AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **30** (2004), Pages 95–101

Labelled Cayley graphs and minimal automata

A.V. Kelarev*

School of Computing
University of Tasmania
Private Bag 100, Hobart
Tasmania 7001
Australia

Abstract

Cayley graphs considered as language recognisers are as powerful as the more general finite state automata. This paper applies Cayley graphs to define a class of automata and describe minimal automata of this type, all their congruences and the Nerode equivalence of states.

Throughout, the word *graph* means a finite directed graph without multiple edges but possibly with loops, and $D = (V, E)$ is a graph. A *language* is a set of words over a finite alphabet X. For standard concepts of automata and languages theory the reader is referred to [5], [7], [14] and [16].

Let G be a groupoid, i.e., a set with a binary operation, and let S be a nonempty subset of G. The *Cayley graph* $\mathrm{Cay}(G, S)$ of G relative to S is defined as the graph with vertex set G and edge set $E(S)$ consisting of all ordered pairs (x, y) such that $xs = y$ for some $s \in S$. Cayley graphs of groups have received serious attention in the literature (see, in particular, [1], [2], [4]). They are significant both in group theory and in constructions of interesting graphs with nice properties.

If we are interested in language recognition, then the concept of a Cayley graph turns out to be as powerful as the more general notion of a finite state automaton (FSA). Indeed, if L is recognised by an FSA, then it is well known and easily verified that L is also recognised by the finite labelled Cayley graph of

$$\mathrm{Syn}(L) = X^*/\mu_L,$$

where μ_L is the the *Myhill congruence* on the free monoid X^* of all words over X:

$$\mu_L = \{(w_1, w_2) \mid \mathrm{Cont}_L(w_1) = \mathrm{Cont}_L(w_2)\},$$

* The author was supported by IRGS grant K12511 and by ARC Discovery grant DP0449469.

$$\mathrm{Cont}_L(w) = \{(a,b) \mid awb \in L\}.$$

Cayley graphs of groupoids have been used in [8] and [9] to define two-sided automata of labelled graphs and investigate properties of languages recognized by them. The aim of this paper is to give necessary and sufficient conditions for a two-sided automaton of this type to be minimal. To this end we describe all congruences on these FSA and, in particular, Nerode equivalences on the sets of states.

Let $\ell : X \to \{+,-\}$ and $f : X \to V$ be any mappings, and let T be a subset of V. The *two-sided automaton* $\mathrm{Atm}(D) = \mathrm{Atm}(D,T) = \mathrm{Atm}(D,T,f,\ell)$ of the graph D is the (possibly incomplete) finite state acceptor with

(DA1) the set of states $V \cup \{1\}$;

(DA2) the initial state 1;

(DA3) the set of terminal states T;

(DA4) the next-state function given, for a state u and a letter $x \in X$, by the rule

$$u \cdot x = \begin{cases} f(x) & \text{if } \ell(x) = + \text{ and } (u, f(x)) \in E, \text{ or if } u = 1, \\ u & \text{if } \ell(x) = - \text{ and } (f(x), u) \in E. \end{cases}$$

If a vertex $v \in V$ does not belong to $f(X)$, then this state is inaccessible in $\mathrm{Atm}(D,T)$, and so without loss of generality we may assume that all vertices are images of letters of the alphabet X.

Let $Y \subseteq V$, and let ϱ be an equivalence relation on Y. The class of ϱ containing x is denoted by x/ϱ. If there is no need to indicate the set Y explicitly, we may call the equivalence relation an *incomplete* equivalence relation on V. Often we omit the word 'incomplete' when there is no ambiguity. The set Y is called the *ground set* of ϱ, and is denoted by G_ϱ. An incomplete equivalence relation ϱ on the set of states of $\mathrm{Atm}(D,T)$ is called an incomplete *congruence* if it defines the quotient automaton recognizing the same language. Defining the quotient automaton modulo an incomplete congruence, as usual, one has to drop all states which do not belong to the ground set of the congruence, and then introduce a new transition function on the set of all equivalence classes of the relation. Hence ϱ is an incomplete congruence if and only if the following conditions hold, for all $a, b \in V \cup \{1\}$, $x \in X$,

(C1) if $(a,b) \in \varrho$ and $a \cdot x$ is defined, then $b \cdot x$ is defined too, and $(a \cdot x, b \cdot x) \in \varrho$;

(C2) if $(a,b) \in \varrho$ and $a \in T$, then $b \in T$;

(C3) $(1,1) \in \varrho$ and the class containing 1 is a singleton;

(C4) if $1 \cdot x_1 \cdots x_n \in T$ for some $x_1, \ldots, x_n \in X$, then

$$x_1, \ldots, x_n, 1 \cdot x_1, 1 \cdot x_1 x_2, \ldots, 1 \cdot x_1 \cdots x_n \in G_\varrho.$$

Let ϱ_1 and ϱ_2 be incomplete relations with ground sets S_1 and S_2, respectively. Then we write $\varrho_1 \leq \varrho_2$ if $S_1 \supseteq S_2$ and $\varrho_1 \cap (S_2 \times S_2) \subseteq \varrho_2$. The largest incomplete congruence on $\mathrm{Atm}(D, T)$ is the *Nerode equivalence* η_T described by

$$\begin{aligned}\eta_T \;=\; & \{(1,1)\} \cup \{(a,b) \mid a \cdot u \in T \text{ iff } b \cdot u \in T \text{ for all } u \in X^*; \\ & \text{and } (a \cdot X^*) \cap T \neq \emptyset\} \end{aligned} \tag{1}$$

(see, e.g., [5] or [16]). Denote the equality relation on $\mathrm{Atm}(D, T)$ by ι. A congruence is said to be *proper* if it is distinct from ι and η_T. The following sets of letters and vertices are used in our main theorem and proofs:

$$\begin{aligned}
X^{(+)} &= \{x \in X \mid \ell(x) = +\}, \\
X^{(-)} &= \{x \in X \mid \ell(x) = -\}, \\
V^{(+)} &= \{v \in V \mid \exists x \in X^+, f(x) = v\}, \\
V^{(-)} &= \{v \in V \mid \exists x \in X^{(-)}, f(x) = v\}.
\end{aligned}$$

Note that the intersection $V^{(+)} \cap V^{(-)}$ may be nonempty in general. If $v \in V$ and $S \subseteq V$, then put

$$\begin{aligned}
\mathrm{In}^-(v) &= \{w \in V^{(-)} \mid (w, v) \in E\}, \\
\mathrm{Out}^+(v) &= \{w \in V^{(+)} \mid (v, w) \in E\}, \\
\mathrm{In}^-(S) &= \cup_{s \in S} \mathrm{In}^-(s), \\
\mathrm{Out}^+(S) &= \cup_{s \in S} \mathrm{Out}^+(s).
\end{aligned}$$

For a subset S of V, define new equivalence relations

$$\alpha_S = \{(1,1)\} \cup \{(a,b) \mid a, b \in V \setminus S, \mathrm{In}^-(a) = \mathrm{In}^-(b)\}, \tag{2}$$

$$\Theta(T) = \{(1,1)\} \cup (T \times T) \cup ((V \setminus T) \times (V \setminus T)), \tag{3}$$

and consider auxiliary sets

$$\begin{aligned}
\beta_S^T &= \{(a,b) \mid \mathrm{Out}^+(a) \setminus S = \mathrm{Out}^+(b) \setminus S \text{ and } a, b \in T\}, \\
\beta_S^{V \setminus T} &= \{(a,b) \mid \mathrm{Out}^+(a) \setminus S = \mathrm{Out}^+(b) \setminus S \text{ and } a, b \in V \setminus T\}.
\end{aligned}$$

We introduce new relation β_S as the following disjoint union

$$\beta_S = \{(1,1)\} \cup \beta_S^T \cup \beta_S^{V \setminus T}. \tag{4}$$

Clearly, β_S is an equivalence relation on the set of states of $\mathrm{Atm}(D, T)$. Our main theorem describes all incomplete congruences on the automaton $\mathrm{Atm}(G, T, f, \ell)$.

A *path* in the graph $D = (V, E)$ means a directed path, i.e., a sequence of vertices $v_0, v_1, \ldots, v_n$ such that $(v_i, v_{i+1}) \in E$ for $i = 0, 1, \ldots, n-1$. Denote by T_+ the set of all elements $v \in V$ such that either $v \in T$ or there exist a vertex $t \in T \cap V^{(+)}$ and a path $v = v_0, v_1, \ldots, v_n = t$, from v to t with $n \geq 1$ and all vertices $v_1, \ldots, v_n$ in $V^{(+)}$. Let $C = C_D$ be the set of all vertices $c \in V$ such that $c \notin T_+$ and if $c \in V^{(-)}$ then $(v, c) \notin E$ for all $v \in T_+$.

THEOREM 1 *The automaton* $\mathrm{Atm}(D,T,f,\ell)$ *is minimal if and only if*

$$\alpha_\emptyset \cap \beta_\emptyset \cap \Theta(T) = \iota,$$

and for each $c \in V^{(-)}$ *either* $c \in T_+$ *or there exists* $v \in T_+$ *such that* $(v,c) \in E$.

THEOREM 2 *Let* ϱ *be an incomplete equivalence relation on* $\mathrm{Atm}(D,T,f,\ell)$*, and let* $S = V \setminus G_\varrho$*. Then* ϱ *is a congruence of this automaton if and only if* S *is a subset of* C_D *and*

$$\varrho \subseteq \alpha_S \cap \beta_S \cap \Theta(T). \tag{5}$$

COROLLARY 3 *The Nerode equivalence on* $\mathrm{Atm}(D,T,f,\ell)$ *is equal to*

$$\eta = (\alpha_S \cap \beta_S \cap \Theta(T)) \setminus (C_D \times C_D). \tag{6}$$

Proof of Theorem 2. The 'only if' part. Take any incomplete congruence ϱ of the automaton $\mathrm{Atm}(D,T,f,\ell)$.

Let us begin by showing that condition (C4) implies that $S = V \setminus G_\varrho$ is a subset of $C = C_D$. To this end consider any vertex v which does not belong to C. All we have to verify is that v lies in G_ϱ. In view of the definitions of C the following cases may occur.

Case 1. $v \in T$. Then $1 \cdot v = v \in T$, and so $1 \cdot v \in G_\varrho$ by condition $(C4)$.

Case 2. $v \notin T$ and $v \in T_+$. Then the definition of T_+ means that there exist a vertex $t \in T \cap V^{(+)}$ and a path $v = v_0, v_1, \ldots, v_n = t$, from v to t with $n \geq 1$ and all vertices $v_1, \ldots, v_n$ in $V^{(+)}$. By the definition of $\mathrm{Atm}(D,T,f,\ell)$ we get

$$1 \cdot v_0 v_1 \ldots v_n = t \in T.$$

Hence condition (C4) yields $v = 1 \cdot v_0 \in G_\varrho$.

Case 3. $c \in V^{(-)}$ and $(v,c) \in E$ for some $v \in T$. By (DA4), $1 \cdot vc = v \in T$. Therefore $v = 1 \cdot v \in G_\varrho$ in view of (C4).

Case 4. $c \in V^{(-)}$ and $(v,c) \in E$ for some $v \in T_+$, $v \notin T$. Then there exist $t \in T \cap V^{(+)}$ and a path $v = v_0, v_1, \ldots, v_n = t$, from v to t with $n \geq 1$ and all vertices $v_1, \ldots, v_n$ in $V^{(+)}$ such that $(v,c) \in E$. It follows from (DA4) that

$$1 \cdot vcv_1v_2 \cdots v_n = t \in T.$$

Hence (C4) implies $v \in G_\varrho$ again.

Thus in all cases it follows from (C4) and the definition of $\mathrm{Atm}(D,T,f,\ell)$ that $v \in G_\varrho$. This means that $S \subseteq C$.

In order to verify the inclusion (5), pick an arbitrary pair (a,b) in ϱ. We have to check that (a,b) belongs to all three equivalence relations in the right hand side of (5). Since $(1,1)$ belongs to all of them, by (C3) we may assume $a, b \neq 1$. Condition (C2) shows that (a,b) always lies in $\Theta(T)$. Therefore it remains to prove that (a,b) belongs to $\alpha_S \cap \beta_S$.

Suppose to the contrary that $(a, b) \notin \alpha_S$. Since $S = V \setminus G_\varrho$ and $\varrho \subseteq G_\varrho \times G_\varrho$, we have $a, b \notin S$. Therefore it follows from the definition of α_S that $\mathrm{In}^-(a) \neq \mathrm{In}^-(b)$. We may assume that there exists $u \in \mathrm{In}^-(a) \setminus \mathrm{In}^-(b)$. Choose x in $X^{(-)}$ such that $f(x) = u$. Then $ax = a$ and bx is undefined. This contradicts condition (C1) and shows that $(a, b) \in \alpha_S$.

If there exists an element u in $\mathrm{Out}^+(a) \cap \overline{S} \setminus \mathrm{Out}^+(b) \cap \overline{S}$, then $u = f(x)$ for some $x \in X^{(+)}$; whence $ax = x$ and bx is undefined, a contradiction to (C1). Therefore $\mathrm{Out}^+(a) \cap \overline{S} \subseteq \mathrm{Out}^+(b) \cap \overline{S}$. The reversed inclusion is proven in exactly the same way; whence

$$\mathrm{Out}^+(a) = \mathrm{Out}^+(b). \tag{7}$$

In proving that $(a, b) \in \beta$ first note that if $a, b \in T$, then $\mathrm{Out}^+(a) = \mathrm{Out}^+(b)$ implies $(a, b) \in \beta^T$. If, however, a or b is not in T, then $a, b \in V \setminus T$ as indicated above. Hence $(a, b) \in \beta^{V \setminus T}$ again, and we get $(a, b) \in \beta$. Therefore $(a, b) \in \beta$ in both cases. Thus (5) is satisfied.

The 'if' part. Let ϱ be an incomplete equivalence relation such that $S = V \setminus G_\varrho$ is a subset of C and the inclusion (5) holds. We claim that ϱ is a congruence.

Indeed, since $\varrho \subseteq \Theta(T)$, conditions (C2) and (C3) are obvious. In order to verify (C1), choose an arbitrary pair $(a, b) \in \varrho$ and $x \in X$ such that ax is defined. Note that $a, b \notin S$ by the definition of G_ϱ. The following cases are possible.

Case 1: $\ell(x) = -$. Since $(a, b) \in \alpha_S$, we get $\mathrm{In}^-(a) = \mathrm{In}^-(b)$. If $f(x) \notin \mathrm{In}^-(a)$, then ax and bx are undefined. This contradiction shows that $f(x) \in \mathrm{In}^-(a)$. Therefore $ax = a$, $bx = b$, and so $(ax, bx) \in \varrho$.

Case 2: $\ell(x) = +$. Since $(a, b) \in \beta$, we get $\mathrm{Out}^+(a) \setminus S = \mathrm{Out}^+(b) \setminus S$. If $f(x) \notin \mathrm{Out}^+(a)$, then ax and bx are undefined, a contradiction. Therefore $f(x) \in \mathrm{Out}^+(a) \setminus S \subseteq \mathrm{Out}^+(b)$, and so bx is defined too. It follows that $(ax, bx) = (f(x), f(x)) \in \varrho$, because $\ell(x) = +$.

Thus, if ax is defined, then (ax, bx) always belongs to ϱ, i.e., (C1) holds.

It remains to prove condition (C4). Choose any elements $x_1, \ldots, x_n \in X$ such that $1 \cdot x_1 \cdots x_n \in T$. All we have to verify is that $x_1, \ldots, x_n$, $1 \cdot x_1$, $1 \cdot x_1 x_2, \ldots$, $1 \cdot x_1 \cdots x_n$ are not in S.

Denote by $i_1, i_2, \ldots, i_m$ all integers such that $x_{i_1}, \ldots, x_{i_m} \in X^{(+)}$ and $i_1 \le i_2 \le \cdots \le i_m$. Clearly, all $x_{i_1}, \ldots, x_{i_m}$ are in T_+. Consider any k such that $1 \le k \le n$.

First, suppose that $\ell(x_k) = +$. Then $k = \ell_q$ for some q, and $x_q = 1 \cdot x_1 \cdots x_n$.

If $q = m$, then it follows from (DA4) that $x_q = 1 \cdot x_1 \cdots x_n \in T$. Hence $1 \cdot x_1 \cdots x_q = x_q \notin C$.

If $q < m$, then (DA4) implies

$$1 \cdot x_q \cdots x_n = 1 \cdot x_1 \cdots x_n \in T$$

Hence $x_q \in T^+$, and so $1 \cdot x_1 \cdots x_q = x_q \notin C$ again.

Second, consider the case where $\ell(x_k) = -$.

If $i_1 > k$, then $1 \cdot x_1 \cdots x_q = x_1 \in T_+$. This equality immediately implies that

$1 \cdot x_1 \cdots x_q \notin C$. Besides, the same equality together with the definition of C via T_+ yield that $x_q \notin C$.

If $i_1 \leq k$, then denote by r the maximum integer with $i_r \leq k$. We get $1 \cdot x_1 \cdots x_q = x_{i_r} \in T_+$. This equality immediately shows that $1 \cdot x_1 \cdots x_q \notin C$. Besides, the same equality together with the definition of C also yield that $x_q \notin C$.

Thus we see that x_q and $1 \cdot x_1 \cdots x_q$ are not in C. Therefore they do not belong to $S \subseteq C$. This means that (C4) is satisfied, which completes the proof. □

Proof of Corollary 3 follows immediately from Theorem 2, because the Nerode equivalence is the largest congruence and the intersection in the right hand side of (5) is an equivalence relation. □

Proof of Theorem 1. An automaton is minimal if and only if its Nerode equivalence is the identity relation. Hence the proof follows from the definition of the set C_D and Theorem 2 or Corollary 3. □

References

[1] L. Babai, Automorphism groups, isomorphism, reconstruction, in *Handbook of Combinatorics*, Elsevier Sci., 1995, 1447–1540.

[2] N. Biggs, *Algebraic Graph Theory*, Cambridge University Press, 1994.

[3] D. Gusfield, *Algorithms on Strings, Trees, and Sequences*, Cambridge University Press, 1997.

[4] M.-C. Heydemann, Cayley graphs and interconnection networks, in *Graph Symmetry: Algebraic Methods and Applications* (Montreal, Canada, July 1–12, 1996), Kluwer, Dordrecht, 1997, 167–224.

[5] M. Ito, *Algebraic Theory of Automata and Languages*, World Scientific, New York, 2001.

[6] A. V. Kelarev, On undirected Cayley graphs, *Australas. J. Combin.* **25** (2002), 73–78.

[7] A. V. Kelarev, *Graph Algebras and Automata*, Marcel Dekker, 2003.

[8] A. V. Kelarev, M. Miller and O. V. Sokratova, Directed graphs and closure properties for languages, *12th Australasian Workshop on Combinatorial Algorithms* (Ed. E.T. Baskoro), 2001, 118–125.

[9] A. V. Kelarev, M. Miller and O. V. Sokratova, Languages recognized by two-sided automata of graphs, *Proc. Estonian Academy of Science*, to appear.

[10] A. V. Kelarev and C. E. Praeger, On transitive Cayley graphs of groups and semigroups, *European J. Combinatorics* **24** (2003), 59–72.

[11] A. V. Kelarev and O. V. Sokratova, *Languages recognized by a class of finite automata*, Acta Cybernetica **15** (2001), 45–52.

[12] A. V. Kelarev and O. V. Sokratova, *On congruences of automata defined by directed graphs*, Theoretical Computer Science, in press.

[13] G. Lallement, *Semigroups and Combinatorial Applications*, Wiley, New York, 1979.

[14] G. Păun and A. Salomaa (Eds.), *New Trends in Formal Languages*, Springer-Verlag, Berlin, 1997.

[15] J. E. Pin (Ed.), *Formal Properties of Finite Automata and Applications*, Lec. Notes Comp. Science 386, Springer, New York, 1989.

[16] G. Rozenberg, A. Salomaa (Eds.), *Handbook of Formal Languages*, Vol. 1, 2, 3, Springer, New York, 1997.

(Received 14 Dec 2002)