L11 Problem Set 4

Ramana Kumar (rk436)

December 15, 2010

1 Uniqueness of Dijkstra's local optimum

Fix the adjacency matrix $\mathbf{A}$, the vertex set V, and the source vertex i. A run of Dijkstra's algorithm deals with three variables, q, $\mathbf{R}$, and S. The series of values $q_2, \ldots, q_{|V|}$ serves to characterize runs, since the variables $\mathbf{R}_k$ and S_k at any iteration $k > 1$ are defined in terms of q_k, $\mathbf{R}_{k-1}$, and S_{k-1}, and $\mathbf{R}_1$ and S_1 are always initialized the same way. In particular $S_1 = \{i\}$, $S_k = \{q_k\} \cup S_{k-1}$ for $1 < k \leq |V|$, $\mathbf{R}_1(i,i) = \bar{1}$, $\mathbf{R}_1(i,j) = \mathbf{A}(i,j)$ for $j \in V - \{i\}$, $\mathbf{R}_k(i,j) = \mathbf{R}_{k-1}(i,j)$ for $1 < k \leq |V|$ and $j \in S_k$[1], and $\mathbf{R}_k(i,j) = \mathbf{R}_{k-1}(i,j) \oplus (\mathbf{R}_{k-1}(i,q_k) \otimes \mathbf{A}(q_k,j))$ for $1 < k \leq |V|$ and $j \in V - S_k$. Thus we may specify a partial run of the algorithm of k iterations by giving values $q_1, q_2, \ldots, q_k$, subject to the condition that these values could have been chosen. That condition is summarized as $q_1 = i$ and $\mathbf{R}_{k-1}(i,q_k) = \min_{j \in V - S_{k-1}}(\{\mathbf{R}_{k-1}(i,j)\})$ for $1 < k \leq |V|$.

The proof that follows is very technical. In this paragraph, we provide a high-level sketch. The first main lemma is that whenever the algorithm has a choice of two vertexes, a run that chooses the first then the second agrees after two iterations with a run that chooses the second then the first (Lemma 4). This result is extended to choices of multiple vertexes: any run that chooses them in some permutation agrees at the end of the permutation with a run that chooses them in some other permutation (Corollary 2). Finally, we show that any run eventually agrees with a run that chooses vertexes that were shown to be minimal earliest (Lemma 5). This ensures we have complete permutations to work with: otherwise, some vertex that gains minimal weight because of some of the original choices might infiltrate a permutation of those original choices and prevent us from using Corollary 2.

Lemma 1.
$\forall kvw.\ 1 \leq k \leq |V| \wedge v \in S_k \wedge w \in V - S_k \implies \mathbf{R}_k(i,v) \leq \mathbf{R}_k(i,w)$

(Weights of vertexes in S are no greater than of vertexes outside S.)

Proof. This is Observation 2 from lectures 13 and 14. □

Lemma 2.
$\forall kj.\ 1 \leq k < |V| \wedge j \in V \implies \mathbf{R}_k(i,j) \geq \mathbf{R}_{k+1}(i,j)$

(The sequence of weights for a vertex is non-increasing.)

[1] This is Observation 1 from lectures 13 and 14.

Proof. If $j \in S_{k+1}$, then $\mathbf{R}_{k+1}(i,j) = \mathbf{R}_k(i,j)$, which means $\mathbf{R}_k(i,j) \geq \mathbf{R}_{k+1}(i,j)$ since $\oplus$ is idempotent. Otherwise, if $j \in V - S_{k+1}$,

$$
\begin{aligned}
&\mathbf{R}_k(i,j) \oplus \mathbf{R}_{k+1}(i,j) \\
&= \mathbf{R}_k(i,j) \oplus (\mathbf{R}_k(i,j) \oplus (\mathbf{R}_k(i,q_{k+1}) \otimes \mathbf{A}(q_{k+1},j))) \\
&= (\mathbf{R}_k(i,j) \oplus \mathbf{R}_k(i,j)) \oplus (\mathbf{R}_k(i,q_{k+1}) \otimes \mathbf{A}(q_{k+1},j)) && \oplus \text{ associative} \\
&= \mathbf{R}_k(i,j) \oplus (\mathbf{R}_k(i,q_{k+1}) \otimes \mathbf{A}(q_{k+1},j)) && \oplus \text{ idempotent} \\
&= \mathbf{R}_{k+1}(i,j)
\end{aligned}
$$

□

Corollary 1.
$\forall nkv.\ v \in V \wedge 1 \leq k < k+n \leq |V| \wedge \mathbf{R}_k(i,v) = \mathbf{R}_k(i,q_{k+1}) \implies \mathbf{R}_{k+n}(i,v) = \mathbf{R}_k(i,v)$

(The weight of a minimal-weight vertex does not change.)

Proof. By induction on n. For the base case we are assuming $k < k+0$, which is false, so the result is immediate. For the inductive case we must show $\mathbf{R}_{k+n+1}(i,v) = \mathbf{R}_k(i,v)$, where $v \in V$, $1 \leq k < k+n+1 \leq |V|$, and $\mathbf{R}_k(i,v) = \mathbf{R}_k(i,q_{k+1})$. The inductive hypothesis is $\mathbf{R}_{h+n}(i,w) = \mathbf{R}_h(i,w)$ whenever $w \in V$, $\mathbf{R}_h(i,w) = \mathbf{R}_h(i,q_{h+1})$, and $1 \leq h < h+n \leq |V|$.

Taking $h = k$ and $w = v$ we obtain $\mathbf{R}_{k+n}(i,v) = \mathbf{R}_k(i,v)$. If $v \in S_{k+n+1}$ then $\mathbf{R}_{k+n+1}(i,v) = \mathbf{R}_{k+n}(i,v)$, and the result follows. Otherwise, if $v \in V - S_{k+n+1}$, then since $q_{k+1} \in S_{k+n+1}$ we have $\mathbf{R}_{k+n+1}(i,q_{k+1}) \leq \mathbf{R}_{k+n+1}(i,v)$ by Lemma 1, and thus $\mathbf{R}_k(i,v) = \mathbf{R}_k(i,q_{k+1}) = \mathbf{R}_{k+n+1}(i,q_{k+1}) \leq \mathbf{R}_{k+n+1}(i,v)$. Now by Lemma 2 we have $\mathbf{R}_{k+n+1}(i,v) \leq \mathbf{R}_{k+n}(i,v) = \mathbf{R}_k(i,v)$. By antisymmetry it follows that $\mathbf{R}_{k+1}(i,v) = \mathbf{R}_k(i,v)$. □

Lemma 3.
Let $q_1, \ldots, q_{|V|}$ be a run, and let $q'_1, \ldots, q'_k$ be a partial run. If $S'_k = S_k$ and $\mathbf{R}'_k(i,j) = \mathbf{R}_k(i,j)$ for all $j \in V$, then it is possible to extend the partial run q' so that $S'_{k+n} = S_{k+n}$ and $\mathbf{R}'_{k+n}(i,j) = \mathbf{R}_{k+n}(i,j)$ for all $j \in V$.

(If a run agrees with another at some iteration, it can be forced to agree on all later iterations.)

Proof. By induction on n. For the base case, we must show $S'_k = S_k$ and $\mathbf{R}'_k(i,j) = \mathbf{R}_k(i,j)$ for all $j \in V$, but this is one of our assumptions. For the inductive case, we must show q' can be extended so that $S'_{k+n+1} = S_{k+n+1}$ and $\mathbf{R}'_{k+n+1}(i,j) = \mathbf{R}_{k+n+1}(i,j)$ for all $j \in V$. The inductive hypothesis is that q' can be extended so that $S'_{k+n} = S_{k+n}$ and $\mathbf{R}'_{k+n}(i,j) = \mathbf{R}_{k+n}(i,j)$ for all $j \in V$. Take the extension provided by the inductive hypothesis, and add $q'_{k+n+1} = q_{k+n+1}$. Then $S'_{k+n+1} = S'_{k+n} \cup \{q_{n+1}\} = S_{k+n} \cup \{q_{n+1}\} = S_{k+n+1}$, and $\mathbf{R}'_{k+n+1}(i,j) = \mathbf{R}'_{k+n}(i,j) = \mathbf{R}_{k+n}(i,j)$ for $j \in S_{k+n+1}$, and $\mathbf{R}'_{k+n+1}(i,j) = \mathbf{R}'_{k+n}(i,j) \oplus (\mathbf{R}'_{k+n}(i,q'_{k+n+1}) \otimes \mathbf{A}(q'_{k+n+1},j)) = \mathbf{R}_{k+n}(i,j) \oplus (\mathbf{R}_{k+n}(i,q_{k+n+1}) \otimes \mathbf{A}(q_{k+n+1},j)) = \mathbf{R}_{k+n+1}(i,j)$ for $j \in V - S_{k+n+1}$. □

Lemma 4.
Let $q_1, \ldots, q_k, q_{k+1}$ be a partial run with $1 < k < |V|$. Suppose $\mathbf{R}_{k-1}(i,q_k) = \mathbf{R}_{k-1}(i,q_{k+1})$. Let q' be a partial run satisfying $q'_k = q_{k+1}$, $q'_{k+1} = q_k$, $S'_{k-1} = S_{k-1}$, and $\mathbf{R}'_{k-1}(i,j) = \mathbf{R}_{k-1}(i,j)$ for all $j \in V$. Then $S'_{k+1} = S_{k+1}$ and $\mathbf{R}'_{k+1}(i,j) = \mathbf{R}_{k+1}(i,j)$ for all $j \in V$.

(The order in which two equal-weighted vertexes are chosen for adjacent iterations does not matter.)

Proof. We first show $S'_{k+1} = S_{k+1}$.

$$\begin{aligned}
S'_{k+1} &= \{q'_{k+1}\} \cup S'_k \\
&= \{q_k\} \cup \{q'_k\} \cup S'_{k-1} \\
&= \{q_k\} \cup \{q_{k+1}\} \cup S_{k-1} \\
&= \{q_{k+1}\} \cup \{q_k\} \cup S_{k-1} \\
&= S_{k+1}
\end{aligned}$$

We now show $\mathbf{R}'_{k+1}(i,j) = \mathbf{R}_{k+1}(i,j)$ for all $j \in V$, by cases on which part of V contains j. If $j \in S_{k-1}$, then $j \in S_k$ and $j \in S_{k+1}$ since $S_{k-1} \subseteq S_k \subseteq S_{k+1}$, and also $j \in S'_{k-1} \subseteq S'_k \subseteq S'_{k+1}$, since $S'_{k-1} = S_{k-1}$. Therefore $\mathbf{R}'_{k+1}(i,j) = \mathbf{R}'_k(i,j) = \mathbf{R}'_{k-1}(i,j) = \mathbf{R}_{k-1}(i,j) = \mathbf{R}_k(i,j) = \mathbf{R}_{k+1}(i,j)$, as required, since $\mathbf{R}'_{k-1}(i,j) = \mathbf{R}_{k-1}(i,j)$ and $\mathbf{R}$ stays fixed on vertexes in S.

Otherwise, if $j \in V - S_{k-1}$, either $j = q_k$ or $j = q_{k+1}$ or $j \in V - S_{k+1}$. We address the first two cases first. For the case $j = q_k$, we reason

$$\begin{aligned}
\mathbf{R}'_{k+1}(i,q_k) &= \mathbf{R}'_{k+1}(i,q'_{k+1}) \\
&= \mathbf{R}'_k(i,q'_{k+1}) && \text{since } q'_{k+1} \in S'_{k+1} \\
&= \mathbf{R}'_{k-1}(i,q'_{k+1}) \oplus (\mathbf{R}'_{k-1}(i,q'_k) \otimes \mathbf{A}(q'_k,q'_{k+1})) && \text{since } q'_{k+1} \in V - S'_k \\
&= \mathbf{R}_{k-1}(i,q_k) \oplus (\mathbf{R}_{k-1}(i,q_{k+1}) \otimes \mathbf{A}(q_{k+1},q_k)) \\
&= \mathbf{R}_{k-1}(i,q_k) \oplus (\mathbf{R}_{k-1}(i,q_k) \otimes \mathbf{A}(q_{k+1},q_k)) && \text{since } \mathbf{R}_{k-1}(i,q_k) = \mathbf{R}_{k-1}(i,q_{k+1}) \\
&= \mathbf{R}_{k-1}(i,q_k) && \text{by RINF} \\
&= \mathbf{R}_k(i,q_k) && \text{since } q_k \in S_k \\
&= \mathbf{R}_{k+1}(i,q_k) && \text{since } q_k \in S_{k+1}
\end{aligned}$$

Symmetrically, for $j = q_{k+1}$, we reason

$$\begin{aligned}
\mathbf{R}'_{k+1}(i,q_{k+1}) &= \mathbf{R}'_{k+1}(i,q'_k) \\
&= \mathbf{R}'_k(i,q'_k) && \text{since } q'_k \in S'_{k+1} \\
&= \mathbf{R}'_{k-1}(i,q'_k) && \text{since } q'_k \in S'_k \\
&= \mathbf{R}'_{k-1}(i,q'_k) \oplus (\mathbf{R}'_{k-1}(i,q'_k) \otimes \mathbf{A}(q'_{k+1},q'_k)) && \text{by RINF} \\
&= \mathbf{R}_{k-1}(i,q_{k+1}) \oplus (\mathbf{R}_{k-1}(i,q_{k+1}) \otimes \mathbf{A}(q_k,q_{k+1})) \\
&= \mathbf{R}_{k-1}(i,q_{k+1}) \oplus (\mathbf{R}_{k-1}(i,q_k) \otimes \mathbf{A}(q_k,q_{k+1})) && \text{since } \mathbf{R}_{k-1}(i,q_k) = \mathbf{R}_{k-1}(i,q_{k+1}) \\
&= \mathbf{R}_k(i,q_{k+1}) && \text{since } q_{k+1} \in V - S_k \\
&= \mathbf{R}_{k+1}(i,q_{k+1}) && \text{since } q_{k+1} \in S_{k+1}
\end{aligned}$$

Finally, for $j \in V - S_{k+1}$, we first observe $j \in V - S'_k$ since $S'_k \subseteq S'_{k+1} = S_{k+1}$. Similarly $j \in V - S_k$. In part of the derivation above, we showed $\mathbf{R}'_{k-1}(i,q'_k) = \mathbf{R}_k(i,q_{k+1})$, and it follows that $\mathbf{R}_k(i, q_{k+1}) = \mathbf{R}_{k-1}(i, q_{k+1})$. Then, remembering $\mathbf{R}_{k-1}(i, q_k) = \mathbf{R}_{k-1}(i, q_{k+1})$,

$$
\begin{aligned}
&\mathbf{R}'_{k+1}(i,j) \\
&= \mathbf{R}'_k(i,j) \oplus (\mathbf{R}'_k(i,q'_{k+1}) \otimes \mathbf{A}(q'_{k+1},j)) && \text{since } j \in V - S'_{k+1} \\
&= \mathbf{R}'_k(i,j) \oplus ((\mathbf{R}'_{k-1}(i,q'_{k+1}) \oplus (\mathbf{R}'_{k-1}(i,q'_k) \otimes \mathbf{A}(q'_k,q'_{k+1}))) \otimes \mathbf{A}(q'_{k+1},j)) && \text{since } q'_{k+1} \in V - S'_k \\
&= \mathbf{R}'_k(i,j) \oplus ((\mathbf{R}_{k-1}(i,q_k) \oplus (\mathbf{R}_{k-1}(i,q_{k+1}) \otimes \mathbf{A}(q'_k,q'_{k+1}))) \otimes \mathbf{A}(q'_{k+1},j)) \\
&= \mathbf{R}'_k(i,j) \oplus ((\mathbf{R}_{k-1}(i,q_k) \oplus (\mathbf{R}_{k-1}(i,q_k) \otimes \mathbf{A}(q'_k,q'_{k+1}))) \otimes \mathbf{A}(q'_{k+1},j)) \\
&= \mathbf{R}'_k(i,j) \oplus (\mathbf{R}_{k-1}(i,q_k) \otimes \mathbf{A}(q'_{k+1},j)) && \text{by RINF} \\
&= (\mathbf{R}'_{k-1}(i,j) \oplus (\mathbf{R}'_{k-1}(i,q'_k) \otimes \mathbf{A}(q'_k,j))) \oplus (\mathbf{R}_{k-1}(i,q_k) \otimes \mathbf{A}(q'_{k+1},j)) && \text{since } j \in V - S'_k \\
&= (\mathbf{R}_{k-1}(i,j) \oplus (\mathbf{R}_{k-1}(i,q_{k+1}) \otimes \mathbf{A}(q_{k+1},j))) \oplus (\mathbf{R}_{k-1}(i,q_k) \otimes \mathbf{A}(q_k,j)) \\
&= \mathbf{R}_{k-1}(i,j) \oplus (\mathbf{R}_{k-1}(i,q_k) \otimes \mathbf{A}(q_k,j)) \oplus (\mathbf{R}_{k-1}(i,q_{k+1}) \otimes \mathbf{A}(q_{k+1},j)) && \text{since } \oplus \text{ comm., assoc.} \\
&= \mathbf{R}_k(i,j) \oplus (\mathbf{R}_{k-1}(i,q_{k+1}) \otimes \mathbf{A}(q_{k+1},j)) && \text{since } j \in V - S_k \\
&= \mathbf{R}_k(i,j) \oplus (\mathbf{R}_k(i,q_{k+1}) \otimes \mathbf{A}(q_{k+1},j)) \\
&= \mathbf{R}_{k+1}(i,j) && \text{since } j \in V - S_{k+1}
\end{aligned}
$$

□

Corollary 2.

Let $q_1, \ldots, q_k, q_{k+1}, \ldots, q_{k+n}$ be a partial run with $1 \leq k \leq k+n \leq |V|$. Suppose $\mathbf{R}_k(i, q_{k+1}) = \mathbf{R}_k(i, q_{k+2}) = \cdots = \mathbf{R}_k(i, q_{k+n})$. Let $q'_1, \ldots, q'_k, q'_{k+1}, \ldots, q'_{k+n}$ be a partial run satisfying $S'_k = S_k$, $\mathbf{R}'_k(i,j) = \mathbf{R}_k(i,j)$ for all $j \in V$, and such that $[q'_{k+1}, \ldots, q'_{k+n}]$ is a permutation of $[q_{k+1}, \ldots, q_{k+n}]$. Then $S'_{k+n} = S_{k+n}$ and $\mathbf{R}'_{k+n}(i,j) = \mathbf{R}_{k+n}(i,j)$ for all $j \in V$.

(The order in which any sequence of equal-weighted vertexes are chosen for adjacent iterations does not matter.)

Proof. The basic idea is to use Lemma 4 to move the vertex that is first in q closer to the beginning of the permutation in q'. When it reaches the beginning, we jump forward one iteration and are are left with a smaller permutation. There are two inductions, one nested in the inductive case of the other.

First, by induction on n. For the base case, we must show $S'_k = S_k$ and $\mathbf{R}'_k(i,j) = \mathbf{R}_k(i,j)$ for all $j \in V$. But this is an assumption.

For the inductive case, we must show $S'_{k+n+1} = S_{k+n+1}$ and $\mathbf{R}'_{k+n+1}(i,j) = \mathbf{R}_{k+n+1}(i,j)$ for all $j \in V$, given two runs $q_1, \ldots, q_{k+n+1}$ and $q'_1, \ldots, q'_{k+n+1}$ satisfying $1 \leq k \leq k+n+1 \leq |V|$, $\mathbf{R}_k(i, q_{k+1}) = \cdots = \mathbf{R}_k(i, q_{k+n+1})$, $S'_k = S_k$, $\mathbf{R}'_k(i,j) = \mathbf{R}_k(i,j)$ for all $j \in V$, and $[q'_{k+1}, \ldots, q'_{k+n+1}]$ a permutation of $[q_{k+1}, \ldots, q_{k+n+1}]$. The inductive hypothesis is that $S'_{h+n} = S_{h+n}$ and $\mathbf{R}'_{h+n}(i,j) = \mathbf{R}_{h+n}(i,j)$ for all $j \in V$ for any two runs $q_1, \ldots, q_{h+n}$ and $q'_1, \ldots, q'_{h+n}$ satisfying $1 \leq h \leq h+n \leq |V|$, $\mathbf{R}_h(i, q_{h+1}) = \cdots = \mathbf{R}_h(i, q_{h+n})$, $S'_h = S_h$, $\mathbf{R}'_h(i,j) = \mathbf{R}_h(i,j)$ for all $j \in V$, and $[q'_{h+1}, \ldots, q'_{h+n}]$ a permutation of $[q_{h+1}, \ldots, q_{h+n}]$. Since $[q'_{k+1}, \ldots, q'_{k+n+1}]$ and $[q_{k+1}, \ldots, q_{k+n+1}]$ are permutations, the vertex q_{k+1} is equal to q'_{k+1+d} for some $0 \leq d \leq n$. We proceed by induction on d.

For the base case, we must show $S'_{k+n+1} = S_{k+n+1}$ and $\mathbf{R}'_{k+n+1}(i,j) = \mathbf{R}_{k+n+1}(i,j)$ for all $j \in V$ under the assumption $q'_{k+1} = q_{k+1}$. In this case, take $h = k+1$ so that $q_1, \ldots, q_{h+n} = q_1, \ldots, q_{k+n+1}$ and $q'_1, \ldots, q'_{h+n} = q'_1, \ldots, q'_{k+n+1}$. Observe that $1 \leq h \leq h+n \leq |V|$ because $1 \leq k \leq k+1 \leq k+n+1 \leq |V|$. Also, in the proof of Lemma 3 we saw that if two partial runs agree on S and $\mathbf{R}$ at some iteration $k+n$, and if they agree on the next chosen vertex q_{k+n+1}, then they agree on S and $\mathbf{R}$ at iteration $k+n+1$. In our case take $n = 0$ and since we have $S'_k = S_k$, $\mathbf{R}'_k(i,j) = \mathbf{R}_k(i,j)$ for all $j \in V$, and $q'_{k+1} = q_{k+1}$, then we get $S'_h = S_h$ and $\mathbf{R}_{h'}(i,j) =$

$\mathbf{R}_h(i,j)$ for all $j \in V$, since $h = k+1$. Additionally, $[q'_{h+1},\ldots,q_{h+n}] = [q'_{k+2},\ldots,q'_{k+n+1}]$ is a permutation of $[q_{h+1},\ldots,q_{h+n}] = [q_{k+2},\ldots,q_{k+n+1}]$ because we assume $[q'_{k+1},\ldots,q'_{k+n+1}]$ is a permutation of $[q_{k+1},\ldots,q_{k+n+1}]$ and $q_{k+1} = q'_{k+1}$: removing equal elements from the front of two permutations leaves two smaller permutations. To use the inductive hypothesis for the induction on n, it remains to show that $\mathbf{R}_h(i,q_{h+1}) = \cdots = \mathbf{R}_h(i,q_{h+n})$, that is $\mathbf{R}_{k+1}(i,q_{k+2}) = \cdots = \mathbf{R}_{k+1}(i,q_{k+n+1})$. We are assuming $\mathbf{R}_k(i,q_{k+1}) = \cdots = \mathbf{R}_k(i,q_{k+n+1})$, that is $\mathbf{R}_k(i,q_{k+x}) = \mathbf{R}_k(i,q_{k+1})$ for $1 \le x \le n+1$. By Corollary 1 it follows that $\mathbf{R}_{k+1}(i,q_{k+x}) = \mathbf{R}_k(i,q_{k+x}) = \mathbf{R}_k(i,q_{k+1})$ for $1 \le x \le n+1$. Thus in particular $\mathbf{R}_{k+1}(i,q_{k+2}) = \cdots = \mathbf{R}_{k+1}(i,q_{k+n+1}) = \mathbf{R}_k(i,q_{k+1})$. So we can use the inductive hypothesis for the induction on n, which gives us $S'_{h+n} = S_{h+n}$ and $\mathbf{R}'_{h+n}(i,j) = \mathbf{R}_{h+n}(i,j)$ for all $j \in V$, which is our desired result since $h = k+1$.

For the inductive case, we must show $S'_{k+n+1} = S_{k+n+1}$ and $\mathbf{R}'_{k+n+1}(i,j) = \mathbf{R}_{k+n+1}(i,j)$ for all $j \in V$ under the assumption $q_{k+1} = q'_{k+1+d+1}$ where $0 \le d{+}1 \le n$. The inductive hypothesis is that $S''_{k+n+1} = S_{k+n+1}$ and $\mathbf{R}''_{k+n+1}(i,j) = \mathbf{R}_{k+n+1}(i,j)$ for all $j \in V$ whenever $q_{k+1} = q''_{k+1+d}$. Consider the partial run q'' given by $q''_x = q'_x$ for $1 \le x \le k+d$, and $q''_{k+d+1} = q'_{k+d+2}$ and $q''_{k+d+2} = q'_{k+d+1}$. This is a possible partial run because we assume q' is possible, and q'' only differs on equal-weighted vertexes: we are assuming $\mathbf{R}_k(i,q_{k+1}) = \cdots = \mathbf{R}_k(i,q_{k+d+2})$ and q' has a permutation of the values of q in this range so they are also all equal, and Corollary 1 ensures they will stay equal, so $\mathbf{R}'_{k+d}(i,q_{k+d+1}) = \mathbf{R}'_{k+d}(i,q_{k+d+2})$. Therefore we may apply Lemma 4 to q' and q'' to obtain $S''_{k+d+2} = S'_{k+d+2}$ and $\mathbf{R}''_{k+d+2}(i,j) = \mathbf{R}'_{k+d+2}(i,j)$ for all $j \in V$. By Lemma 3, and since $k+d+2 \le k+n+1$, we obtain $S''_{k+n+1} = S'_{k+n+1}$ and $\mathbf{R}''_{k+n+1}(i,j) = \mathbf{R}'_{k+n+1}(i,j)$ for all $j \in V$. Now $q_{k+1} = q'_{k+d+2} = q''_{k+d+1}$, so we can apply the inductive hypothesis for the induction on d to obtain $S''_{k+n+1} = S_{k+n+1}$ and $\mathbf{R}''_{k+n+1}(i,j) = \mathbf{R}_{k+n+1}(i,j)$ for all $j \in V$. It follows that $S'_{k+n+1} = S_{k+n+1}$ and $\mathbf{R}'_{k+n+1}(i,j) = \mathbf{R}_{k+n+1}(i,j)$ for all $j \in V$ as required. □

We will now fix a particular run and then show that any other run is eventually equivalent to it. Pick an arbitrary ordering l of the vertexes in V, which maps each subset $T \subseteq V$ to a list $l(T)$ of the subset's elements. We define the series q^* alongside a helper variable T. Take $T_1 = \{i\}$, $[q^*_k,\ldots,q^*_{k+|T_k|-1}] = l(T_k)$, and $T_{k+1} = \{v \in V - S^*_k \mid \mathbf{R}^*_k(i,v) = \min_{j \in V - S^*_k}(\{\mathbf{R}^*_k(i,v)\})\}$, for $1 \le k+1 \le |V|$. In other words, T_k is the set of choices for q^*_k, and q^* exhausts this set before picking any other vertexes. Equivalently, q^* always picks a vertex that was shown to have minimal weight earliest. That this is a possible run is a consequence of Lemma 1 and Corollary 1: the minimal-weight vertexes from iteration k will continue to have minimal weights until they are picked.

Lemma 5.

Let $q_1,\ldots,q_{|V|}$ be a run. Suppose $S_k = S^*_k$ and $\mathbf{R}_k(i,j) = \mathbf{R}^*_k(i,j)$ for all $j \in V$, for some $1 \le k \le |V|$. Then $S_{|V|} = S^*_{|V|}$, and $\mathbf{R}_{|V|}(i,j) = \mathbf{R}^*_{|V|}(i,j)$ for all $j \in V$.

(Any run that agrees somewhere with q^* agrees finally with q^*.)

Proof. The basic idea is to use Lemma 4 to move any vertexes in q whose minimality was found "late" to a later iteration, until the initial segment of choices contains all those whose minimality was found earliest. Then we use Corollary 2 because disagreement with q^* is only up to a permutation. There are two inductions, a complete induction on how close we are to exhausting V, and within that an induction on the number/position of any "late" vertexes. The process to have in mind is of swapping "late" vertexes forward until there are none left, then jumping across the whole permutation, and repeating this until there's nothing left in V.

By complete induction on $|V|-k$. The inductive hypothesis is that for all h such that $k < h \le |V|$, if $S'_h = S^*_h$ and $\mathbf{R}'_h(i,j) = \mathbf{R}^*_h(i,j)$ for all $j \in V$, then $S'_{|V|} = S^*_{|V|}$ and $\mathbf{R}'_{|V|}(i,j) = \mathbf{R}^*_{|V|}(i,j)$ for all $j \in V$.

If $k = |V|$, we are done, so assume $k < |V|$. Let T denote T_{k+1} from now on. We know $\{q^*_{k+1}, \ldots, q^*_{k+|T|}\} = T$, and $\mathbf{R}^*_k(i, q^*_{k+1}) = \cdots = \mathbf{R}^*_k(i, q^*_{k+|T|})$. Let d be the least number satisfying $T \subseteq \{q_{k+1}, \ldots, q_{k+|T|+d}\}$ and $k + |D| \leq k + |T| + d \leq |V|$. Such a number exists since $T \subseteq V - S^*_k = V - S_k$, so certainly $T \subseteq \{q_{k+1}, \ldots, q_{|V|}\}$. Define $D = \{q_{k+1}, \ldots, q_{k+|T|+d}\}$. Whenever $D \neq T$, let m be the greatest number such that $q_{k+m} \in D$ but $q_{k+m} \notin T$.

We will proceed by induction on the lexicographic combination of the measures $|D| - |T|$ and $d + |T| - m$, so we consider a run q' to be less than a run q if either $|D'| - |T| < |D| - |T|$ or both $|D'| - |T| = |D| - |T|$ and $d + |T| - m' < d + |T| - m$. In other words, write $q' \prec q$ if $d' < d$ or $d' = d$ and $m < m'$, then we proceed by well-founded induction on $\prec$. The inductive hypothesis is that whenever $q' \prec q$ and q' satisfies $S'_k = S^*_k$ and $\mathbf{R}'_k(i,j) = \mathbf{R}^*_k(i,j)$ for all $j \in V$, then $S'_{|V|} = S^*_{|V|}$, and $\mathbf{R}'_{|V|}(i,j) = \mathbf{R}^*_{|V|}(i,j)$ for all $j \in V$.

Suppose $|D| = |T|$, that is $\{q_{k+1}, \ldots, q_{k+|T|+d}\} = T$. Then we can apply Corollary 2 to obtain $S_{k+|T|} = S^*_{k+|T|}$ and $\mathbf{R}_{k+|T|}(i,j) = \mathbf{R}^*_{k+|T|}(i,j)$ for all $j \in V$. Since $k + |T| > k$, we can apply the inductive hypothesis for the induction on $|V| - k$ to get $S_{|V|} = S^*_{|V|}$ and $\mathbf{R}_{|V|}(i,j) = \mathbf{R}^*_{|V|}(i,j)$ for all $j \in V$ as required.

Otherwise we have $D \neq T$ and may consider m. Observe that $m \geq 1$ since $q_{k+m} \in D$. Observe also that $q_{k+m+1} \in T$, because otherwise, if $q_{k+m+1} \in D$ then $m+1$ is a greater candidate for m, but if $q_{k+m+1} \notin D$ then $T \subseteq \{q_{k+1}, \ldots, q_{k+m}\}$ and $m - |T|$ is a smaller candidate for d. We can also deduce that $q_{k+1} \in T$, since $\mathbf{R}_k(i, q_{k+1}) = \min_{j \in V - S_k}(\{\mathbf{R}_k(i,j)\}) = \min_{j \in V - S^*_k}(\{\mathbf{R}^*_k(i,j)\}) = \mathbf{R}^*_k(i, q^*_{k+1})$, and this is the criterion for membership in T.

Define a sequence q' by $q'_{k+m} = q_{k+m+1}$, $q'_{k+m+1} = q'_{k+m}$, and $q' = q$ elsewhere. Since q and q' do not differ before $k+m$, we have $S'_{k+m-1} = S_{k+m-1}$ and $\mathbf{R}'_{k+m-1}(i,j) = \mathbf{R}_{k+m-1}(i,j)$ for all $j \in V$. Also, $1 < k + m < |V|$ because $1 \leq k$ and $m \geq 1$, and $k + m \leq k + |T| + d \leq |V|$. Now $\mathbf{R}_{k+m-1}(i, q_{k+m}) = \min_{j \in V - S_{k+m-1}}(\{\mathbf{R}_{k+m-1}(i,j)\}) \leq \mathbf{R}_{k+m-1}(i, q_{k+m+1})$ since $q_{k+m+1} \in V - S_{k+m-1}$. But $\mathbf{R}_{k+m-1}(i, q_{k+m+1}) \leq \mathbf{R}_k(i, q_{k+m+1})$ by Lemma 2 and $\mathbf{R}_k(i, q_{k+m+1}) = \mathbf{R}^*_k(i, q_{k+m+1}) = \mathbf{R}^*_k(i, q_{k+1})$ since $q_{k+1} \in T$. So we have $\mathbf{R}_{k+m-1}(i, q_{k+m+1}) \leq \mathbf{R}^*_k(i, q_{k+1})$, but $\mathbf{R}^*_k(i, q_{k+1}) = \mathbf{R}_{k+m-1}(i, q_{k+1})$ by Corollary 1, and $\mathbf{R}_{k+m-1}(i, q_{k+1}) \leq \mathbf{R}_{k+m-1}(i, q_{k+m})$ by Lemma 1. In summary, $\mathbf{R}_{k+m-1}(i, q_{k+m+1}) \leq \mathbf{R}_{k+m-1}(i, q_{k+m})$, and by antisymmetry, this means $\mathbf{R}_{k+m-1}(i, q_{k+m}) = \mathbf{R}_{k+m-1}(i, q_{k+m+1})$. Thus, q' is a possible run: it differs from q only on equal-weighted vertexes. Furthermore, we can apply Lemma 4 to obtain $S'_{k+m+1} = S_{k+m+1}$ and $\mathbf{R}'_{k+m+1}(i,j) = \mathbf{R}_{k+m+1}(i,j)$ for all $j \in V$. Since q and q' agree on all iterations after $k+m+1$, it follows that $S'_{|V|} = S_{|V|}$ and $\mathbf{R}'_{|V|}(i,j) = \mathbf{R}_{|V|}(i,j)$ for all $j \in V$.

Since q' does not differ from q until iteration $k+m$, and $k < k+m$, we have $S'_k = S_k$ and $\mathbf{R}'_k(i,j) = \mathbf{R}_k(i,j)$ for all $j \in V$. Therefore $S'_k = S^*_k$ and $\mathbf{R}'_k(i,j) = \mathbf{R}^*_k(i,j)$ for all $j \in V$. Furthermore, we have $q' \prec q$: if q_{k+m+1} was the last vertex in T for q then $d' = d - 1$, otherwise $d' = d$ and $m' = m + 1$ since $q'_{k+m+1} = q'_{k+m}$ is the last vertex not in T for q'. Therefore we can apply the inductive hypothesis for the induction on $\prec$ to obtain $S'_{|V|} = S^*_{|V|}$, and $\mathbf{R}'_{|V|}(i,j) = \mathbf{R}^*_{|V|}(i,j)$ for all $j \in V$.

Combining these two results, we get $S_{|V|} = S^*_{|V|}$ and $\mathbf{R}_{|V|}(i,j) = \mathbf{R}^*_{|V|}(i,j)$ for all $j \in V$ as required. □

Theorem. Let q and q' be runs. Then $\mathbf{R}_{|V|}(i,j) = \mathbf{R}'_{|V|}(i,j)$ for all $j \in V$.

(Uniqueness of the output of Dijkstra's algorithm.)

Proof. Note that $S_1 = S'_1 = S^*_1$ and $\mathbf{R}_1(i,j) = \mathbf{R}'_1(i,j) = \mathbf{R}^*_1(i,j)$ for all $j \in V$. Therefore by Lemma 5, both runs agree with q^* at iteration $|V|$. It follows that they both have the same output $\mathbf{R}^*_{|V|}(i,j)$. □

2 If $\mathcal{P}_{\min}$ is a semiring

Any singleton $\{a\}$ is in $\mathcal{P}_{\min}(S, \leq)$, because it is clearly finite and $\min_{\leq}(\{a\}) = \{x \mid x \in \{a\} \wedge \forall b \in \{a\}.\ \neg(b < a)\} = \{a \mid \neg(a < a)\} = \{a\}$ since $a < a$ is always false.

Observe that $\{a\} \hat{\otimes} \{b\} = \min_{\leq}(\{x \otimes y \mid x \in \{a\}, y \in \{b\}\}) = \min_{\leq}(a \otimes b) = \{a \otimes b\}$ for all $a, b \in S$.

Observe that $\{a\} \hat{\oplus} \{b\} = \min_{\leq}(\{a, b\}) = \{x \mid x \in \{a, b\} \wedge \forall y \in \{a, b\}.\ \neg(y < x)\} = \{a \mid \neg(b < a)\} \cup \{b \mid \neg(a < b)\}$, but this may be in general be any subset of $\{a, b\}$.

3 For $\mathcal{P}_{\min}$ to be a semiring

It is sufficient that the order associated with $\oplus$ is a lower semilattice, that is, every finite subset of S has a greatest lower bound. (This is in addition to the assumption that S is an idempotent semiring.)

Under this assumption, we prove $\mathcal{P}_{\min}$ is a semiring as follows. First, note that $\min_{\leq}(A) = \{\wedge(A)\}$ for all finite non-empty subsets of S. So if $A \in \mathcal{P}_{\min}(S, \leq)$, then $A = \min_{\leq}(A) = \{\wedge(A)\}$. For the empty set we have $\min_{\leq}(\emptyset) = \emptyset$; we omit the proofs involving $\emptyset$ for their simplicity.

$(\mathcal{P}_{\min}(S, \leq), \hat{\oplus}, \emptyset)$ a commutative monoid

Associativity

$$\begin{aligned}
& A \hat{\oplus} (B \hat{\oplus} C) \\
& = \min_{\leq}(\{\wedge(A)\} \cup \min_{\leq}(\{\wedge(B)\} \cup \{\wedge(C)\})) \\
& = \{\wedge(\{\wedge(A), \wedge(\{\wedge(B), \wedge(C)\})\})\} \\
& = \{\wedge(\{A, \wedge(\{B, C\})\})\} \\
& = \{\wedge(\{A, B, C\})\} \\
& = \{\wedge(\{\wedge(\{A, B\}), C\})\} \\
& = \{\wedge(\{\wedge(\{\wedge(A), \wedge(B)\}), \wedge(C)\})\} \\
& = \min_{\leq}(\{\min_{\leq}(\{\wedge(A)\} \cup \{\wedge(B)\} \cup \{\wedge(A)\}) \\
& = (A \hat{\oplus} B) \hat{\oplus} C
\end{aligned}$$

Commutativity

$$A \hat{\oplus} B = \min_{\leq}(A \cup B) = \min_{\leq}(B \cup A) = B \hat{\oplus} A$$

Identity

$$A \hat{\oplus} \emptyset = \min_{\leq}(A \cup \emptyset) = \min_{\leq}(A) = A = \min_{\leq}(A) = \min_{\leq}(\emptyset \cup A) = \emptyset \hat{\oplus} A$$

$(\mathcal{P}_{\min}(S, \leq), \hat{\otimes}, \{\bar{1}\})$ a monoid

Associativity

$$
\begin{aligned}
& A \mathbin{\hat{\otimes}} (B \mathbin{\hat{\otimes}} C) \\
& = \min_{\leq}(\{a \otimes x \mid a \in \{\wedge(A)\}, x \in \min_{\leq}(\{b \otimes c \mid b \in \{\wedge(B)\}, c \in \{\wedge(C)\}\})\}) \\
& = \min_{\leq}(\{\wedge(A) \otimes x \mid x \in \{\wedge(\{\wedge(B) \otimes \wedge(C)\})\}\}) \\
& = \min_{\leq}(\{\wedge(A) \otimes \wedge(\{\wedge(B) \otimes \wedge(C)\})\}) \\
& = \min_{\leq}(\{\wedge(A) \otimes \wedge(B) \otimes \wedge(C)\}) \\
& = \min_{\leq}(\{\wedge(\{\wedge(A) \otimes \wedge(B)\}) \otimes \wedge(C)\}) \\
& = \min_{\leq}(\{x \otimes c \mid c \in \{\wedge(C)\}, x \in \min_{\leq}(\{a \otimes b \mid a \in \{\wedge(A)\}, b \in \{\wedge(B)\}\})\}) \\
& (A \mathbin{\hat{\otimes}} B) \mathbin{\hat{\otimes}} C
\end{aligned}
$$

Identity

$$
\begin{aligned}
A \mathbin{\hat{\otimes}} \{\bar{1}\} & = \min_{\leq}(\{a \otimes b \mid a \in A, b \in \{\bar{1}\}\}) \\
& = \min_{\leq}(\{a \otimes \bar{1} \mid a \in A\}) \\
& = \min_{\leq}(\{a \mid a \in A\}) \\
& = \min_{\leq}(A) = A = \min_{\leq}(A) \\
& = \min_{\leq}(\{a \mid a \in A\}) \\
& = \min_{\leq}(\{\bar{1} \otimes a \mid a \in A\}) \\
& = \min_{\leq}(\{b \otimes a \mid b \in \{\bar{1}\}, a \in A\}) \\
& = \{\bar{1}\} \mathbin{\hat{\otimes}} A
\end{aligned}
$$

Annihilator

$A \hat{\otimes} \emptyset = \min_{\leq}(\{a \otimes b \mid a \in A, b \in \emptyset\}) = \min_{\leq}(\emptyset) = \emptyset = \min_{\leq}(\emptyset) = \min_{\leq}(\{b \otimes a \mid b \in \emptyset, a \in A\}) = \emptyset \hat{\otimes} A$

Distributivity

Left

$$
\begin{aligned}
& A \mathbin{\hat{\otimes}} (B \mathbin{\hat{\oplus}} C) \\
& = \min_{\leq}(\{\wedge(A) \otimes \wedge(\{\wedge(B), \wedge(C)\})\}) \\
& = \min_{\leq}(\{\wedge(A) \otimes \wedge(\{B, C\})\}) \\
& = \{\wedge(\{\wedge(A) \otimes \wedge(\{B, C\})\})\} \\
& = \{\wedge(\{\wedge(A) \otimes \wedge(B), \wedge(A) \otimes \wedge(C)\})\} \\
& = \{\wedge(\{\wedge(A) \otimes \wedge(B)\} \cup \{\wedge(A) \otimes \wedge(C)\})\} \\
& = \min_{\leq}(\{\wedge(A) \otimes \wedge(B)\} \cup \{\wedge(A) \otimes \wedge(C)\}) \\
& = \{\wedge(A) \otimes \wedge(B)\} \mathbin{\hat{\oplus}} \{\wedge(A) \otimes \wedge(C)\} \\
& = (A \mathbin{\hat{\otimes}} B) \mathbin{\hat{\oplus}} (A \mathbin{\hat{\otimes}} C)
\end{aligned}
$$

Right

$$
\begin{aligned}
&(A \mathbin{\hat{\oplus}} B) \mathbin{\hat{\otimes}} C \\
&= \min_{\leq}(\{x \otimes \wedge(C) \mid x \in \{\wedge(\{A, B\})\}\}) \\
&= \{\wedge(\{\wedge(\{A, B\}) \otimes \wedge(C)\})\} \\
&= \{\wedge(\{\wedge(A) \otimes \wedge(C), \wedge(B) \otimes \wedge(C)\})\} \\
&= \min_{\leq}(\{\wedge(A) \otimes \wedge(C)\} \cup \{\wedge(B) \otimes \wedge(C)\}) \\
&= \{\wedge(A) \otimes \wedge(C)\} \mathbin{\hat{\oplus}} \{\wedge(B) \otimes \wedge(C)\} \\
&= \{a \otimes c \mid a \in A, c \in C\} \mathbin{\hat{\oplus}} \{b \otimes c \mid b \in B, c \in C\} \\
&= (A \mathbin{\hat{\otimes}} C) \mathbin{\hat{\oplus}} (B \mathbin{\hat{\otimes}} C)
\end{aligned}
$$