Decidability of the Multiplicity Equivalence of Multitape Finite Automata

T. HARJU AND J. KARHUMÄKI

DEPT. OF MATHEMATICS
UNIVERSITY OF TURKU
SF-20500 TURKU, FINLAND

ABSTRACT. Using a result of B.H. Neumann we extend Eilenberg's Equality Theorem, [E], to a general result which implies that the multiplicity equivalence problem of two (nondeterministic) multitape finite automata is decidable. As a corollary we solve a long standing open problem in automata theory, namely, the equivalence problem for multitape deterministic finite automata.

1. INTRODUCTION

One of the oldest and most famous problems in automata theory is the equivalence problem for deterministic multitape finite automata. The notion of multitape finite automaton, or multitape automaton for short, was introduced by Rabin and Scott in their classic paper of 1959, [RS]. They also showed that, unlike for ordinary (one-tape) finite automata, nondeterministic multitape automata are more powerful than the deterministic ones. This holds already in the case of two tapes.

As a central model of automata, multitape automata have gained plenty of attention. However, many important problems have remained open, including the equivalence problem in the deterministic case. For nondeterministic multitape automata (even for two-tape automata, which are normally called finite transducers) the equivalence problem is a standard example of an undecidable problem, see [Be]. This undecidability result was first proved in 1968 by Griffiths, [G].

The equivalence problem of multitape deterministic automata has, as far as we know, been expected to be decidable. It seems that in this context "equivalence" implies "structural similarity". Despite this the equivalence problem has been solved only in a few special cases. The oldest result is that of Bird from 1973,[Bi] which solves the problem for two-tape deterministic automata. An alternative solution to the two-tape case was given in [V]. Numerous attempts, see [L], [Ki], [CK], to solve the general problem have lead to only modest success so far. The difficulty of the equivalence problem is already manifested in the fact that the inclusion problem for multitape deterministic automata is easily seen to be undecidable.

Our approach is as follows. Instead of deterministic multitape automata we consider nondeterministic multitape automata with multiplicities. Thus we ask whether two given multitape automata are *multiplicitly equivalent*, that is, whether they accept the same n-tuples of words exactly the same number of times. The multiplicity equivalence clearly reduces to ordinary equivalence if the automata are deterministic, and even when they are unambiguous. The multiplicity equivalence problem for finite transducers has been considered an important open problem of its own, see [Ka].

Consequently, we attack a nontrivial generalization of one of the famous open problems in automata theory. Hence a few explaining words are in order. First of all, intuitively, the deterministic behaviour of nondeterministic devices is in a sense captured by multiplicities. A nice example of this correspondence is Eilenberg's Equality Theorem, [E]. It shows that in order to test the equivalence of two deterministic (one-tape) automata and to test the multiplicity equivalence of two nondeterministic (one-tape) automata it is enough to consider the computations of exactly the same lengths (in terms of the size of state sets). Secondly, the multiplicity considerations provide new tools to attack the original problem. Indeed, as shown by Eilenberg's proof of Equality Theorem, methods of classical algebra become applicable. This turns out decisive.

Eilenberg showed that the multiplicity equivalence of one-tape automata is decidable when the multiplicities are taken from a subsemiring R of a field. Eilenberg's proof extends immediately to one-tape automata, where the multiplicities are taken from a subsemiring R of a division ring. In particular, the semiring R need not be commutative. The more general form of the semiring R yields a proof of the decidability of the multiplicity equivalence problem for the multitape automata.

Here we need a result of B.H. Neumann, [N], which states that the ring of all formal power series over a fully ordered group and well ordered supports is a division ring.

For the elementary results of division rings we refer to [J]. Formal power series in connection to automata theory are well treated in [SS] and [BR]. Fully ordered groups and the results needed for these, including the above mentioned Neumann's result, can be found in [F] and in a more general setting in [C] and [P]. For the automata theoretic prerequisites we refer to [Be] and [E].

2. Reduction to One-Tape Automata

The following definition of a nondeterministic multitape automaton with multiplicities from a given semiring R is in accordance with Eilenberg's definition of the corresponding one-tape automaton in [E]. We assume that a semiring always contains an identity element.

Let Σ_i be alphabets for $i = 1,2,\ldots,n$, and let Σ_i^* be the free monoids generated by Σ_i. We denote the empty word by 1. Let $S = \Sigma_1^* \times \Sigma_2^* \times \cdots \times \Sigma_n^*$. For an element $s = (s_1,\ldots,s_n) \in S$ we let the *length* of s be the sum $|s| = \sum_{i=1}^n |s_i|$ of the lengths of its components. Clearly, S is generated as a monoid by the elements of length one. We denote this generator set by $S^{(1)}$.

Let R be a semiring. An *R-S-automaton* is defined as $A = (Q, E, \mu, I, T)$, where Q is a finite set of states, $E \subseteq Q \times S \times Q - Q \times (1,1,\ldots,1) \times Q$ is a finite set of transitions, $\mu : E \to R$ is a multiplicity function, I is a set of initial states and T is a set of final states.

We assume that an R-S-automaton reads at least one symbol from one of its tapes in each step of a computation, that is, we do not allow transitions of the form $(q,1,1,\ldots,1,p)$. In fact, the multiplicity equivalence problem for finite transducers is undecidable if we allow the transitions which read and write the empty word. To see this consider two finite transducers T_1 and T_2 and define two new transducers by adding the loops $(q,1,1,q)$ to each state q of T_1 and T_2, respectively. The new transducers have infinitely many computations for each input-output pair and, consequently the original transducers are equivalent (without multiplicity) just in case the modified transducers are multiplicitly equivalent. Hence the undecidability follows.

A *computation* of A is any sequence $p = e_1 \cdot e_2 \cdot \ldots \cdot e_k$ of transitions such that $e_i = (q_{i-1}, s_i, q_i) \in E$ $(i = 1,2,\ldots,k)$. The *label* of p is the element $s = s_1 \cdot s_2 \cdot \ldots \cdot s_k$, and p is *successful* if q_0 is an initial state and q_k is a final state. The *multiplicity* of p is the element $p\mu = e_1\mu \cdot \ldots \cdot e_k\mu$ of R. The *multiplicity* of an element $s \in S$ is defined as the sum $sA = \sum_p p\mu$ over all successful computations with label s. Thus an R-S-automaton A defines a mapping $A : S \to R$.

An R-S-automaton A is in a *normal form* if its transitions are in $Q \times S^{(1)} \times Q$. Each R-S-automaton A can be transformed to a multiplicitly equivalent R-S-automaton which is in a normal form by dissecting the transitions $e \in E$ of A to computations in a standard way. The function μ must be modified so that it gives the value 1 for all but one of the added transitions, the remaining transition obtains the value $e\mu$ of the original transition.

Let M be an arbitrary monoid and consider the set of all formal power series, $R\langle\langle M \rangle\rangle$, over M with coefficients in the semiring R. Define the sum and product in $R\langle\langle M \rangle\rangle$ in a natural way:

$$\sum_s n_s s + \sum_s m_s s = \sum_s (n_s + m_s)$$

and

$$(\sum_s n_s s)(\sum_s m_s s) = \sum_s (\sum_{uv=s} n_u m_v) s.$$

We note that the product in $R\langle\langle S\rangle\rangle$ is well defined for our choice of S. In fact, the product is needed here only in the polynomial semiring $R\langle S\rangle$ which consists of all finite formal sums $\sum_{s\in S} n_s s$ and which is a subsemiring of $R\langle\langle S\rangle\rangle$. However, in Section 3 formal power series over (fully ordered) groups are used and then the product is not automatically well defined any more.

We now reduce the multiplicity equivalence problem of R-S-automata to the multiplicity equivalence problem of one-tape automata over a one-letter alphabet $\Sigma = \{a\}$ which takes the multiplicities from the polynomial semiring $R\langle S\rangle$.

Let $A = (Q, E, \mu, I, T)$ be an R-S-automaton in normal form and define an $R\langle S\rangle$-Σ^*-automaton $A^{(a)} = (Q, E^{(a)}, \mu^{(a)}, I, T)$ by setting

$$E^{(a)} = \{(q, a, p) \mid (q, s, p) \in E\}$$

and

$$(q, a, p)\mu^{(a)} = \sum_{s\in S^{(1)}} (q, s, p)\mu \cdot s.$$

THEOREM 2.1. *Let A_1 and A_2 be R-S-automata in normal form. Then $sA_1 = sA_2$ for all $s \in S$ if and only if $uA_1^{(a)} = uA_2^{(a)}$ for all $u \in \Sigma^*$.*

PROOF: Every successful computation in A_i, $i = 1, 2$, labeled by s has length $|s|$. Thus $sA_1 = sA_2$ for all $s \in S$ if and only if for all $k \geq 0$, $sA_1 = sA_2$ for all s with $|s| = k$. This is equivalent to $\sum_{|s|=k}(sA_1)s = \sum_{|s|=k}(sA_2)s$ for all k. But $\sum_{|s|=k}(sA_i)s = a^k A_i^{(a)}$ for $i = 1, 2$ and hence the claim follows. □

3. DECIDABILITY RESULTS

We firstly restate Eilenberg's Equality Theorem, [E,pp 143 - 145], for division rings.

THEOREM 3.1. *Let R be a subsemiring of a division ring. Then normal form R-Σ^*-automata A_1 and A_2 are multiplicitly equivalent if and only if $sA_1 = sA_2$ for all $s \in \Sigma^*$ with $|s| < card(Q_1) + card(Q_2)$, where Q_i is the state set of A_i for $i = 1, 2$.*

The proof in [**E**] for a subsemiring of a (commutative) field K is based on the following properties of fields: Let V be a finite dimensional vector space over the field K. If U is a subspace of V then the dimension of U is at most that of V and if U has the same dimension as V then $U = V$. This dimension result is equally valid for division rings, see [**J**], and hence the proof of Theorem 8.1 of [**E**] generalizes as such to subsemirings of division rings.

Our next step is to use a result of Neumann, [**N**]. We refer also to [**C**], [**F**] and [**P**] for this result. We start by introducing the power series needed in the next theorem.

A group G is said to be *fully ordered* if there exists a linear ordering $\leq$ of G, which respects right and left multiplication: for all g, h, t, if $g < h$ then $gt < ht$ and $tg < th$. Let P be a division ring, G a fully ordered group and let $B = \sum_g n_g g \in P\langle\langle G\rangle\rangle$. The *support* of B is the set $\{g \in G : n_g \neq 0\}$. Let $P_{wo}\langle\langle G\rangle\rangle$ denote the family of all series from $P\langle\langle G\rangle\rangle$ with well ordered support, i.e., the series for which every subset of the support has a least element with respect to the ordering of G. The well ordered power series are used instead of the general power series in order to obtain a ring structure. Indeed, the product of two (general) series from $P\langle\langle G\rangle\rangle$ is not necessarily well defined, see e.g. [**C**].

THEOREM 3.2. *Let G be a fully ordered group and P a division ring. Then $P_{wo}\langle\langle G\rangle\rangle$ is a division ring containing $P\langle G\rangle$ as a subring.*

We need the result that every direct product of free groups is fully ordered. It is by no means an easy task to fully order a free group. This can be done using a general result of Neumann stating that a group G is fully ordered if the factor groups in the lower central series of G are torsion-free and the series terminates at the trivial group. The Magnus-Witt theorem says that the free groups possess this lower series property. Another proof makes use of the following Vinogradov's result, see [**P**]: The free product of fully ordered groups is again fully ordered. Now a free group is a free product of cyclic groups and since the cyclic groups are easily fully ordered we obtain the result for free groups.

THEOREM 3.3. *Every free group is fully ordered.*

Moreover, if the groups $G_1, \ldots, G_k$ are fully ordered then their direct product $G_1 \times G_2 \times \cdots \times G_k$ can also be fully ordered. To see this let $\leq_i$ be the full ordering for G_i, $i = 1, 2, \ldots, k$, and define the ordering $\leq$ for $G_1 \times G_2 \times \cdots \times G_k$ by: $(g_1, \ldots, g_k) < (h_1, \ldots, h_k)$

if and only if there is a j such that $g_j < h_j$ and for all $i < j$, $g_i = h_i$. Clearly, the ordering $\leq$ is a full ordering in the direct product.

THEOREM 3.4. *The direct product of fully ordered groups is fully ordered.*

If M is a submonoid of a fully ordered group G then $P\langle M\rangle$ is a subsemiring of $P\langle G\rangle$ and the latter is contained in the division ring $P_{wo}\langle\langle G\rangle\rangle$. Hence

THEOREM 3.5. *Let M be a submonoid of a fully ordered group and let P be a division ring. Then $P\langle M\rangle$ is a subsemiring of a division ring.*

The direct product $S = \Sigma_1^* \times \Sigma_2^* \times \cdots \times \Sigma_k^*$ of the free monoids Σ_i^* is a submonoid of the fully ordered group $F_1 \times F_2 \times \cdots \times F_k$, where F_i is the free group generated by Σ_i for $i = 1, 2, \ldots, k$. Thus combining the previous results with Theorem 2.1 we obtain the following theorem.

THEOREM 3.6. *Let S be a direct product of free monoids and let R be a subsemiring of a division ring. For two normal form R-S-automata A_1 and A_2, $sA_1 = sA_2$ for all $s \in S$ if and only if $sA_1 = sA_2$ for all s with $|s| < card(Q_1) + card(Q_2)$, where Q_i is the state set for A_i, $i = 1, 2$.*

Thus the multiplicity equivalence problem for R-S-automata satisfying the demands of the previous theorem reduces to testing the equality for a finite set of elements. The effectiveness of the testing depends on the semiring R. To be more precise let $A_i = (Q_i, E_i, \mu_i, I_i, T_i)$ for $i = 1, 2$ be two R-S-automata and let $k = \text{card}(Q_1) + \text{card}(Q_2)$. Then A_1 and A_2 are multiplicitly equivalent if and only if $sA_1 = sA_2$ for all $s \in S$ with $|s| < k$, where $sA_i \in R\langle S\rangle$ is a polynomial over R. In particular, if R is $\mathbb{N}$ or $\mathbb{Q}$, the equivalence of two polynomials becomes decidable.

THEOREM 3.7. *Let S be a direct product of finitely many free monoids. Then it is decidable whether or not two $\mathbb{Q}$-S-automata are multiplicitly equivalent.*

We obtain the *n-tape finite automata* as $\mathbb{Q}$-S-automata by setting the multiplicity $e\mu$ equal to 1 for all transitions $e = (p, s, q)$ of the automaton.

THEOREM 3.8. *The multiplicity equivalence problem for n-tape finite automata is decidable.*

An n-tape finite automaton A is *unambiguous* if for each $s \in S$ there is at most one computation of A which accepts s. Hence A is unambiguous if and only if $s\mu = 1$ when A accepts s and $s\mu = 0$ otherwise. In this case the semiring R does not play any role and by the above theorem we can decide whether two given unambiguous n-tape finite automata are equivalent. We note here that it is undecidable to determine whether a multitape automaton is unambiguous.

No matter how an *n-tape deterministic finite automaton* is defined in details, it is natural to require the unambiguity.

THEOREM 3.9. *The equivalence problem for the n-tape deterministic finite automata is decidable.*

ACKNOWLEDGEMENT. The authors are grateful to G. Duchamp and J. Sakarovitch for their critical comments which improved the presentation of this paper.

REFERENCES

[Be] Berstel, J., *Transductions and Context-Free Languages*, B.G. Teubner, Stuttgart, 1979.

[BR] Berstel, J. and Reutenauer, C., *Rational Series and Their Languages*, Springer-Verlag, Berlin, 1988.

[Bi] Bird, M., The equivalence problem for deterministic two-tape automata, *J. Comput. System Sci.* 7 (1973) 218 - 236.

[C] Cohn, P.M., *Free Rings and their Realtions*, Academic Press, New York London, 1985 (2nd ed).

[CK] Culik II, K. and Karhumäki, J., IIDTOL matching of computations of multitape automata, *Acta Informatica*, to appear.

[E] Eilenberg, S., *Automata, Languages, and Machines, Vol.A*, Academic Press, New York, 1974.

[F] Fuchs, L., *Partially Ordered Algebraic Systems*, Pergamon Press, Oxford, 1963.

[G] Griffiths, T.V., The usolvability of the equivalence problem for λ-free nondeterministic generalized machines, *JACM* 15 (1968) 409 - 413.

[J] Jacobson, N., *Lectures in Abstract Algebra, Vol. II*, Van Nostrand, New York, 1953.

[Ka] Karhumäki, J., On recent trends in formal language theory, *Lecture Notes in Computer Science* 267,

136 - 162, Springer-Verlag, New York, 1987.

[Ki] Kinber, E., The inclusion problem for some classes of deterministic multitape automata, *Theoret. Comput. Sci.* 26 (1983) 1 - 24.

[L] Lewis, H.R., A new decidability problem with applications, *Proceedings of 18th FOCS Conference* (1979) 62 - 73.

[N] Neumann, B.H., On ordered division rings, *Trans. Amer. Math. Soc.*, 66 (1949) 202 - 252.

[P] Passman D.S., *The Algebraic Structure of Group Rings*, John Wiley & Sons, New York, 1977.

[RS] Rabin, M. and Scott, D., Finite automata and their decision problems, *IBM J. Res. Develop.* 3 (1959) 114 - 125.

[SS] Salomaa,A. and Soittola, M., *Automata-Theoretic Aspects of Formal Power Series*, Springer-Verlag, New York, 1978.

[V] Valiant, L.G., The equivalence problem for deterministic finite-turn pushdown automata, *Inform. Control*, 25 (1974) 123 - 133.