DES Exercise

Aaron Blumenfeld

Show that if the DES key K encrypts P to C, then $\overline{K}$ encrypts $\overline{P}$ to $\overline{C}$.

Proof. First observe that since any K_i is obtained from K by a permutation, shifts, and extraction of bits, if K gives us the subkeys K_i, then $\overline{K}$ gives us the subkeys $\overline{K_i}$, so assume for notational convenience that K is one of the subkeys.

Now the first step is the initial permutation. It's fairly evident that $\text{perm}(\overline{P}) = \overline{\text{perm}(P)}$. The next step is the 16 rounds of DES with the equations

$$L_i = R_{i-1} \text{ and } R_i = L_{i-1} \oplus f(R_{i-1}, K_i).$$

We will see that for one round $R(P)$, $R(\overline{P}) = \overline{C}$ when $R(P) = C$. Then the result follows for 16 rounds. Finally, we switch left and right halves and apply perm^{-1}, which clearly also preserves complementation.

Now for one round, write $P = P_0 P_1, C = C_0 C_1$. We know $C_0 = P_1$ and $C_1 = P_0 \oplus f(P_1, K)$. We want to show that $\overline{P_0 P_1} \mapsto \overline{C_0 C_1}$. We know that $\overline{P_1} = \overline{C_0}$, so it suffices to show that $\overline{P_0} \oplus f(\overline{P_1}, \overline{K}) = \overline{C_1}$.

Since $C_1 = P_0 \oplus f(P_1, K)$, we have $\overline{C_1} = \overline{P_0 \oplus f(P_1, K)} = \overline{P_0} \oplus f(P_1, K)$, so we show $f(\overline{P_1}, \overline{K}) = f(P_1, K)$.

Now f first expands P_1, then XORs $E(P_1) \oplus K$, then the S-box stuff. Expanding bits clearly preserves complementing, in other words, $E(\overline{P_1}) = \overline{E(P_1)}$, and $E(P_1) \oplus K = \overline{E(P_1)} \oplus \overline{K}$. From this equality, the output of the S-boxes must be the same, and the result follows. $\square$

Remark: We used the facts that $\overline{S} = S + 1$, and $1 + 1 = 0$, where 1 and 0 denote the strings of all 1s and all 0s, respectively. These also imply that $\overline{S + T} = S + T + 1 = \overline{S} + T$, and that $\overline{S} + \overline{T} = S + 1 + T + 1 = S + T$.