In class we've described the power set construction for implementing any NFA (without ϵ-transitions) as a DFA. We did not prove that the construction works as advertised. Our textbook says, "The construction of M obviously works correctly."

For students who want more rigor, I now offer a proof. In my opinion, the proof is relatively scant on educational value, for its length (even though I omit two sub-proofs). Understanding the steps of the proof is about as difficult as understanding the construction in the first place.

For these reasons, I often don't present detailed proofs about the simple constructions early in this course. Later in the course we will do more intense constructions (some taking multiple days of class) that will be argued in more detail.

Anyway, here's the proof.

Let $N = (Q_N, \Sigma, q_{0N}, F_N, \delta_N)$ be an NFA without ϵ-transitions. Define a DFA $M = (Q_M, \Sigma, q_{0M}, F_M, \delta_M)$ by

$$\begin{aligned} Q_M &= \wp(Q_N), \\ q_{0M} &= \{q_{0N}\}, \\ F_M &= \{R \subseteq Q_N : R \cap F_N \neq \emptyset\}, \\ \delta_M(R, a) &= \bigcup_{r \in R} \delta_N(r, a). \end{aligned}$$

Let $y_1 \cdots y_m \in \Sigma^*$ be an input string. I will argue that the following statements are logically equivalent:

1. The DFA M accepts $y_1 \cdots y_m$.
2. There exist $q_0, q_1, \ldots, q_m \in Q_M$ such that $q_0 = q_{0M}$, $q_m \in F_M$, and $q_{i+1} = \delta_M(q_i, y_{i+1})$ for $i = 0, \ldots, m-1$.
3. There exist $q_0, q_1, \ldots, q_m \subseteq Q_N$ such that $q_0 = \{q_{0N}\}$, $q_m \cap F_N \neq \emptyset$, and
$$q_{i+1} = \bigcup_{r \in q_i} \delta_N(r, y_{i+1}).$$
4. There exist $s_0, s_1, \ldots, s_m \in Q_N$ such that $s_0 = q_{0N}$, $s_m \in F_N$, and $s_{i+1} \in \delta_N(s_i, y_{i+1})$.
5. The NFA N accepts $y_1 \cdots y_m$.

Conditions 1 and 2 are equivalent, because Condition 2 is simply the formal statement of what it means for a DFA to accept a string $y_1 \cdots y_m$ (p. 40). Conditions 2 and 3 are equivalent by the definition of the DFA M. Conditions 4 and 5 are equivalent by the definition of acceptance of a string by an NFA (p. 54). It remains to show that Conditions 3 and 4 are equivalent; then we can conclude that M and N accept exactly the same strings.

Suppose that Condition 3 is satisfied. Choose $s_m \in q_m \cap F_N$ arbitrarily; such a choice is possible because $q_m \cap F_N$ is non-empty. Then

$$s_m \in q_m = \bigcup_{r \in q_{m-1}} \delta_N(r, y_m).$$

By the definition of union, there is at least one $r \in q_{m-1}$ such that $s_m \in \delta_N(r, y_m)$. Let s_{m-1} be that r. Then

$$s_{m-1} \in q_{m-1} = \bigcup_{r \in q_{m-2}} \delta_N(r, y_{m-1}).$$

By the same reasoning, we obtain an $s_{m-2} \in q_{m-2}$ such that $s_{m-1} \in \delta_N(s_{m-2}, y_{m-1})$. Repeating this argument, we obtain $s_m, s_{m-1}, s_{m-2}, s_{m-3}, \ldots, s_0 = q_{0N}$ that satisfy Condition 4. [By "repeating this argument" I mean that a proof by induction could be performed. Fill in that gap if you like.]

Conversely, suppose that Condition 4 is satisfied. Define $q_0 = \{q_{0N}\}$, and then

$$q_{i+1} = \bigcup_{r \in q_i} \delta_N(r, y_{i+1})$$

for $i = 0, \ldots, m-1$. Then $s_i \in q_i$ for $i = 0, \ldots, m$. [These statements requires another proof by induction.] Thus $q_m \cap F_N$ contains s_m and is non-empty. All of Condition 3 is satisfied.