Corrigendum for
Arithmetic Complexity, Kleene Closure, and Formal Power Series
Eric Allender, V Arvind, Meena Mahajan
Theory of Computing Systems 36(4): 303–328, 2003.

Pierre McKenzie and Sambuddha Roy pointed out that the proof of statements (b) and (c) in Theorem 7.3 are buggy. The main flaw is that the identity $e$ of the group $F$ may not be the identity of the monoid, and so the claim that $w \in (A_{F,r})^* \iff w \notin$ Test does not work.

In this corrigendum, we show:

- With a slight change to Definition 7.1, the statement of Theorem 7.3 holds unchanged. In our opinion, this is the most interesting way to correct the error in the original paper. We present a complete proof below. For completeness, we also mention another way to correct the error:
- Leaving Definition 7.1 unchanged, a weaker version of Theorem 7.3 holds (with only minor adjustments to the proof given in the paper).

First, we present the modified version of Theorem 7.3 that holds using the original version of Definition 7.1

**Theorem 7.3 (Variant)** *(a) Let $A$ be any finite nonsolvable monoid. Then there exists a group $F \subseteq A$ and a constant $r > 0$ such that the $(A_{F,r})^*$ closure problem is* NC$^1$-*complete.*

*(b) Let $A$ be any finite monoid, and let $F$ be a group contained in $A$, with the same identity $e$ as the monoid identity. Then the $(A_{F,r})^*$ closure problem is reducible via* AC$^0$-*Turing reductions to the word problem over the finite monoid $A$.*

*(c) If $A$ is a finite solvable monoid and $F$ is a group in it with the same identity as $A$, then the $(A_{F,r})^*$ closure problem is in* ACC$^0$. *Furthermore, if $A$ is an aperiodic monoid then the $(A_{F,r})^*$ closure problem is in* AC$^0$.

We now proceed to give a modification to Definition 7.1, with the property that that both Corollary 7.2 and Theorem 7.3 are true, as stated in the original paper.

**Definition 7.4 (Modified from Definition 7.1 in the paper)** *Let $A$ be a finite monoid. There is a natural homomorphism $v : A^* \mapsto A$ that maps a word $w$ to its valuation $v(w)$ in the monoid $A$. Let $F$ be a group contained in $A$, let $e$ denote the identity of $F$, and let $r$ be a positive integer. The language $A_{F,r} \subseteq A^*$ is defined as $A_{F,r} = \{w \in A^* \mid |w| \leq r, v(ew) \in F\}$.*

The original definition required that $v(w)$ be a group element; instead, we now require $v(ew)$ to be a group element.

The $(A_{F,r})^*$ *closure problem* is the decision problem $(A_{F,r})^*$. Since $A_{F,r}$ is finite, $(A_{F,r})^*$ is a regular language, and thus the $(A_{F,r})^*$ closure problem is always in NC$^1$.

With the revised definition, Corollary 7.2 still holds (with the same proof), because the monoid $A = S_5$ is itself a group, and $F$ is a subgroup.

We now state and prove Theorem 7.3 (using the revised definition of $A_{F,r}$).

**Theorem 7.3** *(a) Let $A$ be any nonsolvable monoid. Then there exists a group $F \subseteq A$ and a constant $r > 0$ such that the $(A_{F,r})^*$ closure problem is* NC$^1$*-complete.*

*(b) The $(A_{F,r})^*$ closure problem is reducible via* AC$^0$*-Turing reductions to the word problem over the finite monoid $A$.*

*(c) If $A$ is a solvable monoid then the $(A_{F,r})^*$ closure problem is in* ACC$^0$*. Furthermore, if $A$ is an aperiodic monoid then the $(A_{F,r})^*$ closure problem is in* AC$^0$*.*

*Proof.*

(a) Since $A$ is a nonsolvable monoid, $A$ contains a nontrivial nonsolvable group $G$ with identity $e$.[1] Since the word problem over $G$ is NC$^1$-complete [Bar89], it suffices to show an AC$^0$ reduction from the word problem over $G$ to an appropriate $A^*_{F,r}$ closure problem. To be precise, the word problem we consider is

$$W := \{w \in G^* \mid v(w) = e\}$$

Let $G = \{g_1, g_2, \dots, g_m\}$. Consider the word $u = \prod_{1 \le i \le m} g_i^{-1} g_i$ in $A^*$. Let $w = w_1 w_2 \dots w_n$ be an instance of $W$. We map the instance $w$ to the word $z = (\prod_{1 \le i \le n-1} w_i u) w_n$. Notice that $v(z) = v(w)$. Furthermore, it is not hard to see that by virtue of inserting the word $u$ between $w_i$ and $w_{i+1}$ for $1 \le i \le n-1$ we have ensured that the word $z$ can be decomposed into $z = \alpha_1 \alpha_2 \dots \alpha_n$, where for $1 \le i \le n-1$ we have $|\alpha_i| < 4m$, $w_i$ is included in $\alpha_i$, and $v(\alpha_i) = e$. Since $v(z) = v(w)$, it follows that $w \in W$ iff $z$ can be decomposed as $\alpha_1 \alpha_2 \dots \alpha_n$, where each $\alpha_i$ is of length at most $4m - 1$ and $v(\alpha_i) = e$ for all $i$. Clearly, $v(e\alpha_i) = v(e)v(\alpha_i) = e$ as well.

**Note:** The last sentence above is the only new thing in the proof of part (a).

Letting $F = \{e\}$ and $r = 4m - 1$ the above argument shows that $w \mapsto z$ is an AC$^0$ reduction from the NC$^1$-complete word problem $W$ to the $(A_{F,r})^*$ closure problem.

(b) We devise a test that characterizes membership in $(A_{F,r})^*$, using the following claim.

**Claim 7.4** *Let $x, y$ be words in $A^*$, and suppose $v(ex) \in F$. Then*

$$v(ey) \in F \iff v(exy) \in F$$

*Proof.* ($\Leftarrow$:)

$$\begin{aligned} v(ey) &= v(e)v(y) = ev(y) \\ &= [v(ex)]^{-1} v(ex) v(y) \quad \text{(since } v(ex) \in F\text{, it has an inverse)} \\ &= [v(ex)]^{-1} v(exy), \quad \text{which is in } F \text{ because } v(exy) \in F. \end{aligned}$$

[1] Notice that $e$ could be different from the monoid identity.

(⇒:)

$$\begin{aligned} v(exy) &= v(ex)v(y) = v(ex)ev(y) \qquad (\text{since } v(ex) \in F,\ v(ex) = v(ex)e) \\ &= v(ex)v(e)v(y) = v(ex)v(ey), \quad \text{which is in } F \text{ because } v(ex), v(ey) \in F. \end{aligned}$$

□

For any $w = w_1w_2 \dots w_n$ with each $w_i \in A$, and for $0 \leq i < j \leq n$, let $w[i, j]$ denote the subword $w_{i+1} \dots w_j$. We construct a circuit for $(A_{F,r})^*$ that uses oracle gates for the following word problem $W$ over the monoid $A$:

$$W := \{w \in A^* \mid v(ew) \in F\}$$

The circuit will have an oracle gate for $w[0, j]$ for each $1 \leq j \leq n$. Let the output of the oracle gate be the bit $b_j$; thus

$$\text{For } 1 \leq j \leq n, \quad b_j = \begin{cases} 1 & \text{if } v(ew[0, j]) \in F \\ 0 & \text{otherwise} \end{cases}$$

We set $b_0 = 1$. Now we place circuitry to check that

(a) $b_n = 1$, and

(b) the string $b = b_0b_1 \dots b_n$ does not have $r$ consecutive zeroes.

It is clear that these checks can be performed in AC$^0$. To see why these checks characterize membership in $(A_{F,r})^*$, note that:

If $w \in (A_{F,r})^*$, then we can decompose $w$ into short strings $w = x_1x_2 \dots x_m$ such that each $x_i$ has length at most $r$ and each $v(ex_i)$ is in $F$. By the claim above, $v(ey) \in F$ for each prefix $y$ of the form $x_1x_2 \dots x_j$. Thus at each such position, the string $b$ will have a 1, and these positions are at most $r$ positions apart.

If the 1s in $b$ are never separated by $r$ or more zeroes, then there is a sequence $0 = l_0 < l_1 < l_2 < \dots < l_m = n$ such that for each $j$, $l_j - l_{j-1} \leq r$, and $v(ew[0, l_j]) \in F$. By the above claim, each $v(ew[l_{j-1}, l_j])$ is also in $F$. This gives the required decomposition witnessing $w \in (A_{F,r})^*$.

This completes the proof of part (b).

(c) This is an immediate consequence of part (b) and the results of [Bar89, BT88].

□

# Acknowledgments

The discussion about the flaw and the possible work-arounds took place while Eric Allender, Pierre McKenzie and Meena Mahajan were at Dagstuhl seminar 11121 (March 2011).

# References

[Bar89] D.A. Barrington. Bounded-width polynomial size branching programs recognize exactly those languages in $\mathrm{NC}^1$. *Journal of Computer and System Sciences*, 38:150–164, 1989.

[BT88] D.A. Barrington and D. Thérien. Finite monoids and the fine structure of $\mathrm{NC}^1$. *Journal of the Association of Computing Machinery*, 35:941–952, 1988.