Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 26 (1980)

Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: THE FAST SKEW-CLOSURE ALGORITHM

Autor: Fischer, M. J. / Paterson, M. S.

Kapitel: 5. Proofs of correctness

DOI: https://doi.org/10.5169/seals-51079

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 17.02.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

${A^V}_{ii}$ is a subgroup of G and two diagonal elements in the same (weak) component are conjugate since we may show:

$$ {A^V}_{ii} \cdot g = g \, . \, {A^V}_{jj} = {A^V}_{ij} \quad \text{for any} \quad g \in {A^V}_{ij} $$

In particular if all circuits on non-empty edges correspond to the group identity then in A^V each entry has at most one element. For example given a matrix A over $< \mathbf{R}, + >$ we determine from A^V for each component of the graph whether there are (weak) circuits with non-zero sums. If all circuits sum to zero then the graph is a "potential" graph, i.e. there is a function pot : $\mathbf{R} \to \{\text{vertices}\}$ such that each edge $< u, v >$ has the value (pot (v) − pot (u)). Similarly over $< \mathbf{Z}_k, + >$ we may determine whether each weak circuit of a directed graph has zero sum where forward and backward edges are accounted $+1$ and -1 respectively. Naturally we may find it convenient in some cases to hold only a homomorphic image of $P(G)$ for the computations e.g.

$$ \begin{aligned} h(\varnothing) &= \varnothing \\ h(\{g\}) &= g \\ h(a) &= \omega \quad \text{when} \quad |a| > 1 . \end{aligned} $$

5. Proofs of correctness

An operator ϕ is *monotonic* if $A \subseteq B$ implies $A^\phi \subseteq B^\phi$. ψ_i is *not* a monotonic operator but rather surprisingly Ψ *is*. To simplify our proofs we introduce several monotonic operators. Define ϕ_i by the program

$A_{i*} := A_{ii}^V A_{i*}$

for $k := i + 1$ step 1 until n do $A_{k*} := A_{k*} \cup \overline{A_{ik}} A_{i*}$

and ϕ_i' analogously using "$i - 1$ step -1 until 1". Both are obviously monotonic. Φ and Φ' are defined from ϕ_i and ϕ_i' in a similar way to Ψ and Ψ'. Although $\Psi \subseteq \Phi$ is evident, the following result is not.

THEOREM 5. $\Psi = \Phi$ *(and* $\Psi' = \Phi'$*)*.

Proof. Consider ψ_i applied to an arbitrary matrix A and suppose it selects the index k with $A_{ik} \neq \varnothing$. (If no index is selected then of course $A^{\psi_i} = A^{\phi_i}$). We verify that:

(i) $A^{\phi_i \, \phi_{i+1} \cdots \phi_{k-1}} = A^{\phi_{i+1} \cdots \phi_{k-1} \, \phi_i}$ and similarly for ψ_i in place of ϕ_i

and (ii) $A^{\psi_i \, \phi_k} = A^{\phi_i \, \phi_k}$

(i) is immediate since ϕ_i and ψ_i do not affect any rows with indices between i and k.
To verify (ii) we check that $A^{\psi_i \, \phi_k} \supseteq A^{\phi_i}$ since for $j > k$

$$(A^{\psi_i \, \phi_k})_{j*} \supseteq \overline{\overline{A_{ik}} \, A_{ij}} \, \overline{A_{ik}} \, A_{ii}^{V} \, A_{i*}$$
$$\supseteq \overline{A_{ij}} \, A_{ii}^{V} \, A_{i*}$$

We also note that $\phi_k \, \phi_k = \phi_k$
The proof of the Theorem is by induction on i from n to 1 for the equation

$$\phi_i \ldots \phi_n = \psi_i \ldots \psi_n$$

This is trivial for $i = n$, while for $i = 1$ it is the result to be proved. Suppose the equation true for $i + 1$, and then for an arbitrary A:

$$A^{\psi_i \, \psi_{i+1} \cdots \psi_n} = A^{\psi_i \, \phi_{i+1} \cdots \phi_n} \quad \text{by inductive hypothesis}$$

Either $A^{\psi_i} = A^{\phi_i}$ and we are done or $\exists \, k > i$ which is selected in ψ_i on A. Then

$$\begin{aligned} A^{\psi_i \, \phi_{i+1} \cdots \phi_k} &= A^{\phi_{i+1} \cdots \phi_{k-1} \, \psi_i \, \phi_k} && \text{by (i)} \\ &= A^{\phi_{i+1} \cdots \phi_{k-1} \, \phi_i \, \phi_k} && \text{by (ii)} \\ &= A^{\phi_i \cdots \phi_k} && \text{by (i)} \end{aligned}$$

The induction step now follows easily. □

In the proof of the Main Theorem below we need the following results.

LEMMA 1.

(i) $\Phi\Phi = \Phi$ *(and* $\Phi'\Phi' = \Phi'$*)*

(ii) $A^{\Phi\Phi'} \supseteq \bar{A}A \vee A$ *(and* $A^{\Phi'\Phi} \supseteq \bar{A}A \vee A$*)*

(iii) $A^{\Phi\Phi'\Phi} \supseteq \bar{A}\bar{A}A \vee \bar{A}A \vee A$

Proof.

(i) We may verify directly that for $i \leqslant j$, $\phi_j \, \phi_i \subseteq \phi_i \, \phi_j$

Then

$$
\begin{aligned}
\Phi\Phi &= \phi_1 \dots \phi_n \phi_1 \dots \phi_n \\
&\subseteq \phi_1\phi_1\phi_2\phi_2 \dots \phi_n\phi_n \quad \text{by repeated application of above inclusion} \\
&= \Phi \subseteq \Phi\Phi
\end{aligned}
$$

(ii) Consider an arbitrary contribution $\overline{A_{ik}}\, A_{ij}$ to $\bar{A}A$.

If $k > i$ then $\overline{A_{ik}}\, A_{ij} \subseteq A^{\phi_i} \subseteq A^{\Phi}$

else $\overline{A_{ik}}\, A_{ij} \subseteq A^{\phi'_i} \subseteq A^{\Phi'}$

(iii)
$$
\begin{aligned}
A^{\Phi\Phi'\Phi} = (A^{\Phi\Phi'})^{\Phi'\Phi} &\supseteq (\bar{A}A \vee A)^{\Phi'\Phi} \\
&\supseteq (\bar{A}A \vee \bar{A})(\bar{A}A \vee A) \\
&\supseteq \bar{A}\bar{A}A \vee \bar{A}A
\end{aligned}
$$
□

Lemma 2. If $B \supseteq \bar{A}\bar{A}A \cup \bar{A}A \cup A$ and U is defined by

$$
\begin{aligned}
U_{ij} &= B_{ij} \quad \text{if} \quad i \leqslant j \\
&= \varnothing \quad \text{il} \quad i > j
\end{aligned}
$$

then $\bar{B}\, U^V B \supseteq \bar{A}A^V A$

Proof.

If $j \leqslant k$, $A_{ij}\, A_{jk} \subseteq A_{ij}\, B_{jk} \subseteq A_{ij}\, U_{jk}$

If $j \geqslant k$, $A_{ij}\, A_{jk} \subseteq A_{ij}\, \bar{A}_{ji}\, A_{ij}\, A_{jk} \subseteq A_{ij}\, \bar{B}_{jk} \subseteq A_{ij}\, \bar{U}_{jk}$

Thus $AA \subseteq A\,(U \cup \bar{U})$. Similarly $\bar{A}\bar{A} \subseteq (U \cup \bar{U})\,\bar{A}$

Also $\bar{A}A \subseteq B$ and $\bar{A}A \subseteq \bar{B}$, so that $\bar{A}A \subseteq (U \cup \bar{U})$

From these inclusions we may derive

$$
\begin{aligned}
\bar{A}^+ . A^+ &\subseteq (U \cup \bar{U})^+ \\
\bar{A}^+ . A^+ &\subseteq \bar{B}\, U^V \\
\bar{A}^+ . A^+ &\subseteq U^V B \\
\bar{A}^+ . A^+ &\subseteq \bar{B}\, U^V B
\end{aligned}
$$

and finally

$$
\bar{A}A^V A = (\bar{A}^+ A^+)^+ \subseteq \bar{B}\, U^V B
$$
□

We shall consider weak paths which start with a backward edge, end with a forward edge and contain only those edges $< i, j >$ with $r \leqslant i \leqslant j$ for some threshold r. Hence we define the operators π_r for $1 \leqslant r \leqslant n + 1$.

$$X^{\pi_r} = \overline{X}(U^{(r)})^V X \cup X$$

$$\text{where } U^{(r)}{}_{ij} = X_{ij} \text{ if } r \leqslant i \leqslant j$$

$$= \varnothing \text{ otherwise}$$

LEMMA 3.

$$\pi_r \subseteq \phi_r \pi_{r+1} \quad \textit{for } 1 \leqslant r \leqslant n\,.$$

Proof. Let X be an arbitrary matrix, with $U^{(r)}$ defined as above and

$$Y = U^{(r)} \cup \overline{U^{(r)}}. \text{ Let } Z = X^{\phi_r}.$$

$$Y_{jr}\, Y^*_{rr}\, Y_{rk} \subseteq \overline{X_{rj}}\, X_{rr}^V X_{rk} \subseteq Z_{jk}$$

and likewise

$$Y_{jr}\, Y^*_{rr}\, Y_{rk} \subseteq \overline{Z_{jk}}$$

Similarly to deal with the ends of the paths,

$$\overline{X_{r*}}\, Y_{rr}{}^*\, Y_{rk} \subseteq \overline{Z_{k*}} \qquad \text{if} \quad r < k$$

$$Y_{jr}\, Y_{rr}{}^*\, X_{r*} \subseteq Z_{j*} \qquad \text{if} \quad r < i$$

$$\overline{X_{r*}}\, Y_{rr}{}^*\, X_{r*} \subseteq \overline{Z_{r*}} Z_{r*} \qquad \text{in any case}$$

These inequalities show that internal edges of a path which visit vertex r can be replaced, so that $Z^{\pi_{r+1}}$ is sufficient. □

The effort is now behind us and the Main Theorem comes easily.

THEOREM 6.

$$\text{(i)} \quad Q = \Psi\Psi'\Psi\Psi'$$

$$\text{(ii)} \quad V = R\Psi'\Psi\Psi'$$

$$(iii) \quad W = S\Psi\Psi'$$

Proof. The only matters requiring detailed proof are that the righthand transforms include Q. Let A be an arbitrary matrix.

For (i), define $B = A^{\Psi\Psi'\Psi}$

$$\begin{aligned} &= A^{\Phi\Phi'\Phi} && \text{by Theorem 5} \\ &\supseteq \bar{A}\bar{A}A \cup \bar{A}A \cup A && \text{by Lemma 1 (iii)} \end{aligned}$$

Therefore $A^{Q} \subseteq B^{\pi_1}$ from Lemma 2

For (ii) and (iii), let $B = A^{S}$

$$\begin{aligned} A^{R\Psi'\Psi} &= (I \cup A)^{\Phi'\Phi} && \text{by Theorem 5} \\ &\supseteq (I \cup \bar{A})(I \cup A) && \text{by Lemma 1 (ii)} \\ &\supseteq A \cup \bar{A} \\ &= B \end{aligned}$$

Also in this case, $A^{Q} \subseteq B^{\pi_1}$
In view of Theorem 5 and Lemma 1 (i) we have only to show now that $B^{\pi_1} \subseteq B^{\Phi\Phi'}$ to complete the proof. Using Lemma 3 repeatedly:

$$\pi_1 \subseteq \phi_1\pi_2 \subseteq \phi_1\phi_2\pi_3 \subseteq \ldots \subseteq \Phi\pi_{n+1}$$

But

$$X^{\pi_{n+1}} = \bar{X}X \cup X \subseteq X^{\Phi\Phi'}$$

therefore

$$\pi_1 \subseteq \Phi\Phi\Phi' = \Phi\Phi' \qquad \square$$

6. Conclusion

The close examination of a simple, practical matrix algorithm has led us to novel theoretical questions and to potentially useful generalizations of the algorithm. The principal contribution of this work to the programmer is the introduction of several very fast closure algorithms and the establishment of their correctness. The problems we have encountered in the theory of relations and closure operations have whetted our curiosity and suggest that further investigation may be rewarding.

Acknowledgment. We wish to thank Richard Ladner for discussions concerning this paper and its relation to security problems in protection systems.