DISKRET MATEMATIK

A Proof of Warshall's algorithm

The following note contains a simple lemma which is the key idea behind Warshall's algorithm.

We consider a binary relation R on a set A. We say that a finite list $z_1, \ldots, z_k$ of elements of A *connects* x and y iff

- $k = 0$ and $R\ x\ y$,
- $k \geq 1$ and $R\ x\ z_1,\ R\ z_1\ z_2, \ldots, R\ z_k\ y$.

We will be concerned with the transitive closure R^+ of R which may be defined as the relation $R^+\ x\ y$ which holds iff there exists a finite list of elements connecting x and y.

We introduce the following notation: if I a subset of A and $z \in A$ then I, z is the subset of elements $x \in A$ such that $x \in I$ or $x = z$. Also $R^+_I\ x\ y$ is the relation defined like R^+ but where the elements are required to be in I that is $R^+_I\ x\ y$ holds iff there exists a finite list whose elements are in I connecting x and y.

Lemma: If $R^+_{I,z}\ x\ y$ then

- either $R^+_I\ x\ y$,
- or $R^+_I\ x\ z$ and $R^+_I\ z\ y$.

Proof: The proof is direct by induction on the list $z_1, \ldots, z_k$ connecting x and y.

If $k = 0$ we have $R\ x\ y$ and hence $R^+_I\ x\ y$.

If $z_1, \ldots, z_k, z_{k+1}$ connects x and y then $z_1, \ldots, z_k$ connects x and z_{k+1} and $R\ z_{k+1}\ y$. By induction hypothesis, we have two cases, each of one splitting in two subcases:

- $R^+_I\ x\ z_{k+1}$. If $z_{k+1} \epsilon I$ we have $R^+_I\ x\ y$. Otherwise $z_{k+1} = z$ and hence $R^+_I\ x\ z$ and $R\ z\ y$ (and so $R^+_I\ z\ y$ as well),
- $R^+_I\ x\ z$ and $R^+_I\ z\ z_{k+1}$. Once more, there are two cases. If $z_{k+1} \epsilon I$ we have $R^+_I\ x\ z$ and $R^+_I\ z\ y$. Otherwise $z_{k+1} = z$ and hence $R^+_I\ x\ z$ and $R\ z\ y$ (and so $R^+_I\ z\ y$ as well).

□

Corollary: If we have an algorithm for deciding $R\ x\ y$ we have an algorithm for deciding $R^+_I\ x\ y$ for any finite I.

Proof: We prove this by induction on the finite set I. If I is empty, then R^+_I is R which is decidable by hypothesis. The induction step follows from the equivalence

$$R^+_{I,z}\ x\ y \equiv [R^+_I\ x\ y \vee [R^+_I\ x\ z \wedge R^+_I\ z\ y.]]$$

□

The same idea may be used to compute the minimal cost for connecting x and y. We suppose that for each x and y we have a value $d\ x\ y \in [0, \infty]$ which gives the cost of a direct connection between x and y. Then we can define

$$d_{I,z}\ x\ y = min\ (d_I\ x\ y)\ (d_I\ x\ z + d_I\ z\ y).$$

The *cost* $c(z_1, \ldots, z_k)$ of a list $z_1, \ldots, z_k$ connecting x and y is defined by

- $d\ x\ y$ if $k = 0$,
- $d\ x\ z_1 + \ldots + d\ z_k\ y$ if $k \geq 1$.

We are interested in the *minimal cost* of connecting x and y by elements in I. If c is this minimal cost it means that

- there exists $z_1, \ldots, z_k$ connecting x and y such that $c(z_1, \ldots, z_k) = c$,
- for *any* $z_1, \ldots, z_k$ connecting x and y we have $c \leq c(z_1, \ldots, z_k)$.

Lemma: If d_I is the minimal cost function for connecting two elements by a list in I then $d_{I,z}$ is a minimal cost function for connecting two elements by a list in I, z.

Proof: If $z_1, \ldots, z_k$ connects x and y in I, z there are two cases: either we have $z_i \epsilon I$ for all i or we can write this list as $zs_1, z, zs_2, \ldots, z, zs_p, y$. In both cases the cost of $z_1, \ldots, z_k$ is $\geq d_{I,z}\ x\ y$. Furthermore, we have two cases:

- $d_I\ x\ y \leq d_I\ x\ z + d_I\ z\ y$: by assumption we have zs connecting x and y *in* I such that $c(zs) = d_I\ x\ y = d_{I,z}\ x\ y$.
- $d_I\ x\ z + d_I\ z\ y \leq d_I\ x\ y$: by assumption we have zs connecting x and z in I such that $c(xz) = d_I\ x\ z$. We have also ts connecting z and y in I such that $c(ts) = d_I\ z\ y$. Hence, zs, z, ts connects x and y in I, z and $c(zs, z, ts) = d_I\ x\ z + d_I\ z\ y = d_{I,z}\ x\ y$.

In both cases we find us connecting x and y in I, z such that $c(us) = d_{I,z}\ x\ y$. □