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: 3. The quadratic monoid

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

that of product [2]) is no greater than that of T, to within a constant factor. However we have been unable to show the converse.

Open Problem 1. Is there an $O(n^2)$ matrix-based algorithm for the T'-closure?

3. The quadratic monoid

To satisfy our curiosity we investigated the monoid generated by the composition of closures corresponding to polynomials of degree at most two. For any set of transformations E let M_E be the monoid generated by compositions of elements of E. For any polynomial $P(X, \overline{X})$, define $Z_P : A \rightarrow (\mu X. X \geqslant A \vee P(X, \overline{X}))$
and then

$$\Pi_r = \{ Z_P \mid \deg(P) \leqslant r \}.$$

THEOREM 3. $M_{\Pi_2} = M_{\{R, S, Q, Q', T, T'\}}$ *and the monoid is finite.*

Proof. The equality follows from the finiteness since

$$Z_{P_1 \vee P_2} = \bigvee_m \left(Z_{P_1} \cdot Z_{P_2}\right)^m$$
$$\in M_{\{Z_{P_1}, Z_{P_2}\}} \quad \textit{if} \text{ this is finite.}$$

$M_{\{R, S, Q, Q', T, T'\}}$ is examined explicitly below and is found to contain exactly fifty elements. □

We write A for the monoid identity given by $A^A = A$ and $[Z_1, \ldots, Z_k]$ for the closure $\bigvee_m (Z_1 \vee \ldots \vee Z_k)^m$. Together with the obvious idempotencies of closures we have the following sufficient defining relations.

$$W \stackrel{\text{def}}{=} [S, Q, Q', T, T']$$
$$= QQ' = Q'Q = QT' = Q'T' = SQ = SQ' = ST = ST'$$
$$V \stackrel{\text{def}}{=} [R, S, Q, Q', T, T'] = WR = RQ = RQ' = RT'$$
$$QT = [Q, T] \qquad Q'T = [Q', T]$$
$$T'Q = T'TQ = T'QT \qquad T'Q' = T'TQ' = T'Q'T$$
$$TT' = T'T \quad * \stackrel{\text{def}}{=} RT = TR \qquad RS = SR$$

The closures in the monoid are

$$V \quad : \quad A^V = (\overline{A} \vee A)^*$$
$$W \quad : \quad A^W = (\overline{A} \vee A)^+$$

$[Q, T]$: $A^{[Q,T]} = A^V . A$

$[Q', T]$: $A^{[Q',T]} = A . A^V$

$[T, T']$: $A^{[T,T']} = A \vee A^V . (AA \vee \bar{A}\bar{A}) . A^V$

$*, [R, S], R, S, Q, Q', T, T'$ and Λ.

The monoid can be counted after expressing its elements in a canonical form by the following rules.

(i) Using $RS = SR$, $RT = TR$, $RQ = RQ' = RT' = QQ'R$, we can bring any occurrence of R to the end of the product

(ii) Using $SQ = SQ' = ST = ST' = QQ'$, we can assume that any S occurs at the end of the rest of the product

(iii) $QT' = Q'T' = T'QQ'$ and $TT' = T'T$ allow us to bring any T' to the front of the remainder.

(iv) The elements generated by Q, Q', T are found to be

$$\Lambda, Q, Q', T, TQ, TQ', QT, Q'T, W$$

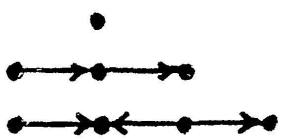
Prefixing these with T' yields only 4 new elements

$$T', T'Q, T'Q', T'T$$

(v) The 50 elements of the monoid are given by

$$\{\Lambda, Q, Q', T, T', TQ, TQ', QT, Q'T, T'Q, T'Q', T'T\} . \{\Lambda, R, S, SR\} \cup \{W, V\}$$

These elements are distinguishable by their effect on the graph



The "fast" monoid generated by the $O(n^2)$ operations R, S, Q, Q' has only 14 elements

$$\{\Lambda, Q, Q'\} . \{\Lambda, R, S, SR\} \cup \{W, V\}$$

Of computational interest are the relations

$$RQ = V \quad \text{and} \quad QQ' = SQ = W$$

which yield efficient ways to compute these common closures. Note that in some contexts the Q' closure may be more rapid to compute than S.

We illustrate some of the proofs for the results above.

THEOREM 4.

CANCELLATION LEMMA. *For all* A, $A\bar{A}A \geqslant A$.

Proof. $(A\bar{A}A)_{ij} \geqslant A_{ij}\bar{A}_{ji}A_{ij} = A_{ij}A_{ij}A_{ij} \geqslant A_{ij}$ □

(i) $RQ = V$

(ii) $QQ' = W$

(iii) $[Q, T] = QT$ and $A^{QT} = A^{V} . A$

Proof.

(i) If we show that $RQ \geqslant S$ the result follows easily. But

$$A^{RQ} \geqslant (I \vee A)^{Q} \geqslant A \vee \bar{A}I = A \vee \bar{A} = A^{S}$$

(ii) Again the only non-trivial part is that $QQ' \geqslant S$

$$A^{QQ'} \geqslant (A \vee \bar{A}A)^{Q'} \geqslant A \vee \bar{A}A . \bar{A} \geqslant A^{S}$$

by the Cancellation Lemma.

(iii) By inspection, $A^{[Q, T]} \leqslant A^{V} . A$

However,

$$A^{V} . A = A^{*} . \bar{A}A^{V}A \vee A^{*} . A \leqslant (A^{Q})^{T} \leqslant A^{[Q,T]}$$ □

One of the harder results to prove is that $TT' = T'T$. We leave it as an exercise for the reader.

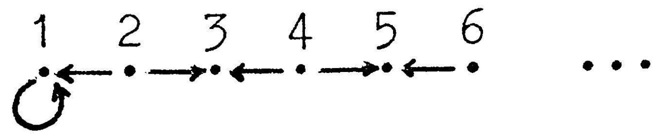
We have found that each mapping in Π_2 is defined by a regular set over $\{A, \bar{A}\}$, however in Π_3 there are «non-regular» mappings, e.g. $Z_{XX\bar{X} \vee \bar{X}XX}$.

The finiteness of M_{Π_2} does not persist for large r. We show by the example below that M_{Π_4} is infinite.

Open Problem 2. Is M_{Π_3} finite?

Example. Let $J = Z_{\bar{X}XXX}$, $K = Z_{XXX\bar{X}}$

$Z_{XXXX \vee XXXX} \notin M_{\{J,K\}}$ and so $M_{\{J,K\}}$ is infinite, since for the infinite graph shown below:



$(JK)^m$ adds all edges $< i, j >$ with $i, j \leqslant 2m$

and $(JK)^m J$ adds all edges $< i, j >$ with $i, j \leqslant 2m + 1$

Therefore J, JK, JKJ, ... are all distinct.

4. Generalized algorithm for power-group algebras

To elucidate the correctness of the algorithm and to encompass some more general applications we need to generalize from the $\{0, 1\}$ Boolean algebra to a slightly richer structure. The *power-group algebra* $P(G)$ is a structure defined from an arbitrary group G. The elements of $P(G)$ are the subsets of G; the operations we require are *union* ($\cup$), complex *product*:

$$ab = \{ gh \mid g \in a, \ h \in b \} \quad \text{for} \quad a, b \subseteq G$$

and *converse*:

$$\bar{a} = \{ g^{-1} \mid g \in a \}$$

$P(G)$ is a monoid with respect to product with identity $\lambda = \{\text{identity}_G\}$. As before we shall be considering matrices over the structure, with matrix product and union defined in the obvious way from product and union in $P(G)$, and matrix *converse* defined by

$$(\bar{A})_{ij} = \overline{A_{ji}}$$

The key properties of power-group algebras which are needed are given below

Lemma. *Let a, b be elements and A, B matrices*

(i) $\bar{\bar{a}} = a$; $\bar{\bar{A}} = A$

(ii) $\overline{ab} = \bar{b}\bar{a}$; $\overline{AB} = \bar{B}\bar{A}$

(iii) *if $a \neq \varnothing$ then $a\bar{a} \supseteq \lambda$; $A\bar{A}A \supseteq A$*