Dijkstra,Kleene,Knuth

(revised version)

Bernhard Möller

Institut für Informatik, Universität Augsburg

1 The Shortest Path Problem

informal problem statement:

- given:
  - directed graph (n, e)
  - with node set n and non-negatively weighted edge set e
  - a starting node $s \in n$
- task: for each $v \in n$ return
  - length of a shortest path from s to v
  - or ∞ if there is no path from s to v.

algebraic formulation:

- calculate $d = s \,;\, e^*$
- where ; is path concatenation (under adjustment of costs)

aim of derivation: eliminate the expensive star operation

earlier version: [Backhouse et al. 92/94]

2 Some Properties of Paths

- general idea: work with an algebra of path sets (and their costs)
- edge sets: sets of paths with 2 nodes
- node sets: sets of singleton paths
- concatenation: glue at common intermediate node (associative)
- for node set m and path set a
  - $m\,;a$ set of paths in a that start in m-nodes
  - $a\,;m$ set of paths in a that end in m-nodes
- hence set n of *all* nodes is the identity of composition
- a^* arbitrary finite iteration of a, i.e., all paths that can be constructed out of an arbitrary finite number of a-paths

choice:

- $a \mathbin{[\!]} b$: for all pairs of nodes take shortest connecting paths provided by a or b
- refinement order: $a \sqsubseteq b \ =_{df}\ a \mathbin{[\!]} b = b$
  (b refines a iff it offers the less costly paths)
- since singleton paths are always cheapest (cost 0), set n of all nodes refines all sets: $a \sqsubseteq n$
- a full graph may offer better paths than a restricted one:
  $m\,;a \sqsubseteq a$
- composition distributes over choice, hence is $\sqsubseteq$-isotone
- convention: composition binds tighter than choice

further details in Appendix II

three essential properties used in the derivation:

- for graph node p and path set a:

  $$p\,;a\,;p \;\sqsubseteq\; p \qquad \textit{(no detours)}$$

  since all path costs are non-negative, any path from p to itself cannot be cheaper than the 0-cost trivial singleton path consisting just of p

- $$a^* = n \mathbin{[\!]} a\,;a^* = n \mathbin{[\!]} a^*\,;a \qquad \textit{(star recursion)}$$

  iteration of a either uses zero a-paths or one a-path followed/preceded by zero or more others

- $(b \mathbin{[\!]} c)^*$: arbitrary alternations of b paths and c paths

  $$\begin{aligned}(b \mathbin{[\!]} c)^* &= c^*\,;(n \mathbin{[\!]} b\,;(c \mathbin{[\!]} b)^*) \qquad \textit{(path grouping)}\\ &= (n \mathbin{[\!]} (b \mathbin{[\!]} c)^*\,;b)\,;c^*\end{aligned}$$

  exhibit maximal c-sequences at the beginning or end

3 Dijkstra's Algorithm

central ideas:

- generalise the problem by using a set *ok* of nodes for which the problem is solved exactly
- initially, *ok* is empty
- extend this set node by node till all are in *ok*
- for each node outside *ok* the algorithm computes an approximation to d, viz.
- the length of a shortest path whose interior nodes are from *ok*

formalisation:

- use the path algebra with node set n and edge set e
- for $ok \leq \mathsf{n}$ define generalised function dd by

$$dd(ok) =_{df} s\,;(ok\,;e)^*$$

- expresses that $dd(ok)$ only considers paths with interior nodes in ok
- then, by neutrality of n w.r.t. composition, $\mathsf{d} = dd(\mathsf{n})$
- "strategy": extract maximal subexpressions of form $\mathsf{p}\,;\mathsf{a}\,;\mathsf{p}$ to allow application of no-detours rule

- plan of derivation: find an inductive version of dd that does not use star operations anymore
- maintain the invariant that dd solves the problem exactly, i.e., using *all* possible paths, for end nodes in ok:

$$s\,;(ok\,;e)^*\,;ok \;=\; s\,;e^*\,;ok$$

- more compactly,

$$dd(ok)\,;ok \;=\; \mathrm{d}\,;ok \tag{1}$$

- **induction base:** $ok = \emptyset$

$$dd(\emptyset) \;=\; s\,;\emptyset^* \;=\; s\,;\mathrm{n} \;=\; s$$

- invariant holds trivially for $dd(\emptyset)$

induction step: calculate behaviour of dd when ok is extended by a node $w \leq \neg ok$

from this infer how to choose w appropriately to maintain the invariant

$$
\begin{array}{ll}
 & dd(w \,[]\, ok) \\
= & \{\!\mid \text{definition } dd \text{ and distributivity} \mid\!\} \\
 & s \,;\, (w \,;\, e \,[]\, ok \,;\, e)^* \\
= & \{\!\mid \text{path grouping and distributivity} \mid\!\} \\
 & s \,;\, (ok \,;\, e)^* \,;\, (n \;\, [] \;\, w \,;\, e \,;\, ((w \,[]\, ok) \,;\, e)^*) \\
= & \{\!\mid \text{definition } dd \text{ and abbreviation } h =_{df} (w \,[]\, ok) \,;\, e \mid\!\} \\
 & dd(ok) \,;\, (n \;\, [] \;\, w \,;\, e \,;\, h^*)
\end{array}
$$

simplification of second alternative ($h =_{df} (w \,[\!]\, ok) ; e$):

$$w ; e ; h^*$$

$=$ {| star recursion and definition of h |}

$$w ; e \,[\!]\, w ; e ; h^* ; (w \,[\!]\, ok) ; e$$

$=$ {| distributivity |}

$$w ; e \,[\!]\, w ; e ; h^* ; w ; e \,[\!]\, w ; e ; h^* ; ok ; e$$

$=$ {| middle summand $\sqsubseteq$ first one by no-detours rule |}

$$w ; e \,[\!]\, w ; e ; h^* ; ok ; e$$

substituted back:

$$dd(w \,[\!]\, ok) = dd(ok) ; (n \;[\!]\; w ; e \;[\!]\; w ; e ; h^* ; ok ; e)$$

now continue simplification with third alternative (after distribution)

$$
\begin{array}{ll}
 & dd(ok)\,;w\,;\mathrm{e}\,;\mathrm{h}^*\,;ok\,;\mathrm{e} \\
\sqsubseteq & \{\!\mid \text{since } w\,;\mathrm{e} \sqsubseteq \mathrm{e} \text{ and } \mathrm{h} \sqsubseteq \mathrm{e} \mid\!\} \\
 & dd(ok)\,;\mathrm{e}\,;\mathrm{e}^*\,;ok\,;\mathrm{e} \\
\sqsubseteq & \{\!\mid \text{definition of } dd(ok) \text{ and star rules} \mid\!\} \\
 & \mathrm{s}\,;\mathrm{e}^*\,;ok\,;\mathrm{e} \\
= & \{\!\mid \text{definition of } \mathrm{d} = \mathrm{s}\,;\mathrm{e}^* \text{ and invariant } \mathrm{d}\,;ok \;=\; dd(ok)\,;ok \mid\!\} \\
 & dd(ok)\,;ok\,;\mathrm{e} \\
\sqsubseteq & \{\!\mid \text{definition of } dd(ok) = \mathrm{s}\,;(ok\,;\mathrm{e})^* \text{ and star rule} \mid\!\} \\
 & dd(ok)
\end{array}
$$

informal interpretation: shortest paths to nodes outside *ok* cannot loop back through *ok*

- in sum:

$$dd(w \mathbin{[]} ok) \;=\; dd(ok)\,;(n \mathbin{[]} w\,;e) \qquad (*)$$

- algebraic equivalent of the usual set of assignments

$$dd[v] = \mathsf{min}\,(dd[v], dd[w] \mathbin{[]} weight(w,v))$$

  for $v \leq n$
- (where by the invariant $dd(ok)\,;ok \;=\; d\,;ok$ only the subset $\neg ok - \{w\}$ needs to be considered)

- now choose w such that the invariant holds for $w \mathbin{[]} ok$ again
- sufficient: $d\,;w = dd(w \mathbin{[]} ok)\,;w$
- by $(*)$ and no-detours rule the rhs is equal to $dd(ok)\,;w$

abbreviation: $\mathsf{f} =_{df} dd(ok) = \mathsf{s} ; (ok ; \mathsf{e}^*)$

$\mathsf{d} ; w$

$= \quad \{\!\![$ definition of d $]\!\!\}$

$\mathsf{s} ; \mathsf{e}^* ; w$

$= \quad \{\!\![$ path grouping, using $e = ok ; \mathsf{e} \, [\!] \, \neg ok ; \mathsf{e}$ $]\!\!\}$

$\mathsf{s} ; (ok ; \mathsf{e}^*) ; (\mathsf{n} \, [\!] \, \neg ok ; \mathsf{e} ; \mathsf{e}^*) ; w$

$= \quad \{\!\![$ definitions of f and setting $\mathsf{e}^+ =_{df} \mathsf{e} ; \mathsf{e}^*$ $]\!\!\}$

$\mathsf{f} ; (\mathsf{n} \, [\!] \, \neg ok ; \mathsf{e}^+) ; w$

$= \quad \{\!\![$ splitting $\neg ok$ into its nodes and distributivity $]\!\!\}$

$\mathsf{f} ; w \;\; [\!] \;\; ([\!]_{v \leq \neg ok} \; \mathsf{f} ; v ; \mathsf{e}^+ ; w)$

so goal achieved if $[\!]_{v \leq \neg ok} \; \mathsf{f} ; v ; \mathsf{e}^+ ; w \;\; \sqsubseteq \;\; \mathsf{f} ; w$

reduction:

$$\textstyle[]_{v \leq \neg ok} \mathsf{f} \,;v\,;\mathsf{e}^+ \,;w \sqsubseteq \mathsf{f}\,;w$$

$\Leftrightarrow$ $\{\![$ universal characterisation of choice $]\!\}$

$$\forall\, v \leq \neg ok : \mathsf{f}\,;v\,;\mathsf{e}^+\,;w \sqsubseteq \mathsf{f}\,;w$$

$\Leftarrow$ $\{\![$ instance $\mathsf{f}\,;w\,;\mathsf{e}^+\,;w \sqsubseteq \mathsf{f}\,;w$ of no-detours rule $]\!\}$

$$\forall\, v \leq \neg ok : \mathsf{f}\,;v \sqsubseteq \mathsf{f}\,;w$$

this holds iff w is a node with minimal cost along ok paths complete algorithm:

$$
\begin{array}{rcl}
dd(\emptyset) & = & s \\
dd(ok \,[]\, w) & = & dd(ok)\,;(\mathrm{n} \,[]\, w\,;\mathrm{e}) \\
 & & \text{if } ok \neq \emptyset \text{ and } w \leq \neg ok \text{ satisfies} \\
 & & \forall\, v \leq \neg ok \;:\; dd(ok)\,;v \sqsubseteq dd(ok)\,;w
\end{array}
$$

4 Knuth's Generalisation

observations:

- edge XY with weight m corresponds to an automaton transition $X \xrightarrow{m} Y$
- matrix algebra approach works, because the problem is essentially about automata/regular languages
- Knuth generalises this to a context-free setting

approach:

- use restricted cfgs of with productions of the shape $(n \geq 0)$

$$X_i ::= f(X_{i1}, \ldots, X_{in})$$

- and associated $\mathbb{N}$-valued interpreting functions f^I that are
- isotone in each argument
- *superior*, i.e., satisfy

$$\forall\, j : f^I(x_1, \ldots, x_n) \geq x_j$$

- task: compute for all i

$$m(X_i) =_{df} \min\{w^I : w \in L(X_i)\}$$

the shortest path example:

- edge $X \xrightarrow{m} Y$ gives production

$$X ::= f(Y)$$

- with $f^I(x) =_{df} m + x$
- f is isotone and superior
- for start node S add a production $S ::= 0$

algorithm:

- use again a set ok and an auxiliary function mm
- ok is the set of nonterminals X for which $\mathrm{m}(\mathsf{X})$ has been determined
- for all other Y the value $mm(\mathsf{Y})$ approximates $\mathrm{m}(\mathsf{Y})$
- invariant: $\forall\ \mathsf{X} \in ok : mm(\mathsf{X}) = \mathrm{m}(\mathsf{X})$
- initialisation: $ok := \emptyset\,; \forall\ \mathsf{X} : mm(\mathsf{X}) := \infty$

loop:

- if all nonterminals are in ok, stop
- otherwise, for all $Y \notin ok$, compute

  $$mm(Y) =_{df} \min\{f^I(m(X_1),\ldots,m(X_n)) \mid Y ::= f(X_1,\ldots,X_n) \wedge \{X_1,\ldots,X_n\} \subseteq ok\}$$

  (if the set involved is empty then $mm(Y) = \infty$)
- choose a Y with minimum $mm(Y)$
- $ok := ok \cup \{Y\}$
- $m(Y) := mm(Y)$

challenge:

find a nice calculational correctness proof/derivation for Knuth's algorithm

Appendix I: Just for Fun - The Floyd/Warshall Algorithm

this is the all-pairs shortest non-empty path problem

specification even simpler than for Dikstra: compute e^{+}

central idea: use again a set ok that restricts the inner nodes of paths and increment it stepwise

specification of auxiliary function:

$$rt(ok) =_{df} e ; (ok ; e)^{*}$$

("restricted transitive closure")

here another star property is useful:

$$(\mathsf{a} \,[]\, \mathsf{b})^* = \mathsf{a}^* \,;(\mathsf{b}\,;\mathsf{a}^*)^* = (\mathsf{a}^*\,;\mathsf{b})\,;\mathsf{a}^* \qquad \textit{(star of sum)}$$

induction base:

$$rt(\emptyset) = \mathsf{e}\,;\emptyset^* = \mathsf{e}\,;\mathsf{n} = \mathsf{e}$$

induction step: for arbitrary node w:

$rt(ok \mathbin{[\!]} w)$

$=$ $\{\![$ definition rt and distributivity $]\!\}$

$\mathsf{e} ; (ok ; \mathsf{e} \mathbin{[\!]} w ; \mathsf{e})^*$

$=$ $\{\![$ star of sum $]\!\}$

$\mathsf{e} ; (ok ; \mathsf{e})^* ; (w ; \mathsf{e} ; (ok ; \mathsf{e}))^*$

$=$ $\{\![$ fold $\mathsf{e} ; (ok ; \mathsf{e})^*$ twice to $\mathsf{f} =_{df} rt(ok)$ $]\!\}$

$\mathsf{f} ; (w ; \mathsf{f})^*$

$=$ $\{\![$ star recursion and distributivity $]\!\}$

$\mathsf{f} \mathbin{[\!]} \mathsf{f} ; w ; \mathsf{f} ; (w ; \mathsf{f})^*$

$=$ $\{\![$ star recursion and distributivity $]\!\}$

$\mathsf{f} \mathbin{[\!]} \mathsf{f} ; w ; \mathsf{f} \mathbin{[\!]} \mathsf{f} ; w ; \mathsf{f} ; (w ; \mathsf{f})^* ; w ; \mathsf{f}$

$=$ $\{\![$ since third alternative $\sqsubseteq$ second one by no-detours rule $]\!\}$

$\mathsf{f} \mathbin{[\!]} \mathsf{f} ; w ; \mathsf{f}$

to guarantee termination, choose $w \notin ok$

complete algorithm:

$$
\begin{array}{rcl}
rt(\emptyset) & = & e \\
rt(ok \mathbin{[]} w) & = & \mathsf{f} \mathbin{[]} \mathsf{f} \,;w\,; \mathsf{f} \\
 & & \text{where } \mathsf{f} = rt(ok) \text{ and } w \notin ok
\end{array}
$$

depending on the underlying cost semiring (see Appendix II) this is the Floyd or Warshall algorithm

Appendix II: Algebraic Background

Definition 4.1 *semiring*: structure $(S, +, \cdot, \mathbf{0}, n)$ such that

- $(S, +, \mathbf{0})$ is a commutative monoid
- $(S, \cdot, \mathbf{1})$ is a monoid
- the distributive laws hold
- $\mathbf{0}$ is an annihilator: $\mathbf{0} \cdot a = \mathbf{0} = a \cdot \mathbf{0}$

if S is idempotent, i.e., $x + x = x$, the relation $a \leq b \Leftrightarrow_{df} a + b = b$ is a partial order, the *natural* order interpretation:

$$\begin{array}{lcl} + & \leftrightarrow & \text{choice,} \\ \cdot & \leftrightarrow & \text{sequential composition} \\ \mathbf{0} & \leftrightarrow & \text{empty set of choices} \\ \mathbf{1} & \leftrightarrow & \text{identity} \\ \leq & \leftrightarrow & \text{increase in information or in choices} \end{array}$$

Example 4.2 tropical semiring:

- $(\mathsf{min}\,,+) = (\mathbb{N}_\infty\,,\mathsf{min}\,,+,\infty,0)$
- natural ordering: converse of the standard ordering on $\mathbb{N}_\infty$
- $\mathbf{1} = 0$ is the largest element.

generalisation: *cost algebra*

- idempotent semiring with total natural order
- in which **1** is the greatest element

further examples:

- $\mathbb{R}_{\geq 0} \cup \{\infty\}$ with the operations as above
- Booleans $\mathbb{B}$ with implication order

$\mathrm{MAT}(M, S) = (S^{M \times M}, +, \cdot, \mathbf{0}, \mathbf{1})$

- set of matrices with indices in M and elements of semiring S as entries
- again a semiring
- idempotent iff S is
- natural order: componentwise
- $\mathrm{MAT}(M, \mathbb{B})$ isomorphic to semiring $\mathrm{REL}(M)$ of binary relations over M under union and composition

modelling graphs with edge weights:

- $\mathrm{MAT}(N, S)$ where S is a cost algebra representing sets of graph nodes

- *test semiring* [Kozen 97]: pair $(S, \mathsf{test}(S))$ with Boolean subalgebra $\mathsf{test}(S) \subseteq [\mathbf{0}, \mathbf{1}]$ such that
- $\mathbf{0}, \mathbf{1} \in \mathsf{test}(S)$
- $+$ is join and $\cdot$ is meet in $\mathsf{test}(S)$
- S is *discrete* if $\mathsf{test}(S) = \{\mathbf{0}, \mathbf{1}\}$
- $S = (\mathsf{min}\,, +)$ is discrete, but $\mathrm{MAT}(M, S)$ can be made non-discrete:
- choose as tests all matrices with tests on the main diagonal and $\mathbf{0}$ outside

- over discrete S, matrix p is a *point* if it is an atom in $\mathsf{test}(\mathrm{MAT}(M,S))$,
- i.e., if it has exactly one entry $\mathbf{1}$ in its main diagonal (and hence $\mathbf{0}$ everywhere else)
- general tests represent subsets of M in the analogous way
- for points p and q and matrix a

$$(p \cdot a \cdot q)_{uv} = \begin{cases} a_{uv} & \text{if } u = p \land v = q \\ \mathbf{0} & \text{otherwise} \end{cases}$$

Lemma 4.3 Consider a discrete cost algebra S, a point p and an arbitrary matrix a of $\mathrm{MAT}(M, S)$. Then $p \cdot a \cdot p \leq p$.

since $\mathbb{B}$ is a cost algebra, this property holds for the relation semiring $\mathrm{REL}(M)$, too iteration: add Kleene star and plus with standard axioms [Kozen94]

Example 4.4 Since in $(\min, +)$ the multiplicative unit $\mathbf{1} = 0$ is the largest element, and $x^* = \mathbf{1}$ for all $x \leq \mathbf{1}$, we can extend $(\min, +)$ uniquely to a Kleene algebra by setting $n^* = \mathbf{1}$ for all $n \in \mathbb{N}_\infty$.

useful law

$$(b+c)^* = (\mathbf{1}+(b+c)^* \cdot b) \cdot c^* = b^* \cdot (\mathbf{1}+b \cdot (b+c)^*) \qquad \text{(path grouping)}$$

fact [Conway71]: $\mathsf{MAT}(\mathsf{M},\mathsf{S})$ over Kleene algebra S can be extended to a Kleene algebra

Corollary 4.5 *Consider a discrete cost algebra* S*, a point* p *and an arbitrary matrix* a *of* $\mathsf{MAT}(\mathsf{M},\mathsf{S})$*. Then* $\mathsf{p}\cdot\mathsf{a}^*\cdot\mathsf{p}=\mathsf{p}$*.*

reason: $\mathbf{1}\leq\mathsf{a}^*$ holds for all Kleene algebras connection to path problems:

- for graph matrix $a \in MAT(M, S)$ over cost algebra S and $x, y \in M$:
- element a^i_{xy} gives the minimum cost of paths with exactly i edges from x to y
- hence a^*_{xy} is the minimum cost along arbitrary paths from x to y