Let $P$ stand for the conjunction of the conditions

- $P1$: For all integers $i$ such that $1 \leq i \leq s$ we have $f(i) = F(i)$
- $P2$: $t = f(s)$,

and assume that $P$ holds prior to execution of the following line:

$$\text{while } (t > 0 \text{ and } b_{s+1} \neq b_{t+1})\ t = f(t);$$

Our aim is to show that the line will terminate and upon termination we will have that

$$\big(b_{s+1} \neq b_{t+1} \text{ and } F(s+1) = t = 0\big)$$

or

$$\big(b_{s+1} = b_{t+1} \text{ and } F(s+1) = t+1\big).$$

Let $R = (R1 \text{ or } R2)$ stand for this disjunction, respectively.

Termination is easy to see: since $f(t) < t$, we will eventually get $t = 0$ which will ensure termination.

Let $Q = (Q1 \text{ and } Q2)$ for

- $Q1$: $F(s+1) \leq t+1$
- $Q2$: $b_1 b_2 \dots b_t$ is a proper prefix and a suffix of $b_1 b_2 \dots b_s$.

Note that upon initialisation we have $t = f(s) = F(s)$ from $P$, and that in all cases

$$F(i+1) \leq F(i) + 1,$$

hence $Q1$ must hold. Since $t = F(s)$ we also get that $b_1 \dots b_t$ is a proper prefix and a suffix of $b_1 \dots b_s$, so $Q$ is established.

Now assume $Q$. When $t = f(t)$ is executed, we must initially have $t > 0$ and $b_{s+1} \neq b_{t+1}$. Since from $Q2$ we know $b_1 \dots b_t$ is a proper prefix and a suffix of $b_1 \dots b_s$, the fact that $b_{s+1} \neq b_{t+1}$ tells us that $F(s+1)$ is strictly less than $t+1$, indeed that

$$F(s+1) \leq f(t) + 1$$

because $t > 0$. $Q$ will therefore remain invariant under the assignment, because $b_1 \dots b_{f(t)}$ will be a proper prefix and suffix of $b_1 \dots b_s$ since it is such with respect to $b_1 \dots b_t$.

Since $Q$ is invariant, when the loop terminates we will have $Q$ and

$$(t = 0) \text{ or } (b_{s+1} = b_{t+1}).$$

If $t = 0$, then $Q1$ implies $F(s+1) \leq 1$. If $b_{s+1} \neq b_{t+1}$ then evidently $F(s+1) = 0$, so $R1$ holds. If $b_{s+1} = b_{t+1}$ then clearly $F(s+1) = 1 = t+1$ since $t = 0$. Thus $R2$ holds. Hence we have $R$ established.

On the other hand, if $b_{s+1} = b_{t+1}$, since from $Q2$ we know $b_1 \dots b_t$ is a proper prefix and a suffix of $b_1 \dots b_s$, it follows that $b_1 \dots b_t b_{t+1}$ sustains the same relation to $b_1 \dots b_s b_{s+1}$. But then, by definition, we must have

$$t + 1 \leq F(s + 1),$$

since $F(s + 1)$ is the *longest* proper prefix and suffix of $b_1 \dots b_s b_{s+1}$. This last inequality combines with $Q1$ to establish $R2$, which implies $R$.