, $\Delta Q_{t-3} = \pm 2^{31}$, and $\Delta W_t = 0$.
- $\Delta T_t = \Delta f_t + \Delta Q_{t-3} + \Delta W_t = (\pm 2^{31}) + (\pm 2^{31}) + 0 = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_t: none
- $\Delta T_t = 0 \Rightarrow \Delta R_t = 0$.
- $\Delta Q_{t+1} = \Delta Q_t + \Delta R_t = (\pm 2^{31}) + 0 = 0$.

Step 50:

- $\Delta Q_{50} = \pm 2^{31}$.
- $\Delta f_{50} = 0$, $\Delta Q_{47} = \pm 2^{31}$, and $\Delta W_{50} = \pm 2^{31}$.
- $\Delta T_{50} = \Delta f_{50} + \Delta Q_{47} + \Delta W_{50} = 0 + (\pm 2^{31}) + (\pm 2^{31}) = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{50}: none
- $\Delta T_{50} = 0 \Rightarrow \Delta R_{50} = 0$.
- $\Delta Q_{51} = \Delta Q_{50} + \Delta R_{50} = (\pm 2^{31}) + 0 = \pm 2^{31}$.

Steps 51 to 59:

- $\Delta Q_t = \pm 2^{31}$.
- $\Delta f_t = \pm 2^{31}$, $\Delta Q_{t-3} = \pm 2^{31}$, and $\Delta W_t = 0$.
- $\Delta T_t = \Delta f_t + \Delta Q_{t-3} + \Delta W_t = (\pm 2^{31}) + (\pm 2^{31}) + 0 = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_t: none
- $\Delta T_t = 0 \Rightarrow \Delta R_t = 0$.
- $\Delta Q_{t+1} = \Delta Q_t + \Delta R_t = (\pm 2^{31}) + 0 = 0$.

Step 60:

- $\Delta Q_{60} = \pm 2^{31}$.
- $\Delta f_{60} = 0$, $\Delta Q_{57} = \pm 2^{31}$, and $\Delta W_6 0 = \pm 2^{31}$.
- $\Delta T_{60} = \Delta f_{60} + \Delta Q_{58} + \Delta W_{60} = 0 + (\pm 2^{31}) + (\pm 2^{31}) = 0$.
  - the add-differences $(\pm 2^{31})$ and $(\pm 2^{31})$ cancel each other out modulo 2^{32}.
- Condition(s) on ΔT_{60}: none
- $\Delta T_{60} = 0 \Rightarrow \Delta R_{60} = 0$.
- $\Delta Q_{61} = \Delta Q_{60} + \Delta R_{60} = (\pm 2^{31}) + 0 = \pm 2^{31}$.

Step 61:

– $\Delta Q_{61} = \pm 2^{31}$.
– $\Delta f_{61} = \pm 2^{31}$, $\Delta Q_{58} = \pm 2^{31}$, and $\Delta W_{61} = +2^{15}$.
– $\Delta T_{61} = \Delta f_{61} + \Delta Q_{58} + \Delta R_{61} = (\pm 2^{31}) + (\pm 2^{31}) + (-2^{15}) = -2^{15}$.
  • the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
– Condition(s) on ΔT_{61}:
  • $\Delta = (-2^{15})$ must not propagate past bit 21 since we do not want to affect lower order bits (condition I). The probability that this condition holds is $(1 - 2^{-7})$ since $1 \in \Delta T_{61}[21 - 15]$ to ensure there is no propagation past bit 21.
– $S(61) = 10$, so $\Delta T_{61} = -2^{15} \Rightarrow \Delta R_{61} = -2^{15+10=25} = -2^{25}$.
– $\Delta Q_{62} = \Delta Q_{61} + \Delta R_{61} = (\pm 2^{31}) + (-2^{25}) = \pm 2^{31} - 2^{25}$.

Steps 62 to 63:

– $\Delta Q_t = \pm 2^{31} - 2^{25}$.
– $\Delta f_t = \pm 2^{31}$, $\Delta Q_{t-3} = \pm 2^{31}$, and $\Delta W_t = 0$.
– $\Delta T_t = \Delta f_t + \Delta Q_{t-3} + \Delta W_t = (\pm 2^{31}) + (\pm 2^{31}) + 0 = 0$.
  • the add-differences ($\pm 2^{31}$) and ($\pm 2^{31}$) cancel each other out modulo 2^{32}.
– Condition(s) on ΔT_t: none
– $\Delta T_t = 0 \Rightarrow \Delta R_t = 0$.
– $\Delta Q_{t+1} = \Delta Q_t + \Delta R_t = (\pm 2^{31} - 2^{25}) + 0 = \pm 2^{31} - 2^{25}$.

Assuming all of our conditions are met, the end result of the differential for the second block is

$$\begin{aligned}\Delta Q_{61} &= \pm 2^{31},\\ \Delta Q_{62} &= \pm 2^{31} - 2^{25},\\ \Delta Q_{63} &= \pm 2^{31} - 2^{25},\\ \Delta Q_{64} &= \pm 2^{31} - 2^{25}.\end{aligned}$$

Thus, we have our collision:

$$\begin{aligned}\Delta IHV^{(2)}[0] &= \Delta IHV^{(1)}[0] + \Delta Q_{61} = (\pm 2^{31}) + (\pm 2^{31}) = 0,\\ \Delta IHV^{(2)}[3] &= \Delta IHV^{(1)}[3] + \Delta Q_{62} = (\pm 2^{31} - 2^{25}) + (\pm 2^{31} + 2^{25}) = 0,\\ \Delta IHV^{(2)}[2] &= \Delta IHV^{(1)}[2] + \Delta Q_{63} = (\pm 2^{31} - 2^{25}) + (\pm 2^{31} + 2^{25}) = 0,\\ \Delta IHV^{(2)}[1] &= \Delta IHV^{(1)}[1] + \Delta Q_{64} = (\pm 2^{31} - 2^{25}) + (\pm 2^{31} + 2^{25}) = 0.\end{aligned}$$

6.4 Summary of the Probabilities of the Conditions for the First Block

For each step in both blocks, the probabilities for the conditions on the ΔT_t were presented. These probabilities will now be summarized. For the first block, we have the following. Note that only the steps with conditions are shown.

Step 4: $(2^{-1}) = 0.500$

Step 5: $(2^{-1}) \times (1 - 2^{-8}) = 0.498$
Step 6: $(2^{-1}) \times (1 - 2^{-4}) = 0.469$
Step 7: $(1 - 2^{-5}) \times (1 - 2^{-2}) \times (1 - 2^{-9}) \times (1 - 2^{-8}) \times (2^{-5}) = 0.0226$
Step 8: $(2^{-1}) \times (2^{-1}) \times (1 - 2^{-8}) \times (1 - 2^{-6}) \times (1 - 2^{-2}) = 0.184$
Step 9: $(1 - 2^{-6}) \times (1 - 2^{-6}) \times (1 - 2^{-20}) = 0.969$
Step 10: $(1 - 2^{-5}) \times (1 - 2^{-3}) = 0.848$
Step 11: $(1 - 2^{-9}) \times (1 - 2^{-6}) \times (1 - 2^{-2}) = 0.737$
Step 12: $(1 - 2^{-8}) \times (1 - 2^{-11}) \times (1 - 2^{-6}) = 0.980$ Step 13: $(1 - 2^{-8}) = 0.996$
Step 14: $(1 - 2^{-2}) \times (1 - 2^{-12}) = 0.750$
Step 15: $(1 - 2^{-7}) \times (1 - 2^{-12}) \times (1 - 2^{-3}) = 0.868$
Step 16: $(1 - 2^{-3}) = 0.875$
Step 18: $(1 - 2^{-15}) = 1.000$
Step 19: $(1 - 2^{-3}) = 0.875$
Step 22: $(2^{-1}) = 0.500$
Step 34: $(2^{-1}) = 0.500$
Step 61: $(1 - 2^{-7}) = 0.992$

We denote P^1_{0-63} to be the probability that the conditions on ΔT_t will hold for all 64 steps of the first block. P^1_{0-63} is simply the product of the probabilities shown above. We find that it is:

$$P^1_{0-63} \approx 3.54 \times 10^{-5} \approx 2^{-14.8}.$$

Thus, for a random message, all of the conditions for ΔT_t will hold with probability $2^{-14.8}$. Suppose we define a "ΔT_t-good" message M to be a message such that the conditions for the first round (steps 0 to 15) of the first block are satisfied. A cryptanalyst can readily compute "ΔT_t-good" messages by using single-message modification. The probability that a "ΔT_t-good" message satisfies all of the conditions for the first iteration is then the probability that it satisfies all the probabilities from rounds 2 to 4 (steps 16 to 63). We find this probability, P^1_{16-63} to be

$$P^1_{16-63} \approx 0.190 \approx 2^{-2.4}.$$

Thus, with probability $2^{-2.4}$, a cryptanalyst using single-message modification can satisfy all the conditions for ΔT_t of the first block.

6.5 Summary of the Probabilities of the Conditions for the Second Block

The probability of the conditions on the ΔT_t for each step of the second block is as follows. Note that only the steps with conditions are shown.

Step 1: $(1 - 2^{-7}) = 0.992$
Step 2: $(2^{-1}) \times (1 - 2^{-6}) = 0.492$
Step 3: $(1 - 2^{-6}) \times (1 - 2^{-5}) \times (1 - 2^{1}0) = 0.953$
Step 4: $(1 - 2^{-2}) \times (1 - 2^{-4}) \times (2^{-1}) \times (1 - 2^{-7}) \times (1 - 2^{-15}) \times (1 - 2^{-2}) = 0.262$
Step 5: $(1 - 2^{-2}) \times (1 - 2^{-2}) \times (1 - 2^{-2}) \times (1 - 2^{-6}) \times (1 - 2^{-12}) \times (1 - 2^{-4}) = 0.389$
Step 6: $(2^{-1}) \times (1 - 2^{-11}) \times (1 - 2^{-5}) \times (1 - 2^{-7}) = 0.480$
Step 7: $(1 - 2^{-5}) \times (1 - 2^{-2}) \times (1 - 2^{-9}) \times (1 - 2^{-5}) \times (1 - 2^{-4}) = 0.659$
Step 8: $(2^{-1}) \times (1 - 2^{-7}) \times (1 - 2^{-9}) \times (1 - 2^{-6}) \times (1 - 2^{-2}) \times (1 - 2^{-8}) = 0.364$

Step 9: (1 - 2^{-6}) $\times$ (1 - 2^{-6}) $\times$ (1 - 2^{-20}) = 0.969
Step 10: (1 - 2^{-5}) = 0.969
Step 11: (1 - 2^{-9}) $\times$ (1 - 2^{-6}) = 0.982
Step 12: (1 - 2^{-8}) $\times$ (1 - 2^{-11}) (1 - 2^{-6}) = 0.980
Step 13: (1 - 2^{-8}) = 0.996
Step 14: (1 - 2^{-2}) $\times$ (1 - 2^{-12}) = 0.750
Step 15: (1 - 2^{-7}) $\times$ (1 - 2^{-12}) $\times$ (1 - 2^{-3}) = 0.868
Step 16: (1 - 2^{-3}) = 0.875
Step 18: (1 - 2^{-15}) = 1.000
Step 19: (1 - 2^{-3}) = 0.875
Step 22: (2^{-1}) = 0.500
Step 34: (2^{-1}) = 0.500
Step 61: (1 - 2^{-7}) = 0.992

We denote P^2_{0-63} to be the probability that the conditions on ΔT_t will hold for all 64 steps of the second block. P^1_{0-63} is simply of the probabilities shown above. We find that it is:

$$P^1_{0-63} \approx 6.07 \times 10^{-4} \approx 2^{-10.7}.$$

Thus, for a random message, all of the conditions for ΔT_t will hold with probability $2^{-10.7}$. Again, a cryptanalyst can readily compute "T_t-good" messages using single-message modification. The probability that a "T_t-good" message satisfies all of the conditions for the first iteration is then the probability that it satisfies steps 16 to 63. We find this probability, P^2_{16-63} to be

$$P^2_{16-63} \approx 0.190 \approx 2^{-2.4}.$$

Thus, with probability $2^{-2.4}$, a cryptanalyst using single-message modification can satisfy all the conditions for ΔT_t of the second block.

7 Conditions for the Propagation of the Differences Through the f_t Functions

In presenting the conditions of the propagation of the differences through the f_t functions, we have proven all of the assertions made in [3] regarding bit conditions for the first block except for those mentioned in the sections labeled "Obtaining the Correct ΔQ_t." The discussions provided for those conditions were sufficient. For all other conditions, however, proofs were necessary to provide to explain why each assertion was made. Therefore, after each assertion, the number of the proof that corresponds to that assertion is given. The proofs are then presented in section 8. Note that only the conditions for *Case One* are presented. (We will prove in section 9 that the conditions required for *Case Two* do not produce the desired collision differential.) For the second block, all of the assertions regarding bit conditions are original, based only on a few tables in [3]. As with the first block, after each assertion, the number of the proof that corresponds to that assertion is given. The proofs are then presented in section 8.

7.1 Conditions for the Propagation of the Differences Through the f_t Functions for the First Block

Round 1: $f_t = F(X,\ Y,\ Z)$

Steps 0 to 4:

We have $Q_{t-2} = 0$, $Q_{t-1} = 0$, and $Q_t = 0$, so we will obtain $f_t = 0$. There are no conditions for these steps.

Step 5:

We have $Q_3 = 0$, $Q_4 = 0$, and $Q_5 = -2^6$, and we want to obtain $f_5 = +2^{19} + 2^{11}$.

Obtaining the Correct Q_5:

- $Q_5[21 - 6] = 0$
- $Q_5[22] = 1$

The Constant Bits of Q_5:
$Q_5[j] = 0$, $j \in [31 - 23, 5 - 0]$

- To obtain $f_5[j] = 0$, no conditions are required for $Q_5 \in [31 - 23, 5 - 0]$.

The Non-Constant Bits of Q_5:
$Q_5[j] = +1$, $j \in [21 - 6]$

- To obtain $f_5[j] = 0$, we require $Q_3[j] = Q_4[j]$ for $j \in [21, 20, 18 - 12, 10 - 6]$. See proof 12.
- To obtain $f_5[j] = +1$, we require $Q_3[j] = 0$ and $Q_4[j] = 1$ for $j \in [19, 11]$. See proof 14.

$Q_5[j] = -1$, $j \in [22]$

- To obtain $f_5[j] = 0$, we require $Q_3[j] = Q_4[j]$ for $j \in [22]$. See proof 13.

Summary of the conditions for step 5:

- $Q_3[19, 11] = Q_5[21 - 6] = 0$
- $Q_4[19, 11] = Q_5[22] = 1$
- $Q_3[21, 20, 18 - 12, 10 - 6] = Q_4[21, 20, 18 - 12, 10 - 6]$

Step 6:

We have Q_4, $Q_5 = -2^6$, and $Q_6 = \pm 2^{31} + 2^{23} - 2^6$, and we want to obtain $f_6 = -2^{14} - 2^{10}$.

Obtaining the Correct Q_6:

- $Q_6[23] = 0$
- $Q_6[6] = 1$

The Constant Bits of Q_6:
$Q_6[j] = 0$, $j \in [30 - 24, 22 - 7, 5 - 0]$

- To obtain $f_6[j] = -1$, we require $Q_6[j] = 1$ for $j \in [22]$. See proof 25.
- To obtain $f_6[j] = +1$, we require $Q_6[j] = 1$ for $j \in [21 - 15, 13 - 10]$. See proof 23.
- To obtain $f_6[j] = 0$, we require $Q_6[j] = 0$ for $j \in [14, 9 - 7]$. See proof 22.
- To obtain $f_6[j] = 0$, we need no requirements for $Q_6[30 - 24, 5 - 0]$.

The Non-Constant Bits of Q_6:
$Q_6[j] = +1$, $j \in [23]$

- To obtain $f_6[j] = 0$, we require $Q_4[j] = Q_5[j]$ for $j \in [23]$. See proof 12.

$Q_6[j] =$ -1, $j \in [6]$

- To obtain $f_6[j] = 0$, we require $Q_4[j] = 0$ for $j \in [6]$. See proof 26.

$Q_6[j] = \pm 1$, $j \in [31]$

- To obtain $f_6[j] = 0$, we require $Q_4[j] = Q_5[j]$ for $j \in [31]$. See proof 1.

Summary of the conditions for step 6:

- $Q_4[6] = Q_6[23, 14, 9 - 7] = 0$
- $Q_6[22 - 15, 13 - 10, 6] = 1$
- $Q_4[31, 23] = Q_5[31, 23]$

Step 7:

We have $Q_5 = -2^6$, $Q_6 = \pm 2^{31} + 2^{23} - 2^6$, and $Q_7 = -2^{27} + 2^{23} - 2^6 - 2^0$, and we want to obtain $f_7 = -2^{27} - 2^{25} + 2^{16} + 2^{10} + 2^5 - 2^2$.

Obtaining the Correct Q_7:

- $Q_7[30 - 26, 10 - 6, 4 - 0] = 0$
- $Q_7[25 - 23, 11, 5] = 1$

The Constant Bits of Q_7:
$Q_7[j] = 0$, $j \in [22 - 12]$

- To obtain $f_7[j] = 0$, we require $Q_7[j] = 1$ for $j \in [22]$. See proof 20.
- To obtain $f_7[j] = 0$, we require $Q_7[j] = 1$ for $j \in [21 - 17, 15 - 12]$. See proof 18.
- To obtain $f_7[j] = +1$, we require $Q_7[j] = 0$ for $j \in [16]$. See proof 19.

The Non-Constant Bits of Q_7:
$Q_7[j] = +1$, $j \in [30 - 26, 10 - 6, 4 - 0]$

- To obtain $f_7[j] = 0$, we require $Q_5[j] = Q_6[j]$ for $j \in [30 - 28, 26, 4, 3, 1, 0]$. See proof 12.
- To obtain $f_7[j] = +1$, we require $Q_6[j] = 1$ for $j \in [10]$. See proof 28.
- To obtain $f_7[j] = 0$, we require $Q_6[j] = 0$ for $j \in [9 - 7]$. See proof 2^7.
- To obtain $f_7[j] = 0$, we need no requirements for $Q_7[6]$. See proof 9.
- To obtain $f_7[j] =$ -1, we require $Q_5[j] = 1$ and $Q_6[j] = 0$ for $j \in [27, 2]$. See proof 15.

$Q_7[j] =$ -1, $j \in [25 - 23, 11, 5]$

- To obtain $f_7[j] =$ -1, we require $Q_5[j] = 0$ and $Q_6[j] = 1$ for $j \in [25]$. See proof 17.
- To obtain $f_7[j] = 0$, we require $Q_5[j] = Q_6[j]$ for $j \in [24]$. See proof 13.
- To obtain $f_7[j] = 0$, we require $Q_5[j] = 0$ for $j \in [23]$. See proof 26.
- To obtain $f_7[j] = 0$, we require $Q_6[j] = 1$ for $j \in [11]$. See proof 29.
- To obtain $f_7[j] = +1$, we require $Q_5[j] = 1$ and $Q_6[j] = 0$ for $j \in [5]$. See proof 16.

$Q_7[j] = \pm 1$, $j \in [31]$

- To obtain $f_9[j] = 1$, we require $Q_7[j] = Q_6[j]\ Q_5[j]$ for $j \in [31]$. See proof 2.

Summary of the conditions for step 7:

- $Q_5[25, 23] = Q_6[9, 8, 5, 2] = Q_7[30 - 26, 16, 10 - 6, 4 - 0] = 0$
- $Q_5[5, 2] = Q_6[27, 25, 11, 10] = Q_7[25 - 17, 15 - 11, 5] = 1$
- $Q_5[30 - 28, 26, 24, 4, 3, 1, 0] = Q_6[30 - 28, 26, 24, 4, 3, 1, 0]$
- $Q_7[31] = \overline{Q_6[31] \oplus Q_5[31]}$

Step 8:

We have $Q_6 = \pm 2^{31} + 2^{23} - 2^6$, $Q_7 = -2^{27} + 2^{23} - 2^6 - 2^0$, and $Q_8 = -2^{23} - 2^{17} - 2^{15} + 2^0$, and we want to obtain $f_8 = \pm 2^{31} - 2^{24} + 2^{16} + 2^{10} + 2^6 + 2^0$.

Obtaining the Correct Q_8:

- $Q_8[19 - 17, 15, 0] = 0$
- $Q_8[23, 20, 16] = 1$

The Constant Bits of Q_8:
$Q_8[j] = 0$, $j \in [31 - 24, 22, 21, 14 - 1]$

- To obtain $f_8[j] = 1$, we need no requirements for $Q_8[31]$. See proof 3.
- To obtain $f_8[j] = 0$, we require $Q_8[j] = 0$ for $j \in [30 - 26, 9, 7, 4 - 1]$. See proof 22.
- To obtain $f_8[j] = 0$, we require $Q_8[j] = 0$ for $j \in [25, 11, 5]$. See proof 24.
- To obtain $f_8[j] = -1$, we require $Q_8[j] = 1$ for $j \in [24]$. See proof 25.
- To obtain $f_8[j] = +1$, we require $Q_8[j] = 1$ for $j \in [10, 8]$. See proof 23.
- To obtain $f_8[j] = +1$, we require $Q_8[j] = 1$ for $j \in [6]$. See proof 32.
- To obtain $f_8[j] = 0$, we need no requirements for $Q_8[22, 21, 14 - 12]$.

The Non-Constant Bits of Q_8:
$Q_8[j] = +1$, $j \in [19 - 17, 15, 0]$

- To obtain $f_8[j] = 0$, we require $Q_6[j] = Q_7[j]$ for $j \in [19 - 17, 15]$. See proof 12.
- To obtain $f_8[j] = 0$, we require $Q_6[j] = 1$ for $j \in [0]$. See proof 35.

$Q_8[j] = -1$, $j \in [23, 20, 16]$

- To obtain $f_8[j] = 0$, we need no requirements for $Q_8[23]$. See proof 10.
- To obtain $f_8[j] = 0$, we require $Q_6[j] = Q_7[j]$ for $j \in [20]$. See proof 13.
- To obtain $f_8[j] = +1$, we require $Q_6[j] = 1$ and $Q_7[j] = 0$ for $j \in [16]$. See proof 16.

Summary of the conditions for step 8:

- $Q_7[16] = Q_8[30 - 25, 19 - 17, 15, 11, 9, 7, 5 - 0] = 0$
- $Q_6[16, 0] = Q_7[0] = Q_8[24, 23, 20, 16, 10, 8, 6] = 1$
- $Q_6[20 - 17, 15] = Q_7[20 - 17, 15]$

Step 9:

We have Q_7 = -2^{27} + 2^{23} - 2^6 - 2^0, Q_8 = -2^{23} - 2^{17} - 2^{15} + 2^0, and Q_9 = $\pm 2^{31}$ - 2^6 + 2^0, and we want to obtain $f_9 = \pm 2^{31}$ + 2^{26} - 2^{23} - 2^{20} + 2^6 + 2^0.

Obtaining the Correct Q_9:

- $Q_9[7, 6, 1] = 0$
- $Q_9[8, 0] = 1$

The Constant Bits of Q_9:
$Q_9[j] = 0$, $j \in$ [30 - 9, 5 - 2]

- To obtain $f_9[j] = 0$, we require $Q_9[j] = 1$ for $j \in$ [30 - 27, 10, 9, 4 - 2]. See proof 18.
- To obtain $f_9[j] = +1$, we require $Q_9[j] = 0$ for $j \in$ [26]. See proof 19.
- To obtain $f_9[j] = 0$, we require $Q_9[j] = 1$ for $j \in$ [25, 24, 11, 5]. See proof 20.
- To obtain $f_9[j]$ = -1, we need no requirements for $Q_9[23]$. See proof 34.
- To obtain $f_9[j]$ = -1, we require $Q_9[j] = 1$ for $j \in$ [20]. See proof 25.
- To obtain $f_9[j] = 0$, we require $Q_9[j] = 0$ for $j \in$ [19 - 17, 15]. See proof 22.
- To obtain $f_9[j] = 0$, we require $Q_9[j] = 0$ for $j \in$ [16]. See proof 24.
- To obtain $f_9[j] = 0$, we need no requirements for Q_9[22, 21, 14 - 12].

The Non-Constant Bits of Q_9:
$Q_9[j] = +1$, $j \in$ [7, 6, 1]

- To obtain $f_9[j] = 0$, we require $Q_8[j] = 0$ for $j \in$ [7, 1]. See proof 2^7.
- To obtain $f_9[j] = +1$, we require $Q_8[j] = 1$ for $j \in$ [6]. See proof 28.

$Q_9[j]$ = -1, $j \in$ [8, 0]

- To obtain $f_9[j] = 0$, we require $Q_8[j] = 1$ for $j \in$ [8]. See proof 29.
- To obtain $f_9[j] = +1$, we need no requirements for $Q_9[0]$. See proof 8.

$Q_9[j] = \pm 1$, $j \in$ [31]

- To obtain $f_9[j] = 1$, we require $Q_9[j] = Q_8[j]\ Q_7[j]$ for $j \in$ [31]. See proof 4.

Summary of the conditions for step 9:

- $Q_8[7, 1] = Q_9$[26, 19 - 15, 7, 6, 1] = 0
- $Q_8[8, 6] = Q_9$[30 - 27, 25, 24, 20, 11 - 8, 5 - 2, 0] = 1
- $Q_9[31] = \overline{Q_8[31] \oplus Q_7[31]}$

Step 10:

We have Q_8 = -2^{23} - 2^{17} - 2^{15} + 2^0, Q_9 = $\pm 2^{31}$ - 2^6 + 2^0, and Q_{10} = $\pm 2^{31}$ + 2^{12}, and we want to obtain f_{10} = -2^{23} + 2^{13} + 2^6 + 2^0.

Obtaining the Correct Q_{10}:

- $Q_{10}[13] = 0$

- $Q_{10}[12] = 1$

The Constant Bits of Q_{10}:
$Q_{10}[j] = 0$, $j \in$ [30 - 14, 11 - 0]

- To obtain $f_{10}[j]$ = -1, we require $Q_{10}[j] = 0$ for $j \in$ [23]. See proof 21.
- To obtain $f_{10}[j] = 0$, we require $Q_{10}[j] = 1$ for $j \in$ [20, 16]. See proof 20.
- To obtain $f_{10}[j] = 0$, we require $Q_{10}[j] = 1$ for $j \in$ [19 - 17, 15]. See proof 18.
- To obtain $f_{10}[j] = 0$, we require $Q_{10}[j] = 0$ for $j \in$ [8]. See proof 24.
- To obtain $f_{10}[j] = 0$, we require $Q_{10}[j] = 0$ for $j \in$ [7, 1]. See proof 22.
- To obtain $f_{10}[j] = +1$, we require $Q_{10}[j] = 1$ for $j \in$ [6]. See proof 23.
- To obtain $f_{10}[j] = +1$, we require $Q_{10}[j] = 0$ for $j \in$ [0]. See proof 37.
- To obtain $f_{10}[j] = 0$, we need no requirements for Q_{10}[30 - 24, 22, 21 14, 11 - 9, 5 - 2].

The Non-Constant Bits of Q_{10}:
$Q_{10}[j] = +1$, $j \in$ [13]

- To obtain $f_{10}[j] = +1$, we require $Q_8[j] = 0$ and $Q_9[j] = 1$ for $j \in$ [13]. See proof 14.

$Q_{10}[j]$ = -1, $j \in$ [12]

- To obtain $f_{10}[j] = 0$, we require $Q_8[j] = Q_9[j]$ for $j \in$ [12]. See proof 13.

$Q_{10}[j] = \pm 1$, $j \in$ [31]

- To obtain $f_{10}[j] = 0$, we require $Q_{10}[31] = Q_9[31]\ Q_8[31]$ for $j \in$ [31]. See proof 2.

Summary of the conditions for step 10:

- $Q_8[13] = Q_{10}$[23, 13, 8, 7, 1, 0] $= 0$
- $Q_9[13] = Q_{10}$[20 - 15, 12, 6] $= 1$
- $Q_8[12] = \overline{Q_9[12]}$
- $Q_{10}[31] = \overline{Q_9[31] \oplus Q_8[31]}$

Step 11:

We have $Q_9 = \pm 2^{31}$ - $2^6 + 2^0$, $Q_{10} = \pm 2^{31} + 2^{12}$, and $Q_{11} = 2^{31} + 2^{30}$, and we want to obtain f_{11} = -$2^8 + 2^0$.

Obtaining the Correct Q_{11}:

- $Q_{11}[30] = 0$

The Constant Bits of Q_{11}:
$Q_{11}[j] = 0$, $j \in$ [29 - 0]

- To obtain $f_{11}[j] = 0$, we require $Q_{11}[j] = 0$ for $j \in$ [13]. See proof 22.
- To obtain $f_{11}[j] = 0$, we require $Q_{11}[j] = 0$ for $j \in$ [12]. See proof 24.
- To obtain $f_{11}[j]$ = -1, we require $Q_{11}[j] = 0$ for $j \in$ [8, 0]. See proof 21.
- To obtain $f_{11}[j] = 0$, we require $Q_{11}[j] = 1$ for $j \in$ [7, 6, 1]. See proof 18.
- To obtain $f_{11}[j] = 0$, we need no requirements for Q_{11}[29 - 14, 11 - 9, 5 - 2].

The Non-Constant Bits of Q_{11}:
$Q_{11}[j] = +1,\ j \in [30]$

- To obtain $f_{11}[j] = 0$, we require $Q_9[j] = Q_{10}[j]$ for $j \in [30]$. See proof 12.

$Q_{11}[j] = \pm 1,\ j \in [31]$

- To obtain $f_{11}[j] = 0$, we require $Q_9[j] = Q_{10}[j]$ for $j \in [31]$. See proof 5. Note that since we already have $Q_{10}[31] = Q_9[31]\ Q_8[31]$ from step 10, we obtain $Q_8[31] = 0$.

Summary of the conditions for step 11:

- $Q_8[31] = Q_{11}[13, 12, 8, 0] = 0$
- $Q_{11}[7, 6, 1] = 1$
- $Q_9[30] = Q_{10}[30]$
- $Q_9[31] = \overline{Q_{10}}[31]$

Step 12:

We have $Q_{10} = \pm 2^{31} + 2^{12}$, $Q_{11} = \pm 2^{31} + 2^{30}$, and $Q_{12} = \pm 2^{31}$ - 2^{13} - 2^7, and we want to obtain $f_{12} = \pm 2^{31} + 2^{17} + 2^7$.

Obtaining the Correct Q_{12}:

- $Q_{12}[18$ - $13, 7] = 0$
- $Q_{12}[19, 8] = 1$

The Constant Bits of Q_{12}:
$Q_{12}[j] = 0,\ j \in [30$ - $20, 12$ - $9, 6$ - $0]$

- To obtain $f_{12}[j] = 0$, we require $Q_{12}[j] = 0$ for $j \in [30]$. See proof 22.
- To obtain $f_{12}[j] = 0$, we require $Q_{12}[j] = 1$ for $j \in [12]$. See proof 20.
- To obtain $f_{12}[j] = 0$, we need no requirements for $Q_{12}[29$ - $20, 11$ - $9, 6$ - $0]$.

The Non-Constant Bits of Q_{12}:
$Q_{12}[j] = +1,\ j \in [18$ - $13, 7]$

- To obtain $f_{12}[j] =$ -1, we require $Q_{10}[j] = 1$ and $Q_{11}[j] = 0$ for $j \in [18, 17]$. See proof 15.
- To obtain $f_{12}[j] = 0$, we require $Q_{10}[j] = Q_{11}[j]$ for $j \in [16$ - $14]$. See proof 12.
- To obtain $f_{12}[j] = 0$, we require $Q_{11}[j] = 0$ for $j \in [13]$. See proof 2^7.
- To obtain $f_{12}[j] = +1$, we require $Q_{10}[j] = 0$ and $Q_{11}[j] = 1$ for $j \in [7]$. See proof 14.

$Q_{12}[j] =$ -1, $j \in [19, 8]$

- To obtain $f_{12}[j] = +1$, we require $Q_{10}[j] = 1$ and $Q_{11}[j] = 0$ for $j \in [19]$. See proof 16.
- To obtain $f_{12}[j] = 0$, we require $Q_{10}[j] = Q_{11}[j]$ for $j \in [8]$. See proof 13.

$Q_{12}[j] = \pm 1,\ j \in [31]$

- To obtain $f_{12}[j] = 1$, we require $Q_{10}[j] = Q_{11}[j]$ for $j \in [31]$. See proof 6.

Summary of the conditions for step 12:

- Q_{11}[19 - 17, 13] = Q_{12}[30, 18 - 13, 7] = 0
- Q_{10}[19 - 17] = Q_{12}[19, 12, 8] = 1
- Q_{10}[31, 16 - 14, 8, 7] = Q_{11}[31, 16 - 14, 8, 7]

Step 13:

We have $Q_{11} = \pm 2^{31} + 2^{30}$, $Q_{12} = \pm 2^{31}$ - 2^{13} - 2^7, and $Q_{13} = \pm 2^{31} + 2^{24}$, and we want to obtain $f_{13} = \pm 2^{31}$ - 2^{13}.

Obtaining the Correct Q_{13}:

- $Q_{13}[25] = 0$
- $Q_{13}[24] = 1$

The Constant Bits of Q_{13}:
$Q_{13}[j] = 0$, $j \in$ [30 - 26, 23 - 0]

- To obtain $f_{13}[j] = 0$, we require $Q_{13}[j] = 1$ for $j \in [30]$. See proof 18.
- To obtain $f_{13}[j]$ = -1, we require $Q_{13}[j] = 1$ for $j \in [19]$. See proof 25.
- To obtain $f_{13}[j] = +1$, we require $Q_{13}[j] = 1$ for $j \in$ [18 - 13]. See proof 23.
- To obtain $f_{13}[j] = 0$, we require $Q_{13}[j] = 0$ for $j \in [8]$. See proof 24.
- To obtain $f_{13}[j] = 0$, we require $Q_{13}[j] = 0$ for $j \in [7]$. See proof 22.
- To obtain $f_{13}[j] = 0$, we need no requirements for Q_{13}[29 - 26, 23 - 20, 12 - 9, 6 - 0].

The Non-Constant Bits of Q_{13}:
$Q_{13}[j] = +1$, $j \in [25]$

- To obtain $f_{13}[j] = 0$, we require $Q_{11}[j] = Q_{12}[j]$ for $j \in [25]$. See proof 12.

$Q_{13}[j]$ = -1, $j \in [24]$

- To obtain $f_{13}[j] = 0$, we require $Q_{11}[j] = Q_{12}[j]$ for $j \in [24]$. See proof 13.

$Q_{13}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{13}[j] = 1$, we require $Q_{11}[j] = Q_{12}[j]$ for $j \in [31]$. See proof 6.

Summary of the conditions for step 13:

- Q_{13}[25, 8, 7] = 0
- Q_{13}[30, 24, 19 - 13] = 1
- Q_{11}[31, 25, 24] = Q_{12}[31, 25, 24]

Step 14:

We have $Q_{12} = \pm 2^{31}$ - 2^{13} - 2^7, $Q_{13} = \pm 2^{31} + 2^{24}$, and $Q_{14} = \pm 2^{31}$, and we want to obtain $f_{14} = \pm 2^{31} + 2^{18}$.

Obtaining the Correct Q_{14}: No conditions required

The Constant Bits of Q_{14}:
$Q_{14}[j] = 0$, $j \in$ [30 - 0]

- To obtain $f_{14}[j] = 0$, we require $Q_{14}[j] = 0$ for $j \in [25]$. See proof 22.
- To obtain $f_{14}[j] = 0$, we require $Q_{14}[j] = 0$ for $j \in [24]$. See proof 24.
- To obtain $f_{14}[j] = 0$, we require $Q_{14}[j] = 1$ for $j \in [19, 8]$. See proof 20.
- To obtain $f_{14}[j] = +1$, we require $Q_{14}[j] = 0$ for $j \in [18]$. See proof 19.
- To obtain $f_{14}[j] = 0$, we require $Q_{14}[j] = 1$ for $j \in [17 - 13, 7]$. See proof 18.
- To obtain $f_{14}[j] = 0$, we need no requirements for $Q_{14}[30 - 26, 23 - 20, 12 - 9, 6 - 0]$.

The Non-Constant Bits of Q_{14}:
$Q_{14}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{14}[j] = 1$, we require $Q_{12}[j] = Q_{13}[j]$ for $j \in [31]$. See proof 6.

Summary of the conditions for step 14:

- $Q_{14}[25, 24, 18] = 0$
- $Q_{14}[19, 17 - 13, 8, 7] = 1$
- $Q_{12}[31] = Q_{13}[31]$

Step 15:

We have $Q_{13} = \pm 2^{31} + 2^{24}$, $Q_{14} = \pm 2^{31}$, and $Q_{15} = \pm 2^{31} - 2^{15} + 2^{3}$, and we want to obtain $f_{15} = \pm 2^{31} + 2^{25}$.

Obtaining the Correct Q_{15}:

- $Q_{15}[3] = 0$
- $Q_{15}[15] = 1$

The Constant Bits of Q_{15}:
$Q_{15}[j] = 0$, $j \in [30 - 16, 14 - 4, 2 - 0]$

- To obtain $f_{15}[j] = 0$, we require $Q_{15}[j] = 0$ for $j \in [25]$. See proof 19.
- To obtain $f_{15}[j] = 0$, we require $Q_{15}[j] = 1$ for $j \in [24]$. See proof 20.
- To obtain $f_{15}[j] = 0$, we need no requirements for $Q_{15}[30 - 26, 23 - 16, 14 - 4, 2 - 0]$.

The Non-Constant Bits of Q_{15}:
$Q_{15}[j] = +1$, $j \in [3]$

- To obtain $f_{15}[j] = 0$, we require $Q_{13}[j] = Q_{14}[j]$ for $j \in [3]$. See proof 12.

$Q_{15}[j] = -1$, $j \in [15]$

- To obtain $f_{15}[j] = 0$, we require $Q_{13}[j] = Q_{14}[j]$ for $j \in [8]$. See proof 13.

$Q_{15}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{15}[j] = 1$, we require $Q_{13}[j] = Q_{14}[j]$ for $j \in [31]$. See proof 6.

Summary of the conditions for step 15:

- $Q_{15}[25, 3] = 0$
- $Q_{15}[24, 15] = 1$

- $Q_{13}[31,\ 15,\ 3] = Q_{14}[31,\ 15,\ 3]$

Round 2: $f_t = G(X,\ Y,\ Z)$

Step 16:

We have $Q_{14} = \pm 2^{31}$, $Q_{15} = \pm 2^{31}$ - $2^{15} + 2^3$, and $Q_{16} = \pm 2^{31}$ - 2^{29}, and we want to obtain $f_{16} = \pm 2^{31}$.

Obtaining the Correct Q_{16}:

- $Q_{16}[29] = 1$

The Constant Bits of Q_{14}:
$Q_{14}[j] = 0,\ j \in [30$ - $0]$

- To obtain $f_{16}[j] = 0$, we require $Q_{14}[j] = 0$ for $j \in [29]$. See proof 39.
- To obtain $f_{16}[j] = 0$, we require $Q_{14}[j] = 1$ for $j \in [15]$. See proof 40.
- To obtain $f_{16}[j] = 0$, we require $Q_{14}[j] = 1$ for $j \in [3]$. See proof 41.
- To obtain $f_{16}[j] = 0$, we need no requirements for $Q_{14}[30,\ 28$ - $16,\ 14$ - $4,\ 2$ - $0]$.

The Non-Constant Bits of Q_{14}:
$Q_{14}[j] = \pm 1,\ j \in [31]$

- To obtain $f_{16}[j] = 1$, we require $Q_{15}[j] = Q_{16}[j]$ for $j \in [31]$. See proof 38.

Summary of the conditions for step 16:

- $Q_{14}[29] = 0$
- $Q_{14}[15,\ 3] = 1$
- $Q_{15}[31] = Q_{16}[31]$

Step 17:

We have $Q_{15} = \pm 2^{31}$ - $2^{15} + 2^3$, $Q_{16} = \pm 2^{31}$ - 2^{29}, and $Q_{17} = \pm 2^{31}$, and we want to obtain $f_{17} = \pm 2^{31}$.

Obtaining the Correct Q_{17}: No conditions required

The Constant Bits of Q_{15}:
$Q_{15}[j] = 0,\ j \in [30$ - $16,\ 14$ - $4,\ 2$ - $0]$

- To obtain $f_{17}[j] = 0$, we require $Q_{15}[j] = 1$ for $j \in [29]$. See proof 40.
- To obtain $f_{17}[j] = 0$, we need no requirements for $Q_{15}[30,\ 28$ - $16,\ 14$ - $4,\ 2$ - $0]$.

The Non-Constant Bits of Q_{15}:
$Q_{15}[j] = +1,\ j \in [3]$

- To obtain $f_{17}[j] = 0$, we require $Q_{16}[j] = Q_{17}[j]$ for $j \in [3]$. See proof 43.

$Q_{15}[j]$ = -1, $j \in$ [15]

- To obtain $f_{17}[j] = 0$, we require $Q_{16}[j] = Q_{17}[j]$ for $j \in$ [15]. See proof 42.

$Q_{15}[j] = \pm 1$, $j \in$ [31]

- To obtain $f_{17}[j] = 1$, we require $Q_{16}[j] = Q_{17}[j]$ for $j \in$ [31]. See proof 38.

Summary of the conditions for step 17:

- Q_{15}[29] = 1
- Q_{16}[31, 15, 3] = Q_{17}[31, 15, 3]

Step 18:

We have $Q_{16} = \pm 2^{31}$ - 2^{29}, $Q_{17} = \pm 2^{31}$, and $Q_{18} = \pm 2^{31}$, and we want to obtain $f_{18} = \pm 2^{31}$.

Obtaining the Correct Q_{18}: No conditions required

The Constant Bits of Q_{16}:
$Q_{16}[j] = 0$, $j \in$ [30, 28 - 0]

- To obtain $f_{18}[j] = 0$, we need no requirements for Q_{16}[30, 28 - 0].

The Non-Constant Bits of Q_{16}:
$Q_{16}[j]$ = -1, $j \in$ [29]

- To obtain $f_{18}[j] = 0$, we require $Q_{17}[j] = Q_{18}[j]$ for $j \in$ [15]. See proof 42.

$Q_{16}[j] = \pm 1$, $j \in$ [31]

- To obtain $f_{18}[j] = 1$, we require $Q_{17}[j] = Q_{18}[j]$ for $j \in$ [31]. See proof 38.

Summary of the conditions for step 18:

- Q_{17}[31, 29] = Q_{18}[31, 29]

Step 19:

We have $Q_{17} = \pm 2^{31}$, $Q_{18} = \pm 2^{31}$, and $Q_{19} = \pm 2^{31} + 2^{17}$, and we want to obtain $f_{19} = \pm 2^{31}$.
Obtaining the Correct Q_{19}:

- Q_{19}[17] = 0

The Constant Bits of Q_{17}:
$Q_{17}[j] = 0$, $j \in$ [30 - 0]

- To obtain $f_{19}[j] = 0$, we require $Q_{17}[j] = 0$ for $j \in$ [17]. See proof 44.
- To obtain $f_{19}[j] = 0$, we need no requirements for Q_{17}[30 - 18, 16 - 0].

The Non-Constant Bits of Q_{17}:
$Q_{17}[j] = \pm 1$, $j \in$ [31]

- To obtain $f_{19}[j] = 1$, we require $Q_{18}[j] = Q_{19}[j]$ for $j \in [31]$. See proof 38.

Summary of the conditions for step 19:

- $Q_{17}[17] = Q_{19}[17] = 0$
- $Q_{18}[31] = Q_{19}[31]$

Step 20:

We have $Q_{18} = \pm 2^{31}$, $Q_{19} = \pm 2^{31} + 2^{17}$, and $Q_{20} = \pm 2^{31}$, and we want to obtain $f_{20} = \pm 2^{31}$.

Obtaining the Correct Q_{20}: No conditions required

The Constant Bits of Q_{18}:
$Q_{18}[j] = 0$, $j \in$ [30 - 0]

- To obtain $f_{20}[j] = 0$, we require $Q_{18}[j] = 1$ for $j \in [17]$. See proof 41.
- To obtain $f_{20}[j] = 0$, we need no requirements for Q_{18}[30 - 18, 16 - 0].

The Non-Constant Bits of Q_{18}:
$Q_{18}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{20}[j] = 1$, we require $Q_{19}[j] = Q_{20}[j]$ for $j \in [31]$. See proof 38.

Summary of the conditions for step 20:

- $Q_{18}[17] = 1$
- $Q_{19}[31] = Q_{20}[31]$

Step 21:

We have $Q_{19} = \pm 2^{31} + 2^{17}$, $Q_{20} = \pm 2^{31}$, and $Q_{21} = \pm 2^{31}$, and we want to obtain $f_{21} = \pm 2^{31}$.

Obtaining the Correct Q_{21}: No conditions required

The Constant Bits of Q_{19}:
$Q_{19}[j] = 0$, $j \in$ [30 - 18, 16 - 0]

- To obtain $f_{21}[j] = 0$, we need no requirements for Q_{19}[30 - 18, 16 - 0].

The Non-Constant Bits of Q_{19}:
$Q_{19}[j] = +1$, $j \in [17]$

- To obtain $f_{21}[j] = 0$, we require $Q_{20}[j] = Q_{21}[j]$ for $j \in [17]$. See proof 43.

$Q_{19}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{21}[j] = 1$, we require $Q_{20}[j] = Q_{21}[j]$ for $j \in [31]$. See proof 38.

Summary of the conditions for step 21:

- $Q_{20}[31, 17] = Q_{21}[31, 17]$

Step 22:

We have $Q_{20} = \pm 2^{31}$, $Q_{21} = \pm 2^{31}$, and $Q_{22} = \pm 2^{31}$, and we want to obtain $f_{22} = \pm 2^{31}$.

Obtaining the Correct Q_{22}: No conditions required

The Constant Bits of Q_{20}:
$Q_{20}[j] = 0$, $j \in [30$ - $0]$

- To obtain $f_{22}[j] = 0$, we need no requirements for $Q_{20}[30$ - $0]$.

The Non-Constant Bits of Q_{20}:
$Q_{20}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{22}[j] = 1$, we require $Q_{21}[j] = Q_{22}[j]$ for $j \in [31]$. See proof 38.

Summary of the conditions for step 22:

- $Q_{21}[31] = Q_{22}[31]$

Step 23:

We have $Q_{21} = \pm 2^{31}$, $Q_{22} = \pm 2^{31}$, and $Q_{23} = 0$, and we want to obtain $f_{23} = 0$.

Obtaining the Correct Q_{23}: No conditions required

The Constant Bits of Q_{21}:
$Q_{21}[j] = 0$, $j \in [30$ - $0]$

- To obtain $f_{23}[j] = 0$, we need no requirements for $Q_{21}[30$ - $0]$.

The Non-Constant Bits of Q_{21}:
$Q_{21}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{23}[j] = 0$, we require $Q_{23}[j] = 0$ for $j \in [31]$. See proof 45.

Summary of the conditions for step 23:

- $Q_{23}[31] = 0$

Step 24:

We have $Q_{22} = \pm 2^{31}$, $Q_{23} = 0$, and $Q_{24} = 0$, and we want to obtain $f_{24} = \pm 2^{31}$.

Obtaining the Correct Q_{24}: No conditions required

The Constant Bits of Q_{22}:
$Q_{22}[j] = 0$, $j \in [30$ - $0]$

- To obtain $f_{24}[j] = 0$, we need no requirements for $Q_{22}[30$ - $0]$.

<u>The Non-Constant Bits of Q_{22}:</u>
$Q_{22}[j] = \pm 1,\ j \in [31]$

- To obtain $f_{24}[j] = 1$, we require $Q_{24}[j] = 1$ for $j \in [31]$. See proof 46.

<u>Summary of the conditions for step 24:</u>

- $Q_{24}[31] = 0$

Steps 25 to 31:

We have $Q_{t-2} = 0$, $Q_{t-1} = 0$, and $Q_t = 0$, so we will obtain $f_t = 0$. There are no conditions for these steps.

Round 3: $f_t = H(X,\ Y,\ Z)$

In round 3, the only differences in the Q_t occur in the most significant bit. The sign of the most significant bit is important only when it is rotated to some other bit position. However, during round 3, the differences in the most significant bits are always cancelled out by differences in the most significant bit in either f_t, Q_{t-3}, or W_t. Therefore, in round 3, the sign on the difference the most significant bit does not matter.

Steps 32 to 34:

We have $Q_{t-2} = 0$, $Q_{t-1} = 0$, and $Q_t = 0$, so we will obtain $f_t = 0$. There are no conditions for these steps.

Step 35:

We have $Q_{33} = 0$, $Q_{34} = 0$, and $Q_{35} = \pm 2^{31}$, so we will obtain $f_{35} = \pm 2^{31}$. See proof 47.

Step 36:

We have $Q_{34} = 0$, $Q_{35} = \pm 2^{31}$, and $Q_{36} = \pm 2^{31}$, so we will obtain $f_{36} = 0$. See proof 48.

Steps 37 to 47:

We have $Q_{t-2} = \pm 2^{31}$, $Q_{t-1} = \pm 2^{31}$, and $Q_t = \pm 2^{31}$, so we will obtain $f_t = \pm 2^{31}$. See proof 49.

Round 4: $f_t = I(X,\ Y,\ Z)$

The values of Q46 and Q47 each have two possibilities, $(\Delta Q_{46},\ \Delta Q_{47})$ = (+1, -1). Thus, there are four combinations of $(\Delta Q_{46}, \Delta Q_{47})$. In [7], $(\Delta Q_{46}, \Delta Q_{47})$ = (+1, -1) were chosen as the initial values for the fourth round of the first iteration. Thus, we must impose two conditions:

- ΔQ_{46} = +1 $\Rightarrow Q_{46} = 0$
- ΔQ_{47} = -1 $\Rightarrow Q_{47} = 1$

Steps 48 to 49:

We have $\Delta Q_{t-2} = \pm 2^{31}$, $\Delta Q_{t-1} = \pm 2^{31}$, and $\Delta Q_t = \pm 2^{31}$, and we want to obtain $\Delta f_t = \pm 2^{31}$. Thus, we require that $\Delta Q_{t-2} = \Delta Q_t \Rightarrow Q_{t-2} = Q_t$. See proof 50.

Step 50:

We have $\Delta Q_{48} = \pm 2^{31}$, $\Delta Q_{49} = \pm 2^{31}$, and $\Delta Q_{50} = \pm 2^{31}$, and we want to obtain $\Delta f_{50} = 0$. Thus, we require that $\Delta Q_{48} = -\Delta Q_{50} \Rightarrow Q_{48} = \overline{Q_{50}}$. See proof 51.

Steps 51 to 59:

We have $\Delta Q_{t-2} = \pm 2^{31}$, $\Delta Q_{t-1} = \pm 2^{31}$, and $\Delta Q_t = \pm 2^{31}$, and we want to obtain $\Delta f_t = \pm 2^{31}$. Thus, we require that $\Delta Q_{t-2} = \Delta Q_t \Rightarrow Q_{t-2} = Q_t$. See proof 50.

Step 60:

We have $\Delta Q_{58} = \pm 2^{31}$, $\Delta Q_{59} = \pm 2^{31}$, and $\Delta Q_{60} = \pm 2^{31}$, and we want to obtain $\Delta f_{60} = 0$. Thus, we require that $\Delta Q_{58} = -\Delta Q_{60} \Rightarrow Q_{58} = \overline{Q_{60}}$. See proof 51.

Step 61:

We have $\Delta Q_{59} = \pm 2^{31}$, $\Delta Q_{60} = \pm 2^{31}$, and $\Delta Q_{61} = \pm 2^{31}$, and we want to obtain $\Delta f_{61} = \pm 2^{31}$. Thus, we require that $\Delta Q_{59} = \Delta Q_{61} \Rightarrow Q_{59} = Q_{61}$. See proof 50.

Step 62:

<u>Obtaining the Correct ΔQ_{62}:</u>

- $Q_{62}[25] = 0$

We have $\Delta Q_{60} = 2^{31}$, $\Delta Q_{61} = 2^{31}$, and $\Delta Q_{62} = 2^{31} + 2^{25}$, and we want to obtain $\Delta f_{62} = 2^{31}$. Thus, we must impose two conditions. First, to obtain $\Delta f_{62} = \pm 1$, we require that $\Delta Q_{60} = \Delta Q_{62} \Rightarrow Q_{60} = Q_{62}$. See proof 50. Second, to obtain $f_{62}[25] = 0$, we require that $Q_{60}[25] = 0$. See proof 52.

Step 63:

<u>Obtaining the Correct Q_{63}:</u>

- $Q_{63}[25] = 0$

We have $Q_{61} = 2^{31}$, $Q_{62} = 2^{31} + 2^{25}$, and $Q_{63} = 2^{31} + 2^{25}$, and we want to obtain $f_{63} = 2^{31}$. Thus, we must impose two conditions. First, to obtain $f_{63}[31] = \pm 1$, we require that $Q_{61} = Q_{63} \Rightarrow Q_{61} = Q_{63}$. See proof 50. Second, to obtain $f_{63}[25] = 0$, we require that $Q_{61}[25] = 1$. See proof 53.

7.2 Conditions for the Propagation of the Differences Through the f_t Functions for the Second Block

Round 1: $f_t = F(X,\ Y,\ Z)$

The values of Q_{-2} and Q_{-1} in the second iteration are the same as the values of Q_{62} and Q_{63} in the first iteration, respectively. But Q_{-1} is now described as $\pm 2^{31}$ + 2^{26} - 2^{25} to ensure that the second block differential holds. Since we have rewritten Q_{-1} in this manner, we must impose the following conditions:

- $Q_{-1}[26] = 0$
- $Q_{-1}[25] = 1$

Step 0:

We have $Q_{-2} = \pm 2^{31} + 2^{25}$, $Q_{-1} = \pm 2^{31} + 2^{25}$, and $Q_0 = \pm 2^{31} + 2^{25}$, and we want to obtain $f_0 = \pm 2^{31}$.

Obtaining the Correct Q_0:

- $Q_0[25] = 0$

The Constant Bits of Q_0:
$Q_0[j] = 0$, $j \in$ [30 - 26, 24 - 0]

- To obtain $f_0[j] = 0$, we require $Q_0[j] = 0$ for $Q_0[26]$. See proof 22.
- To obtain $f_0[j] = 0$, no conditions are required for Q_0[30 - 27, 24 - 0].

The Non-Constant Bits of Q_0 : $Q_0[j] = +1$, $j \in$ [25]

- To obtain $f_0[j] = 0$, no conditions are required for $Q_0[25]$. See proof 9.

$Q_0[j] = \pm 1$, $j \in$ [31]

- To obtain $f_0[j] = 1$, we require $Q_{-2}[j] = Q_{-1}[j]$ for $j \in$ [31]. See proof 6.

Summary of the conditions for step 0:

- ΔQ_0[26, 25] = 0
- $Q_{-2}[31] = Q_{-1}[31]$

Step 1:

We have $Q_{-1} = \pm 2^{31} + 2^{25}$, $Q_0 = \pm 2^{31} + 2^{25}$, and $Q_1 = \pm 2^{31} + 2^{25}$, and we want to obtain $f_1 = \pm 2^{31}$.

Obtaining the Correct Q_1:

- $Q_1[25] = 0$

The Constant Bits of Q_1:
$Q_1[j] = 0$, $j \in$ [30 - 26, 24 - 0]

- To obtain $f_1[j] = 0$, no conditions are required for Q_1[30 - 26, 24 - 0].

The Non-Constant Bits of Q_1:
$Q_1[j] = +1$, $j \in$ [25]

- To obtain $f_1[j] = 0$, no conditions are required for Q_1[25]. See proof 11.

$Q_1[j] = \pm 1$, $j \in$ [31]

- To obtain $f_1[j] = 1$, we require $Q_{-1}[j] = Q_0[j]$ for $j \in$ [31]. See proof 6.

Summary of the conditions for step 1:

- $Q_1[25] = 0$
- $Q_{-1}[31] = Q_0[31]$

Step 2:

We have $Q_0 = \pm 2^{31} + 2^{25}$, $Q_1 = \pm 2^{31} + 2^{25}$, and $Q_2 = \pm 2^{31} + 2^{25} + 2^5$, and we want to obtain $f_2 = +2^{25}$.

Obtaining the Correct Q_2:

- $Q_2[25, 5] = 0$

The Constant Bits of Q_2:
$Q_2[j] = 0$, $j \in$ [30 - 26, 24 - 6, 4 - 0]

- To obtain $f_2[j] = 0$, no conditions are required for Q_2[30 - 26, 24 - 6, 4 - 0].

The Non-Constant Bits of Q_2:
$Q_2[j] = +1$, $j \in$ [25, 5]

- To obtain $f_2[j] = +1$, no conditions are required for Q_2[25]. See proof 7.
- To obtain $f_2[j] = 0$, we require $Q_0[j] = Q_1[j]$ for $j \in$ [5]. See proof 12.

$Q_2[j] = \pm 1$, $j \in$ [31]

- To obtain $f_2[j] = 0$, we require $Q_0[j] = \overline{Q_1}[j]$ for $j \in$ [31]. See proof 5.

Summary of the conditions for step 2:

- $Q_2[25, 5] = 0$
- $Q_0[5] = Q_1[5]$
- $Q_0[31] = \overline{Q_1}[31]$

Step 3:

We have $Q_1 = \pm 2^{31} + 2^{25}$, $Q_2 = \pm 2^{31} + 2^{25} + 2^5$, and $Q_3 = \pm 2^{31} + 2^{25} + 2^{16} + 2^{11} + 2^5$, and we want to obtain $f_3 = \pm 2^{31}$ - 2^{27} + 2^{25} - 2^{21} - 2^{11}.

Obtaining the Correct Q_3:

- Q_3[30, 21, 12, 7] = 0
- Q_3[29 - 25, 20 - 16, 11, 6, 5] = 1

<u>The Constant Bits of Q_3:</u>
<u>$Q_3[j] = 0$, $j \in$ [24 - 22, 15 - 13, 10 - 8, 4 - 0]</u>

- To obtain $f_3[j] = 0$, no conditions are required for Q_3[24 - 22, 15 - 13, 10 - 8, 4 - 0].

<u>The Non-Constant Bits of Q_3:</u>
<u>$Q_3[j] = +1$, $j \in$ [30, 21, 12, 7]</u>

- To obtain $f_3[j] = 0$, we require $Q_1[j] = Q_2[j]$ for $j \in$ [30, 12, 7]. See proof 12.
- To obtain $f_3[j]$ = -1, we require $Q_1[j] = 1$ and $Q_2[j] = 0$ for $j \in$ [21]. See proof 15.

$Q_3[j]$ = -1, $j \in$ [29 - 25, 20 - 16, 11, 6, 5]

- To obtain $f_3[j] = 0$, we require $Q_1[j] = Q_2[j]$ for Q_3[29, 28, 20 - 16, 6]. See proof 13.
- To obtain $f_3[j]$ = -1, we require $Q_1[j] = 0$ and $Q_2[j] = 1$ for $j \in$ [27, 11]. See proof 17.
- To obtain $f_3[j] = +1$, no conditions are required for Q_3[25]. See proof 8.
- To obtain $f_3[j] = 0$, we require $Q_1[j] = 0$ for $j \in$ [5]. See proof 26.

$Q_3[j] = \pm 1$, $j \in$ [31]

- To obtain $f_3[j] = 1$, we require $Q_1[j] = Q_2[j]$ for $j \in$ [31]. See proof 6.

<u>Summary of the conditions for step 3:</u>

- Q_1[27, 11] = Q_2[21] = Q_3[30, 21, 12, 7] = 0
- Q_1[21] = Q_2[27, 11] = Q_3[29 - 25, 20 - 16, 11, 6, 5] = 1
- Q_1[31 - 28, 26, 20 - 16, 12, 7 - 5] = Q_2[31 - 28, 26, 20 - 16, 12, 7 - 5]

Step 4:

We have $Q_2 = \pm 2^{31} + 2^{25} + 2^5$, $Q_3 = \pm 2^{31} + 2^{25} + 2^{16} + 2^{11} + 2^5$, and $Q_4 = \pm 2^{31} + 2^{25} + 2^5$ - 2^1, and we want to obtain $f_4 = \pm 2^{31} + 2^{26}$ - $2^{18} + 2^2 + 2^1$.

<u>Obtaining the Correct Q_4:</u>

- Q_4[26, 5, 3 - 1] = 0
- Q4[25, 4] = 1

<u>The Constant Bits of Q_4:</u>
<u>$Q_4[j] = 0$, $j \in$ [30 - 27, 24 - 6, 0]</u>

- To obtain $f_4[j] = 0$, we require $Q_4[j] = 0$ for $j \in$ [30, 21, 12, 7]. See proof 22.
- To obtain $f_4[j] = 0$, we require $Q_4[j] = 0$ for $j \in$ [20, 19, 17, 16, 11, 6]. See proof 24.
- To obtain $f_4[j]$ = -1, we require $Q_4[j] = 1$ for $j \in$ [29 - 27, 18]. See proof 25.
- To obtain $f_4[j] = 0$, no conditions are required for Q_4[24 - 22, 15 - 13, 10 - 8, 0].

<u>The Non-Constant Bits of Q4:</u>
<u>$Q_4[j] = +1$, $j \in$ [26, 5, 3 - 1]</u>

- To obtain $f_4[j]$ = -1, we require $Q_2[j] = 1$ for $j \in$ [26]. See proof 36.
- To obtain $f_4[j]$ = 0, no conditions are required for Q4[5]. See proof 9.
- To obtain $f_4[j]$ = 0, we require $Q_2[j] = Q_3[j]$ for $j \in$ [3]. See proof 12.
- To obtain $f_4[j]$ = +1, we require $Q_2[j]$ = 0 and $Q_3[j]$ = 1 for $j \in$ [2, 1]. See proof 14.

Q_4 $[j]$ = -1, $j \in$ [25, 4]

- To obtain $f_4[j]$ = 0, no conditions are required for Q4[25]. See proof 10.
- To obtain $f_4[j]$ = 0, we require $Q_2[j] = Q_3[j]$ for $j \in$ [4]. See proof 13.

$Q_4[j] = \pm 1$, $j \in$ [31]

- To obtain $f_4[j]$ = 1, we require $Q_2[j] = Q_3[j]$ for $j \in$ [31]. See proof 6.

Summary of the conditions for step 4:

- Q_2[2, 1] = Q_4[30, 26, 21 - 19, 17, 16, 12, 11, 7 - 5, 3 - 1] = 0
- Q_2[26] = Q_3[2, 1] = Q_4[29 - 27, 25, 18, 4] = 1
- Q_2[31, 4, 3] = Q_3[31, 4, 3]

Step 5:

We have $Q_3 = \pm 2^{31} + 2^{25} + 2^{16} + 2^{11} + 2^5$, $Q_4 = \pm 2^{31} + 2^{25} + 2^5 - 2^1$, and $Q_5 = \pm 2^{31} + 2^9 + 2^6 + 2^0$, and we want to obtain $f_5 = +2^{30} + 2^{27} + 2^{25} - 2^{20} - 2^8 - 2^6 + 2^4$.

Obtaining the Correct Q_5:

- Q_5[12, 8, 0] = 0
- Q_5[11 - 9, 7, 6] = 1

The Constant Bits of Q_5:
$Q_5[j]$ = 0, $j \in$ [30 - 13, 5 - 1]

- To obtain $f_5[j]$ = 0, we require $Q_5[j]$ = 1 for $j \in$ [30, 21]. See proof 18.
- To obtain $f_5[j]$ = -1, we require $Q_5[j]$ = 0 for $j \in$ [29, 28, 20]. See proof 21.
- To obtain $f_5[j]$ = 0, we require $Q_5[j]$ = 1 for $j \in$ [27, 19 - 16]. See proof 20.
- To obtain $f_5[j]$ = -1, we require $Q_5[j]$ = 0 for $j \in$ [26, 5]. See proof 33.
- To obtain $f_5[j]$ = -1, no conditions are required for Q_5[25]. See proof 34.
- To obtain $f_5[j]$ = -1, we require $Q_5[j]$ = 1 for $j \in$ [4]. See proof 25.
- To obtain $f_5[j]$ = 0, we require $Q_5[j]$ = 0 for $j \in$ [3 - 1]. See proof 22.
- To obtain $f_5[j]$ = 0, no conditions are required for Q_5[24 - 22, 15 - 13].

The Non-Constant Bits of Q_5:
$Q_5[j]$ = +1, $j \in$ [12, 8, 7, 0]

- To obtain $f_5[j]$ = 0, we require $Q_4[j]$ = 0 for $j \in$ [12, 7]. See proof 2^7.
- To obtain $f_5[j]$ = -1, we require $Q_3[j]$ = 1 and $Q_4[j]$ = 0 for $j \in$ [8]. See proof 15.
- To obtain $f_5[j]$ = 0, we require $Q_3[j] = Q_4[j]$ for $j \in$ [0]. See proof 12.

$Q_5[j]$ = -1, $j \in$ [11 - 9, 6]

- To obtain $f_5[j] = 0$, we require $Q_4[j] = 0$ for $j \in [11, 6]$. See proof 31.
- To obtain $f_5[j] = 0$, we require $Q_3[j] = Q_4[j]$ for $j \in [10, 9]$. See proof 13.

$Q_5[j] = \pm 1$, $j \in [31]$

- To obtain $f_5[j] = 1$, we require $Q_3[j] = Q_4[j]$ for $j \in [31]$. See proof 6.

Summary of the conditions for step 5:

- Q_4[12, 11, 8, 6] = Q4[7] = Q_5[29 - 26, 20, 12, 8, 5, 3 - 0] = 0
- Q_3[8] = Q_5[30, 27, 21, 19 - 16, 11 - 9, 7, 6, 4] = 1
- Q_3[31, 10, 9, 0] = Q_4[31, 10, 9, 0]

Step 6:

We have $Q_4 = \pm 2^{31} + 2^{25} + 2^5 - 2^1$, $Q_5 = \pm 2^{31} + 2^9 + 2^6 + 2^0$, and $Q_6 = \pm 2^{31} - 2^{20} - 2^{16}$, and we want to obtain $f_6 = -2^{25} - 2^{21} - 2^{16} - 2^{11} - 2^{10} - 2^5 + 2^3$.

Obtaining the Correct Q_6:

- Q_6[20, 16] = 0
- Q_6[21, 17] = 1

The Constant Bits of Q_6:
$Q_6[j] = 0$, $j \in$ [30 - 22, 19, 18, 15 - 0]

- To obtain $f_6[j] = 0$, we require $Q_6[j] = 1$ for $j \in [26, 2, 1]$. See proof 18.
- To obtain $f_6[j] = -1$, we require $Q_6[j] = 0$ for $j \in [25]$. See proof 21.
- To obtain $f_6[j] = 0$, we require $Q_6[j] = 0$ for $j \in [12, 8, 7, 0]$. See proof 22.
- To obtain $f_6[j] = -1$, we require $Q_6[j] = 1$ for $j \in [11, 10, 6]$. See proof 25.
- To obtain $f_6[j] = 0$, we require $Q_6[j] = 0$ for $j \in [9]$. See proof 24.
- To obtain $f_6[j] = +1$, we require $Q_6[j] = 0$ for $j \in [5, 3]$. See proof 19.
- To obtain $f_6[j] = 0$, we require $Q_6[j] = 1$ for $j \in [4]$. See proof 20.
- To obtain $f_6[j] = 0$, no conditions are required for Q_6[30 - 27, 24 - 22, 19, 18, 15 - 13].

The Non-Constant Bits of Q_6:
$Q_6[j] = +1$, $j \in [20, 16]$

- To obtain $f_6[j] = 0$, we require $Q_4[j] = Q_5[j]$ for $j \in [20]$. See proof 12.
- To obtain $f_6[j] = +1$, we require $Q_4[j] = 0$ and $Q_5[j] = 1$ for $j \in [16]$. See proof 14.

$Q_6[j] = -1$, $j \in [21, 17]$

- To obtain $f_6[j] = -1$, we require $Q_4[j] = 0$ and $Q_5[j] = 1$ for $j \in [21, 17]$. See proof 17.

$Q_6[j] = \pm 1$, $j \in [31]$

- To obtain $f_6[j] = 0$, we require $Q_4[j] = Q_5[j]$ for $j \in [31]$. See proof 5.

Summary of the conditions for step 6:

- Q_4[21, 17, 16] = Q_6[25, 20, 16, 12, 9 - 7, 5 - 3, 0] = 0

- $Q_5[21, 17, 16] = Q_6[26, 21, 17, 11, 10, 6, 4, 2, 1] = 1$
- $Q_4[20] = \overline{Q_5}[20]$
- $Q_4[31] = \overline{Q_5}[31]$

Step 7:

We have $Q_5 = \pm 2^{31} + 2^9 + 2^6 + 2^0$, $Q_6 = \pm 2^{31}$ - 2^{20} - 2^{16}, and $Q_7 = \pm 2^{31}$ - 2^{27} - 2^6, and we want to obtain $f_7 = \pm 2^{31}$ - $2^{27} + 2^{16}$.

Obtaining the Correct Q_7:

- $Q_7[27, 8 - 6] = 0$
- $Q_7[28, 9] = 1$

The Constant Bits of Q_7:
$Q_7[j] = 0$, $j \in [30, 29, 26 - 10, 5 - 0]$

- To obtain $f_7[j] = 0$, we require $Q_7[j] = 0$ for $j \in [21, 17]$. See proof 24.
- To obtain $f_7[j] = 0$, we require $Q_7[j] = 0$ for $j \in [20]$. See proof 22.
- To obtain $f_7[j] = +1$, we require $Q_7[j] = 1$ for $j \in [16]$. See proof 23.
- To obtain $f_7[j] = 0$, we require $Q_7[j] = 1$ for $j \in [12, 0]$. See proof 18.
- To obtain $f_7[j] = 0$, we require $Q_7[j] = 1$ for $j \in [11, 10]$. See proof 20.
- To obtain $f_7[j] = 0$, no conditions are required for $Q_7[30, 29, 26 - 22, 19, 18, 15 - 13, 5 - 1]$.

The Non-Constant Bits of Q_7:
$Q_7[j] = +1$, $j \in [27, 8 - 6]$

- To obtain $f_7[j] = -1$, we require $Q_5[j] = 1$ and $Q_6[j] = 0$ for $j \in [27]$. See proof 15.
- To obtain $f_7[j] = 0$, we require $Q_6[j] = 0$ for $j \in [8, 7]$. See proof 2^7.
- To obtain $f_7[j] = 0$, we require $Q_6[j] = 1$ for $j \in [6]$. See proof 30.

$Q_7[j] = -1$, $j \in [28, 9]$

- To obtain $f_7[j] = 0$, we require $Q_5[j] = Q_6[j]$ for $j \in [28]$. See proof 13.
- To obtain $f_7[j] = 0$, we require $Q_6[j] = 0$ for $j \in [9]$. See proof 31.

$Q_7[j] = \pm 1$, $j \in [31]$

- To obtain $f_7[j] = 1$, we require $Q_5[j] = Q_6[j]$ for $j \in [31]$. See proof 6.

Summary of the conditions for step 7:

- $Q_6[27, 9 - 7] = Q_7[27, 21, 20, 17, 8 - 6] = 0$
- $Q_5[27] = Q_6[6] = Q_7[28, 16, 12 - 9, 0] = 1$
- $Q_5[31, 28] = Q_6[31, 28]$

Step 8:

We have $Q_6 = \pm 2^{31}$ - 2^{20} - 2^{16}, $Q_7 = \pm 2^{31}$ - 2^{27} - 2^6, and $Q_8 = \pm 2^{31}$ - 2^{23} - $2^{17} + 2^{15}$, and we want to obtain $f_8 = +2^{25} + 2^{16}$ - 2^6.

Obtaining the Correct Q_8:

- Q_8[25 - 23, 16] = 0
- Q_8[26, 17, 15] = 1

The Constant Bits of Q_8:
$Q_8[j]$ = 0, $j \in$ [30 - 27, 22 - 18, 14 - 0]

- To obtain $f_8[j]$ = 0, we require $Q_8[j]$ = 0 for $j \in$ [28]. See proof 24.
- To obtain $f_8[j]$ = 0, we require $Q_8[j]$ = 0 for $j \in$ [27]. See proof 22.
- To obtain $f_8[j]$ = 0, we require $Q_8[j]$ = 1 for $j \in$ [21]. See proof 20.
- To obtain $f_8[j]$ = 0, we require $Q_8[j]$ = 1 for $j \in$ [20]. See proof 18.
- To obtain $f_8[j]$ = -1, we require $Q_8[j]$ = 1 for $j \in$ [9]. See proof 25.
- To obtain $f_8[j]$ = +1, we require $Q_8[j]$ = 1 for $j \in$ [8 - 6]. See proof 23.
- To obtain $f_8[j]$ = 0, no conditions are required for Q_8[30, 29, 22, 19, 18, 14 - 10, 5 - 0].

The Non-Constant Bits of Q_8:
$Q_8[j]$ = +1, $j \in$ [25 - 23, 16]

- To obtain $f_8[j]$ = +1, we require $Q_6[j]$ = 0 and $Q_7[j]$ = 1 for $j \in$ [25]. See proof 14.
- To obtain $f_8[j]$ = 0, we require $Q_6[j]$ = $Q_7[j]$ for $j \in$ [24, 23]. See proof 12.
- To obtain $f_8[j]$ = +1, we require $Q_7[j]$ = 1 for $j \in$ [16]. See proof 28.

$Q_8[j]$ = -1, $j \in$ [26, 17, 15]

- To obtain $f_8[j]$ = 0, we require $Q_6[j]$ = $Q_7[j]$ for $j \in$ [26, 15]. See proof 13.
- To obtain $f_8[j]$ = 0, we require $Q_7[j]$ = 0 for $j \in$ [17]. See proof 31.

$Q_8[j]$ = $\pm$1, $j \in$ [31]

- To obtain $f_8[j]$ = 0, we require $Q_6[j]$ = $Q_7[j]$ for $j \in$ [31]. See proof 5.

Summary of the conditions for step 8:

- Q_6[25] = Q_7[17] = Q_8[28, 27, 25 - 23, 16] = 0
- Q_7[25, 16] = Q_8[26, 21, 20, 17, 15, 9 - 6] = 1
- Q_6[26, 24, 23, 15] = Q_7[26, 24, 23, 15]
- Q_6[31] = $\overline{Q_7}$[31]

Step 9:

We have Q_7 = $\pm 2^{31}$ - 2^{27} - 2^6, Q_8 = $\pm 2^{31}$ - 2^{23} - 2^{17} + 2^{15}, and Q_9 = $\pm 2^{31}$ + 2^6 + 2^0, and we want to obtainf_9 = $\pm 2^{31}$ - 2^{26} + 2^{16} + 2^0.

Obtaining the Correct Q_9:

- Q_9[9, 1] = 0
- Q_9[8 - 6, 0] = 1

The Constant Bits of Q_9:
$Q_9[j]$ = 0, $j \in$ [30 - 10, 5 - 2]

- To obtain $f_9[j]$ = 0, we require $Q_9[j]$ = 1 for $j \in$ [28]. See proof 20.

- To obtain $f_9[j] = 0$, we require $Q_9[j] = 1$ for $j \in [27]$. See proof 18.
- To obtain $f_9[j] = -1$, we require $Q_9[j] = 1$ for $j \in [26]$. See proof 25.
- To obtain $f_9[j] = 0$, we require $Q_9[j] = 0$ for $j \in [25 - 23]$. See proof 22.
- To obtain $f_9[j] = 0$, we require $Q_9[j] = 0$ for $j \in [17, 15]$. See proof 24.
- To obtain $f_9[j] = +1$, we require $Q_9[j] = 1$ for $j \in [16]$. See proof 23.
- To obtain $f_9[j] = 0$, no conditions are required for $Q_9[30, 29, 22 - 18, 14 - 10, 5 - 2]$.

The Non-Constant Bits of Q_9:
$Q_9[j] = +1$, $j \in [9, 1]$

- To obtain $f_9[j] = 0$, we require $Q_8[j] = 1$ for $j \in [9]$. See proof 30.
- To obtain $f_9[j] = 0$, we require $Q_7[j] = Q_8[j]$ for $j \in [1]$. See proof 12.

$Q_9[j] = -1$, $j \in [8 - 6, 0]$

- To obtain $f_9[j] = 0$, we require $Q_8[j] = 1$ for $j \in [8 - 6]$. See proof 29.
- To obtain $f_9[j] = +1$, we require $Q_7[j] = 1$ and $Q_8[j] = 0$ for $j \in [0]$. See proof 16.

$Q_9[j] = \pm 1$, $j \in [31]$

- To obtain $f_9[j] = 1$, we require $Q_7[j] = Q_8[j]$ for $j \in [31]$. See proof 6.

Summary of the conditions for step 9:

- $Q_8[0] = Q_9[25 - 23, 17, 15, 9, 1] = 0$
- $Q_7[0] = Q_8[9 - 6] = Q_9[28 - 26, 15, 8 - 6, 0] = 1$
- $Q_7[31, 1] = Q_8[31, 1]$

Step 10:

We have $Q_8 = \pm 2^{31} - 2^{23} - 2^{17} + 2^{15}$, $Q_9 = \pm 2^{31} + 2^6 + 2^0$, and $Q_{10} = \pm 2^{31} + 2^{12}$, and we want to obtain $f_{10} = \pm 2^{31} + 2^6$.

Obtaining the Correct Q_{10}:

- $Q_{10}[12] = 0$

The Constant Bits of Q_{10}:
$Q_{10}[j] = 0$, $j \in [30 - 13, 11 - 0]$

- To obtain $f_{10}[j] = 0$, we require $Q_{10}[j] = 1$ for $j \in [26, 17, 15]$. See proof 20.
- To obtain $f_{10}[j] = 0$, we require $Q_{10}[j] = 1$ for $j \in [25 - 23, 16]$. See proof 18.
- To obtain $f_{10}[j] = +1$, we require $Q_{10}[j] = 1$ for $j \in [9]$. See proof 23.
- To obtain $f_{10}[j] = -1$, we require $Q_{10}[j] = 1$ for $j \in [8 - 6]$. See proof 25.
- To obtain $f_{10}[j] = 0$, we require $Q_{10}[j] = 0$ for $j \in [1]$. See proof 22.
- To obtain $f_{10}[j] = 0$, we require $Q_{10}[j] = 0$ for $j \in [0]$. See proof 24.
- To obtain $f_{10}[j] = 0$, no conditions are required for $Q_{10}[30 - 27, 22 - 18, 14, 13, 11, 10, 5 - 2]$.

The Non-Constant Bits of Q_{10}:
$Q_{10}[j] = +1$, $j \in [12]$

- To obtain $f_{10}[j] = 0$, we require $Q_8[j] = Q_9[j]$ for $j \in [12]$. See proof 12.

$Q_{10}[j] = \pm1$, $j \in [31]$

- To obtain $f_{10}[j] = 1$, we require $Q_8[j] = Q_9[j]$ for $j \in [31]$. See proof 6.

Summary of the conditions for step 10:

- $Q_{10}[12, 1, 0] = 0$
- $Q_{10}[26 - 23, 17 - 15, 9 - 6] = 1$
- $Q_8[31, 12] = Q_9[31, 12]$

Step 11:

We have $Q_9 = \pm2^{31} + 2^6 + 2^0$, $Q_{10} = \pm2^{31} + 2^{12}$, and $Q_{11} = \pm2^{31}$, and we want to obtain $f_{11} = \pm2^{31}$.

Obtaining the Correct Q_{11}: No conditions required

The Constant Bits of Q_{11}:
$Q_{11}[j] = 0$, $j \in [30 - 0]$

- To obtain $f_{11}[j] = 0$, we require $Q_{11}[j] = 0$ for $j \in [12]$. See proof 22.
- To obtain $f_{11}[j] = 0$, we require $Q_{11}[j] = 1$ for $j \in [9, 1]$. See proof 18.
- To obtain $f_{11}[j] = 0$, we require $Q_{11}[j] = 1$ for $j \in [8 - 6, 0]$. See proof 20.
- To obtain $f_{11}[j] = 0$, no conditions are required for $Q_{11}[30 - 13, 11, 10, 5 - 2]$.

The Non-Constant Bits of Q_{11}:
$Q_{11}[j] = \pm1$, $j \in [31]$

- To obtain $f_{11}[j] = 1$, we require $Q_9[j] = Q_{10}[j]$ for $j \in [31]$. See proof 6.

Summary of the conditions for step 11:

- $Q_{11}[12] = 0$
- $Q_{10}[9 - 6, 1, 0] = 1$
- $Q_9[31] = Q_{10}[31]$

Step 12:

We have $Q_{10} = \pm2^{31} + 2^{12}$, $Q_{11} = \pm2^{31}$, and $Q_{12} = \pm2^{31} - 2^{13} - 2^7$, and we want to obtain $f_{12} = \pm2^{31} + 2^{17}$.

Obtaining the Correct Q_{12}:

- $Q_{12}[18 - 13] = 0$
- $Q_{12}[19, 7] = 0$

The Constant Bits of Q_{12}:
$Q_{12}[j] = 0$, $j \in [30 - 20, 12 - 8, 6 - 0]$

- To obtain $f_{12}[j] = 0$, we require $Q_{12}[j] = 1$ for $j \in [12]$. See proof 18.

- To obtain $f_{12}[j] = 0$, no conditions are required for Q_{12}[30 - 20, 11 - 8, 6 - 0].

The Non-Constant Bits of Q_{12}:
$Q_{12}[j] = +1$, $j \in$ [18 - 13]

- To obtain $f_{12}[j] = +1$, we require $Q_{10}[j] = 0$ and $Q_{11}[j] = 1$ for $j \in$ [18]. See proof 14.
- To obtain $f_{12}[j] =$ -1, we require $Q_{10}[j] = 1$ and $Q_{11}[j] = 0$ for $j \in$ [17]. See proof 15.
- To obtain $f_{12}[j] = 0$, we require $Q_{10}[j] = Q_{11}[j]$ for $j \in$ [16 - 13]. See proof 12.

$Q_{12}[j] =$ -1, $j \in$ [19, 7]

- To obtain $f_{12}[j] = 0$, we require $Q_{10}[j] = Q_{11}[j]$ for $j \in$ [19, 7]. See proof 13.

$Q_{12}[j] = \pm 1$, $j \in$ [31]

- To obtain $f_{12}[j] = 1$, we require $Q_{10}[j] = Q_{11}[j]$ for $j \in$ [31]. See proof 6.

Summary of the conditions for step 12:

- Q_{10}[18] = Q_{11}[17] = Q_{12}[18 - 13] = 0
- Q_{10}[17] = Q_{11}[18] = Q_{12}[19, 12, 7] = 1
- Q_{10}[31, 19, 16 - 13, 7] = Q_{11}[31, 19, 16 - 13, 7]

Step 13:

We have $Q_{11} = \pm 2^{31}$, $Q_{12} = \pm 2^{31}$ - 2^{13} - 2^{7}, and $Q_{13} = \pm 2^{31} + 2^{24}$, and we want to obtain $f_{13} = \pm 2^{31}$ - 2^{13}.

Obtaining the Correct Q_{13}:

- Q_{13}[30] = 0
- Q_{13}[29 - 24] = 0

The Constant Bits of Q_{13}:
$Q_{13}[j] = 0$, $j \in$ [23 - 0]

- To obtain $f_{13}[j] =$ -1, we require $Q_{13}[j] = 1$ for $j \in$ [19]. See proof 25.
- To obtain $f_{13}[j] = +1$, we require $Q_{13}[j] = 1$ for $j \in$ [18 - 13]. See proof 23.
- To obtain $f_{13}[j] = 0$, we require $Q_{13}[j] = 0$ for $j \in$ [7]. See proof 24.
- To obtain $f_{13}[j] = 0$, no conditions are required for Q_{13}[23 - 20, 12 - 8, 6 - 0].

The Non-Constant Bits of Q_{13}:
$Q_{13}[j] = +1$, $j \in$ [30]

- To obtain $f_{13}[j] = 0$, we require $Q_{11}[j] = Q_{12}[j]$ for $j \in$ [30]. See proof 12.

$Q_{13}[j] =$ -1, $j \in$ [29 - 24]

- To obtain $f_{13}[j] = 0$, we require $Q_{11}[j] = Q_{12}[j]$ for $j \in$ [29 - 24]. See proof 13.

$Q_{13}[j] = \pm 1$, $j \in$ [31]

- To obtain $f_{13}[j] = 1$, we require $Q_{11}[j] = Q_{12}[j]$ for $j \in$ [31]. See proof 6.

Summary of the conditions for step 13:

- $Q_{13}[30, 7] = 0$
- $Q_{13}[29 - 24, 19 - 13] = 1$
- $Q_{11}[31 - 24] = Q_{12}[31 - 24]$

Step 14:

We have $Q_{11} = \pm 2^{31} - 2^{13} - 2^{7}$, $Q_{12} = \pm 2^{31} + 2^{24}$, and $Q_{13} = \pm 2^{31}$, and we want to obtain $f_{13} = +2^{30} + 2^{18}$.

Obtaining the Correct Q_{14}: No conditions required

The Constant Bits of Q_{14}:
$Q_{14}[j] = 0$, $j \in [30 - 0]$

- To obtain $f_{14}[j] = +1$, we require $Q_{14}[j] = 1$ for $j \in [30]$. See proof 23.
- To obtain $f_{14}[j] = 0$, we require $Q_{14}[j] = 0$ for $j \in [29 - 24]$. See proof 24.
- To obtain $f_{14}[j] = 0$, we require $Q_{14}[j] = 1$ for $j \in [19, 7]$. See proof 20.
- To obtain $f_{14}[j] = +1$, we require $Q_{14}[j] = 0$ for $j \in [18]$. See proof 19.
- To obtain $f_{14}[j] = 0$, we require $Q_{14}[j] = 1$ for $j \in [17 - 13]$. See proof 18.
- To obtain $f_{14}[j] = 0$, no conditions are required for $Q_{14}[23 - 20, 12 - 8, 6 - 0]$.

The Non-Constant Bits of Q_{14}:
$Q_{14}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{14}[j] = 0$, we require $Q_{12}[j] = Q_{13}[j]$ for $j \in [31]$. See proof 5.

Summary of the conditions for step 14:

- $Q_{14}[30 - 24, 7] = 0$
- $Q_{14}[19 - 13] = 1$
- $Q_{12}[31] = \overline{Q_{13}}[31]$

Step 15:

We have $Q_{13} = \pm 2^{31} + 2^{24}$, $Q_{14} = \pm 2^{31}$, and $Q_{15} = \pm 2^{31} + 2^{15} + 2^{3}$, and we want to obtain $f_{15} = \pm 2^{31} - 2^{25}$.

Obtaining the Correct Q_{15}:

- $Q_{15}[15, 3] = 0$

The Constant Bits of Q_{15}:
$Q_{15}[j] = 0$, $j \in [30 - 16, 14 - 4, 2 - 0]$

- To obtain $f_{15}[j] = 0$, we require $Q_{15}[j] = 1$ for $j \in [30]$. See proof 18.
- To obtain $f_{15}[j] = 0$, we require $Q_{15}[j] = 1$ for $j \in [29 - 26, 24]$. See proof 20.
- To obtain $f_{15}[j] = -1$, we require $Q_{15}[j] = 0$ for $j \in [25]$. See proof 21.
- To obtain $f_{15}[j] = 0$, no conditions are required for $Q_{15}[23 - 16, 14 - 4, 2 - 0]$.

The Non-Constant Bits of Q_{15}:
$Q_{15}[j] = +1$, $j \in [15, 3]$

- To obtain $f_{15}[j] = 0$, we require $Q_{13}[j] = Q_{14}[j]$ for $j \in [15, 3]$. See proof 12.

$Q_{15}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{15}[j] = 1$, we require $Q_{13}[j] = Q_{14}[j]$ for $j \in [31]$. See proof 6.

Summary of the conditions for step 15:

- $Q_{15}[25, 15, 3] = 0$
- $Q_{15}[30 - 26, 24] = 1$
- $Q_{13}[31, 15, 3] = Q_{14}[31, 15, 3]$

Round 2: $f_t = G(X, Y, Z)$

Step 16:

We have $Q_{14} = \pm 2^{31}$, $Q_{15} = \pm 2^{31} + 2^{15} + 2^{3}$, and $Q_{16} = \pm 2^{31} - 2^{29}$, and we want to obtain $f_{17} = \pm 2^{31}$.

Obtaining the Correct Q_{16}:

- $Q_{16}[29] = 1$

The Constant Bits of Q_{14}:
$Q_{14}[j] = 0$, $j \in [30 - 0]$

- To obtain $f_{16}[j] = 0$, we require $Q_{14}[j] = 0$ for $j \in [29]$. See proof 39.
- To obtain $f_{16}[j] = 0$, we require $Q_{14}[j] = 1$ for $j \in [15, 3]$. See proof 41.
- To obtain $f_{16}[j] = 0$, we need no requirements for $Q_{14}[30, 28 - 16, 14 - 4, 2 - 0]$.

The Non-Constant Bits of Q_{14}:
$Q_{14}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{16}[j] = 1$, we require $Q_{15}[j] = Q_{16}[j]$ for $j \in [31]$. See proof 38.

Summary of the conditions for step 16:

- $Q_{14}[29] = 0$
- $Q_{14}[15, 3] = 1$
- $Q_{15}[31] = Q_{16}[31]$

Step 17:

We have $Q_{15} = \pm 2^{31} + 2^{15} + 2^{3}$, $Q_{16} = \pm 2^{31} - 2^{29}$, and $Q_{17} = \pm 2^{31}$, and we want to obtain $f_{17} = \pm 2^{31}$.

Obtaining the Correct Q_{17}: No conditions required

The Constant Bits of Q_{15}:
$Q_{15}[j] = 0$, $j \in [30 - 16, 14 - 4, 2 - 0]$

- To obtain $f_{17}[j] = 0$, we require $Q_{15}[j] = 1$ for $j \in [29]$. See proof 40.
- To obtain $f_{17}[j] = 0$, we need no requirements for $Q_{15}[30, 28 - 16, 14 - 4, 2 - 0]$.

The Non-Constant Bits of Q_{15}:
$Q_{15}[j] = +1$, $j \in [3]$

- To obtain $f_{17}[j] = 0$, we require $Q_{16}[j] = Q_{17}[j]$ for $j \in [15, 3]$. See proof 43.

$Q_{15}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{17}[j] = 1$, we require $Q_{16}[j] = Q_{17}[j]$ for $j \in [31]$. See proof 38.

Summary of the conditions for step 17:

- $Q_{15}[29] = 1$
- $Q_{16}[31, 15, 3] = Q_{17}[31, 15, 3]$

Step 18:

We have $Q_{16} = \pm 2^{31}$ - 2^{29}, $Q_{17} = \pm 2^{31}$, and $Q_{18} = \pm 2^{31}$, and we want to obtain $f_{18} = \pm 2^{31}$.

Obtaining the Correct Q_{18}: No conditions required

The Constant Bits of Q_{16}:
$Q_{16}[j] = 0$, $j \in [30, 28 - 0]$

- To obtain $f_{18}[j] = 0$, we need no requirements for $Q_{16}[30, 28 - 0]$.

The Non-Constant Bits of Q_{16}:
$Q_{16}[j] = -1$, $j \in [29]$

- To obtain $f_{18}[j] = 0$, we require $Q_{17}[j] = Q_{18}[j]$ for $j \in [15]$. See proof 42.

$Q_{16}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{18}[j] = 1$, we require $Q_{17}[j] = Q_{18}[j]$ for $j \in [31]$. See proof 38.

Summary of the conditions for step 18:

- $Q_{17}[31, 29] = Q_{18}[31, 29]$

Step 19:

We have $Q_{17} = \pm 2^{31}$, $Q_{18} = \pm 2^{31}$, and $Q_{19} = \pm 2^{31} + 2^{17}$, and we want to obtain $f_{19} = \pm 2^{31}$.

Obtaining the Correct Q_{19}:

- $Q_{19}[17] = 0$

The Constant Bits of Q_{17}:
$Q_{17}[j] = 0$, $j \in [30 - 0]$

- To obtain $f_{19}[j] = 0$, we require $Q_{17}[j] = 0$ for $j \in [17]$. See proof 44.

- To obtain $f_{19}[j] = 0$, we need no requirements for Q_{17}[30 - 18, 16 - 0].

The Non-Constant Bits of Q_{17}:
$Q_{17}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{19}[j] = 1$, we require $Q_{18}[j] = Q_{19}[j]$ for $j \in [31]$. See proof 38.

Summary of the conditions for step 19:

- $Q_{17}[17] = Q_{19}[17] = 0$
- $Q_{18}[31] = Q_{19}[31]$

Step 20:

We have $Q_{18} = \pm 2^{31}$, $Q_{19} = \pm 2^{31} + 2^{17}$, and $Q_{20} = \pm 2^{31}$, and we want to obtain $f_{20} = \pm 2^{31}$.

Obtaining the Correct Q_{20}: No conditions required

The Constant Bits of Q_{18}:
$Q_{18}[j] = 0$, $j \in$ [30 - 0]

- To obtain $f_{20}[j] = 0$, we require $Q_{18}[j] = 1$ for $j \in [17]$. See proof 41.
- To obtain $f_{20}[j] = 0$, we need no requirements for Q_{18}[30 - 18, 16 - 0].

The Non-Constant Bits of Q_{18}:
$Q_{18}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{20}[j] = 1$, we require $Q_{19}[j] = Q_{20}[j]$ for $j \in [31]$. See proof 38.

Summary of the conditions for step 20:

- $Q_{18}[17] = 1$
- $Q_{19}[31] = Q_{20}[31]$

Step 21:

We have $Q_{19} = \pm 2^{31} + 2^{17}$, $Q_{20} = \pm 2^{31}$, and $Q_{21} = \pm 2^{31}$, and we want to obtain $f_{21} = \pm 2^{31}$.

Obtaining the Correct Q_{21}: No conditions required

The Constant Bits of Q_{19}:
$Q_{19}[j] = 0$, $j \in$ [30 - 18, 16 - 0]

- To obtain $f_{21}[j] = 0$, we need no requirements for Q_{19}[30 - 18, 16 - 0].

The Non-Constant Bits of Q_{19}:
$Q_{19}[j] = +1$, $j \in [17]$

- To obtain $f_{21}[j] = 0$, we require $Q_{20}[j] = Q_{21}[j]$ for $j \in [17]$. See proof 43.

$Q_{19}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{21}[j] = 1$, we require $Q_{20}[j] = Q_{21}[j]$ for $j \in [31]$. See proof 38.

Summary of the conditions for step 21:

- $Q_{20}[31, 17] = Q_{21}[31, 17]$

Step 22:

We have $Q_{20} = \pm 2^{31}$, $Q_{21} = \pm 2^{31}$, and $Q_{22} = \pm 2^{31}$, and we want to obtain $f_{22} = \pm 2^{31}$.

Obtaining the Correct Q_{22}: No conditions required

The Constant Bits of Q_{20}:
$Q_{20}[j] = 0$, $j \in [30 - 0]$

- To obtain $f_{22}[j] = 0$, we need no requirements for $Q_{20}[30 - 0]$.

The Non-Constant Bits of Q_{20}:
$Q_{20}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{22}[j] = 1$, we require $Q_{21}[j] = Q_{22}[j]$ for $j \in [31]$. See proof 38.

Summary of the conditions for step 22:

- $Q_{21}[31] = Q_{22}[31]$

Step 23:

We have $Q_{21} = \pm 2^{31}$, $Q_{22} = \pm 2^{31}$, and $Q_{23} = 0$, and we want to obtain $f_{23} = 0$.

Obtaining the Correct Q_{23}: No conditions required

The Constant Bits of Q_{21}:
$Q_{21}[j] = 0$, $j \in [30 - 0]$

- To obtain $f_{23}[j] = 0$, we need no requirements for $Q_{21}[30 - 0]$.

The Non-Constant Bits of Q_{21}:
$Q_{21}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{23}[j] = 0$, we require $Q_{23}[j] = 0$ for $j \in [31]$. See proof 45.

Summary of the conditions for step 23:

- $Q_{23}[31] = 0$

Step 24:

We have $Q_{22} = \pm 2^{31}$, $Q_{23} = 0$, and $Q_{24} = 0$, and we want to obtain $f_{24} = \pm 2^{31}$.

Obtaining the Correct Q_{24}: No conditions required

The Constant Bits of Q_{22}:
$Q_{22}[j] = 0$, $j \in [30 - 0]$

- To obtain $f_{24}[j] = 0$, we need no requirements for $Q_{22}[30$ - $0]$.

The Non-Constant Bits of Q_{22}:
$Q_{22}[j] = \pm 1$, $j \in [31]$

- To obtain $f_{24}[j] = 1$, we require $Q_{24}[j] = 1$ for $j \in [31]$. See proof 46.

Summary of the conditions for step 24:

- $Q_{24}[31] = 0$

Steps 25 to 31:

We have $Q_{t-2} = 0$, $Q_{t-1} = 0$, and $Q_t = 0$, so we will obtain $f_t = 0$. There are no conditions for these steps.

Round 3: $f_t = H(X,\ Y,\ Z)$

In round 3, the only differences in the Q_t occur in the most significant bit. The sign of the most significant bit is important only when it is rotated to some other bit position. However, during round 3, the differences in the most significant bits are always cancelled out by differences in the most significant bit in either f_t, Q_{t-3}, or W_t. Therefore, in round 3, the sign on the difference the most significant bit does not matter.

Steps 32 to 34:

We have $Q_{t-2} = 0$, $Q_{t-1} = 0$, and $Q_t = 0$, so we will obtain $f_t = 0$. There are no conditions for these steps.

Step 35:

We have $Q_{33} = 0$, $Q_{34} = 0$, and $Q_{35} = \pm 2^{31}$, so we will obtain $f_{35} = \pm 2^{31}$. See proof 47.

Step 36:

We have $Q_{34} = 0$, $Q_{35} = \pm 2^{31}$, and $Q_{36} = \pm 2^{31}$, so we will obtain $f_{36} = 0$. See proof 48.

Steps 37 to 47:

We have $Q_{t-2} = \pm 2^{31}$, $Q_{t-1} = \pm 2^{31}$, and $Q_t = \pm 2^{31}$, so we will obtain $f_t = \pm 2^{31}$. See proof 49.

Round 4: $f_t = I(X,\ Y,\ Z)$

The values of Q46 and Q47 each have two possibilities, $(\Delta Q_{46},\ \Delta Q_{47})$ = (-1, +1). Thus, there are four combinations of $(\Delta Q_{46}, \Delta Q_{47})$. In [7], $(\Delta Q_{46}, \Delta Q_{47})$ = (-1, +1) were chosen as the initial values for the fourth round of the first iteration. Thus, we must impose two conditions:

- $\Delta Q_{46} =$ -1 $\Rightarrow Q_{46} = 1$

- $\Delta Q_{47} = +1 \Rightarrow Q_{47} = 0$

Steps 48 to 49:

We have $\Delta Q_{t-2} = \pm 2^{31}$, $\Delta Q_{t-1} = \pm 2^{31}$, and $\Delta Q_t = \pm 2^{31}$, and we want to obtain $\Delta f_t = \pm 2^{31}$. Thus, we require that $\Delta Q_{t-2} = \Delta Q_t \Rightarrow Q_{t-2} = Q_t$. See proof 50.

Step 50:

We have $\Delta Q_{48} = \pm 2^{31}$, $\Delta Q_{49} = \pm 2^{31}$, and $\Delta Q_{50} = \pm 2^{31}$, and we want to obtain $\Delta f_{50} = 0$. Thus, we require that $\Delta Q_{48} = -\Delta Q_{50} \Rightarrow Q_{48} = \overline{Q_{50}}$. See proof 51.

Steps 51 to 59:

We have $\Delta Q_{t-2} = \pm 2^{31}$, $\Delta Q_{t-1} = \pm 2^{31}$, and $\Delta Q_t = \pm 2^{31}$, and we want to obtain $\Delta f_t = \pm 2^{31}$. Thus, we require that $\Delta Q_{t-2} = \Delta Q_t \Rightarrow Q_{t-2} = Q_t$. See proof 50.

Step 60:

We have $\Delta Q_{58} = \pm 2^{31}$, $\Delta Q_{59} = \pm 2^{31}$, and $\Delta Q_{60} = \pm 2^{31}$, and we want to obtain $\Delta f_{60} = 0$. Thus, we require that $\Delta Q_{58} =-\Delta Q_{60} \Rightarrow Q_{58} = \overline{Q_{60}}$. See proof 51.

Step 61:

We have $\Delta Q_{59} = \pm 2^{31}$, $\Delta Q_{60} = \pm 2^{31}$, and $\Delta Q_{61} = \pm 2^{31}$, and we want to obtain $\Delta f_{61} = \pm 2^{31}$. Thus, we require that $\Delta Q_{59} = \Delta Q_{61} \Rightarrow Q_{59} = Q_{61}$. See proof 50.

Step 62:

<u>Obtaining the Correct ΔQ_{62}:</u>

- $Q_{62}[25] = 1$

We have $\Delta Q_{60} = 2^{31}$, $\Delta Q_{61} = 2^{31}$, and $\Delta Q_{62} = 2^{31}$ - 2^{25}, and we want to obtain $\Delta f_{62} = 2^{31}$. Thus, we must impose two conditions. First, to obtain $\Delta f_{62} = \pm 1$, we require that $\Delta Q_{60} = \Delta Q_{62} \Rightarrow Q_{60} = Q_{62}$. See proof 50. Second, to obtain $f_{62}[25] = 0$, we require that $Q_{60}[25] = 0$. See proof 54.

Step 63:
<u>Obtaining the Correct ΔQ_{63}:</u>

- $Q_{63}[25] = 1$

We have $\Delta Q_{61} = 2^{31}$, $\Delta Q_{62} = 2^{31}$ - 2^{25}, and $Q_{63} = 2^{31}$ - 2^{25}, and we want to obtain $f_{63} = 2^{31}$. Thus, we must impose two conditions. First, to obtain $f_{63}[31] = \pm 1$, we require that $Q_{61} = Q_{63} \Rightarrow Q_{61} = Q_{63}$. See proof 50. Second, to obtain $f_{63}[25] = 0$, we require that $Q_{61}[25] = 1$. See proof 55.

7.3 Complexity of the Attack

Tables 3, 4, 5, and 6 on the following four pages summarize the conditions for the propagation of the differences through the f_t functions for the first and second blocks. A random message will satisfy all of the conditions for the first block with probability 2^{-277} since the values of A, B, H, I, and J are arbitrary. Similarly, a random message will satisfy all of the conditions for the second block with probability 2^{-319} since the values of A, C, I, and J are arbitrary. These probabilities preclude a second pre-image attack. The vast majority of the conditions, however, occur during the first 16 steps of each block. Only 39 in each block do not.

Suppose we define an "f_t-good" message as a message which satisfies all of the conditions for the first round. With single-message modification, we can find "f_t-good" messages with probability 2^{-39} for each block. For our collision differential to hold, our message must be both "T_t-good" and "f_t-good." We found in section 6 that the probability of obtaining a "T_t-good" message was $2^{-2.4}$ for each block. Therefore, the probability of finding a message which is both "T_t-good" and "f_t-good" for each block is:

$$2^{-39} \times 2^{-2.4} \approx 2^{-41}.$$

This means that the complexity of the attack for each block is 2^{41}. Thus, the complexity of the overall attack is:

$$2^{41} + 2^{41} = 2^{42}.$$

8 Proofs

We use the following notation for each proof:

"$\pm$" $\Rightarrow \Delta X = \pm 1$, i.e., X' - $X = \pm 1$
"+" $\Rightarrow \Delta X = +1$, i.e., X' - $X = +1$
"-" $\Rightarrow \Delta X =$ -1, i.e., X' - $X =$ -1
"0" $\Rightarrow \Delta X = 0$, i.e., $X' = X$.

For the title of each proof, we use the shorthand format $(x\ y\ z\ w)$ where
$x\ y\ z\ w \Rightarrow \Delta Q_t = x$, $\Delta Q_{t-1} = y$, $\Delta Q_{t-2} = z$, and $\Delta f_t = w$.

For example,

$+\ 0\ +\ + \Rightarrow \Delta Q_t = +1$, $\Delta Q_{t-1} = 0$, $\Delta Q_{t-2} = +1$, and $\Delta f_t = +1$.

8.1 Proofs for Round 1

For round 1, note that $f_t = F(X,\ Y,\ Z) = (X \wedge Y) \vee (\neg X \wedge Z)$.

1: $\pm$ 0 0 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (\pm 1,\ 0,\ 0)$, i.e., Q'_t - $Q_t = \pm 1$, $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = Q_{t-2}$.

t	Conditions on Q_t			
	Case One	Eq	Def	None
3	`.........vvv0vvvvvvv0vvvv0......`	13v	3	16
4	`C.......0^^^1^^^^^^^1^^^^0......`	13^	5	11
5	`Cvvv1v0v0100000000000000001vv1v1`	8v	24	
6	`B^^^0^1^01111111101111000010^^0^1`	8^	24	
7	`A0000011111111101111100000100000`		32	
8	`000000011..100010.0v010101000000`	1v	28	3
9	`E1111011...100000.1^..1100111101`	1^	25	6
10	`A1......0..111111101...001....00`		17	15
11	`A0....vv....000...00...011....10`	2v	15	15
12	`A0....^^....10000001...10.......`	2^	12	18
13	`A1....01....1111111....00...1...`		14	18
14	`A.0...00....1011111....11...1...`		14	18
15	`H.1...01........1...........0...`		6	26
		Eq	Def	Combined
	Subtotal $0 \leq t \leq 15$: *Case One*	24	219	243
	Case Two	Eq	Def	None
3	`.........vvv0vvvvvvv0vvvv0......`	13v	3	16
4	`0.......0^^^1^^^^^^^1^^^^0......`	13^	5	11
5	`0...0v0v0100000000000000001vv1v1`	5v	24	3
6	`....1^1^01111111101111000010^^0^1`	5^	23	4
7	`1...1011111111101111100000100000`		29	2
8	`0...00011..100010.0v010101000000`	1v	25	6
9	`E...1011...100000.1^..1100111101`	1^	22	9
10	`A1......0..111111101...001....00`		17	15
11	`A0....vv....000...00...011....10`	2v	15	15
12	`A0....^^....10000001...10.......`	2^	12	18
13	`A1....01....1111111....00...1...`		14	18
14	`A.0...00....1011111....11...1...`		14	18
15	`H.1...01........1...........0...`		6	26
		Eq	Def	Combined
	Subtotal $0 \leq t \leq 15$: *Case Two*	21	209	230

Table 3. Conditions for on Q_t, $15 \leq t \leq 32$ in the first block. There are two variables with two possibilities each: $A \in \{0,1\}$, $B \in \{0,1\}$, with $C = \overline{A \oplus B}$, $E = \overline{A}$. The column headed by "Eq" contains the number of equality relationships of the form $Q_t[j] = Q_{t-1}[j]$. The column headed by "Def" contains the number of definitions of the form $Q_t[j] = 0$ or $Q_t[j] = 1$. The column headed by "None" contains the number of bits with no conditions. When computing subtotals, the column headed by "Comb." contains the combination of equality relationships and definitions.

t	Conditions on Q_t	Eq	Def	None
14	`A.0...00....1011111....11...1...`			
15	`H.1...01........1...........0...`			
16	`H.1.............v...........v...`	2v	2	28
17	`H.v...........0.^...........^...`	1v,2^	2	27
18	`H.^...........1.................`	1^	2	29
19	`H.............0.................`		2	30
20	`H.............v.................`	1v	1	30
21	`H.............^.................`	1^	1	30
22	`H...............................`		1	31
23	`0...............................`		1	31
24	`1...............................`		1	31
25-45	`................................`			32
46	`I...............................`		1	31
47	`J...............................`		1	31
48	`I...............................`		1	31
49	`J...............................`		1	31
50	`K...............................`		1	31
51	`J...............................`		1	31
52	`K...............................`		1	31
53	`J...............................`		1	31
54	`K...............................`		1	31
55	`J...............................`		1	31
56	`K...............................`		1	31
57	`J...............................`		1	31
58	`K...............................`		1	31
59	`J...............................`		1	31
60	`I.....0.........................`		2	30
61	`J.....1.........................`		2	30
62	`I.....0.........................`		2	30
63	`J.....0.........................`		2	30
		Eq	Def	Combined
	Sub-total: $16 \leq t \leq 31$	4	13	17
	Sub-total: $32 \leq t \leq 47$	-	2	2
	Sub-total: $48 \leq t \leq 63$	-	20	20
	SubTotal: $16 \leq t \leq 63$ (This Table)	4	35	
	Sub-total: $-2 \leq t \leq 15$: *Case One*	24	219	243
	Sub-total: $-2 \leq t \leq 15$: *Case Two*	21	209	230
	Total: $-2 \leq t \leq 63$: *Case One*	28	254	282
	Total: $-2 \leq t \leq 63$: *Case Two*	25	244	269

Table 4. Conditions for on Q_t, $15 \leq t \leq 32$ in the first block. There are three new variables with two possibilities each: $H \in \{0, 1\}$, $I \in \{0, 1\}$, and $J \in \{0, 1\}$, with $K = \overline{I}$. The column headed by "Eq" contains the number of equality relationships of the form $Q_t[j] = Q_{t-1}[j]$. The column headed by "Def" contains the number of definitions of the form $Q_t[j] = 0$ or $Q_t[j] = 1$. The column headed by "None" contains the number of bits with no conditions. In the last few rows, the column headed by "Comb." contains the combination of equality relationships and definitions.

t	Conditions on Q_t	Eq	Def	None
-2	`A.....0.........................`		2	30
-1	`A....01.........................`		3	29
0	`A....00...................v.....`	1v	3	28
1	`Bvvv010...1vvvvv...v0...v1^.....`	10v,1^	7	14
2	`B^^^110...0^^^^^...^1...^10vv00.`	2v,10^	10	10
3	`B011111...011111...01vv1011^^11v`	3v,2^	21	6
4	`B011101...000100...00^^00001000^`	3^	23	6
5	`A100101...101111...0111001010000`		26	6
6	`A..0010v1.10..101..0110001010110`	1v	24	7
7	`B..1011^1.00..011..1111000....v1`	1v,1^	19	11
8	`B..001000.11..101..v..1111....^0`	1v,1^	17	13
9	`B..111000.....010..^..0111....01`	1^	16	15
10	`B....1111...v0111100..1111....00`	1v	18	13
11	`Bvvvvvvv....^1011100..1111....11`	7v,1^	14	10
12	`B^^^^^^^....10000001....1.......`	7^	10	15
13	`A0111111....1111111.....0...1...`		17	15
14	`A1000000....1011111.....1...1...`		17	15
15	`C1111101........0...........0...`		10	22
		Eq	Def	Combined
	Sub-total: $-2 \leq t \leq 15$	27	257	

Table 5. Conditions on ∇Q_t, $-2 \leq t \leq 15$, of the second block to get the correct propagation of differences through f_t. The attacker can allow $A \in \{0,1\}$, $C \in \{0,1\}$ with $B = \overline{A}$. The column headed by "Eq" contains the number of relationships of the form $Q_t[j] = Q_{t-1}[j]$. The column headed by "Def" contains the number of definitions of the form $Q_t[j] = 0$ or $Q_t[j] = 1$. The column headed by "None" contains the number of bits with no conditions. In the last row, the column headed by "Comb." contains the combination of equality relationships and definitions. Note the conditions on Q_{-2},Q_{-1}, Q_0 apply to the intermediate hash value $IHV^{(1)}$.

t	Conditions on Q_t	Eq	Def	None
14	A1000000....1011111.....1...1...			
15	C1111101........0...........0...			
16	C.1.............v...........v...	2v	2	28
17	C.v...........0.^...........^...	2^,1v	2	27
18	C.^...........1.................	1^	2	29
19	C.............0.................		2	30
20	C.............v.................	1v	1	30
21	C.............^.................	1^	1	30
22	C...............................		1	31
23	0...............................		1	31
24	1...............................		1	31
25-31	....			32
32-45	....			32
46	I...............................		1	31
47	J...............................		1	31
48	I...............................		1	31
49	J...............................		1	31
50	K...............................		1	31
51	J...............................		1	31
52	K...............................		1	31
53	J...............................		1	31
54	K...............................		1	31
55	J...............................		1	31
56	K...............................		1	31
57	J...............................		1	31
58	K...............................		1	31
59	J...............................		1	31
60	I.....0.........................		2	30
61	J.....1.........................		2	30
62	I.....1.........................		2	30
63	J.....1.........................		2	30
		Eq	Def	Combined
	Sub-total: $16 \leq t \leq 31$	4	13	
	Sub-total: $32 \leq t \leq 47$	-	2	
	Sub-total: $48 \leq t \leq 63$	-	20	
	SubTotal: $16 \leq t \leq 63$ (This Table)	4	35	
	Sub-total: $-2 \leq t \leq 15$ (Table 5)	27	257	
	Total: $-2 \leq t \leq 63$	31	292	323

Table 6. Conditions on ∇Q_t, $16 \leq t \leq 63$, of the second block to get the correct propagation of differences through f_t. There are two new variables with two possibilities each: $I \in \{0,1\}$, and $J \in \{0,1\}$, with $K = \overline{I}$. The column headed by "Eq" contains the number of equality relationships of the form $Q_t[j] = Q_{t-1}[j]$. The column headed by "Def" contains the number of definitions of the form $Q_t[j] = 0$ or $Q_t[j] = 1$. The column headed by "None" contains the number of bits with no conditions. In the last few rows, the column headed by "Comb." contains the combination of equality relationships and definitions.

We want $\Delta f_t = 0$, i.e., $f_t' = f_t$.

$f_t' = F[Q_t', Q_{t-1}', Q_{t-2}']$ $\quad$ $f_t = F[Q_t, Q_{t-1}, Q_{t-2}]$
$f_t' = [(Q_t' \wedge Q_{t-1}') \vee (\neg Q_t' \wedge Q_{t-2}')]$ $\quad$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$

To ensure $f_t = \pm 1$, we require that $Q_t = Q_t = \overline{Q_{t-1} \oplus Q_{t-2}}$. Now, Q_t' - Q_t = -1, +1, $Q_{t-1} = Q_{t-1}$ = (0, 1), and Q_{t-2}' - Q_{t-2} = -1, +1. We consider four possibilities. First, we have $Q_{t-1} = 0$ and $Q_{t-2} = 0$, so Q_t = 1. This gives us $Q_t = 1$, $Q_t' = 0$, $Q_{t-1} = Q_{t-1}' = 0$, $Q_{t-2} = 0$, and $Q_{t-2}' = 1$. Thus,

$f_t' = [(Q_t' \wedge Q_{t-1}') \vee (\neg Q_t' \wedge Q_{t-2}')]$ $\quad$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f_t' = [(0 \wedge 0) \vee (1 \wedge 1)]$ $\quad$ $f_t' = [(1 \wedge 0) \vee (0 \wedge 0)]$
$f_t' = [0 \vee 1]$ $\quad$ $f_t = [0 \vee 0]$
$f_t' = 1.$ $\quad$ $f_t = 0.$

Second, when $Q_t' = 0$, $Q_t = 1$, $Q_{t-1}' = Q_{t-1} = Q_{t-2} = Q_{t-2}' = 1$, then

$f_t' = [(Q_t' \wedge Q_{t-1}') \vee (\neg Q_t' \wedge Q_{t-2}')]$ $\quad$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f_t' = [(0 \wedge) \vee (1 \wedge 1)]$ $\quad$ $f_t = [(1 \wedge 1) \vee (0 \wedge 1)]$
$f_t' = [0 \vee 1]$ $\quad$ $f_t = [1 \vee 0]$
$f_t' = 1.$ $\quad$ $f_t = 1.$

Third, when $Q_t' = 1$, $Q_t = 0$, $Q_{t-1}' = Q_{t-1} = Q_{t-2} = Q_{t-2}' = 0$, then

$f_t' = [(Q_t' \wedge Q_{t-1}') \vee (\neg Q_t' \wedge Q_{t-2}')]$ $\quad$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
f_t' $[(1 \wedge 0) \vee (0 \wedge 0)]$ $\quad$ $f_t = [(0 \wedge 0) \vee (1 \wedge 0)]$
$f_t' = [0 \vee 0]$ $\quad$ $f_t = [0 \vee 0]$
$f_t' = 0.$ $\quad$ $f_t = 0.$

Fourth, when $Q_t' = 1$, $Q_t = 0$, $Q_{t-1}' = Q_{t-1} = Q_{t-2} = Q_{t-2}' = 1$, then

$f_t' = [(Q_t' \wedge Q_{t-1}') \vee (\neg Q_t' \wedge Q_{t-2}')]$ $\quad$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f_t' = [(1 \wedge 1) \vee (0 \wedge 1)]$ $\quad$ $f_t = [(0 \wedge 1) \vee (1 \wedge 1)]$
$f_t' = [1 \vee 0]$ $\quad$ $f_t = [0 \vee 1]$
$f_t' = 1.$ $\quad$ $f_t = 1.$

Condition(s) required for this proof: $Q_{t-1} = Q_{t-2}$

2: $\pm$ $\pm$ 0 0

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2}) = (\pm 1, \pm 1, 0)$, i.e., Q_t' - Q_t = ± 1, Q_{t-1}' - Q_{t-1} = ± 1, and Q_{t-2}' = Q_{t-2}. We want $\Delta f_t = 0$, i.e., $f_t' = f_t$.

$f_t' = F[Q_t', Q_{t-1}', Q_{t-2}']$ $\quad$ $f_t = F[Q_t, Q_{t-1}, Q_{t-2}]$
$f_t' = [(Q_t' \wedge Q_{t-1}') \vee (\neg Q_t' \wedge Q_{t-2}')]$ $\quad$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$

To ensure $f_t = 0$, we require that $Q_t = \overline{Q_{t-1} \oplus Q_{t-2}}$. Now, Q'_t - Q_t = -1, +1, Q'_{t-1} - Q_{t-1} = -1, +1, and $Q'_{t-2} = Q_{t-2}$ = (0, 1). We consider four possibilities. First, we have $Q_{t-1} = 0$ and $Q_{t-2} = 0$, so $Q_t = 1$. This gives us $Q_t = 1$, $Q'_t = 0$, $Q_{t-1} = 0$, $Q'_{t-1} = 1$, and $Q_{t-2} = Q'_{t-2} = 0$. Thus,

$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$	$f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(0 \wedge 1) \vee (1 \wedge 0)]$	$f'_t = [(1 \wedge 0) \vee (0 \wedge 0)]$
$f'_t = [0 \vee 0]$	$f_t = [0 \vee 0]$
$f'_t = 0.$	$f_t = 0.$

Second, we have $Q_{t-1} = 0$ and $Q_{t-2} = 1$, so $Q_t = 0$. This gives us $Q_t = 0$, $Q'_t = 1$, $Q_{t-1} = 0$, $Q'_{t-1} = 1$, and $Q_{t-2} = Q'_{t-2} = 1$. Thus,

$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$	$f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(1 \wedge 1) \vee (0 \wedge 1)]$	$f_t = [(0 \wedge 0) \vee (1 \wedge 1)]$
$f'_t = [1 \vee 0]$	$f_t = [0 \vee 1]$
$f'_t = 1.$	$f_t = 1.$

Third, we have $Q_{t-1} = 1$ and $Q_{t-2} = 0$, so $Q_t = 0$. This gives us $Q_t = 0$, $Q'_t = 1$, $Q_{t-1} = 1$, $Q'_{t-1} = 0$, and $Q_{t-2} = Q'_{t-2} = 0$. Thus,

$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$	$f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
f'_t $[(1 \wedge 0) \vee (0 \wedge 0)]$	$f_t = [(0 \wedge 1) \vee (1 \wedge 0)]$
$f'_t = [0 \vee 0]$	$f_t = [0 \vee 0]$
$f'_t = 0.$	$f_t = 0.$

Fourth, we have $Q_{t-1} = 1$ and $Q_{t-2} = 1$, so $Q_t = 1$. This gives us $Q_t = 1$, $Q'_t = 0$, $Q_{t-1} = 1$, $Q'_{t-1} = 0$, and $Q_{t-2} = Q'_{t-2} = 1$. Thus,

$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$	$f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(0 \wedge 0) \vee (1 \wedge 1)]$	$f_t = [(1 \wedge 1) \vee (0 \wedge 1)]$
$f'_t = [0 \vee 1]$	$f_t = [1 \vee 0]$
$f'_t = 1.$	$f_t = 1.$

Condition(s) required for this proof: $Q_t = Q_t = \overline{Q_{t-1} \oplus Q_{t-2}}$.

3: 0 ± ± ±

We are given: (ΔQ_t, ΔQ_{t-1}, ΔQ_{t-2}) = (0, ±1, ±1), i.e., $Q'_t = Q_t$, Q'_{t-1} - Q_{t-1} = ±1, and Q'_{t-2} - Q_{t-2} = ±1.
We want: $\Delta f_t = \pm 1$, i.e.,f'_t - f_t = ±1.

$f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}]$	$f_t = F[Q_t, Q_{t-1}, Q_{t-2}]$
$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$	$f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$

To ensure $f_t = \pm 1$, no requirements are necessary. Now, Q'_t = Qt, and Q'_{t-1} - Q_{t-1} = -1, +1, and $\Delta Q'_{t-2}$ - Q_{t-2} = -1, +1. We consider eight possibilities. First, when $Q'_t = Q_t = 0$, $Q'_{t-1} = 0$, $Q_{t-1} = 1$, $\Delta Q'_{t-2} = 0$, and $Q_{t-2} = 1$, then

$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$	$f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(0 \wedge 0) \vee (1 \wedge 0)]$	$f_t = [(0 \wedge 1) \vee (1 \wedge 1)]$
$f'_t = [0 \vee 0]$	$f_t = [0 \vee 1]$
$f'_t = 0.$	$f_t = 1.$

Second, when $Q'_t = Q_t = 0$, $Q'_{t-1} = 0$, $Q_{t-1} = 1$, $\Delta Q'_{t-2} = 1$, and $Q_{t-2} = 0$, then

$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$	$f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(0 \wedge 0) \vee (1 \wedge 1)]$	$f_t = [(0 \wedge 1) \vee (1 \wedge 0)]$
$f'_t = [0 \vee 1]$	$f_t = [0 \vee 0]$
$f'_t = 1.$	$f_t = 0.$

Third, when $Q'_t = Q_t = 0$, $Q'_{t-1} = 1$, $Q_{t-1} = 0$, $\Delta Q'_{t-2} = 0$, and $Q_{t-2} = 1$, then

$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$	$f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(0 \wedge 1) \vee (1 \wedge 0)]$	$f_t = [(0 \wedge 0) \vee (1 \wedge 1)]$
$f'_t = [0 \vee 0]$	$f_t = [0 \vee 1]$
$f'_t = 0.$	$f_t = 1.$

Fourth, when $Q'_t = Q_t = 0$, $Q'_{t-1} = 1$, $Q_{t-1} = 0$, $\Delta Q'_{t-2} = 1$, and $Q_{t-2} = 0$, then

$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$	$f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(0 \wedge) \vee (1 \wedge 1)]$	$f_t = [(0 \wedge 0) \vee (1 \wedge 0)]$
$f'_t = [0 \vee 1]$	$f_t = [0 \vee 0]$
$f'_t = 1.$	$f_t = 0.$

Fifth, when $Q'_t = Q_t = 1$, $Q'_{t-1} = 0$, $Q_{t-1} = 1$, $\Delta Q'_{t-2} = 0$, and $Q_{t-2} = 1$, then

$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$	$f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t\ [(1 \wedge 0) \vee (0 \wedge 0)]$	$f_t = [(1 \wedge 1) \vee (0 \wedge 1)]$
$f'_t = [0 \vee 0]$	$f_t = [1 \vee 0]$
$f'_t = 0.$	$f_t = 1.$

Sixth, when $Q'_t = Q_t = 1$, $Q'_{t-1} = 0$, $Q_{t-1} = 1$, $\Delta Q'_{t-2} = 1$, and $Q_{t-2} = 0$, then

$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$	$f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t\ [(1 \wedge 0) \vee (0 \wedge 1)]$	$f_t = [(1 \wedge 1) \vee (0 \wedge 0)]$
$f'_t = [0 \vee 0]$	$f_t = [1 \vee 0]$
$f'_t = 0.$	$f_t = 1.$

Seventh, when $Q'_t = Q_t = 1$, $Q'_{t-1} = 1$, $Q_{t-1} = 0$, $\Delta Q'_{t-2} = 0$, and $Q_{t-2} = 1$, then

$$\begin{array}{ll} f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(1 \wedge 1) \vee (0 \wedge 0)] & f_t = [(1 \wedge 0) \vee (0 \wedge 1)] \\ f'_t = [1 \vee 0] & f_t = [0 \vee 0] \\ f'_t = 1. & f_t = 0. \end{array}$$

Eighth, when $Q'_t = Q_t = 1$, $Q'_{t-1} = 1$, $Q_{t-1} = 0$, $\Delta Q'_{t-2} = 1$, and $Q_{t-2} = 0$, then

$$\begin{array}{ll} f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(1 \wedge 1) \vee (0 \wedge 1)] & f'_t = [(1 \wedge 0) \vee (0 \wedge 0)] \\ f'_t = [1 \vee 0] & f_t = [0 \vee 0] \\ f'_t = 1. & f_t = 0. \end{array}$$

Condition(s) required for this proof: none

4: $\pm$ 0 $\pm$ $\pm$

We are given: (ΔQ_t, ΔQ_{t-1}, ΔQ_{t-2}) = ($\pm$1, 0, $\pm$1), i.e., Q'_t - Q_t = $\pm$1, $Q'_{t-1} = Q_{t-1}$, and Q'_{t-2} - Q_{t-2} = $\pm$1.
We want: $\Delta f_t = \pm 1$, i.e., f'_t - f_t = $\pm$1.

$$\begin{array}{ll} f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \end{array}$$

To ensure $f_t = \pm 1$, we require that $Q_t = Q_t = \overline{Q_{t-1} \oplus Q_{t-2}}$. Now, Q'_t - Q_t = -1, +1, $Q_{t-1} = Q_{t-1}$ = (0, 1), and Q'_{t-2} - Q_{t-2} = -1, +1. We consider four possibilities. First, we have $Q_{t-1} = 0$ and $Q_{t-2} = 0$, so Q_t = 1. This gives us $Q_t = 1$, $Q'_t = 0$, $Q_{t-1} = Q'_{t-1} = 0$, $Q_{t-2} = 0$, and $Q'_{t-2} = 1$. Thus,

$$\begin{array}{ll} f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(0 \wedge 0) \vee (1 \wedge 1)] & f'_t = [(1 \wedge 0) \vee (0 \wedge 0)] \\ f'_t = [0 \vee 1] & f_t = [0 \vee 0] \\ f'_t = 1. & f_t = 0. \end{array}$$

Second, we have $Q_{t-1} = 0$ and $Q_{t-2} = 1$, so $Q_t = 0$. This gives us $Q_t = 0$, $Q'_t = 1$, $Q_{t-1} = Q'_{t-1} = 1$, $Q_{t-2} = 0$, and $Q'_{t-1} = 1$. Thus,

$$\begin{array}{ll} f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(1 \wedge 1) \vee (0 \wedge 1)] & f_t = [(0 \wedge 1) \vee (1 \wedge 0)] \\ f'_t = [1 \vee 0] & f_t = [0 \vee 0] \\ f'_t = 1. & f_t = 0. \end{array}$$

Third, we have $Q_{t-1} = 1$ and $Q_{t-2} = 0$, so $Q_t = 0$. This gives us $Q_t = 0$, $Q'_t = 1$, $Q_{t-1} = Q'_{t-1} = 0$, $Q_{t-2} = 1$, and $Q'_{t-2} = 0$. Thus,

$$\begin{array}{ll}
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t\ [(1 \wedge 0) \vee (0 \wedge 0)] & f_t = [(0 \wedge 0) \vee (1 \wedge 1)] \\
f'_t = [0 \vee 0] & f_t = [0 \vee 1] \\
f'_t = 0. & f_t = 1.
\end{array}$$

Fourth, we have $Q_{t-1} = 1$ and $Q_{t-2} = 1$, so $Q_t = 1$. This gives us $Q_t = 1$, $Q'_t = 0$, $Q_{t-1} = Q'_{t-1} = 1$, $Q_{t-2} = 1$, and $Q'_{t-2} = 0$. Thus,

$$\begin{array}{ll}
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(0 \wedge 1) \vee (1 \wedge 0)] & f_t = [(1 \wedge 1) \vee (0 \wedge 1)] \\
f'_t = [0 \vee 0] & f_t = [1 \vee 0] \\
f'_t = 0. & f_t = 1.
\end{array}$$

Condition(s) required for this proof: $Q_t = Q_t = \overline{Q_{t-1} \oplus Q_{t-2}}$

5: $\pm\ \pm\ \pm\ 0$

We are given: $(\mathit{\Delta} Q_t,\ \mathit{\Delta} Q_{t-1},\ \mathit{\Delta} Q_{t-2}) = (\pm 1,\ \pm 1,\ \pm 1)$, i.e., Q'_t - $Q_t = \pm 1$, Q'_{t-1} - $Q_{t-1} = \pm 1$, and Q'_{t-2} - $Q_{t-2} = \pm 1$.
We want $\mathit{\Delta} f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll}
f'_t = F[Q'_t,\ Q'_{t-1},\ Q'_{t-2}] & f_t = F[Q_t,\ Q_{t-1},\ Q_{t-2}] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]
\end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-1} = \overline{Q_{t-2}}$. This gives us $Q_{t-1} = \overline{Q_{t-2}} = (0,\ 1)$. We also have $Q_t = (0,\ 1)$. We consider four possibilities. First, when $Q_t = 0$, $Q'_t = 1$, $Q_{t-1} = 0$, $Q'_{t-1} = 1$, $Q_{t-2} = 1$, and $Q'_{t-2} = 0$, then

$$\begin{array}{ll}
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(1 \wedge 1) \vee (0 \wedge 0)] & f_t = [(0 \wedge 0) \vee (1 \wedge 1)] \\
f'_t = [1 \vee 0] & f_t = [0 \vee 1] \\
f'_t = 1. & f_t = 1.
\end{array}$$

Second, when $Q_t = 0$, $Q'_t = 1$, $Q_{t-1} = 1$, $Q'_{t-1} = 0$, $Q_{t-2} = 0$, and $Q'_{t-2} = 1$, then

$$\begin{array}{ll}
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(1 \wedge 0) \vee (0 \wedge 1)] & f_t = [(0 \wedge 1) \vee (1 \wedge 0)] \\
f'_t = [0 \vee 0] & f_t = [0 \vee 0] \\
f'_t = 0. & f_t = 0.
\end{array}$$

Third, when $Q_t = 1$, $Q'_t = 0$, $Q_{t-1} = 0$, $Q'_{t-1} = 1$, $Q_{t-2} = 1$, and $Q'_{t-2} = 0$, then

$$\begin{array}{ll}
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(0 \wedge 1) \vee (1 \wedge 0)] & f_t = [(1 \wedge 0) \vee (0 \wedge 1)] \\
f'_t = [0 \vee 0] & f_t = [0 \vee 0] \\
f'_t = 0. & f_t = 0.
\end{array}$$

Fourth, when $Q_t = 0$, $Q'_t = 1$, $Q_{t-1} = 0$, $Q'_{t-1} = 1$, $Q_{t-2} = 1$, and $Q'_{t-2} = 0$, then

$$\begin{array}{ll} f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(1 \wedge 1) \vee (0 \wedge 0)] & f_t = [(0 \wedge 0) \vee (1 \wedge 1)] \\ f'_t = [1 \vee 0] & f_t = [0 \vee 1] \\ f'_t = 1. & f_t = 1. \end{array}$$

Condition(s) required for this proof: $Q_{t-1} = \overline{Q_{t-2}}$

6: ± ± ± ±

We are given: (ΔQ_t, ΔQ_{t-1}, ΔQ_{t-2}) = (±1, ±1, ±1), i.e., Q'_t - Q_t = ±1, Q'_{t-1} - Q_{t-1} = ±1, and Q'_{t-2} - Q_{t-2} = ±1.
We want: $\Delta f_t = \pm 1$, i.e., f'_t - f_t = ±1.

$$\begin{array}{ll} f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-1} = Q_{t-2}$. This gives us $Q_{t-1} = Q_{t-2}$ = (0, 1). We also have Q_t = (0, 1). We consider four possibilities. First, when $Q_t = 0$, $Q'_t = 1$, $Q_{t-1} = 0$, $Q'_{t-1} = 1$, $Q_{t-2} = 0$, and Q'_{t-2} = 1, then

$$\begin{array}{ll} f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(1 \wedge 1) \vee (0 \wedge 1)] & f_t = [(0 \wedge 0) \vee (1 \wedge 0)] \\ f'_t = [1 \vee 0] & f_t = [0 \vee 0] \\ f'_t = 1. & f_t = 0. \end{array}$$

Second, when $Q_t = 0$, $Q'_t = 1$, $Q_{t-1} = 1$, $Q'_{t-1} = 0$, $Q_{t-2} = 1$, and $Q'_{t-2} = 0$, then

$$\begin{array}{ll} f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t\ [(1 \wedge 0) \vee (0 \wedge 0)] & f_t = [(0 \wedge 1) \vee (1 \wedge 1)] \\ f'_t = [0 \vee 0] & f_t = [0 \vee 1] \\ f'_t = 0. & f_t = 1. \end{array}$$

Third, when $Q_t = 1$, $Q'_t = 0$, $Q_{t-1} = 0$, $Q'_{t-1} = 1$, $Q_{t-2} = 0$, and $Q'_{t-2} = 1$, then

$$\begin{array}{ll} f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(0 \wedge) \vee (1 \wedge 1)] & f'_t = [(1 \wedge 0) \vee (0 \wedge 0)] \\ f'_t = [0 \vee 1] & f_t = [0 \vee 0] \\ f'_t = 1. & f_t = 0. \end{array}$$

Fourth, when $Q_t = 0$, $Q'_t = 1$, $Q_{t-1} = 0$, $Q'_{t-1} = 1$, $Q_{t-2} = 0$, and $Q'_{t-2} = 1$, then

$$
\begin{array}{ll}
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(1 \wedge 1) \vee (0 \wedge 1)] & f_t = [(0 \wedge 0) \vee (1 \wedge 0)] \\
f'_t = [1 \vee 0] & f_t = [0 \vee 0] \\
f'_t = 1. & f_t = 0.
\end{array}
$$

Condition(s) required for this proof: $Q_{t-1} = Q_{t-2}$

7: + + + +

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (+1,\ +1,\ +1)$, i.e., $Q'_t = Q'_{t-1} = Q'_{t-2} = 1$ and $Q_t = Q_{t-1} = Q_{t-2} = 0$.
We want: $\Delta f_t = +1$, i.e., $f'_t = 1$ amd $f_t = 0$.

$$
\begin{array}{ll}
f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(1 \wedge 1) \vee (0 \wedge 1)] & f_t = [(0 \wedge 0) \vee (1 \wedge 0)] \\
f'_t = [1 \vee 0] & f_t = [0 \vee 0] \\
f'_t = 1. & f_t = 0.
\end{array}
$$

Condition(s) required for this proof: none

8: - + + +

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (-1,\ +1,\ +1)$, i.e., $Q_t = Q'_{t-1} = Q'_{t-2} = 1$ and $Q'_t = Q_{t-1} = Q_{t-2} = 0$.
We want: $\Delta f_t = +1$, i.e., $f'_t = 1$ amd $f_t = 0$.

$$
\begin{array}{ll}
f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(0 \wedge) \vee (1 \wedge 1)] & f'_t = [(1 \wedge 0) \vee (0 \wedge 0)] \\
f'_t = [0 \vee 1] & f_t = [0 \vee 0] \\
f'_t = 1. & f_t = 0.
\end{array}
$$

Condition(s) required for this proof: none

9: + - + 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (+1,\ -1,\ +1)$, i.e., $Q'_t = Q_{t-1} = Q'_{t-2} = 1$ and $Q_t = Q'_{t-1} = Q_{t-2} = 0$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$

$$
\begin{array}{ll}
f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(1 \wedge 0) \vee (0 \wedge 1)] & f_t = [(0 \wedge 1) \vee (1 \wedge 0)] \\
f'_t = [0 \vee 0] & f_t = [0 \vee 0] \\
f'_t = 0. & f_t = 0.
\end{array}
$$

Condition(s) required for this proof: none

10: - - + 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2})$ = (-1, -1, +1), i.e., $Q_t = Q_{t-1} = Q'_{t-2} = 1$ and $Q'_t = Q'_{t-1} = Q_{t-2} = 0$. We want $\Delta f_t = 0$, i.e., $f'_t = f_t$

$$\begin{array}{ll} f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(0 \wedge 0) \vee (1 \wedge 1)] & f_t = [(1 \wedge 1) \vee (0 \wedge 0)] \\ f'_t = [0 \vee 1] & f_t = [1 \vee 0] \\ f'_t = 1. & f_t = 1. \end{array}$$

Condition(s) required for this proof for this proof: none

11: + + - 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2})$ = (+1, +1, -1), i.e., $Q'_t = Q'_{t-1} = Q_{t-2} = 1$ and $Q_t = Q_{t-1} = Q'_{t-2} = 0$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$

$$\begin{array}{ll} f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(1 \wedge 1) \vee (0 \wedge 0)] & f_t = [(0 \wedge 0) \vee (1 \wedge 1)] \\ f'_t = [1 \vee 0] & f_t = [0 \vee 1] \\ f'_t = 1. & f_t = 1. \end{array}$$

Condition(s) required for this proof: none

12: + 0 0 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2})$ = (+1, 0, 0), i.e., $Q'_t = 1$, $Q_t = 0$, $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = Q_{t-2}$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll} f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(1 \wedge Q'_{t-1}) \vee (0 \wedge Q'_{t-2})] & f_t = [(0 \wedge Q_{t-1}) \vee (1 \wedge Q_{t-2})] \end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-1} = Q_{t-2}$. From this, we have $Q'_{t-1} = Q_{t-1} = Q_{t-2} = Q'_{t-2} = (0, 1)$. When $Q'_{t-1} = Q_{t-1} = Q_{t-2} = Q'_{t-2} = 0$, then

$$\begin{array}{ll} f'_t = [(1 \wedge Q'_{t-1}) \vee (0 \wedge Q'_{t-2})] & f_t = [(0 \wedge Q_{t-1}) \vee (1 \wedge Q_{t-2})] \\ f'_t\ [(1 \wedge 0) \vee (0 \wedge 0)] & f_t = [(0 \wedge 0) \vee (1 \wedge 0)] \\ f'_t = [0 \vee 0] & f_t = [0 \vee 0] \\ f'_t = 0. & f_t = 0. \end{array}$$

When $Q'_{t-1} = Q_{t-1} = Q_{t-2} = Q'_{t-2} = 1$, then

$$\begin{array}{ll} f'_t = [(1 \wedge Q'_{t-1}) \vee (0 \wedge Q'_{t-2})] & f_t = [(0 \wedge Q_{t-1}) \vee (1 \wedge Q_{t-2})] \\ f'_t = [(1 \wedge 1) \vee (0 \wedge 1)] & f_t = [(0 \wedge 1) \vee (1 \wedge 1)] \\ f'_t = [1 \vee 0] & f_t = [0 \vee 1] \\ f'_t = 1. & f_t = 1. \end{array}$$

Condition(s) required for this proof: $Q'_{t-1} = Q_{t-2}$

13: - 0 0 0

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2})$ = (-1, 0, 0), i.e., $Q'_t = 0$, $Q_t = 1$, $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = Q_{t-2}$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll} f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(0 \wedge Q'_{t-1}) \vee (1 \wedge Q'_{t-2})] & f_t = [(1 \wedge Q_{t-1}) \vee (0 \wedge Q_{t-2})] \end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-1} = Q_{t-2}$. From this, we have $Q'_{t-1} = Q_{t-1} = Q_{t-2} = Q'_{t-2}$ = (0, 1). When $Q'_{t-1} = Q_{t-1} = Q_{t-2} = Q_{t-2} = 0$, then

$$\begin{array}{ll} f'_t = [(0 \wedge Q'_{t-1}) \vee (1 \wedge Q'_{t-2})] & f_t = [(1 \wedge Q_{t-1}) \vee (0 \wedge Q_{t-2})] \\ f'_t = [(0 \wedge 0) \vee (1 \wedge 0)] & f'_t = [(1 \wedge 0) \vee (0 \wedge 0)] \\ f'_t = [0 \vee 0] & f_t = [0 \vee 0] \\ f'_t = 0. & f_t = 0. \end{array}$$

When $Q'_{t-1} = Q_{t-1} = Q_{t-2} = Q'_{t-2} = 1$, then

$$\begin{array}{ll} f'_t = [(0 \wedge Q'_{t-1}) \vee (1 \wedge Q'_{t-2})] & f_t = [(1 \wedge Q_{t-1}) \vee (0 \wedge Q_{t-2})] \\ f'_t = [(0 \wedge) \vee (1 \wedge 1)] & f_t = [(1 \wedge 1) \vee (0 \wedge 1)] \\ f'_t = [0 \vee 1] & f_t = [1 \vee 0] \\ f'_t = 1. & f_t = 1. \end{array}$$

Condition(s) required for this proof: $Q'_{t-1} = Q_{t-2}$

14: + 0 0 +

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2}) = (+1, 0, 0)$, i.e., $Q'_t = 1$, $Q_t = 0$, $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = Q_{t-2}$.
We want: $\Delta f_t = +1$, i.e., $f'_t = 1$ amd $f_t = 0$.

$$\begin{array}{ll} f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(1 \wedge Q'_{t-1}) \vee (0 \wedge Q'_{t-2})] & f_t = [(0 \wedge Q_{t-1}) \vee (1 \wedge Q_{t-2})] \end{array}$$

To ensure $f_t = +1$, we require that $Q_{t-1} = 1$ and $Q_{t-2} = 0$. From this, we have $Q'_{t-1} = Q_{t-1} = 1$ and $Q_{t-2} = Q'_{t-2} = 0$. Thus,

$$
\begin{array}{ll}
f'_t = [(1 \wedge Q'_{t-1}) \vee (0 \wedge Q'_{t-2})] & f_t = [(0 \wedge Q_{t-1}) \vee (1 \wedge Q_{t-2})] \\
f'_t = [(1 \wedge 1) \vee (0 \wedge 0)] & f_t = [(0 \wedge 1) \vee (1 \wedge 0)] \\
f'_t = [1 \vee 0] & f_t = [0 \vee 0] \\
f'_t = 1. & f_t = 0.
\end{array}
$$

Condition(s) required for this proof: $Q_{t-1} = 1$ and $Q_{t-2} = 0$

15: + 0 0 -

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (+1,\ 0,\ 0)$, i.e., $Q'_t = 1$, $Q_t = 0$, $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = Q_{t-2}$.
We want: Δf_t = -1, i.e., $f'_t = 0$ and $f_t = 1$.

$$
\begin{array}{ll}
f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(1 \wedge Q'_{t-1}) \vee (0 \wedge Q'_{t-2})] & f_t = [(0 \wedge Q_{t-1}) \vee (1 \wedge Q_{t-2})]
\end{array}
$$

To ensure f_t = -1, we require that $Q_{t-1} = 0$ and $Q_{t-2} = 1$. From this, we have $Q'_{t-1} = Q_{t-1} = 0$ and $Q'_{t-2} = Q_{t-2} = 1$. Thus,

$$
\begin{array}{ll}
f'_t = [(1 \wedge Q'_{t-1}) \vee (0 \wedge Q'_{t-2})] & f_t = [(0 \wedge Q_{t-1}) \vee (1 \wedge Q_{t-2})] \\
f'_t = [(1 \wedge 0) \vee (0 \wedge 1)] & f_t = [(0 \wedge 0) \vee (1 \wedge 1)] \\
f'_t = [0 \vee 0] & f_t = [0 \vee 1] \\
f'_t = 0. & f_t = 1.
\end{array}
$$

Condition(s) required for this proof: $Q_{t-1} = 0$ and $Q_{t-2} = 1$

16: - 0 0 +

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2})$ = (-1, 0, 0), i.e., $Q'_t = 0$, $Q_t = 1$, $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = Q_{t-2}$.
We want: $\Delta f_t = +1$, i.e., $f'_t = 1$ amd $f_t = 0$.

$$
\begin{array}{ll}
f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(0 \wedge Q'_{t-1}) \vee (1 \wedge Q'_{t-2})] & f_t = [(1 \wedge Q_{t-1}) \vee (0 \wedge Q_{t-2})]
\end{array}
$$

To ensure $f_t = +1$, we require that $Q_{t-1} = 0$ and $Q_{t-2} = 1$. From this, we have $Q'_{t-1} = Q_{t-1} = 0$ and $Q_{t-2} = Q'_{t-2} = 1$. Thus,

$$
\begin{array}{ll}
f'_t = [(0 \wedge Q'_{t-1}) \vee (1 \wedge Q'_{t-2})] & f_t = [(1 \wedge Q_{t-1}) \vee (0 \wedge Q_{t-2})] \\
f'_t = [(0 \wedge 0) \vee (1 \wedge 1)] & f_t = [(1 \wedge 0) \vee (0 \wedge 1)] \\
f'_t = [0 \vee 1] & f_t = [0 \vee 0] \\
f'_t = 1. & f_t = 0.
\end{array}
$$

Condition(s) required for this proof: $Q_{t-1} = 0$ and $Q_{t-2} = 1$

17: - 0 0 -

We are given: (ΔQ_t, ΔQ_{t-1}, ΔQ_{t-2}) = (-1, 0, 0), i.e., $Q'_t = 0$, $Q_t = 1$, $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = Q_{t-2}$.
We want: Δf_t = -1, i.e., $f'_t = 0$ and $f_t = 1$.

$$
\begin{array}{ll}
f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(0 \wedge Q'_{t-1}) \vee (1 \wedge Q'_{t-2})] & f_t = [(1 \wedge Q_{t-1}) \vee (0 \wedge Q_{t-2})]
\end{array}
$$

To ensure f_t = -1, we require that $Q_{t-1} = 1$ and $Q_{t-2} = 0$. From this, we have $Q'_{t-1} = Q_{t-1} = 1$ and $Q'_{t-2} = Q_{t-2} = 0$. Thus,

$$
\begin{array}{ll}
f'_t = [(0 \wedge Q'_{t-1}) \vee (1 \wedge Q'_{t-2})] & f_t = [(1 \wedge Q_{t-1}) \vee (0 \wedge Q_{t-2})] \\
f'_t = [(0 \wedge 1) \vee (1 \wedge 0)] & f_t = [(1 \wedge 1) \vee (0 \wedge 0)] \\
f'_t = [0 \vee 0] & f_t = [1 \vee 0] \\
f'_t = 0. & f_t = 1.
\end{array}
$$

Condition(s) required for this proof: $Q_{t-1} = 1$ and $Q_{t-2} = 0$

18: 0 0 + 0

We are given: (ΔQ_t, ΔQ_{t-1}, ΔQ_{t-2}) = (0, 0, +1), i.e., $Q'_t = Q_t$, $Q'_{t-1} = Q_{t-1}$, $Q'_{t-2} = 1$, and $Q_{t-2} = 0$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$
\begin{array}{ll}
f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge 1)] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge 0)]
\end{array}
$$

To ensure $f_t = 0$, we require that $Q_t = 1$. From this, we have $Q'_t = Q_t = 1$. Now, $Q'_{t-1} = Q_{t-1} = (0, 1)$. When $Q'_{t-1} = Q_{t-1} = 0$, then

$$
\begin{array}{ll}
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge 1)] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge 0)] \\
f'_t = [(1 \wedge 0) \vee (0 \wedge 1)] & f'_t = [(1 \wedge 0) \vee (0 \wedge 0)] \\
f'_t = [0 \vee 0] & f_t = [0 \vee 0] \\
f'_t = 0. & f_t = 0.
\end{array}
$$

When $Q'_{t-1} = Q_{t-1} = 1$, then

$$
\begin{array}{ll}
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge 1)] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge 0)] \\
f'_t = [(1 \wedge 1) \vee (0 \wedge 1)] & f_t = [(1 \wedge 1) \vee (0 \wedge 0)] \\
f'_t = [1 \vee 0] & f_t = [1 \vee 0] \\
f'_t = 1. & f_t = 1.
\end{array}
$$

Condition(s) required for this proof: $Q_t = 1$

19: 0 0 + +

We are given: $(\mathit{\Delta} Q_t,\ \mathit{\Delta} Q_{t-1},\ \mathit{\Delta} Q_{t-2}) = (0,\ 0,\ +1)$, i.e., $Q'_t = Q_t$, $Q'_{t-1} = Q_{t-1}$, $Q'_{t-2} = 1$, and $Q_{t-2} = 0$.
We want: $\mathit{\Delta} f_t = +1$, i.e., $f'_t = 1$ amd $f_t = 0$.

$f'_t = F[Q'_t,\ Q'_{t-1},\ Q'_{t-2}]$ $\quad$ $f_t = F[Q_t,\ Q_{t-1},\ Q_{t-2}]$
$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$ $\quad$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge 1)]$ $\quad$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge 0)]$

To ensure $f_t = +1$, we require that $Q_t = 0$. From this, we have $Q'_t = Q_t = 0$. Now, $Q'_{t-1} = Q_{t-1} = (0, 1)$. When $Q'_{t-1} = Q_{t-1} = 0$, then

$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge 1)]$ $\quad$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge 0)]$
$f'_t = [(0 \wedge 0) \vee (1 \wedge 1)]$ $\quad$ $f_t = [(0 \wedge 0) \vee (1 \wedge 0)]$
$f'_t = [0 \vee 1]$ $\quad$ $f_t = [0 \vee 0]$
$f'_t = 1.$ $\quad$ $f_t = 0.$

When $Q'_{t-1} = Q_{t-1} = 1$, then

$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge 1)]$ $\quad$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge 0)]$
$f'_t = [(0 \wedge) \vee (1 \wedge 1)]$ $\quad$ $f_t = [(0 \wedge 1) \vee (1 \wedge 0)]$
$f'_t = [0 \vee 1]$ $\quad$ $f_t = [1 \vee 0]$
$f'_t = 1.$ $\quad$ $f_t = 0.$

Condition(s) required for this proof: $Q_t = 0$

20: 0 0 - 0

We are given: $(\mathit{\Delta} Q_t,\ \mathit{\Delta} Q_{t-1},\ \mathit{\Delta} Q_{t-2}) = (0,\ 0,\ \text{-}1)$, i.e., $Q'_t = Q_t$, $Q'_{t-1} = Q_{t-1}$, $Q'_{t-2} = 0$, and $Q_{t-2} = 1$.
We want $\mathit{\Delta} f_t = 0$, i.e., $f'_t = f_t$.

$f'_t = F[Q'_t,\ Q'_{t-1},\ Q'_{t-2}]$ $\quad$ $f_t = F[Q_t,\ Q_{t-1},\ Q_{t-2}]$
$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$ $\quad$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge 0)]$ $\quad$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge 1)]$

To ensure $f_t = 0$, we require that $Q_t = 1$. From this, we have $Q'_t = Q_t = 1$. Now, $Q'_{t-1} = Q_{t-1} = (0, 1)$. When $Q'_{t-1} = Q_{t-1} = 0$, then

$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge 0)]$ $\quad$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge 1)]$
$f'_t\ [(1 \wedge 0) \vee (0 \wedge 0)]$ $\quad$ $f_t = [(1 \wedge 0) \vee (0 \wedge 1)]$
$f'_t = [0 \vee 0]$ $\quad$ $f_t = [0 \vee 0]$
$f'_t = 0.$ $\quad$ $f_t = 0.$

When $Q'_{t-1} = Q_{t-1} = 1$, then

$$
\begin{array}{ll}
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge 0)] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge 1)] \\
f'_t = [(1 \wedge 1) \vee (0 \wedge 0)] & f_t = [(1 \wedge 1) \vee (0 \wedge 1)] \\
f'_t = [1 \vee 0] & f_t = [1 \vee 0] \\
f'_t = 1. & f_t = 1.
\end{array}
$$

Condition(s) required for this proof: $Q_t = 1$

21: 0 0 - -

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (0,\ 0,\ \text{-}1)$, i.e., $Q'_t = Q_t$, $Q'_{t-1} = Q_{t-1}$, $Q'_{t-2} = 0$, and $Q_{t-2} = 1$.
We want: $\Delta f_t = \text{-}1$, i.e., $f'_t = 0$ and $f_t = 1$.

$$
\begin{array}{ll}
f'_t = F[Q'_t,\ Q'_{t-1},\ Q'_{t-2}] & f_t = F[Q_t,\ Q_{t-1},\ Q_{t-2}] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge 0)] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge 1)]
\end{array}
$$

To ensure $f_t = 0$, we require that $Q_t = 0$. From this, we have $Q'_t = Q_t = 0$. Now, $Q'_{t-1} = Q_{t-1} = (0,\ 1)$. When $Q'_{t-1} = Q_{t-1} = 0$, then

$$
\begin{array}{ll}
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge 0)] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge 1)] \\
f'_t = [(0 \wedge 0) \vee (1 \wedge 0)] & f_t = [(0 \wedge 0) \vee (1 \wedge 1)] \\
f'_t = [0 \vee 0] & f_t = [0 \vee 1] \\
f'_t = 0. & f_t = 1.
\end{array}
$$

When $Q'_{t-1} = Q_{t-1} = 1$, then

$$
\begin{array}{ll}
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge 0)] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge 1)] \\
f'_t = [(0 \wedge 1) \vee (1 \wedge 0)] & f_t = [(0 \wedge 1) \vee (1 \wedge 1)] \\
f'_t = [0 \vee 0] & f_t = [0 \vee 1] \\
f'_t = 0. & f_t = 0.
\end{array}
$$

Condition(s) required for this proof: $Q_t = 0$

22: 0 + 0 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (0,\ +1,\ 0)$, i.e., $Q'_t = Q_t\ \ Q'_{t-1} = 1$, $Q_{t-1} = 0$, and $Q'_{t-2} = Q_{t-2}$,.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$
\begin{array}{ll}
f'_t = F[Q'_t,\ Q'_{t-1},\ Q'_{t-2}] & f_t = F[Q_t,\ Q_{t-1},\ Q_{t-2}] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(Q'_t \wedge 1) \vee (\neg Q'_t \wedge Q'_{t-2})] & f'_t = [(Q'_t \wedge 0) \vee (\ Q'_t \wedge Q_{t-2})]
\end{array}
$$

To ensure $f_t = 0$, we require that $Q_t = 0$. From this, we have $Q'_t = Q_t = 0$. Now, $Q'_{t-2} = Q_{t-2} = (0, 1)$. When $Q'_{t-2} = Q_{t-2} = 0$, then

$$\begin{array}{ll} f'_t = [(Q'_t \wedge 1) \vee (\neg Q'_t \wedge Q'_{t-2})] & f'_t = [(Q'_t \wedge 0) \vee (\ Q'_t \wedge Q_{t-2})] \\ f'_t = [(0 \wedge 1) \vee (1 \wedge 0)] & f_t = [(0 \wedge 0) \vee (1 \wedge 0)] \\ f'_t = [0 \vee 0] & f_t = [0 \vee 0] \\ f'_t = 0. & f_t = 0. \end{array}$$

When $Q'_{t-2} = Q_{t-2} = 1$, then

$$\begin{array}{ll} f'_t = [(Q'_t \wedge 1) \vee (\neg Q'_t \wedge Q'_{t-2})] & f'_t = [(Q'_t \wedge 0) \vee (\ Q'_t \wedge Q_{t-2})] \\ f'_t = [(0 \wedge) \vee (1 \wedge 1)] & f_t = [(0 \wedge 0) \vee (1 \wedge 1)] \\ f'_t = [0 \vee 1] & f_t = [0 \vee 1] \\ f'_t = 1. & f_t = 1. \end{array}$$

Condition(s) required for this proof: $Q_t = 0$

23: 0 + 0 +

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (0,\ +1,\ 0)$, i.e., $Q'_t = Q_t$, $Q'_{t-1} = 1$, $Q_{t-1} = 0$, and $Q'_{t-2} = Q_{t-2}$.
We want: $\Delta f_t = +1$, i.e., $f'_t = 1$ amd $f_t = 0$.

$$\begin{array}{ll} f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(Q'_t \wedge 1) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge 0) \vee (\neg Q_t \wedge Q_{t-2})] \end{array}$$

To ensure $f_t = +1$, we require that $Q_t = 1$ From this, we have $Q'_t = Q_t = 1$. Thus,

$$\begin{array}{ll} f'_t = [(Q'_t \wedge 1) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge 0) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(1 \wedge 0) \vee (0 \wedge Q'_{t-2})] & f_t = [(1 \wedge 0) \vee (0 \wedge Q_{t-2})] \\ f'_t = [1 \vee 0] & f_t = [0 \vee 0] \\ f'_t = 1. & f_t = 0. \end{array}$$

Condition(s) required for this proof: $Q_t = 1$

24: 0 - 0 0

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2}) = (0, \text{-}1, 0)$, i.e., $Q'_t = Q_t$, $Q'_{t-1} = 0$, $Q_{t-1} = 1$, and $Q'_{t-2} = Q_{t-2}$,.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll} f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(Q'_t \wedge 0) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge 1) \vee (\neg Q_t \wedge Q_{t-2})] \end{array}$$

To ensure $f_t = 0$, we require that $Q_t = 0$. From this, we have $Q'_t = Q_t = 0$. Now, $Q'_{t-2} = Q_{t-2} = (0, 1)$. When $Q'_{t-2} = Q_{t-2} = 0$, then

$$\begin{array}{ll} f'_t = [(Q'_t \wedge 0) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge 1) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(0 \wedge 0) \vee (1 \wedge 0)] & f_t = [(0 \wedge 1) \vee (1 \wedge 0)] \\ f'_t = [0 \vee 0] & f_t = [0 \vee 0] \\ f'_t = 0. & f_t = 0. \end{array}$$

When $Q'_{t-2} = Q_{t-2} = 1$, then

$$\begin{array}{ll} f'_t = [(Q'_t \wedge 0) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge 1) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(0 \wedge 0) \vee (1 \wedge 1)] & f_t = [(0 \wedge 1) \vee (1 \wedge 1)] \\ f'_t = [0 \vee 1] & f_t = [0 \vee 1] \\ f'_t = 1. & f_t = 1. \end{array}$$

Condition(s) required for this proof: $Q_t = 0$

25: 0 - 0 -

We are given: $(\mathit{\Delta} Q_t, \mathit{\Delta} Q_{t-1}, \mathit{\Delta} Q_{t-2}) = (0, -1, 0)$, i.e., $Q'_t = Q_t$, $Q'_{t-1} = 0$, $Q_{t-1} = 1$, and $Q'_{t-2} = Q_{t-2}$. We want: $\mathit{\Delta} f_t =$ -1, i.e., $f'_t = 0$ and $f_t = 1$.

$$\begin{array}{ll} f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(Q'_t \wedge 0) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge 1) \vee (\neg Q_t \wedge Q_{t-2})] \end{array}$$

To ensure $f_t =$ -1, we require that $Q_t = 1$. From this, we have $Q'_t = Q_t = 1$. Thus,

$$\begin{array}{ll} f'_t = [(Q'_t \wedge 0) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge 1) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(1 \wedge 0) \vee (0 \wedge Q'_{t-2})] & f_t = [(1\ 1)\ (0\ Q_{t-2})] \\ f'_t = [0 \vee 0] & f_t = [1 \vee 0] \\ f'_t = 0. & f_t = 1. \end{array}$$

Condition(s) required for this proof: $Q_t = 1$

26: - + 0 0

We are given: $(\mathit{\Delta} Q_t, \mathit{\Delta} Q_{t-1}, \mathit{\Delta} Q_{t-2}) =$ (-1, +1, 0), i.e., $Q_t = Q'_{t-1} = 1$ $Q'_t = Q_{t-1} = 0$, and $Q'_{t-2} = Q_{t-2}$.
We want $\mathit{\Delta} f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll} f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(0 \wedge 1) \vee (1 \wedge Q'_{t-2})] & f_t = [(1 \wedge 0) \vee (0 \wedge Q_{t-2})] \end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-2} = 0$ From this, we have $Q'_{t-2} = Q_{t-2} = 0$. Thus,

$f'_t = [(0 \wedge 1) \vee (1 \wedge Q'_{t-2})]$ $f_t = [(1 \wedge 0) \vee (0 \wedge Q_{t-2})]$
$f'_t = [(0 \wedge 1) \vee (1 \wedge 0)]$ $f_t = [(1 \wedge 0) \vee (0 \wedge 0)]$
$f'_t = [0 \vee 0]$ $f_t = [0 \vee 0]$
$f'_t = 0.$ $f_t = 0.$

Condition(s) required for this proof: $Q_{t-2} = 0$

27: + 0 + 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (+1,\ 0,\ +1)$, i.e., $Q'_t = Q'_{t-2} = 1$, $Q_t = Q_{t-2} = 0$, and $Q'_{t-1} = Q_{t-1}$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}]$ $f_t = F[Q_t, Q_{t-1}, Q_{t-2}]$
$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(1 \wedge Q'_{t-1}) \vee (0 \wedge 1)]$ $f_t = [(0 \wedge Q_{t-1}) \vee (1 \wedge 0)]$

To ensure $f_t = 0$, we require that $Q_{t-1} = 0$. From this, we have $Q'_{t-1} = Q_{t-1} = 0$. Thus,

$f'_t = [(1 \wedge Q'_{t-1}) \vee (0 \wedge 1)]$ $f_t = [(0 \wedge Q_{t-1}) \vee (1 \wedge 0)]$
$f'_t = [(1 \wedge 0) \vee (0 \wedge 1)]$ $f_t = [(0 \wedge 0) \vee (1 \wedge 0)]$
$f'_t = [0 \vee 0]$ $f_t = [0 \vee 0]$
$f'_t = 0.$ $f_t = 0.$

Condition(s) required for this proof: $Q_{t-1} = 0$

28: + 0 + +

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (+1,\ 0,\ +1)$, i.e., $Q'_t = Q'_{t-2} = 1$, $Q_t = Q_{t-2} = 0$, and $Q'_{t-1} = Q_{t-1}$.
We want: $\Delta f_t = +1$, i.e., $f'_t = 1$ amd $f_t = 0$.

$f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}]$ $f_t = F[Q_t, Q_{t-1}, Q_{t-2}]$
$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$ $f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(1 \wedge Q'_{t-1}) \vee (0 \wedge 1)]$ $f_t = [(0 \wedge Q_{t-1}) \vee (1 \wedge 0)]$

To ensure $f_t = +1$, we require that $Q_{t-1} = 1$. From this, we have $Q'_{t-1} = Q_{t-1} = 1$. Thus,
$f'_t = [(1 \wedge Q'_{t-1}) \vee (0 \wedge 1)]$ $f_t = [(0 \wedge Q_{t-1}) \vee (1 \wedge 0)]$
$f'_t = [(1 \wedge 1) \vee (0 \wedge 1)]$ $f_t = [(0 \wedge 1) \vee (1 \wedge 0)]$
$f'_t = [1 \vee 0]$ $f_t = [0 \vee 0]$
$f'_t = 1.$ $f_t = 0.$

Condition(s) required for this proof: $Q_{t-1} = 1$

29: - 0 + 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2})$ = (-1, 0, +1), i.e., $Q'_t = Q_{t-2} = 0$, $Q_t = Q'_{t-2} = 1$, and $Q'_{t-1} = Q_{t-1}$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll}
f'_t = F[Q'_t,\, Q'_{t-1},\, Q'_{t-2}] & f_t = F[Q_t,\, Q_{t-1},\, Q_{t-2}] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(0 \wedge Q'_{t-1}) \vee (1 \wedge 1)] & f_t = [(1 \wedge Q_{t-1}) \vee (0 \wedge 0)]
\end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-1} = 1$. From this, we have $Q'_{t-1} = Q_{t-1} = 1$. Thus,

$$\begin{array}{ll}
f'_t = [(0 \wedge Q'_{t-1}) \vee (1 \wedge 1)] & f_t = [(1 \wedge Q_{t-1}) \vee (0 \wedge 0)] \\
f'_t = [(0 \wedge) \vee (1 \wedge 1)] & f_t = [(1 \wedge 1) \vee (0 \wedge 0)] \\
f'_t = [0 \vee 1] & f_t = [1 \vee 0] \\
f'_t = 1. & f_t = 1.
\end{array}$$

Condition(s) required for this proof: $Q_{t-1} = 1$

30: + 0 - 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2})$ = (+1, 0, -1), i.e., $Q'_t = Q_{t-2} = 1$, $Q_t = Q'_{t-2} = 0$, and $Q'_{t-1} = Q_{t-1}$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll}
f'_t = F[Q'_t,\, Q'_{t-1},\, Q'_{t-2}] & f_t = F[Q_t,\, Q_{t-1},\, Q_{t-2}] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(1 \wedge Q'_{t-1}) \vee (0 \wedge 0)] & f_t = [(0 \wedge Q_{t-1}) \vee (1 \wedge 1)]
\end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-1} = 1$. From this, we have $Q'_{t-1} = Q_{t-1} = 1$. Thus,

$$\begin{array}{ll}
f'_t = [(1 \wedge Q'_{t-1}) \vee (0 \wedge 0)] & f_t = [(0 \wedge Q_{t-1}) \vee (1 \wedge 1)] \\
f'_t = [(1 \wedge 1) \vee (0 \wedge 0)] & f_t = [(0 \wedge 1) \vee (1 \wedge 1)] \\
f'_t = [1 \vee 0] & f_t = [0 \vee 1] \\
f'_t = 1. & f_t = 1.
\end{array}$$

Condition(s) required for this proof: $Q_{t-1} = 1$

31: - 0 - 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2})$ = (-1, 0, -1), i.e., $Q_t = Q_{t-2} = 1$, $Q'_t = Q'_{t-2} = 0$, and $Q'_{t-1} = Q_{t-1}$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll}
f'_t = F[Q'_t,\, Q'_{t-1},\, Q'_{t-2}] & f_t = F[Q_t,\, Q_{t-1},\, Q_{t-2}] \\
f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\
f'_t = [(0 \wedge Q'_{t-1}) \vee (1 \wedge 0)] & f_t = [(1 \wedge Q_{t-1}) \vee (0 \wedge 1)]
\end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-1} = 0$. From this, we have $Q'_{t-1} = Q_{t-1} = 0$. Thus,

$$\begin{array}{ll} f'_t = [(0 \wedge Q'_{t-1}) \vee (1 \wedge 0)] & f_t = [(1 \wedge Q_{t-1}) \vee (0 \wedge 1)] \\ f'_t = [(0 \wedge 0) \vee (1 \wedge 0)] & f_t = [(1 \wedge 0) \vee (0 \wedge 1)] \\ f'_t = [0 \vee 0] & f_t = [0 \vee 0] \\ f'_t = 0. & f_t = 0. \end{array}$$

Condition(s) required for this proof: $Q_{t-1} = 0$

32: 0 + - +

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2}) = (0, +1, -1)$, i.e., $Q'_t = Q_t$, $Q'_{t-1} = Q_{t-2} = 1$, and $Q_{t-1} = Q'_{t-2} = 0$. We want: $\Delta f_t = +1$, i.e., $f'_t = 1$ amd $f_t = 0$.

$$\begin{array}{ll} f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(Q'_t \wedge 1) \vee (\neg Q'_t \wedge 0)] & f_t = [(Q_t \wedge 0) \vee (\neg Q_t \wedge 1)] \end{array}$$

To ensure $f_t = +1$, we require that $Q_t = 1$ From this, we have $Q'_t = Q_t = 1$. Thus,

$$\begin{array}{ll} f'_t = [(Q'_t \wedge 1) \vee (\neg Q'_t \wedge 0)] & f_t = [(Q_t \wedge 0) \vee (\neg Q_t \wedge 1)] \\ f'_t = [(1 \wedge 1) \vee (0 \wedge 0)] & f_t = [(1 \wedge 0) \vee (0 \wedge 1)] \\ f'_t = [1 \vee 0] & f_t = [0 \vee 0] \\ f'_t = 1. & f_t = 0. \end{array}$$

Condition(s) required for this proof: $Q_t = 1$

33: 0 + - -

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2}) = (0, +1, -1)$, i.e., $Q'_t = Q_t$, $Q'_{t-1} = Q_{t-2} = 1$, and $Q_{t-1} = Q'_{t-2} = 0$. We want: $\Delta f_t = -1$, i.e., $f'_t = 0$ and $f_t = 1$.

$$\begin{array}{ll} f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = F[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})] & f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})] \\ f'_t = [(Q'_t \wedge 1) \vee (\neg Q'_t \wedge 0)] & f_t = [(Q_t \wedge 0) \vee (\neg Q_t \wedge 1)] \end{array}$$

To ensure $f_t = +1$, we require that $Q_t = 0$ From this, we have $Q'_t = Q_t = 0$. Thus,

$$\begin{array}{ll} f'_t = [(Q'_t \wedge 1) \vee (\neg Q'_t \wedge 0)] & f_t = [(Q_t \wedge 0) \vee (\neg Q_t \wedge 1)] \\ f'_t = [(0 \wedge 1) \vee (1 \wedge 0)] & f_t = [(0 \wedge 0) \vee (1 \wedge 1)] \\ f'_t = [0 \vee 0] & f_t = [0 \vee 1] \\ f'_t = 0. & f_t = 1. \end{array}$$

Condition(s) required for this proof: $Q_t = 0$

34: 0 - - -

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2})$ = (0, -1, -1), i.e., $Q'_t = Q_t$, $Q'_{t-1} = Q'_{t-2} = 0$, and $Q_{t-1} = Q_{t-2} = 1$.
We want: Δf_t = -1, i.e., $f'_t = 0$ and $f_t = 1$.

$f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}]$ $\quad f_t = F[Q_t, Q_{t-1}, Q_{t-2}]$
$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$ $\quad f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(Q'_t \wedge 0) \vee (\neg Q'_t \wedge 0)]$ $\quad f_t = [(Q_t \wedge 1) \vee (\neg Q_t \wedge 1)]$

To ensure f_t = -1, no requirements are necessary. Q_t = (0, 1). From this, we have $Q'_t = Q_t$ = (0, 1). When $Q'_t = Q_t = 0$, then

$f'_t = [(Q'_t \wedge 0) \vee (\neg Q'_t \wedge 0)]$ $\quad f_t = [(Q_t \wedge 1) \vee (\neg Q_t \wedge 1)]$
$f'_t = [(0 \wedge 0) \vee (1 \wedge 0)]$ $\quad f_t = [(0 \wedge 1) \vee (1 \wedge 1)]$
$f'_t = [0 \vee 0]$ $\quad f_t = [0 \vee 1]$
$f'_t = 0.$ $\quad f_t = 1.$

When $Q'_t = Q_t = 1$, then

$f'_t = [(Q'_t \wedge 0) \vee (\neg Q'_t \wedge 0)]$ $\quad f_t = [(Q_t \wedge 1) \vee (\neg Q_t \wedge 1)]$
f'_t $[(1 \wedge 0) \vee (0 \wedge 0)]$ $\quad f_t = [(1 \wedge 1) \vee (0 \wedge 1)]$
$f'_t = [0 \vee 0]$ $\quad f_t = [1 \vee 0]$
$f'_t = 0.$ $\quad f_t = 1.$

Condition(s) required for this proof: none

35: + + 0 0

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2})$ = (+1, +1, 0), i.e., $Q'_t = Q'_{t-1} = 1$, $Q_t = Q_{t-1} = 0$, and $Q'_{t-2} = Q_{t-2}$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$

$f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}]$ $\quad f_t = F[Q_t, Q_{t-1}, Q_{t-2}]$
$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$ $\quad f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(1 \wedge 1) \vee (0 \wedge Q'_{t-2})]$ $\quad f_t = [(0 \wedge 0) \vee (1 \wedge Q_{t-2})]$

To ensure $f_t = 0$, we require that $Q_{t-2} = 1$. From this, we have $Q'_{t-2} = Q_{t-2} = 1$. Thus,

$f'_t = [(1 \wedge 1) \vee (0 \wedge Q'_{t-2})]$ $\quad f_t = [(0 \wedge 0) \vee (1 \wedge Q_{t-2})]$
$f'_t = [(1 \wedge 1) \vee (0 \wedge 1)]$ $\quad f_t = [(0 \wedge 0) \vee (1 \wedge 1)]$
$f'_t = [1 \vee 0]$ $\quad f_t = [0 \vee 1]$
$f'_t = 1.$ $\quad f_t = 1.$

Condition(s) required for this proof: $Q_{t-2} = 1$

36: + - 0 -

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2})$ = (+1, -1, 0), i.e., $Q'_t = Q_{t-1} = 1$, $Q_t = Q'_{t-1} = 0$, and $Q'_{t-2} =$

Q_{t-2}.
We want: Δf_t = -1, i.e., $f'_t = 0$ and $f_t = 1$.

$f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}]$ $\quad f_t = F[Q_t, Q_{t-1}, Q_{t-2}]$
$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$ $\quad f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(1 \wedge 0) \vee (0 \wedge Q'_{t-2})]$ $\quad f_t = [(0 \wedge 1) \vee (1 \wedge Q_{t-2})]$

To ensure f_t = -1, we require that $Q_{t-2} = 1$. From this, we have $Q_{t-2} = Q'_{t-2} = 1$. Thus,

$f'_t = [(1 \wedge 0) \vee (0 \wedge Q'_{t-2})]$ $\quad f_t = [(0 \wedge 1) \vee (1 \wedge Q_{t-2})]$
$f'_t = [(1 \wedge 0) \vee (0 \wedge 1)]$ $\quad f_t = [(0 \wedge 1) \vee (1 \wedge 1)]$
$f'_t = [0 \vee 0]$ $\quad f_t = [0 \vee 1]$
$f'_t = 0.$ $\quad f_t = 1.$

Condition(s) required for this proof: $Q_{t-2} = 1$

37: 0 - + +

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2})$ = (0, -1, +1), i.e., Q'_t = Qt , $Q'_{t-1} = Q_{t-2} = 0$, and $Q_{t-1} = Q'_{t-2} = 1$.
We want: $\Delta f_t = +1$, i.e., $f'_t = 1$ amd $f_t = 0$.

$f'_t = F[Q'_t, Q'_{t-1}, Q'_{t-2}]$ $\quad f_t = F[Q_t, Q_{t-1}, Q_{t-2}]$
$f'_t = [(Q'_t \wedge Q'_{t-1}) \vee (\neg Q'_t \wedge Q'_{t-2})]$ $\quad f_t = [(Q_t \wedge Q_{t-1}) \vee (\neg Q_t \wedge Q_{t-2})]$
$f'_t = [(Q'_t \wedge 0) \vee (\neg Q'_t \wedge 1)]$ $\quad f_t = [(Q_t \wedge 1) \vee (\neg Q_t \wedge 0)]$

To ensure $f_t = +1$, we require that $Q_t = 0$. From this, we have $Q'_t = Q_t = 0$. Thus,

$f'_t = [(Q'_t \wedge 0) \vee (\neg Q'_t \wedge 1)]$ $\quad f_t = [(Q_t \wedge 1) \vee (\neg Q_t \wedge 0)]$
$f'_t = [(0 \wedge 0) \vee (1 \wedge 1)]$ $\quad f_t = [(0 \wedge 1) \vee (1 \wedge 0)]$
$f'_t = [0 \vee 1]$ $\quad f_t = [0 \vee 0]$
$f'_t = 1.$ $\quad f_t = 0.$

Condition(s) required for this proof: $Q_t = 0$

8.2 Proofs for Round 2

For round 2, note that $f_t = G(X, Y, Z) = (Z \wedge X) \vee (\neg Z \wedge Y)$.

38: ± ± ± ±

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2})$ = (1, 1, 1), i.e., Q'_t - $Q_t = \pm 1$, Q'_{t-1} - $Q_{t-1} = \pm 1$, and Q'_{t-2} - $Q_{t-2} = \pm 1$.
We want: $\Delta f_t = \pm 1$, i.e.,f'_t - $f_t = \pm 1$.

$f'_t = G[Q'_t, Q'_{t-1}, Q'_{t-2}]$ $\quad f_t = G[Q_t, Q_{t-1}, Q_{t-2}]$
$f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})]$ $\quad f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})]$

To ensure $f_t = \pm 1$, we require that $Q_t = Q_{t-1}$. From this, we have $Q_t = Q_{t-1} = (0, 1)$ and $Q_{t-2} = (0, 1)$. Thus, we consider four possibilities. First, we consider when $Q_t = Q_{t-1} = 0$, $Q'_t = Q'_{t-1} = 1$, $Q_{t-2} = 0$, and $Q'_{t-2} = 1$. Thus,

$$\begin{array}{ll} f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})] & f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})] \\ , f'_t = [(1 \wedge 1) \vee (0 \wedge 1)] & f_t = [(0 \wedge 0) \vee (1 \wedge 0)] \\ f'_t = [1 \vee 0] & f_t = [0 \vee 0] \\ f'_t = 1. & f_t = 0. \end{array}$$

Second, we consider when $Q_t = Q_{t-1} = 0$, $Q'_t = Q'_{t-1} = 1$, $Q_{t-2} = 1$, and $Q'_{t-2} = 0$. Thus,

$$\begin{array}{ll} f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})] & f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})] \\ , f'_t = [(0 \wedge) \vee (1 \wedge 1)] & f'_t = [(1 \wedge 0) \vee (0 \wedge 0)] \\ f'_t = [0 \vee 1] & f_t = [0 \vee 0] \\ f'_t = 1. & f_t = 0. \end{array}$$

Third, we consider when $Q_t = Q_{t-1} = 1$, $Q'_t = Q'_{t-1} = 0$, $Q_{t-2} = 0$, and $Q'_{t-2} = 1$. Thus,

$$\begin{array}{ll} f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})] & f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})] \\ , f'_t = [(1 \wedge 0) \vee (1 \wedge 1)] & f_t = [(1 \wedge 0) \vee (1 \wedge 1)] \\ f'_t = [0 \vee 0] & f_t = [0 \vee 1] \\ f'_t = 0. & f_t = 1. \end{array}$$

Fourth, we consider when $Q_t = Q_{t-1} = 1$, $Q'_t = Q'_{t-1} = 0$, $Q_{t-2} = 1$, and $Q'_{t-2} = 0$. Thus,

$$\begin{array}{ll} f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})] & f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})] \\ , f'_t = [(0 \wedge 0) \vee (1 \wedge 0)] & f_t = [(1 \wedge 1) \vee (0 \wedge 1)] \\ f'_t = [0 \vee 0] & f_t = [1 \vee 0] \\ f'_t = 0. & f_t = 1. \end{array}$$

Condition(s) required for this proof: $Q_t = Q_{t-1}$

39: - 0 0 0

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2})$ = (-1, 0, 0), i.e., $Q'_t = 0$, $Q_t = 1$, $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = Q_{t-2}$. We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll} f'_t = G[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = G[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})] & f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})] \\ f'_t = [(Q'_{t-2} \wedge 0) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})] & f_t = [(Q_{t-2} \wedge 1) \vee (\neg Q_{t-2} \wedge Q_{t-1})] \end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-2} = 0$. From this, we have $Q'_{t-2} = Q_{t-2} = 0$. Now, $Q'_{t-1} = Q_{t-1}$ = (0, 1). When $Q'_{t-1} = Q_{t-1} = 0$, then

$f_t' = [(Q_{t-2}' \wedge 0) \vee (\neg Q_{t-2}' \wedge Q_{t-1}')]$ $f_t = [(Q_{t-2} \wedge 1) \vee (\neg Q_{t-2} \wedge Q_{t-1})]$
$f_t' = [(0 \wedge 0) \vee (1 \wedge 0)]$ $f_t = [(0 \wedge 1) \vee (1 \wedge 0)]$
$f_t' = [0 \vee 0]$ $f_t = [0 \vee 0]$
$f_t' = 0.$ $f_t = 0.$

When $Q_{t-1}' = Q_{t-1} = 1$, then
$f_t' = [(Q_{t-2}' \wedge 0) \vee (\neg Q_{t-2}' \wedge Q_{t-1}')]$ $f_t = [(Q_{t-2} \wedge 1) \vee (\neg Q_{t-2} \wedge Q_{t-1})]$
$f_t' = [(0 \wedge 0) \vee (1 \wedge 1)]$ $f_t = [(0 \wedge 1) \vee (1 \wedge 1)]$
$f_t' = [0 \vee 1]$ $f_t = [0 \vee 1]$
$f_t' = 1.$ $f_t = 1.$

Condition(s) required for this proof: $Q_{t-2} = 0$

40: 0 - 0 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (0, -1, 0)$, i.e., $Q_t' =$ Qt , $Q_{t-1}' = 0$, $Q_{t-1} = 1$, and $Q_{t-2}' = Q_{t-2}$.
We want $\Delta f_t = 0$, i.e., $f_t' = f_t$.

$f_t' = G[Q_t', Q_{t-1}', Q_{t-2}']$ $f_t = G[Q_t, Q_{t-1}, Q_{t-2}]$
$f_t' = [(Q_{t-2}' \wedge Q_t') \vee (\neg Q_{t-2}' \wedge Q_{t-1}')]$ $f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})]$
$f_t' = [(Q_{t-2}' \wedge Q_t') \vee (\neg Q_{t-2}' \wedge 0)]$ $f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge 1)]$

To ensure $f_t = 0$, we require that $Q_{t-2} = 1$. From this, we have $Q_{t-2}' = Q_{t-2} = 1$. Now, $Q_t' = Q_t = (0, 1)$. When $Q_t = Q_t = 0$, then

$f_t' = [(Q_{t-2}' \wedge Q_t') \vee (\neg Q_{t-2}' \wedge 0)]$ $f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge 1)]$
f_t' $[(1 \wedge 0) \vee (0 \wedge 0)]$ $f_t = [(1 \wedge 0) \vee (0 \wedge 1)]$
$f_t' = [0 \vee 0]$ $f_t = [0 \vee 0]$
$f_t' = 0.$ $f_t = 0.$

When $Q_t' = Q_t = 1$, then

$f_t' = [(Q_{t-2}' \wedge Q_t') \vee (\neg Q_{t-2}' \wedge 0)]$ $f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge 1)]$
$f_t' = [(1 \wedge 1) \vee (0 \wedge 0)]$ $f_t = [(1 \wedge 1) \vee (0 \wedge 1)]$
$f_t' = [1 \vee 0]$ $f_t = [1 \vee 0]$
$f_t' = 1.$ $f_t = 1.$

Condition(s) required for this proof: $Q_{t-2} = 1$

41: 0 + 0 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (0, +1, 0)$, i.e., $Q_t' =$ Qt , $Q_{t-1}' = 1$, $Q_{t-1} = 0$, and $Q_{t-2}' = Q_{t-2}$.
We want $\Delta f_t = 0$, i.e., $f_t' = f_t$.

$$\begin{array}{ll}
f'_t = G[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = G[Q_t, Q_{t-1}, Q_{t-2}] \\
f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})] & f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})] \\
f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge 1)] & f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge 0)]
\end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-2} = 1$. From this, we have $Q'_{t-2} = Q_{t-2} = 1$. Now, $Q'_t = Q_t = (0, 1)$. When $Q_t = Q_t = 0$, then

$$\begin{array}{ll}
f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge 1)] & f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge 0)] \\
f'_t = [(1 \wedge 0) \vee (0 \wedge 1)] & f'_t = [(1 \wedge 0) \vee (0 \wedge 0)] \\
f'_t = [0 \vee 0] & f_t = [0 \vee 0] \\
f'_t = 0. & f_t = 0.
\end{array}$$

When $Q'_t = Q_t = 1$, then

$$\begin{array}{ll}
f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge 1)] & f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge 0)] \\
f'_t = [(1 \wedge 1) \vee (0 \wedge 1)] & f_t = [(1 \wedge 1) \vee (0 \wedge 0)] \\
f'_t = [1 \vee 0] & f_t = [1 \vee 0] \\
f'_t = 1. & f_t = 1.
\end{array}$$

Condition(s) required for this proof: $Q_{t-2} = 1$

42: 0 0 - 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (0,\ 0,\ \text{-}1)$, i.e., $Q'_t = Q_t$, $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = 0$, $Q_{t-2} = 1$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll}
f'_t = G[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = G[Q_t, Q_{t-1}, Q_{t-2}] \\
f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})] & f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})] \\
f'_t = [(0 \wedge Q'_t) \vee (1 \wedge Q'_{t-1})] & f_t = [(1 \wedge Q_t) \vee (0 \wedge Q_{t-1})]
\end{array}$$

To ensure $f_t = 0$, we require that $Q_t = Q_{t-1}$. From this, we have $Q'_t = Q_t = Q_{t-1} = Q'_{t-1} = (0, 1)$. When $Q'_t = Q_t = Q_{t-1} = Q'_{t-1} = 0$, then

$$\begin{array}{ll}
f'_t = [(0 \wedge Q'_t) \vee (1 \wedge Q'_{t-1})] & f_t = [(1 \wedge Q_t) \vee (0 \wedge Q_{t-1})] \\
f'_t = [(0 \wedge 0) \vee (1 \wedge 0)] & f'_t = [(1 \wedge 0) \vee (0 \wedge 0)] \\
f'_t = [0 \vee 0] & f_t = [0 \vee 0] \\
f'_t = 0. & f_t = 0.
\end{array}$$

When $Q'_t = Q_t = Q_{t-1} = Q'_{t-1} = 1$, then

$$\begin{array}{ll}
f'_t = [(0 \wedge Q'_t) \vee (1 \wedge Q'_{t-1})] & f_t = [(1 \wedge Q_t) \vee (0 \wedge Q_{t-1})] \\
f'_t = [(0 \wedge) \vee (1 \wedge 1)] & f_t = [(1 \wedge 1) \vee (0 \wedge 1)] \\
f'_t = [0 \vee 1] & f_t = [1 \vee 0] \\
f'_t = 1. & f_t = 1.
\end{array}$$

Condition(s) required for this proof: $Q_t = Q_{t-1}$

43: 0 0 + 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (0,\ 0,\ +1)$, i.e., Q'_t = Qt , $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = 1$, Q_{t-2} = 0.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$
\begin{array}{ll}
f'_t = G[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = G[Q_t, Q_{t-1}, Q_{t-2}] \\
f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})] & f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})] \\
f'_t = [(1 \wedge Q'_t) \vee (0 \wedge Q'_{t-1})] & f_t = [(0 \wedge Q_t) \vee (1 \wedge Q_{t-1})]
\end{array}
$$

To ensure $f_t = 0$, we require that $Q_t = Q_{t-1}$. From this, we have $Q'_t = Q_t = Q_{t-1} = Q'_{t-1} = (0, 1)$. When $Q'_t = Q_t = Q_{t-1} = Q'_{t-1} = 0$, then

$$
\begin{array}{ll}
f'_t = [(1 \wedge Q'_t) \vee (0 \wedge Q'_{t-1})] & f_t = [(0 \wedge Q_t) \vee (1 \wedge Q_{t-1})] \\
f'_t\ [(1 \wedge 0) \vee (0 \wedge 0)] & f_t = [(0 \wedge 0) \vee (1 \wedge 0)] \\
f'_t = [0 \vee 0] & f_t = [0 \vee 0] \\
f'_t = 0. & f_t = 0.
\end{array}
$$

When $Q'_t = Q_t = Q_{t-1} = Q'_{t-1} = 1$, then

$$
\begin{array}{ll}
f'_t = [(1 \wedge Q'_t) \vee (0 \wedge Q'_{t-1})] & f_t = [(0 \wedge Q_t) \vee (1 \wedge Q_{t-1})] \\
f'_t = [(1 \wedge 1) \vee (0 \wedge 1)] & f_t = [(0 \wedge 1) \vee (1 \wedge 1)] \\
f'_t = [1 \vee 0] & f_t = [0 \vee 1] \\
f'_t = 1. & f_t = 1.
\end{array}
$$

Condition(s) required for this proof: $Q_t = Q_{t-1}$

44: + 0 0 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (+1,\ 0,\ 0)$, i.e., $Q'_t = 1$, $Q_t = 0$, $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = Q_{t-2}$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$
\begin{array}{ll}
f'_t = G[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = G[Q_t, Q_{t-1}, Q_{t-2}] \\
f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})] & f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})] \\
f'_t = [(Q'_{t-2} \wedge 1) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})] & f_t = [(Q_{t-2} \wedge 0) \vee (\neg Q_{t-2} \wedge Q_{t-1})]
\end{array}
$$

To ensure $f_t = 0$, we require that $Q_{t-2} = 0$. From this, we have $Q'_{t-2} = Q_{t-2} = 0$. Now, $Q'_{t-1} = Q_{t-1}$ = (0, 1). When $Q'_{t-1} = Q_{t-1} = 0$, then

$$
\begin{array}{ll}
f'_t = [(Q'_{t-2} \wedge 1) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})] & f_t = [(Q_{t-2} \wedge 0) \vee (\neg Q_{t-2} \wedge Q_{t-1})] \\
f'_t = [(0 \wedge 1) \vee (1 \wedge 0)] & f_t = [(0 \wedge 0) \vee (1 \wedge 0)] \\
f'_t = [0 \vee 0] & f_t = [0 \vee 0] \\
f'_t = 0. & f_t = 0.
\end{array}
$$

When $Q'_{t-1} = Q_{t-1} = 1$, then

$f'_t = [(Q'_{t-2} \wedge 1) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})]$ $f_t = [(Q_{t-2} \wedge 0) \vee (\neg Q_{t-2} \wedge Q_{t-1})]$
$f'_t = [(0 \wedge) \vee (1 \wedge 1)]$ $f_t = [(0 \wedge 0) \vee (1 \wedge 1)]$
$f'_t = [0 \vee 1]$ $f_t = [0 \vee 1]$
$f'_t = 1.$ $f_t = 1.$

Condition(s) required for this proof: $Q_{t-2} = 0$

45: 0 ± ± 0

We are given: $(\varDelta Q_t, \varDelta Q_{t-1}, \varDelta Q_{t-2}) = (0, \pm 1, \pm 1)$, i.e., Q'_t = Qt , Q'_{t-1} - $Q_{t-1} = \pm 1$, and Q'_{t-2} - $Q_{t-2} = \pm 1$.
We want $\varDelta f_t = 0$, i.e., $f'_t = f_t$.

$f'_t = G[Q'_t, Q'_{t-1}, Q'_{t-2}]$ $f_t = G[Q_t, Q_{t-1}, Q_{t-2}]$
$f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})]$ $f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})]$

To ensure $f_t = 0$, we require that $Q_t = 0$. From this, we have $Q'_t = Q_t = 0$. From step 22, we showed $Q_{21} = Q_{22}$, so we know $Q_{t-1} = Q_{t-2}$.
Thus, we consider two possibilities. First, we consider when $Q_{t-1} = Q_{t-2} = 0$ and $Q'_{t-1} = Q'_{t-2} = 1$. Thus,

$f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})]$ $f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})]$
$f'_t = [(1 \wedge 0) \vee (0 \wedge 1)]$ $f_t = [(0 \wedge 0) \vee (1 \wedge 0)]$
$f'_t = [0 \vee 0]$ $f_t = [0 \vee 0]$
$f'_t = 0.$ $f_t = 0.$

Second, we consider when $Q_{t-1} = Q_{t-2} = 1$ and $Q'_{t-1} = Q'_{t-2} = 0$. Thus,

$f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})]$ $f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})]$
$f'_t = [(0 \wedge 0) \vee (1 \wedge 0)]$ $f_t = [(1 \wedge 0) \vee (0 \wedge 1)]$
$f'_t = [0 \vee 0]$ $f_t = [0 \vee 0]$
$f'_t = 0.$ $f_t = 0.$

Condition(s) required for this proof: $Q_t = 0$

46: 0 0 ± ±

We are given: $(\varDelta Q_t, \varDelta Q_{t-1}, \varDelta Q_{t-2}) = (0, 0, \pm 1)$, i.e., Q'_t = Qt , $Q'_{t-1} = Q_{t-1}$, and Q'_{t-2} - $Q_{t-2} = \pm 1$.
We want: $\varDelta f_t = \pm 1$, i.e.,f'_t - $f_t = \pm 1$.

$f'_t = G[Q'_t, Q'_{t-1}, Q'_{t-2}]$ $f_t = G[Q_t, Q_{t-1}, Q_{t-2}]$
$f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})]$ $f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})]$

To ensure $f_t = 1$, we require that $Q_t = 1$. From this, we have $Q'_t = Q_t = 1$. From step 23, we showed $Q_{23} = 0$, so we know $Q_{t-1} = 0$. Thus, we consider two possibilities. First, we consider when $Q_{t-2} = 0$ and $Q'_{t-2} = 1$. Thus,

$f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})]$	$f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})]$
$f'_t = [(1 \wedge 1) \vee (0 \wedge 0)]$	$f_t = [(0 \wedge 1) \vee (1 \wedge 0)]$
$f'_t = [1 \vee 0]$	$f_t = [0 \vee 0]$
$f'_t = 1.$	$f_t = 0.$

Second, we consider when $Q_{t-2} = 1$ and $Q'_{t-2} = 0$. Thus,

$f'_t = [(Q'_{t-2} \wedge Q'_t) \vee (\neg Q'_{t-2} \wedge Q'_{t-1})]$	$f_t = [(Q_{t-2} \wedge Q_t) \vee (\neg Q_{t-2} \wedge Q_{t-1})]$
$f'_t = [(0 \wedge 1) \vee (1 \wedge 0)]$	$f_t = [(1 \wedge 1) \vee (0 \wedge 0)]$
$f'_t = [0 \vee 0]$	$f_t = [1 \vee 0]$
$f'_t = 0.$	$f_t = 1.$

Condition(s) required for this proof: $Q_t = 1$

8.3 Proofs for Round 3

For round 3, note that $f_t = H(X,\ Y,\ Z) = X \oplus Y \oplus Z$.

47: $\pm$ 0 0 $\pm$

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (\pm 1,\ 0,\ 0)$, i.e., Q'_t - $Q_t = \pm 1$, $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = Q_{t-2}$.
We want: $\Delta f_t = \pm 1$, i.e.,f'_t - $f_t = \pm 1$.

$f'_t = H[Q'_t,\ Q'_{t-1},\ Q'_{t-2}]$	$f_t = H[Q_t,\ Q_{t-1},\ Q_{t-2}]$
$f'_t = Q'_t \oplus (Q'_{t-1} \oplus Q'_{t-2})$	$f_t = Q_t \oplus (Q_{t-1} \oplus Q_{t-2})$
$f'_t = Q'_t \oplus (Q'_{t-1} \oplus Q'_{t-2})$	$f_t = Q_t \oplus (Q_{t-1} \oplus Q_{t-2})$
$f'_t = Q'_t$	$f_t = Q_t$

Since Q'_t - $Q_t = \pm 1$, we have f'_t - $f_t = \pm 1$, as desired.
Condition(s) required for this proof: none

48: $\pm$ $\pm$ 0 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (\pm 1,\ \pm 1,\ 0)$, i.e., Q'_t - $Q_t = \pm 1$, Q'_{t-1} - $Q_{t-1} = \pm 1$, and $Q'_{t-2} = Q_{t-2}$.
We want: $\Delta f_t = \pm 1$, i.e.,f'_t - $f_t = \pm 1$.

$f'_t = H[Q'_t,\ Q'_{t-1},\ Q'_{t-2}]$	$f_t = H[Q_t,\ Q_{t-1},\ Q_{t-2}]$
$f'_t = (Q'_t \oplus Q'_{t-1}) \oplus Q'_{t-2}$	$f_t = (Q_t \oplus Q_{t-1}) \oplus Q_{t-2}$
$f'_t = (Q'_t \oplus Q'_{t-1}) \oplus Q'_{t-2}$	$f_t = (Q_t \oplus Q_{t-1}) \oplus Q_{t-2}$
$f'_t = Q'_{t-2}$	$f_t = Q_{t-2}$

Since $Q'_{t-2} = Q_{t-2}$, we have $f'_t = f_t$, as desired.
Condition(s) required for this proof: none

49: $\pm$ $\pm$ $\pm$ $\pm$

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (\pm 1,\ \pm 1,\ \pm 1)$, i.e., Q'_t - $Q_t = \pm 1$, Q'_{t-1} - $Q_{t-1} = \pm 1$, and Q'_{t-2} - $Q_{t-2} = \pm 1$.
We want: $\Delta f_t = \pm 1$, i.e.,f'_t - $f_t = \pm 1$

$f'_t = H[Q'_t,\ Q'_{t-1},\ Q'_{t-2}]$ $\quad f_t = H[Q_t,\ Q_{t-1},\ Q_{t-2}]$
$f'_t = (Q'_t \oplus Q'_{t-1}) \oplus Q'_{t-2}$ $\quad f_t = (Q_t \oplus Q_{t-1}) \oplus Q_{t-2}$
$f'_t = (Q'_t \oplus Q'_{t-1}) \oplus Q'_{t-2}$ $\quad f_t = (Q_t \oplus Q_{t-1}) \oplus Q_{t-2}$
$f'_t = Q'_{t-2}$ $f_t = Q_{t-2}$

Since Q'_{t-2} - $Q_{t-2} = \pm 1$, we have f'_t - $f_t = \pm 1$, as desired.
Condition(s) required for this proof: none

8.4 Proofs for Round 4

For round 4, note that $f_t = I(X,\ Y,\ Z) = Y \oplus (X \vee Z)$.

50: $\pm$ $\pm$ $\pm$ $\pm$

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2}) = (\pm 1,\ \pm 1,\ \pm 1)$, i.e., Q_t - $Q_t = \pm 1$, Q'_{t-1} - $Q_{t-1} = \pm 1$, and Q'_{t-2} - $Q_{t-2} = \pm 1$.
We want: $\Delta f_t = \pm 1$, i.e.,f'_t - $f_t = \pm 1$.

$f'_t = I[Q'_t,\ Q'_{t-1},\ Q'_{t-2}]$ $\quad f_t = I[Q_t,\ Q_{t-1},\ Q_{t-2}]$
$f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2})$ $\quad f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2})$

To ensure $f_t = 1$, we require that $Q_t = Q_{t-2}$.
From this, we have $Q_t = Q_{t-2} =$ -1, +1 and $Q_{t-1} =$ -1, +1. Thus, we consider four possibilities. First, we consider when $Q_t = Q_{t-2} =$ -1 and $Q_{t-1} =$ -1. This gives us $Q_t = Q_{t-2} = 1$, $Q'_t = Q'_{t-2} = 0$, $Q_{t-1} = 1$, and $Q'_{t-1} = 0$. Thus,

$f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2})$ $\quad f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2})$
$f'_t = 0 \oplus (0 \vee 1)$ $\quad f_t = 1 \oplus (1 \vee 0)$
$f'_t = 0 \oplus 1$ $\quad f_t = 1 \oplus 1$
$f'_t = 1.$ $\quad f_t = 0.$

Second, we consider when $Q_t = Q_{t-2} =$ -1 and $Q_{t-1} =$ +1. This gives us $Q_t = Q_{t-2} = 1$, $Q'_t = Q'_{t-2} = 0$, $Q_{t-1} = 0$, and $Q'_{t-1} = 1$. Thus,

$f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2})$ $f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2})$
$f'_t = 1 \oplus (0 \vee 1)$ $f_t = 0 \oplus (1 \vee 0)$
$f'_t = 1 \oplus 1$ $f_t = 0 \oplus 1$
$f'_t = 0.$ $f_t = 1.$

Third, we consider when $Q_t = Q_{t-2} = +1$ and $Q_{t-1} =$ -1. This gives us $Q_t = Q_{t-2} = 0$, $Q'_t = Q'_{t-2} = 1$, $Q_{t-1} = 1$, and $Q'_{t-1} = 0$. Thus,

$f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2})$ $f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2})$
$f'_t = 0 \oplus (1 \vee 0)$ $f_t = 1 \oplus (0 \vee 1)$
$f'_t = 0 \oplus 1$ $f_t = 1 \oplus 1$
$f'_t = 1.$ $f_t = 0.$

Fourth, we consider when $Q_t = Q_{t-2} = +1$ and $Q_{t-1} = +1$. This gives us $Q_t = Q_{t-2} = 0$, $Q'_t = Q'_{t-2} = 1$, $Q_{t-1} = 1$, and $Q'_{t-1} = 0$. Thus,

$f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2})$ $f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2})$
$f'_t = 1 \oplus (1 \vee 0)$ $f_t = 0 \oplus (0 \vee 1)$
$f'_t = 1 \oplus 1$ $f_t = 0 \oplus 1$
$f'_t = 0.$ $f_t = 1.$

Condition(s) required for this proof: $Q_t = Q_{t-2}$ ==¿ $Q_t = Q_{t-2}$

51: $\pm$ $\pm$ $\pm$ 0

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2}) = (\pm 1, \pm 1, \pm 1)$, i.e., Q_t - $Q_t = \pm 1$, Q'_{t-1} - $Q_{t-1} = \pm 1$, and Q'_{t-2} - $Q_{t-2} = \pm 1$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$f'_t = I[Q'_t, Q'_{t-1}, Q'_{t-2}]$ $f_t = I[Q_t, Q_{t-1}, Q_{t-2}]$
$f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2})$ $f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2})$

To ensure $f_t = 1$, we require that $Q_t =$ - Q_{t-2}.
From this, we have $Q_t =$ - $Q_{t-2} =$ -1, +1 and $Q_{t-1} =$ -1, +1. Thus, we consider four possibilities. First, we consider when $Q_t =$ -1, $Q_{t-2} = +1$, and $Q_{t-1} =$ -1. This gives us $Q_t = 1$, $Q_{t-2} = 0$, $Q'_t = 0$, $Q'_{t-2} = 1$, $Q_{t-1} = 1$, and $Q'_{t-1} = 0$. Thus,

$f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2})$ $f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2})$
$f'_t = 0 \oplus (0 \vee 0)$ $f_t = 1 \oplus (1 \vee 1)$
$f'_t = 0 \oplus 0$ $f_t = 1 \oplus 1$
$f'_t = 0.$ $f_t = 0.$

Second, we consider when $Q_t =$ -1, $Q_{t-2} = +1$, and $Q_{t-1} = +1$. This gives us $Q_t = 1$, $Q_{t-2} = 0$, $Q'_t = 0$, $Q'_{t-2} = 1$, $Q_{t-1} = 0$, and $Q'_{t-1} = 1$. Thus,

$$\begin{array}{ll} f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2}) & f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2}) \\ f'_t = 1 \oplus (0 \vee 0) & f_t = 0 \oplus (1 \vee 1) \\ f'_t = 1 \oplus 0 & f_t = 0 \oplus 1 \\ f'_t = 1. & f_t = 1. \end{array}$$

Third, we consider when Q_t = +1, Q_{t-2} = -1, and Q_{t-1} = -1. This gives us $Q_t = 0$, $Q_{t-2} = 1$, $Q'_t = 1$, $Q'_{t-2} = 0$, $Q_{t-1} = 1$, and $Q'_{t-1} = 0$. Thus,

$$\begin{array}{ll} f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2}) & f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2}) \\ f'_t = 0 \oplus (1 \vee 1) & f_t = 1 \oplus (0 \vee 0) \\ f'_t = 0 \oplus 1 & f_t = 1 \oplus 0 \\ f'_t = 1. & f_t = 1. \end{array}$$

Fourth, we consider when Q_t = +1, Q_{t-2} = -1, and Q_{t-1} = +1. This gives us $Q_t = 0$, $Q_{t-2} = 1$, $Q'_t = 1$, $Q'_{t-2} = 0$, $Q_{t-1} = 1$, and $Q'_{t-1} = 0$. Thus,

$$\begin{array}{ll} f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2}) & f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2}) \\ f'_t = 1 \oplus (1 \vee 1) & f_t = 0 \oplus (0 \vee 0) \\ f'_t = 1 \oplus 1 & f_t = 0 \oplus 0 \\ f'_t = 0. & f_t = 0. \end{array}$$

Condition(s) required for this proof: Q_t = - Q_{t-2} ==¿ $Q_t = Q_{t-2}$

52: + 0 0 0

We are given: $(\Delta Q_t, \Delta Q_{t-1}, \Delta Q_{t-2}) = (+1, 0, 0)$, i.e., $Q'_t = 1$, $Q_t = 0$, $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = Q_{t-2}$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll} f'_t = I[Q'_t, Q'_{t-1}, Q'_{t-2}] & f_t = I[Q_t, Q_{t-1}, Q_{t-2}] \\ f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2}) & f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2}) \\ f'_t = Q'_{t-1} \oplus (1 \vee \neg Q'_{t-2}) & f_t = Q_{t-1} \oplus (0 \vee \neg Q_{t-2}) \end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-2} = 0$. From this, we have $Q'_{t-2} = Q_{t-2} = 0$. Now, $Q'_{t-1} = Q_{t-1}$ = (0, 1). When $Q'_{t-1} = Q_{t-1} = 0$, then

$$\begin{array}{ll} f'_t = Q'_{t-1} \oplus (1 \vee \neg Q'_{t-2}) & f_t = Q_{t-1} \oplus (0 \vee \neg Q_{t-2}) \\ f'_t = 0 \oplus (1 \vee 1) & f_t = 0 \oplus (0 \vee 1) \\ f'_t = 0 \oplus 1 & f_t = 0 \oplus 1 \\ f'_t = 1. & f_t = 1. \end{array}$$

When $Q'_{t-1} = Q_{t-1} = 1$, then

$$\begin{array}{ll} f'_t = Q'_{t-1} \oplus (1 \vee \neg Q'_{t-2}) & f_t = Q_{t-1} \oplus (0 \vee \neg Q_{t-2}) \\ f'_t = 1 \oplus (1 \vee 1) & f_t = 1 \oplus (0 \vee 1) \\ f'_t = 1 \oplus 1 & f_t = 1 \oplus 1 \\ f'_t = 0. & f_t = 0. \end{array}$$

Condition(s) required for this proof: $Q_{t-2} = 0$

53: + + 0 0

We are given: $(\varDelta Q_t,\ \varDelta Q_{t-1},\ \varDelta Q_{t-2}) = (+1,\ +1,\ 0)$, i.e., $Q'_t = Q'_{t-1} = 1$, $Q_t = Q_{t-1} = 0$, and $Q'_{t-2} = Q_{t-2}$.
We want $\varDelta f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll} f'_t = I[Q'_t,\, Q'_{t-1},\, Q'_{t-2}] & f_t = I[Q_t,\, Q_{t-1},\, Q_{t-2}] \\ f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2}) & f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2}) \\ f'_t = 1 \oplus (1 \vee \neg Q'_{t-2}) & f_t = 0 \oplus (0 \vee \neg Q_{t-2}) \end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-2} = 1$. From this, we have $Q'_{t-2} = Q_{t-2} = 1$. Thus,

$$\begin{array}{ll} f'_t = 1 \oplus (1 \vee \neg Q'_{t-2}) & f_t = 0 \oplus (0 \vee \neg Q_{t-2}) \\ f'_t = 1 \oplus (1 \vee 0) & f_t = 0 \oplus (0 \vee 0) \\ f'_t = 1 \oplus 1 & f_t = 0 \oplus 0 \\ f'_t = 0. & f_t = 0. \end{array}$$

Condition(s) required for this proof: $Q_{t-2} = 1$

54: - 0 0 0

We are given: $(\varDelta Q_t,\ \varDelta Q_{t-1},\ \varDelta Q_{t-2}) = (-1,\ 0,\ 0)$, i.e., $Q'_t = 0$, $Q_t = 1$, $Q'_{t-1} = Q_{t-1}$, and $Q'_{t-2} = Q_{t-2}$.
We want $\varDelta f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll} f'_t = I[Q'_t,\, Q'_{t-1},\, Q'_{t-2}] & f_t = I[Q_t,\, Q_{t-1},\, Q_{t-2}] \\ f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2}) & f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2}) \\ f'_t = Q'_{t-1} \oplus (0 \vee \neg Q'_{t-2}) & f_t = Q'_{t-1}\ (1\ Q_{t-2}) \end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-2} = 0$. From this, we have $Q'_{t-2} = Q_{t-2} = 0$. Now, $Q'_{t-1} = Q_{t-1} = (0,\ 1)$. When $Q'_{t-1} = Q_{t-1} = 0$, then

$$\begin{array}{ll} f'_t = Q'_{t-1} \oplus (0 \vee \neg Q'_{t-2}) & f_t = Q_{t-1} \oplus (1 \vee \neg Q_{t-2}) \\ f'_t = 0 \oplus (0 \vee 1) & f_t = 0 \oplus (1 \vee 1) \\ f'_t = 0 \oplus 1 & f_t = 0 \oplus 1 \\ f'_t = 1. & f_t = 1. \end{array}$$

When $Q'_{t-1} = Q_{t-1} = 1$, then

$$\begin{array}{ll} f'_t = Q'_{t-1} \oplus (0 \vee \neg Q'_{t-2}) & f_t = Q_{t-1} \oplus (1 \vee \neg Q_{t-2}) \\ f'_t = 1 \oplus (0 \vee 1) & f_t = 1 \oplus (1 \vee 1) \\ f'_t = 1 \oplus 1 & f_t = 1 \oplus 1 \\ f'_t = 0. & f_t = 0. \end{array}$$

Condition(s) required for this proof: $Q_{t-2} = 0$

55: - - 0 0

We are given: $(\Delta Q_t,\ \Delta Q_{t-1},\ \Delta Q_{t-2})$ = (-1, -1, 0), i.e., $Q_t = Q_{t-1} = 1$, $Q'_t = Q'_{t-1} = 0$, and $Q'_{t-2} = Q_{t-2}$.
We want $\Delta f_t = 0$, i.e., $f'_t = f_t$.

$$\begin{array}{ll} f'_t = I[Q'_t,\ Q'_{t-1},\ Q'_{t-2}] & f_t = I[Q_t,\ Q_{t-1},\ Q_{t-2}] \\ f'_t = Q'_{t-1} \oplus (Q'_t \vee \neg Q'_{t-2}) & f_t = Q_{t-1} \oplus (Q_t \vee \neg Q_{t-2}) \\ f'_t = 0 \oplus (0 \vee \neg Q'_{t-2}) & f_t = 1 \oplus (1 \vee \neg Q_{t-2}) \end{array}$$

To ensure $f_t = 0$, we require that $Q_{t-2} = 1$. From this, we have $Q'_{t-2} = Q_{t-2} = 1$. Thus,

$$\begin{array}{ll} f'_t = 0 \oplus (0 \vee \neg Q'_{t-2}) & f_t = 1 \oplus (1 \vee \neg Q_{t-2}) \\ f'_t = 0 \oplus (0 \vee 0) & f_t = 1 \oplus (1 \vee 0) \\ f'_t = 0 \oplus 0 & f_t = 1 \oplus 1 \\ f'_t = 0. & f_t = 0. \end{array}$$

Condition(s) required for this proof: $Q_{t-2} = 1$

9 Errata

In scrutinizing [3], several errors were found. We have divided the errors into three sections. Trivial errors are simply misprints and do not affect the attack in any way as a whole. The minor errors are more important, yet they still do not affect the overall attack. The two significant errors, however, have a considerable effect on the attack. In correcting the first error, we will show that the complexity of the attack is only about half of what was stated in [3]. In correcting the second, we will show that *Case Two* as presented in [3] does not succeed in fulfilling the conditions required for the collision differential to hold.

9.1 Trivial Errors

Page 4, Description of the f_t functions:
$F(X,\ Y,\ Z) = (X \wedge Y) \oplus (\neg X \wedge Z),\ 0 \le t \le 15 \rightarrow F(X,\ Y,\ Z) = (X \wedge Y) \vee (\neg X \wedge Z),\ 0 \le t \le 15$
$G(X,\ Y,\ Z) = (Z \wedge X) \oplus (\neg Z \wedge Y),\ 0 \le t \le 15 \rightarrow G(X,\ Y,\ Z) = (Z \wedge X) \vee (\neg Z \wedge Y),\ 0 \le t \le 15$

Page 7, Condition III:

$$\delta R_t = \sum_{j=25}^{31} +2^{j+12 \pmod{32}} = \sum_{j=5}^{31} +2^j \rightarrow \delta R_t = \sum_{j=25}^{31} +2^{j+12 \pmod{32}} = \sum_{j=5}^{11} +2^j$$

Page 9, Round 8:
Conditions on T_6 → Conditions on T_8
δT_8 = (+2^{31} - 2^{24} + 2^{16} + 2^{10} + 2^8 + 2^6) + (-2^{-6}) → δT_8 = (+2^{31} - 2^{24} + 2^{16} + 2^{10} + 2^8 + 2^6) + (-2^6)

Page 13, Round 18:
δQ_{18} = +2^{31} + 2^{17} → δQ_{18} = +2^{31}

Page 13, Round 19:
$\delta Q_{t-3} = Q_{19}$ = +2^{31} - 2^{17} → $\delta Q_{t-3} = Q_{16}$ = +2^{31} - 2^{17}

Page 14, Round 25:
$\delta Q_{t-3} = Q_{19}$ = +2^{31} → $\delta Q_{t-3} = Q_{22}$ = +2^{31}

Page 16, Round 61:
$\delta Q_{62} = \delta Q_{61} + R_{61}$ = (+2^{31}) + (0) = +2^{31} + 2^{25} → $Q_{62} = Q_{61} + R_{61}$ = (+2^{31}) + (+2^{25}) = +2^{31} + 2^{25}

Page 18, Round 5:
$0 \in T_5$[11 - 18] → $0 \in T_5$[18 - 11]

Page 18, Round 10:
$0 \in T_{10}$[14, 12] → $0 \in T_{10}$[14 - 12]

Page 18, Round 11:
$1 \in T_{11}$[22, 17] → $1 \in T_{11}$[22 - 17]

Page 30, $\nabla Q_9[31] = \pm 1$:
$Q_8[31] = \overline{Q_7[31] \oplus Q_8[31]} \rightarrow Q_9[31] = \overline{Q_7[31] \oplus Q_8[31]}$

Page 33, Constant bits of Q_{11}:
For $j \in$ [8, 0], $\nabla f_{11}[j]$ = +1, requires $Q_{11}[j] = 0$ → For $j \in$ [8, 0], $\nabla f_{11}[j]$ = -1, requires $Q_{11}[j] = 0$

Page 34, Non-Constant bits of Q_{11}:
$f_{11}*[30] = f_{11}[30]$, requires $Q_9*[30] = Q_9[30] = Q_{10}[30]$ → $f_{11}*[30] = f_{11}[30]$, requires $Q_{10}*[30] = Q_{10}[30] = Q_9[30]$

Page 35, Obtaining the Correct ΔQ_t:
Since $Q_{11}[7] = 1$ and $Q_{11}[7] = 0$ are already specified → Since $Q_{11}[7] = 1$ and $Q_{10}[7] = 0$ are already specified

Page 35, Obtaining the Correct f_t:
For $j \in$ [30 - 20, 11, 10, 9, 6 - 0] → For $j \in$ [29 - 20, 11, 10, 9, 6 - 0]

Page 44, Obtaining the Correct f_t:
$\Delta Q_{15}[j] = 0$, for $j \in$ [30 - 17, 14 - 44, 2, 1, 0] → $\Delta Q_{15}[j] = 0$, for $j \in$ [30 - 16, 14 - 4, 2, 1, 0]

Page 51, Caption for Table 7:
For rounds 16 to 31 of the first block $\rightarrow$ For rounds 32 to 47 of the first block

Page 51, Round 35:
The attacker has $\delta Q_{32} = 0$, $\delta Q_{34} = 0$, and $\delta Q_{35} = \pm 2^{31}$ $\rightarrow$ The attacker has $\delta Q_{33} = 0$, $\delta Q_{34} = 0$, and $\delta Q_{35} = \pm 2^{31}$

Page 58, Caption for Table 11:
Conditions for on Q_t, $15 \leq t \leq 32$, in the first block $\rightarrow$ Conditions on Q_t, $3 \leq t \leq 15$, in the first block

Page 59, Caption for Table 12:
Conditions for on Q_t, $15 \leq t \leq 32$, in the first block $\rightarrow$ Conditions on Q_t, $16 \leq t \leq 63$, in the first block

Page 68, Caption for Table 17:
Add-differences for rounds 16 to 63 of the second block $\rightarrow$ Add-differences for the second block

9.2 Minor Errors

Page 11, Round 12:
δT_{12} = -2^{16} + 2^6 + 2^0 $\rightarrow$ δT_{12} = +2^{17} + 2^6 + 2^0
δ = (-2^{16} + 2^6 + 2^0) $\rightarrow$ δ = (+2^{17} + 2^6 + 2^0)
δT_{12} = -$2^{16+7=23}$ + $2^{6+7=13}$ + $2^{0+7=7}$ $\rightarrow$ δT_{12} = +$2^{17+7=24}$ + $2^{6+7=13}$ + $2^{0+7=7}$

Page 18, Round 6:
$1 \in T_6[13 - 10] \Rightarrow$ Probability: (1 - 2^{-5}) $\rightarrow$ $1 \in T_6[13 - 10] \Rightarrow$ Probability: (1 - 2^{-4})

Page 18, Round 9:
$0 \in T_9[19 - 2] \Rightarrow$ Probability: (1 - 2^{-18}) $\rightarrow$ $0 \in T_9[19 - 0] \Rightarrow$ Probability: (1 - 2^{-20})

Page 18, Round 12:
δ = (-2^{16} + 2^6 + 2^0) $\rightarrow$ δ = (+2^{17} + 2^6 + 2^0)
$0 \in \delta T_{12}[24 - 16] \Rightarrow$ Probability: (1 - 2^{-9}) $\rightarrow$ $0 \in \delta T_{12}[24 - 17] \Rightarrow$ Probability: (1 - 2^{-8})
$0 \in \delta T_{12}[15 - 6] \Rightarrow$ Probability: (1 - 2^{-10}) $\rightarrow$ $0 \in \delta T_{12}[16 - 6] \Rightarrow$ Probability: (1 - 2^{-11})
$0 \in \delta T_{12}[5 - 2] \Rightarrow$ Probability: (1 - 2^{-4}) $\rightarrow$ $0 \in \delta T_{12}[5 - 0] \Rightarrow$ Probability: (1 - 2^{-6})

Page 30, Summary of the Requirements resulting from this round:
$Q_8[7, 1] = Q_9[26, 19 - 15] = 0 \rightarrow Q_8[7, 1] = Q_9[26, 19 - 15, 7, 6, 1] = 0$

Page 53, Round 48:
Obtaining $\mathit{\Delta} f_{48} = 0$, requires $\nabla Q_{48}[31] = \nabla Q_{48}[31]$ $\rightarrow$ Obtaining $\mathit{\Delta} f_{60} = 0$, requires $\nabla Q_{48}[31] = \nabla Q_{46}[31]$

Page 54, Round 49:
Obtaining $\mathit{\Delta} f_{49} = 0$, requires $\nabla Q_{49}[31] = \nabla Q_{49}[31]$ $\rightarrow$ Obtaining $\mathit{\Delta} f_{49} = 0$, requires $\nabla Q_{49}[31] = \nabla Q_{47}[31]$

Page 54, Round 50:
Obtaining $\mathit{\Delta} f_{50} = 0$, requires $\nabla Q_{50}[31]$ = -$\nabla Q_{50}[31]$ $\rightarrow$ Obtaining $\mathit{\Delta} f_{50} = 0$, requires $\nabla Q_{50}[31]$ = -$\nabla Q_{48}[31]$

Page 54, Rounds 51 to 59:
Obtaining $f_t = 0$, requires $Q_t[31] = Q_t[31] \rightarrow$ Obtaining $f_t = 0$, requires $Q_t[31] = \nabla Q_{t-2}[31]$

Page 55, Round 60:
Obtaining $\Delta f_{60} = 0$, requires $\nabla Q_{60}[31]$ = -$\nabla Q_{60}[31] \rightarrow$ Obtaining $\Delta f_{60} = 0$, requires $\nabla Q_{60}[31]$ = -$\nabla Q_{58}[31]$

Page 55, Round 61:
Obtaining $\Delta f_{61} = 0$, requires $\nabla Q_{61}[31] = \nabla Q_{61}[31] \rightarrow$ Obtaining $\Delta f_{61} = 0$, requires $\nabla Q_{61}[31] = \nabla Q_{59}[31]$

Page 56, Round 62:
Obtaining $\Delta f_{62} = 0$, requires $\nabla Q_{62}[31] = \nabla Q_{62}[31] \rightarrow$ Obtaining $\Delta f_{62} = 0$, requires $\nabla Q_{62}[31] = \nabla Q_{60}[31]$

Page 56, Round 63:
Obtaining $\Delta f_{63} = 0$, requires $\nabla Q_{63}[31] = \nabla Q_{63}[31] \rightarrow$ Obtaining $\Delta f_{63} = 0$, requires $\nabla Q_{63}[31] = \nabla Q_{61}[31]$

Page 60, Second block:
For a given choice of the values A, B, H, I, $J \rightarrow$ For a given choice of the values A, C, I, J
For a random message, the probability is $2^{-318} \rightarrow$ For a random message, the probability is 2^{-319}

Page 68, Step 4:
$\Delta f_t = +2^{30} + 2^{26}$ - 2^{18} - $2^3 + 2^1 \rightarrow \Delta f_t = +2^{30} + 2^{26}$ - $2^{18} + 2^3$ - 2^1

Page 68, Step 6:
Δf_t = -2^{31} - 2^{21} - $2^{10} + 2^3 \rightarrow \Delta f_t = +2^{31}$ - 2^{21} - $2^{10} + 2^3$

Page 69, Step 5:
$\nabla Q_t = 2^{31} + 2^9 + 2^6 + 2^0 \rightarrow \nabla Q_t = 2^{31} + 2^9 + 2^8 + 2^6 + 2^0$

9.3 Significant Errors

Significant Error #1. In the table which presents a summary of the probabilities that the T_t would hold in each step, Hawkes, Paddon, and Rose state that T_t would hold with probability 2^{-1} in step 16 since they believed that bit 24 of T_{16} must be 0. However, the true probability is (1 - 2^{-3}) because only one of bits 24, 25, or 26 must be 0 since the left shift for step 16 is 5, not 7. Therefore, the probability that all of the T_t would hold after using single-message modification for each block is $2^{-2.4}$ rather than $2^{-3.2}$. Since the probability that all bits will propagate through the f_t functions in the desired manner for each block is 2^{-39}, the probability that the collision differential will hold for each block is

$$2^{-2.4} \times 2^{-39} = 2^{-41}$$

rather than

$$2^{-3.2} \times 2^{-39} = 2^{-42}$$

as stated in [3]. Thus, the complexity of the attack on both blocks is

$$2^{41} + 2^{41} = 2^{42}$$

rather than

$$2^{42} + 2^{42} = 2^{43}$$

as stated in [3].

Significant Error #2: On page 24 in [3], Hawkes, Paddon, and Rose claim that the add-difference (-2^{27}) in Q_7 does not need to propagate to bit 31, as required in [7]. Rather, they claim that no propagation is necessary and that the propagation only results in a large number of additional conditions which are not needed for the attack to succeed. Thus, Hawkes, Paddon, and Rose consider two cases. *Case One* presents the propagation as illustrated in [7] while *Case Two* requires no propagation for the add-difference (-2^{27}). We will prove that *Case Two* does not succeed in meeting the necessary conditions for collision differential to hold, and therefore, as shown in sectionr̃efsec:conditions, *Case One* is the only viable option. We will do this by examining bit 31 in steps 7, 8, and 9.

According to *Case Two*, since no propagation is necessary for the add-difference (-2^{27}) in Q_7, $\Delta Q_7[31]$ = 0. From steps 5 and 6, we have $\Delta Q_5[31] = 0$ and $\Delta Q_6[31] = \pm 1$.
For the collision differential to hold, it is necessary that $\Delta f_7[31] = 0$. We will now show that $Q_7[31] = 0$ is required for $\Delta f_7[31] = 0$:

We are given: $(\Delta Q_7, \Delta Q_6, \Delta Q_5) = (0, \pm 1, 0)$, i.e., $Q'_7 = Q_7$, Q'_6 - $Q_6 = \pm 1$, and $Q'_5 = Q_5$.
We want: $\Delta f_7 = 0$, i.e., $f'_7 = f_7$.

$$\begin{array}{ll} f'_7 = F[Q'_7, Q'_6, Q'_5] & f_7 = F[Q_7, Q_6, Q_5] \\ f'_7 = [(Q'_7 \wedge Q'_6) \vee (\neg Q'_7 \wedge Q'_5)] & f_7 = [(Q_7 \wedge Q_6) \vee (\neg Q_7 \wedge Q_5)] \end{array}$$

To ensure $\Delta f_7 = 0$, we require that $Q_7 = 0$. From this, we have $Q'_7 = Q_7 = 0$. Now, $Q'_5 = Q_5 = (0, 1)$. Also, we have Q'_6 - Q_6 = -1, +1. We consider four possibilities. First, when $Q'_6 = 0$, $Q_6 = 1$, and $Q'_5 = Q_5$ = 0, then

$$\begin{array}{ll} f'_7 = [(Q'_7 \wedge Q'_6) \vee (\neg Q'_7 \wedge Q'_5)] & f_7 = [(Q_7 \wedge Q_6) \vee (\neg Q_7 \wedge Q_5)] \\ f'_7 = [(0 \wedge 0) \vee (1 \wedge 0)] & f_7 = [(0 \wedge 1) \vee (1 \wedge 0)] \\ f'_7 = [0 \vee 0] & f_7 = [0 \vee 0] \\ f'_7 = 0. & f_7 = 0. \end{array}$$

Second, when $Q'_6 = 0$, $Q_6 = 1$, and $Q'_5 = Q_5 = 1$, then

$$\begin{array}{ll} f'_7 = [(Q'_7 \wedge Q'_6) \vee (\neg Q'_7 \wedge Q'_5)] & f_7 = [(Q_7 \wedge Q_6) \vee (\neg Q_7 \wedge Q_5)] \\ f'_7 = [(0 \wedge 0) \vee (1 \wedge 1)] & f_7 = [(0 \wedge 1) \vee (1 \wedge 1)] \\ f'_7 = [0 \vee 1] & f_7 = [0 \wedge 1] \\ f'_7 = 1. & f_7 = 1. \end{array}$$

Third, when $Q'_6 = 1$, $Q_6 = 0$, and $Q'_5 = Q_5 = 0$, then

$$\begin{array}{ll} f'_7 = [(Q'_7 \wedge Q'_6) \vee (\neg Q'_7 \wedge Q'_5)] & f_7 = [(Q_7 \wedge Q_6) \vee (\neg Q_7 \wedge Q_5)] \\ f'_7 = [(0 \wedge 1) \vee (1 \wedge 0)] & f_7 = [(0 \wedge 0) \vee (1 \wedge 0)] \\ f'_7 = [0 \vee 0] & f_7 = [0 \vee 0] \\ f'_7 = 0. & f_7 = 0. \end{array}$$

Fourth, when $Q'_6 = 1$, $Q_6 = 0$, and $Q'_5 = Q_5 = 1$, then

$f'_7 = [(Q'_7 \wedge Q'_6) \vee (\neg Q'_7 \wedge Q'_5)]$	$f_7 = [(Q_7 \wedge Q_6) \vee (\neg Q_7 \wedge Q_5)]$
$f'_7 = [(0 \wedge 1) \vee (1 \wedge 1)]$	$f_7 = [(0 \wedge 0) \vee (1 \wedge 1)]$
$f'_7 = [0 \vee 1]$	$f_7 = [0 \vee 1]$
$f'_7 = 1.$	$f_7 = 1.$

Condition(s) required for this proof: $Q_7 = 0$

Next, according *Case Two*, $\Delta Q_8[31] = 0$. From steps 6 and 7, we have $\Delta Q_6[31] = \pm 1$ and $\Delta Q_7[31] = 0$. For the collision differential to hold, it is necessary that $\Delta f_8[31] = \pm 1$.

We will now show that $Q_8[31] = 0$ is required for $\Delta f_8[31] = \pm 1$:

We are given: $(\Delta Q_8, \Delta Q_7, \Delta Q_6) = (0, 0, \pm 1)$, i.e., $Q'_8 = Q_8$, $Q'_7 = Q_7$, and Q'_6 - $Q_6 = \pm 1$.
We want: $\Delta f_8 = \pm 1$, i.e., f'_8 - $f_8 = \pm 1$.

$f'_8 = F[Q'_8, Q'_7, Q'_6]$	$f_8 = F[Q_8, Q_7, Q_6]$
$f'_8 = [(Q'_8 \wedge Q'_7) \vee (\neg Q'_8 \wedge Q'_6)]$	$f_8 = [(Q_8 \wedge Q_7) \vee (\neg Q_8 \wedge Q_6)]$

To ensure $\Delta f_8 = \pm 1$, we require that $Q_8 = 0$. From this, we have $Q'_8 = Q_8 = 0$. Now, since $\Delta Q_7 = 0$ and $Q_7 = 0$, $Q'_7 = Q_7 = 0$. Also, we have Q'_6 - Q_6 = -1, +1. We consider two possibilities. First, when $Q'_6 = 0$, and $Q_6 = 1$, then

$f'_8 = [(Q'_8 \wedge Q'_7) \vee (\neg Q'_8 \wedge Q'_6)]$	$f_8 = [(Q_8 \wedge Q_7) \vee (\neg Q_8 \wedge Q_6)]$
$f_8 = [(0 \wedge 0) \vee (1 \wedge 0)]$	$f_8 = [(0 \wedge 0) \vee (1 \wedge 1)]$
$f_8 = [0 \vee 0]$	$f_8 = [0 \vee 1]$
$f_8 = 0.$	$f_8 = 1.$

Second, when $Q'_6 = 1$, and $Q_6 = 0$, then

$f'_8 = [(Q'_8 \wedge Q'_7) \vee (\neg Q'_8 \wedge Q'_6)]$	$f_8 = [(Q_8 \wedge Q_7) \vee (\neg Q_8 \wedge Q_6)]$
$f_8 = [(0 \wedge 0) \vee (1 \wedge 1)]$	$f_8 = [(0 \wedge 0) \vee (1 \wedge 0)]$
$f_8 = [0 \vee 1]$	$f_8 = [0 \vee 0]$
$f_8 = 1.$	$f_8 = 0.$

Condition(s) required for this proof: $Q_8 = 0$

Then, according *Case Two*, no conditions are required for $\Delta f_9[31] = \pm 1$.
This is because $Q_7[31] = 1$ and $Q_8[31] = 0$ implies that $\Delta f_9[31] = \pm 1$.
This statement is true, as shown below:

We are given: $(\Delta Q_9, \Delta Q_8, \Delta Q_7) = (\pm 1, 0, 0)$, i.e., Q'_9 - $Q_9 = \pm 1$, $Q'_8 = Q_8$, and $Q'_7 = Q_7$.
We want: $\Delta f_9 = \pm 1$, i.e.,f'_9 -$f_9 = \pm 1$.

$f'_9 = F[Q'_9, Q'_8, Q'_7]$	$f_9 = F[Q_9, Q_8, Q_7]$
$f'_9 = [(Q'_9 \wedge Q'_8) \vee (\neg Q'_9 \wedge Q'_7)]$	$f_9 = [(Q_9 \wedge Q_8) \vee (\neg Q_9 \wedge Q_7)]$

To ensure $\Delta f_9 = \pm 1$, no requirements are necessary. Now, since $\Delta Q_7 = 0$ and $Q_7 = 1$, $Q'_7 = Q_7 = 1$, and since $\Delta Q_8 = 0$ and $Q_8 = 0$, $Q'_8 = Q_8 = 0$. We consider two possibilities. First, when $Q'_9 = 0$ and $Q_9 = 1$, then

$$\begin{array}{ll} f'_9 = [(Q'_9 \wedge Q'_8) \vee (\neg Q'_9 \wedge Q'_7)] & f_9 = [(Q_9 \wedge Q_8) \vee (\neg Q_9 \wedge Q_7)] \\ f'_9 = [(0 \wedge 0) \vee (1 \wedge 1)] & f_9 = [(1 \wedge 0) \vee (0 \wedge 1)] \\ f'_9 = [0 \vee 1] & f_9 = [0 \vee 0] \\ f'_9 = 1. & f_9 = 0. \end{array}$$

Second, when $Q'_9 = 1$ and $Q_9 = 0$, then

$$\begin{array}{ll} f'_9 = [(Q'_9 \wedge Q'_8) \vee (\neg Q'_9 \wedge Q'_7)] & f_9 = [(Q_9 \wedge Q_8) \vee (\neg Q_9 \wedge Q_7)] \\ f'_9 = [(1 \wedge 0) \vee (0 \wedge 1)] & f_9 = [(0 \wedge 0) \vee (1 \wedge 1)] \\ f'_9 = [0 \vee 0] & f_9 = [0 \vee 1] \\ f'_9 = 0. & f_9 = 1. \end{array}$$

Condition(s) required for this proof: none

But there is a problem. In step 7, we proved that $Q_7[31] = 0$, but now according *Case Two*, $Q_7[31] = 1$. This is impossible. In fact, we will show that if $Q_7[31] = 0$, we cannot have $\Delta f_9[31] = \pm 1$:

We are given: $(\Delta Q_9, \Delta Q_8, \Delta Q_7) = (\pm 1, 0, 0)$, i.e., Q'_9 - $Q_9 = \pm 1$, $Q'_8 = Q_8$, and $Q'_7 = Q_7$.
We want: $\Delta f_9 = \pm 1$, i.e.,f'_9 -$f_9 = \pm 1$.

$$\begin{array}{ll} f'_9 = F[Q'_9, Q'_8, Q'_7] & f_9 = F[Q_9, Q_8, Q_7] \\ f'_9 = [(Q'_9 \wedge Q'_8) \vee (\neg Q'_9 \wedge Q'_7)] & f_9 = [(Q_9 \wedge Q_8) \vee (\neg Q_9 \wedge Q_7)] \end{array}$$

To calculate Δf_9 , no requirements are necessary. Now, since $\Delta Q_7 = 0$ and $Q_7 = 0$, $Q'_7 = Q_7 = 0$, and since $\Delta Q_8 = 0$ and $Q_8 = 0$, $Q'_8 = Q_8 = 0$. We consider two possibilities. First, when $Q'_9 = 0$ and $Q_9 = 1$, then

$$\begin{array}{ll} f'_9 = [(Q'_9 \wedge Q'_8) \vee (\neg Q'_9 \wedge Q'_7)] & f_9 = [(Q_9 \wedge Q_8) \vee (\neg Q_9 \wedge Q_7)] \\ f'_9 = [(0 \wedge 0) \vee (1 \wedge 0)] & f_9 = [(1 \wedge 0) \vee (0 \wedge 0)] \\ f'_9 = [0 \vee 0] & f_9 = [1 \vee 0] \\ f'_9 = 0. & f_9 = 0. \end{array}$$

Second, when $Q'_9 = 1$ and $Q_9 = 0$, then

$$\begin{array}{ll} f'_9 = [(Q'_9 \wedge Q'_8) \vee (\neg Q'_9 \wedge Q'_7)] & f_9 = [(Q_9 \wedge Q_8) \vee (\neg Q_9 \wedge Q_7)] \\ f'_9 = [(1 \wedge 0) \vee (0 \wedge 0)] & f_9 = [(0 \wedge 0) \vee (1 \wedge 0)] \\ f'_9 = [1 \vee 0] & f_9 = [0 \vee 0] \\ f'_9 = 0. & f_9 = 0. \end{array}$$

For both possibilities, $\Delta f_9 = 0$, not $\Delta f_9 = \pm 1$, which was desired. Thus, using the values of $Q_7[31]$ and $Q_8[31]$ calculated in steps 7 and 8, we cannot obtain the desired value of $\Delta f_9[31]$, and we cannot meet all of the necessary conditions for collision differential to hold. If we had chosen *Case One* and propagated the add-difference (-2^{27}) in Q_7 to bit 31, as required in [7], we would have obtained the appropriate condition for

$Q_7[31]$, and therefore we would have been able to obtain the desired value for $\Delta f_9[31]$. As we have illustrated in section 7, *Case One* clearly succeeds in meeting every condition required for the collision differential to hold.

10 Conclusion

This paper has presented a new approach to the recent successful differential attack by Wang *et al.* on the MD5 Message Digest Algorithm. It has built on the work of Hawkes, Paddon, and Rose by adding proofs, examples, illustrations, and corrections to make the attack on MD5 more accessible to the mathematically literate reader.

This paper has made seven original contributions. First, it has compared the unorthodox description of MD5 by Hawkes, Paddon, and Rose to the original description by Ron Rivest. Second, it has supplied examples for conditions that they present for the T_t. Third, it has expanded on the description of the first block of the differential by explaining the conditions on the T_t in each step. Fourth, it has presented an original step by step analysis of the description of the second block based only on the table that Hawkes, Paddon, and Rose provide. Fifth, it has supplied original proofs of their assertions regarding the conditions for the propagation of the differences through the f_t functions for the first block. Sixth, it has provided both assertions and proofs for the conditions for the propagation of the differences through the f_t functions for the second block. Finally, it has corrected two significant errors in the work of Hawkes, Paddon, and Rose, demonstrating that the complexity of the attack was only about half as great as they believed and that their *Case Two* did not succeed in fulfilling the conditions required for the collision differential to hold.

11 Acknowledgements

I am grateful for the suggestions and advice that Philip Hawkes and Gregory Rose have given me. I am also thankful for the motivation and support that John Edman and John Noerenberg provided throughout the process of writing this paper.

References

1. R. Rivest. The md5 message-digest algorithm. 1992.
2. X. Wang, D. Feng, X. Lai, and H. Yu. Collisions for hash functions md4, md5, haval-128 and ripemd. *Cryptology ePrint Archive*, 2000.
3. P. Hawkes, M. Paddon, and G. Rose. Musings on the wang et al. md5 collision. *Cryptology ePrint Archive*, 2004.
4. R. Rivest. The md4 message-digest algorithm. 1992.
5. B. den Boer and A. Bosselaers. Collisions for the compression function of md5. *Advances in Cryptology - Eurocrypt '93*, (vol. 773):293–304, 1994.
6. H. Dobbertin. Cryptanalysis of md5 compress.
7. X. Wang and H. Yu. How to break md5 and other hash functions. http://www.infosec.sdu.edu.cn/paper/md5-attack.pdf, 2005.
8. Jie Liang and Xuejia Lai. Improved collision attack on hash function md5. *Cryptology ePrint Archive*, 2005.
9. John Black, Martin Cochran, and Trevor Highland. A study of the md5 attacks: Insights and improvements. In *FSE*, pages 262–277, 2006.
10. Vlastimil Klima. Finding md5 collisions on a notebook pc using multi-message modifications. *Cryptology ePrint Archive*, 2005.
11. Marc Stevens. Fast collision attack on md5. *Cryptology ePrint Archive*, 2006.
12. Vlastimil Klima. Tunnels in hash functions: Md5 collisions within a minute. *Cryptology ePrint Archive*, 2006.