Proof of correctness - Algorithm Q4

Proposition. *if 1 error occurred in msg, it is at index $i = EC' \oplus EC1$*

Proof. Recall some XOR properties:

(1) $\forall x \;\; x \oplus x = 0$

(2) $\forall x, y \;\; x \oplus y = y \oplus x$ (commutative)

(3) $\forall x, y, z \;\; x \oplus (y \oplus z) = (x \oplus y) \oplus z$ (assosiative)

Let us denote the indices of the active bits (1) in msg by $x_1, \ldots, x_r$ (e.g., if $msg = 0110110$ then $x_1 = 2, x_2 = 3, x_3 = 5, x_4 = 6$). We first consider the case where some index, i, of msg which was 0 became 1 (e.g., if $msg = 0110110$ then the received message is $\mathbf{1}110110$). Thus, $EC1 = x_1 \oplus \ldots \oplus x_r$ and $EC' = x_1 \oplus \ldots \oplus \boldsymbol{i} \oplus \ldots \oplus x_r$ (since index i is active in the received message). We now have:

$$EC' \oplus EC1 = (x_1 \oplus \ldots \oplus \boldsymbol{i} \oplus \ldots \oplus x_r) \oplus (x_1 \oplus \ldots \oplus x_r) \overset{(2)+(3)}{=} i \oplus (x_1 \oplus x_1) \oplus \ldots \oplus (x_r \oplus x_r) \overset{(1)}{=} i \oplus 0 = i$$

For the case where some index of msg which was 1 became 0 we have the same result by the symmetric argument ($EC1$ now contains i and EC' does not). □