Annales Mathematicae et Informaticae
***37** (2010) pp. 77–84*
http://ami.ektf.hu

On the skeleton of a finite transformation semigroup

Attila Egri-Nagy[a b], Chrystopher L. Nehaniv[b]

[a]Department of Computing Science, Eszterházy Károly College, Hungary

[b]School of Computer Science, University of Hertfordshire, United Kingdom

Submitted 5 October 2010; Accepted 13 December 2010

Dedicated to professor Béla Pelle on his 80th birthday

Abstract

There are many ways to construct hierarchical decompositions of transformation semigroups. The holonomy algorithm is especially suitable for computational implementations and it is used in our software package. The structure of the holonomy decomposition is determined by the action of the semigroup on certain subsets of the state set. Here we focus on this structure, the skeleton, and investigate some of its properties that are crucial for understanding and for efficient calculations.

Keywords: transformation semigroup, Krohn-Rhodes decomposition, holonomy algorithm

MSC: 20M20, 20M35, 06A06

1. Introduction

The holonomy decomposition [11, 12, 6, 8, 9, 3] is an important proof technique for the Krohn-Rhodes theory [1, Chapter 5], as it works with transformation semigroups, instead of abstract ones, and it is relatively close to the computer scientist's way of thinking. Our computer algebra package, `SgpDec` [5] is now a mature piece of software, so we can study the holonomy decompositions of semigroups with tens of thousands of elements. Here we concentrate on simpler examples and study the underlying structure of the holonomy decomposition, namely the *skeleton* of the transformation semigroup [6, 9]. It is important to note that this notion is different from the skeleton of an abstract semigroup (biordered set of idempotents) and from the topological concept with the same name.

Mathematical preliminaries

A *transformation semigroup* (X, S) is a finite nonempty set X (the state set) together with a set S of total transformations of X closed under function composition. A semigroup is a *monoid* if it contains the identity element, the identity map in case of transformations. The action on the points (states) $x \in X$ naturally extends to set of points: $P \cdot s = \{p \cdot s \mid p \in P\}$, $P \subseteq X$, $s \in S$. The set $\mathcal{O}(X) = \{X \cdot s \mid s \in S\}$ is the *orbit* of the state set. For finite transformations we use two different notations. The traditional matrix notation uses two rows, one for the elements of X and the second for their corresponding images. We also use the linear (one-line) notation defined in [7] with slight modifications described in [4]. The linear notation is a generalization of the cyclic notation for permutations, therefore the cycle decomposition works as usual. However, for collapsing states we use $[x_{i_1}, \ldots, x_{i_k}; x_i]$ meaning that $x_{i_j} \mapsto x_i$ for all $j \in \{1, \ldots, k\}$. These expressions can be nested recursively and blended with the cycle notation. This mirrors the fact that graphically a finite transformation is a bunch of cycles decorated with trees (incoming collapses). Examples are abundant in Section 3. The linear notation is proved to be very useful in software implementations and it is expected to soon have widespread use.

2. The skeleton

From now on we consider transformation monoids instead of transformation semigroups. From a categorical viewpoint this is a dangerous step (see [10, p22]), but in a computational setting it is natural. The *augmented orbit* of the state set under the action of the semigroup is $\mathcal{O}'(X) = \mathcal{O}(X) \cup \{X\} \cup \big\{\{x\} \mid x \in X\big\}$, i.e. we add the state set itself and the singletons. In case of a monoid, X is already in the orbit.

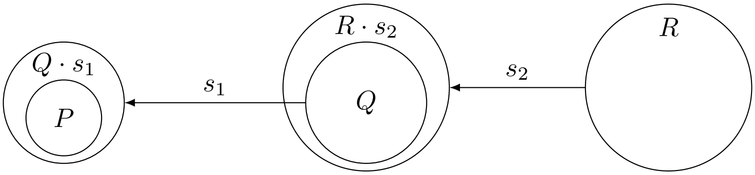
Definition 2.1 ([6, 9]). The *skeleton* of a transformation monoid (X, M) is the augmented orbit equipped with a preorder relation $(\mathcal{O}'(X), \subseteq_M)$. This relation is the generalized inclusion defined by

$$P \subseteq_M Q \iff \exists s \in M \text{ such that } P \subseteq Q \cdot s \quad P, Q \in \mathcal{O}'(X), \tag{2.1}$$

i.e. we can transform Q to include P under the action of M.

The skeleton is a feature of the monoid action, it does not depend on the actual generating set, therefore it is justified to talk about *the* skeleton of the transformation monoid.

It is easy to see that $\subseteq_M$ is a preorder: it is reflexive, since $P \subseteq P \cdot 1$, and it is transitive, since if $P \subseteq Q \cdot s_1$ and $Q \subseteq R \cdot s_2$ then $P \subseteq R \cdot s_2 s_1$, thus $P \subseteq_M R$.



We also define an equivalence relation on $\mathcal{O}'(X)$ by taking the generalized inclusion in both directions: $P \equiv_M Q \iff P \subseteq_M Q$ and $Q \subseteq_M P$. These equivalence classes are the *strong orbits* of the transformation monoid and are denoted by $O_1, \ldots, O_m$. For each equivalence class there will be a component in the hierarchical decomposition.

Height and depth of sets

The *height* of a set $Q \in \mathcal{O}'(X)$ is given by the function $h : \mathcal{O}'(X) \to \mathbb{N}$, which is defined by $h(Q) = 0$ if Q is a singleton, and for $|Q| > 1$, $h(Q)$ is defined by the length of the longest strict generalized inclusion chain(s) in the skeleton starting from a non-singleton set and ending in Q:

$$h(Q) = \max_i (Q_1 \subset_M \cdots \subset_M Q_i = Q),$$

where $|Q_1| > 1$. The height of (X, M) is $h = h(X)$.

It is also useful to speak of *depth* values, which are derived from the height values:

$$d(Q) = h(X) - h(Q) + 1.$$

The top level is depth 1.

Calculating the height values establishes the hierarchical levels in the decomposition, i.e. the number of coordinate positions in the holonomy decomposition is $h(X)$.

Covers

Considering the inclusion relation $(\mathcal{O}'(X), \subseteq)$, the set of *(lower) covers* of a subset $P \in \mathcal{O}'(X)$ is denoted by $\mathcal{C}(P)$. These are the maximal subsets of P. The component of the holonomy decomposition corresponding to a set P is derived from those elements of M that act on $\mathcal{C}(P)$, given that P is a chosen representative of some equivalence class. This action is a restriction of the action of M on $\mathcal{O}'(X)$. Obvious properties of covers are:

$$P = \bigcup_{i=1}^{k} P_i, \quad P_i \subseteq P_j \Longrightarrow P_i = P_j$$

where $P_i \in \mathcal{C}(P)$ and $k = |\mathcal{C}(P)|$.

3. Skeletons with salient features

Nonimage covers

Generalized inclusion by definition allows for the existence of (lower) covers of a set that are not images of the set, i.e. $P_i \in \mathcal{C}(P)$ but there is no $s \in M$ such that $P_i = P \cdot s$. However, we still have to show that these nonreachable maximal subsets are indeed possible. Let's consider the following generator set:
$a = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 1 & 1 & 1 \end{smallmatrix}\right) = [4, 5, 6; 1]$ has the image $\{1, 2, 3\}$,
$b = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 4 & 4 & 5 & 4 & 6 \end{smallmatrix}\right) = ([1, 2, 3; 4], 5)$ and $c = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 4 & 4 & 5 & 6 & 4 \end{smallmatrix}\right) = ([1, 2, 3; 4], 5, 6)$ produce the image $\{4, 5, 6\}$ and form a generator set (a transposition and a cycle) for the symmetric group S_3 acting on the image,
$d = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 4 & 4 & 4 & 5 & 5 \end{smallmatrix}\right) = [1, 2, 3; 4][6; 5]$ together with these point collapsings S_3 produce the images with cardinality 2,
$e = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 4 & 4 & 1 & 2 & 3 \end{smallmatrix}\right) = (1, [[5; 2], [6; 3]; 4])$ maps $\{4, 5, 6\}$ to $\{1, 2, 3\}$ (and permutes 1 and 4),
$f = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 4 & 4 \end{smallmatrix}\right) = (1, 2, 3)[5, 6; 4]$ is just a cycle on $\{1, 2, 3\}$.

The skeleton of the monoid they generate contains a set $\{1, 2, 3\}$ which has nonimage covers, see Fig. 1.

Unfortunately, the existence of nonimage covers makes a computational implementation slightly more complicated, as we really have to calculate with the generalized inclusion, which is the same as dealing with two relations (inclusion, and 'image of' relation).

Width

It is important to know the bound for the number of states in a component of a decomposition. These states are determined by the number of covering sets of the component's underlying set.

Proposition 3.1. *Let $\mathcal{C}(Q)$ be the set of covers of Q and $|Q| = m$, then*

$$|\mathcal{C}(Q)| \leqslant \binom{m}{\lfloor \frac{m}{2} \rfloor}.$$

Proof. $(2^Q, \subseteq)$ has a maximal antichain (a set of mutually incomparable elements) consisting of all subsets with $\lfloor \frac{m}{2} \rfloor$ elements. We then apply Dilworth's Theorem [2], which says that the width (the size of a largest antichain) of a partially ordered set is the same as the minimum number of chains whose union is the partially ordered set itself. This theorem implies that the number of chains needed to cover $(2^Q, \subseteq)$ is equal to $\binom{m}{\lfloor \frac{m}{2} \rfloor}$. Since $\mathcal{O}(X)$ does not necessarily equal 2^Q (it is a subset of it), we need the same number of or less chains to cover the elements of $\mathcal{O}(X)$ below Q in the inclusion relation, i.e. the subsets of Q. The number of chains covering

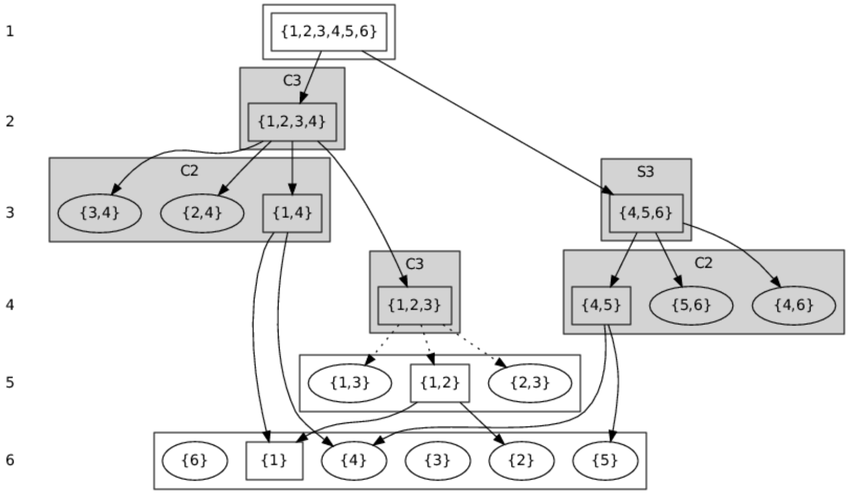


Figure 1: The skeleton of a monoid acting on 6 points (see text for the generators). The nodes are the elements of the augmented orbit. The boxes are the equivalence classes, the rectangular nodes the chosen representatives of a class. The box of the equivalence class is grey if there is a nontrivial subgroup of the monoid acting on the elements of the equivalence class (these groups are isomorphic on equivalent elements). The arrows point to the covers of a set. Dotted arrows indicate nonimage covers. On the side depth values are indicated.

$\mathcal{O}(X)$ below Q is at least the number of the maximal subsets of Q, which are the covers of Q by definition. □

We show that the maximum value can be achieved, so we have a sharp bound. We need the generators of the symmetric group S_n:

$$(2\ 3\ \ldots\ n-1\ 1), (2\ 1\ 3\ \ldots\ n)$$

and an arbitrary transformation t which collapses $\lceil \frac{n}{2} \rceil$ states, thus its rank is $\lfloor \frac{n}{2} \rfloor$. For instance a transformation t given by:

$$t(i) = \begin{cases} i & t \leqslant \lceil \frac{n}{2} \rceil \\ \lceil \frac{n}{2} \rceil & \text{otherwise.} \end{cases}$$

For a concrete example see Fig. 2.

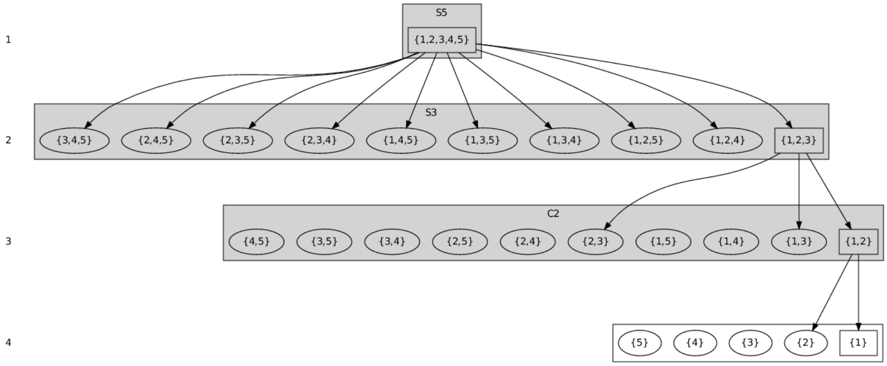


Figure 2: The skeleton of the monoid generated by $\{(1,2),(1,2,3,4,5),[4,5;3] = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 3 & 3 \end{smallmatrix}\right)\}$. The top node 5-element set has 10 covering sets.

Maximum height skeletons

Previous examples may suggest that height could be bounded by the size of the state set. This is far from being true. For instance the semigroup generated by $\{\left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 1 & 6 & 6 & 7 & 7 \end{smallmatrix}\right) = [[[[[3;1];2];4],5;6];7], \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 3 & 4 & 5 & 6 & 5 \end{smallmatrix}\right) = [[1;7];5], \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 3 & 5 & 6 & 7 \end{smallmatrix}\right) = [4;3]\}$ gives rise to a skeleton with height 21. It is easy to see why these high skeletons exist: it is possible to have strict generalized inclusion between sets of the same cardinality. For instance $\{3,4\} \subset_M \{1,2\}$ if M is generated by $s_1 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 1 & 1 \end{smallmatrix}\right) = [3,4;1]$ and $s_2 = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 3 & 4 \end{smallmatrix}\right) = [1;3][2;4]$, where s_1 produces the image $\{1,2\}$, s_2 takes it to $\{3,4\}$, but there is no transformation for the reverse direction.

We do not know an exact bound for the length of the holonomy decompositions yet, but we can summarize the observations of computational experiments.

Experimental observation 3.2. High skeletons tend to have a low number of nontrivial holonomy group components with small cardinality.

It seems that in order to build a high skeleton, we need sufficiently many elements in $\mathcal{O}(X)$, and that is provided by the nontrivial group components' permutations. But on the other hand, if we have a group component with high order, then its subgroups might also be components on lower levels, thus collapsing the hierarchy.

It has been shown [6, Chapter XI by Bret Tilson, pp. 287–312] that the length of the longest essential (containing a nontrivial group) $\mathcal{J}$-class chain in the semigroup (see cited reference for detailed definitions) is a lower bound for the length of the holonomy decomposition. Then the obvious guess would be that it is the same as the length of the longest $\mathcal{J}$-class chains in the semigroups. Again, computational experiments show that this is not the case. The length of the longest $\mathcal{J}$-chain can be smaller, equal to or bigger than the levels of the holonomy decomposition. This is due to the fact that in general we do not act on the semigroup itself but on another set.

4. Conclusions and future work

We carried out an initial analysis of hierarchical decompositions of transformation semigroups using the holonomy algorithm. We showed that when working with the components' state sets we have to deal with covers that are not images of the covered set. We also found a sharp upper bound for the width of the decomposition. However, other properties of the holonomy decomposition, including its height, still need further investigation.

References

[1] Arbib, M. A., editor, Algebraic Theory of Machines, Languages, and Semigroups, *Academic Press*, 1968.

[2] Dilworth, R. P., A decomposition theorem for partially ordered sets, *Annals of Mathematics*, 51 (1950) 161–166.

[3] Dömösi, P., Nehaniv, C. L., Algebraic Theory of Finite Automata Networks: An Introduction, volume 11. *SIAM Series on Discrete Mathematics and Applications*, 2005.

[4] Egri-Nagy, A., Nehaniv, C. L., On straight words and minimal permutators in finite transformation semigroups. *LNCS Lecture Notes in Computer Science*, 2010. Proceedings of the 15th International Conference on Implementation and Application of Automata CIAA, in press.

[5] Egri-Nagy, A., Nehaniv, C. L., `SgpDec` – software package for hierarchical coordinatization of groups and semigroups, implemented in the `GAP` computer algebra system, Version 0.5.25+, 2010. `http://sgpdec.sf.net`.

[6] Eilenberg, S., Automata, Languages and Machines, volume B, *Academic Press*, 1976.

[7] Ganyushkin, O., Mazorchuk, V., Classical Transformation Semigroups, *Algebra and Applications*, Springer, 2009.

[8] Ginzburg, A., Algebraic Theory of Automata, *Academic Press*, 1968.

[9] Holcombe, W. M. L. Algebraic Automata Theory, *Cambridge University Press*, 1982.

[10] Rhodes, J., Steinberg, B., The q-theory of Finite Semigroups, *Springer*, 2008.

[11] Zeiger, H. P., Cascade synthesis of finite state machines, *Information and Control*, 10 (1967) 419–433, plus erratum.

[12] Zeiger, H. P., Yet another proof of the cascade decomposition theorem for finite automata, *Math. Systems Theory*, 1 (1967) 225–228, plus erratum.

Attila Egri-Nagy
Eszterházy Károly College
Institute of Mathematics and Informatics
Department of Computing Science
Eger, Leányka út 4, Hungary
e-mail: attila@egri-nagy.hu

Chrystopher L. Nehaniv
Royal Society Wolfson BioComputation Research Lab
Centre for Computer Science & Informatics Research, University of Hertfordshire
Hatfield, Hertfordshire AL10 9AB, United Kingdom
e-mail: C.L.Nehaniv@herts.ac.uk