Infinite Unfair Shuffles and Associativity

Maurice H. ter Beek

ISTI–CNR, Pisa, Italy

— joint work with *Jetty Kleijn* —

(LIACS, Leiden University, The Netherlands)

Friday 16 September 2005

WORDS’05, Montréal, Canada

Outline

- Introduction and motivation
- Basic definitions and observations
- Decompositions and limit-closed languages
- The main result: shuffling is associative
- Discussion and future work

Introduction

- Consider shuffles of possibly infinite words that may be unfair
  $\Rightarrow$ one of the two words may be delayed indefinitely!

- Unable to find in the literature explicit results concerning the associativity of the shuffle operation as considered here . . .

- Rather than focussing on the single property of associativity, we study the more general issue of the relationship between shuffles of (finite or infinite) words and the shuffles of their finite prefixes
  $\Rightarrow$ characterization of shuffles in terms of their (finite!) prefixes

Motivation: team automata

- Component automaton: ordinary FSA without final states and its alphabet partitioned into input, output and internal actions
  - ⇒ prefix-closed languages that may contain infinite words
- Team automaton: (iterative) composition of component automata that may collaborate by synchronizing on shared actions
  - ⇒ languages may be unfair in the sense that a component may execute *ad infinitum*, never giving others a turn
- Compositionality: language of a team automaton can be defined in terms of the languages of its constituting component automata
  - ⇒ ‘synchronized’ shuffling of languages must be associative

Basis definitions: shuffling

Let $u, v \in \Delta^\infty$. Then

(1) $w \in \Delta^\infty$ is a fair shuffle of u and v if $w = u_1 v_1 u_2 v_2 \cdots$, where $u_i, v_i \in \Delta^*$, for all $i \geq 1$, are such that $u = u_1 u_2 \cdots$ and $v = v_1 v_2 \cdots$

(2) $w \in \Delta^\infty$ is a shuffle of u and v if either

(a) w is a fair shuffle of u and v, or

(b) $w = u_1 v_1 u_2 v_2 \cdots$, where $u_i, v_i \in \Delta^*$, for all $i \geq 1$, and either $u_1 u_2 \cdots \in \text{pref}(u)$ and $v = v_1 v_2 \cdots \in \Delta^\omega$, or $u = u_1 u_2 \cdots \in \Delta^\omega$ and $v_1 v_2 \cdots \in \text{pref}(v)$

$$u \mathbin{|||} v = \{\, w \in \Delta^\infty : w \text{ is a fair shuffle of } u \text{ and } v \,\}$$

$$u \mathbin{||} v = \{\, w \in \Delta^\infty : w \text{ is a shuffle of } u \text{ and } v \,\}$$

$$L_1 \mathbin{|||} L_2 = \bigcup_{u \in L_1,\, v \in L_2} u \mathbin{|||} v \qquad L_1 \mathbin{||} L_2 = \bigcup_{u \in L_1,\, v \in L_2} u \mathbin{||} v$$

Example: fair and unfair shuffling

$a \parallel b = \{ab, ba\}$ $\qquad$ $a^2 \parallel b = \{a^2b, aba, ba^2\}$

$a^n \parallel b = \{\, a^i b a^j : i, j \geq 0,\ i + j = n \,\}$

$\Rightarrow$ every shuffle of a^n and b is fair

$a^\omega \,|||\, b = \{\, a^i b a^\omega : i \geq 0 \,\}$ $\qquad$ $a^\omega \parallel b = (a^\omega \,|||\, b) \cup a^\omega$

$\Rightarrow$ a^ω is an unfair shuffle of a^ω and b

$a^\omega \,|||\, a = a^\omega \parallel a = a^\omega$

$\Rightarrow$ infinite words need not result in unfair shuffles

Shuffling: basic observations

Let $u, v, w \in \Delta^\infty$. Then

(1) (fair) shuffling is commutative: $u \mathbin{|||} v = v \mathbin{|||} u$ and $u \mathbin{||} v = v \mathbin{||} u$

(2) fair shuffling is associative: $u \mathbin{|||} (v \mathbin{|||} w) = (u \mathbin{|||} v) \mathbin{|||} w$

⇒ based on alternative definition $u \mathbin{|||} v = \psi_{\{i,j\}}(\varphi^{-1}_{i,\{j\}}(u) \cap \varphi^{-1}_{j,\{i\}}(v))$

(3) pref$(u) \mathbin{||}$ pref$(v) =$ pref$(u \mathbin{|||} v) =$ pref$(u \mathbin{||} v) =$ pref$(u) \mathbin{|||}$ pref(v)

Example: pref$(a^\omega \mathbin{|||} b) =$ pref$(a^\omega \mathbin{||} b) = \{ a^i b a^\omega : i \geq 0 \} \cup a^*$

⇒ recall that $a^\omega \mathbin{|||} b \neq a^\omega \mathbin{||} b$

Decompositions: definitions

- The associativity of fair shuffling (possibly infinite words) implies the well-known fact that shuffling is associative for finite words
- We seek to express shuffles as limits of shuffles of finite words, and then to apply the associativity of shuffling finite words
- We use the concept of decomposition as an explicit description of how a shuffle is obtained from two given finite words:

Let $w \in \Delta^*$. Then a decomposition of w is a sequence

$$d = (u_1, v_1, u_2, v_2, \ldots, u_n, v_n)$$

with $n \geq 1$, $u_1, v_n \in \Delta^*$, all other $u_i, v_i \in \Delta^+$, and $w = u_1 v_1 \cdots u_n v_n$

If $u_1 \cdots u_n = u$ and $v_1 \cdots v_n = v$, then d is a (u, v)-decomposition of w

Decompositions: basic observations

Decompositions provide a normal form for describing finite shuffles:

Let $u, v, w \in \Delta^*$. Then

there exists a (u, v)-decomposition of w iff $w \in u \mid\mid v$

It is not difficult to see that a shuffle may have several decompositions

$\Rightarrow$ Mateescu's trajectories define unique decompositions

To be able to describe extensions (limits!) of shuffles explicitly, we use the concept of a precedence relation for decompositions:

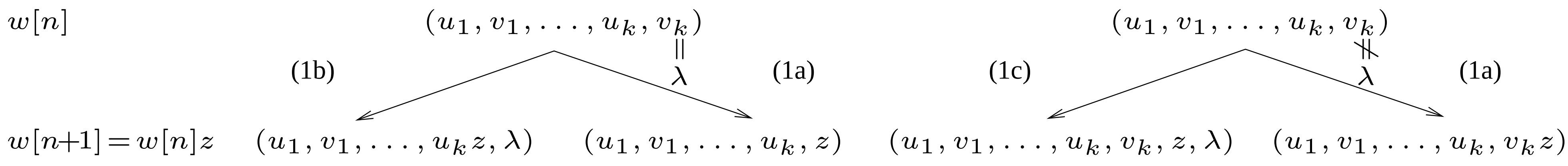
(Directly) preceding decompositions

Let $d = (x_1, y_1, \ldots, x_k, y_k)$ and $d' = (u_1, v_1, \ldots, u_n, v_n)$ be decompositions of $x_1 y_1 \cdots x_k y_k \in \Delta^*$ and $u_1 v_1 \cdots u_n v_n \in \Delta^*$, respectively. Then

(1) d directly precedes d' if $k \leq n$ and for all $1 \leq j \leq k-1$, $x_j = u_j$ and $y_j = v_j$, and — moreover — either

- (a) $k = n$, $x_k = u_k$, and $y_k a = v_k$, for some $a \in \Delta$, or
- (b) $k = n$, $y_k = v_k = \lambda$, and $x_k a = u_k$, for some $a \in \Delta$, or
- (c) $k = n-1$, $y_k \neq \lambda$, $v_{k+1} = \lambda$, and $u_{k+1} = a$, for some $a \in \Delta$

(2) d precedes d' if there exist decompositions $d_0, \ldots, d_\ell$ such that $\ell \geq 0$, $d = d_0$, $d' = d_\ell$, and each d_j directly precedes d_{j+1}.



Decompositions: basic results

For all $i \geq 0$, let d_i be a (u_i, v_i)-decomposition of a word w_i over Δ such that d_i precedes d_{i+1}. Then

$$u = \lim_{i \to \infty} u_i, \quad v = \lim_{i \to \infty} v_i, \text{ and } w = \lim_{i \to \infty} w_i \text{ exist, and } w \in u \mid\mid v$$

Let $u, v \in \Delta^\infty$ be such that alph$(u) \cap$ alph$(v) = \varnothing$ and let $w \in \Delta^\omega$. Then

$$\text{pref}(w) \subseteq \text{pref}(u) \mid\mid \text{pref}(v) \text{ implies } w \in u \mid\mid v$$

$\Rightarrow$ proof uses observation that — thanks to alphabet disjointness — any decomposition of a prefix of w into prefixes of u and v, has a (unique) successor describing a decomposition of the next prefix

Counterexample!

However, in general it is not true that decompositions of prefixes can be extended to decompositions of the next prefix:

Let $u = (a^3 b)^\omega$ and $v = b^\omega$

Then obviously $w = a^3 b^3 \in$ pref$(u) \mid\mid$ pref(v)

- $\Rightarrow$ $d_1 = (a^3, b^3)$ and $d_2 = (a^3 b, b^2)$ are two decompositions of w

Now consider $w' = wa = a^3 b^3 a \in$ pref$(u) \mid\mid$ pref(v)

- $\Rightarrow$ the only decompositions of w' which are directly preceded by a decomposition of prefixes of u and v are $d' = (a^3 b, b^2, a, \lambda)$ and $d'' = (a^3, b^2, ba, \lambda)$, but d_1 neither precedes d' nor d''

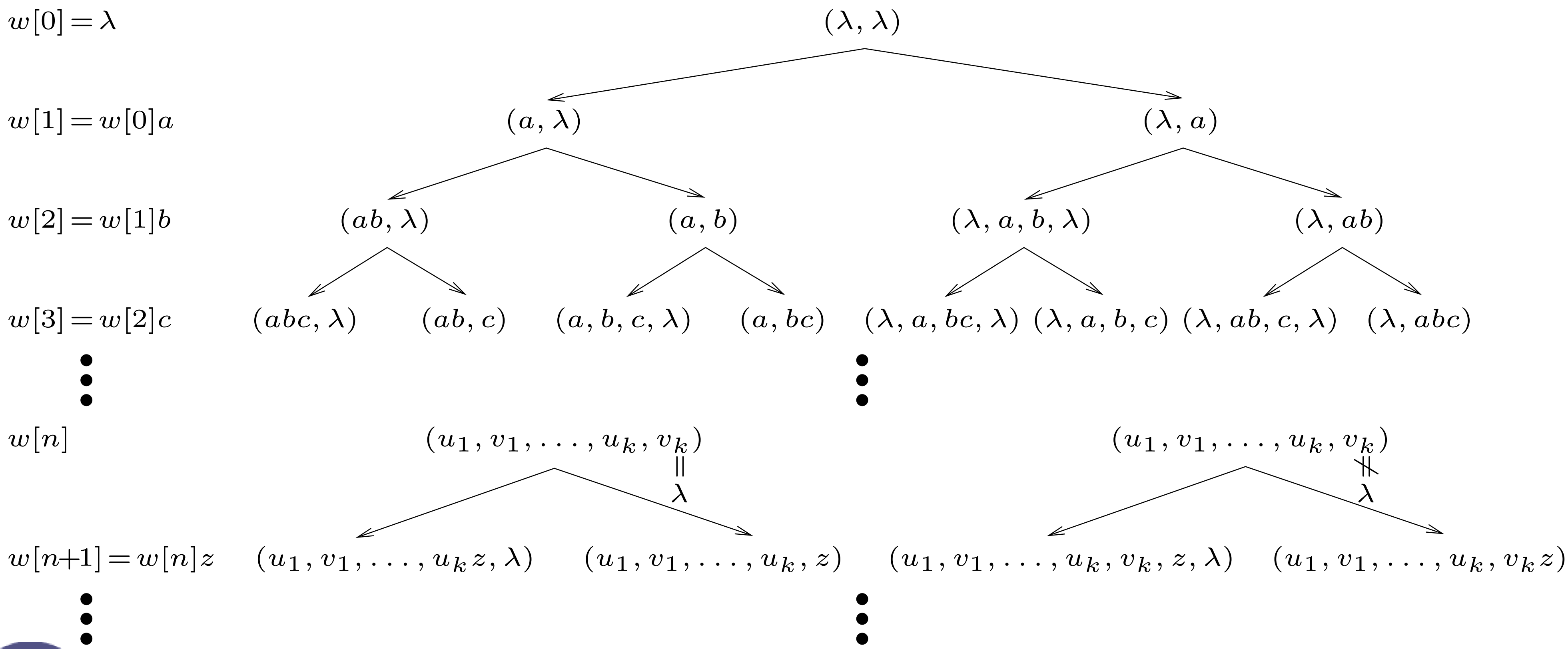
It can be shown that an infinite word may even have infinitely many prefixes with non-extendable decompositions

Saved by König's Lemma

It can however be shown that for all words $u, v \in \Delta^\infty$ and $w \in \Delta^\omega$

$$\text{pref}(w) \subseteq \text{pref}(u) \mid\mid \text{pref}(v) \text{ implies } w \in u \mid\mid v$$

even when u and v have letters in common:



F M&T

Limit-closed languages

Let $K \subseteq \Delta^\infty$. Then

K is limit-closed if for all $w_1 \leq w_2 \leq \cdots \in$ pref(K), $\lim_{n\to\infty} w_n \in K \cup$ pref(K)

$\Rightarrow$ infinitary part of a language is characterized by its finite prefixes

Example: All singleton languages $\{u\}$ as well as all finite languages $L_n = \{\lambda, a, \ldots, a^n\}$ over a unary alphabet are limit-closed

a^* is not limit-closed as $\lim_{n\to\infty} a^n = a^\omega \notin a^*$, but $a^* \cup a^\omega$ and a^ω are

For later use: if $v, w \in \Delta^\infty$, then $v \,||\, w$ is limit-closed

Towards the main result

Let $K, L \subseteq \Delta^\infty$ be limit-closed and let $w \in \Delta^\omega$. Then

$$\text{pref}(w) \subseteq \text{pref}(K) \mid\mid \text{pref}(L) \text{ implies } w \in K \mid\mid L$$

This in general does not hold when either K or L is not limit-closed:

Counterexample: Let $K = a^*$ and $L = \{\lambda\}$. Then

$$\text{pref}(a^\omega) = a^* = \text{pref}(K) \mid\mid \text{pref}(L), \text{ but } a^\omega \notin a^* = K \mid\mid L$$

Fortunately, singleton languages are limit-closed:

Let $u, v \in \Delta^\infty$ and $w \in \Delta^\omega$. Then

$$\text{pref}(w) \subseteq \text{pref}(u) \mid\mid \text{pref}(v) \text{ implies } w \in u \mid\mid v$$

The main result

Recall Theorem 2:

$$\text{pref}(u) \mid\mid \text{pref}(v) = \text{pref}(u \mid\mid\mid v) = \text{pref}(u \mid\mid v) = \text{pref}(u) \mid\mid\mid \text{pref}(v)$$

Thus characterized the shuffles of two words (limit-closed languages) as the limits of the shuffles of the prefixes of these words (languages):

Theorem 5:

Let $u, v \in \Delta^\infty$, let $K, L \subseteq \Delta^\infty$ be limit-closed, and let $w \in \Delta^\omega$. Then

(1) $w \in u \mid\mid v$ iff $\text{pref}(w) \subseteq \text{pref}(u) \mid\mid \text{pref}(v)$

(2) $w \in K \mid\mid L$ iff $\text{pref}(w) \subseteq \text{pref}(K) \mid\mid \text{pref}(L)$

$\Rightarrow$ now ready to prove that shuffling is associative!

Shuffling is associative

Let $u, v, w \in \Delta^\infty$. Then $u \mid\mid (v \mid\mid w) = (u \mid\mid v) \mid\mid w$

Proof: If u, v, w are finite words, shuffling is associative (Cor. 1)
If at least one of them is infinite, then $u \mid\mid (v \mid\mid w)$ and $(u \mid\mid v) \mid\mid w$ consist of infinite words only!
Let $x \in u \mid\mid (v \mid\mid w)$:

$\Rightarrow$ pref$(x) \subseteq$ pref$(u) \mid\mid$ pref$(v \mid\mid w)$ (Thm. 5(2))

$\Rightarrow$ pref$(x) \subseteq$ pref$(u) \mid\mid$ (pref$(v) \mid\mid$ pref(w)) (Thm. 2)

$\Rightarrow$ pref$(x) \subseteq$ (pref$(u) \mid\mid$ pref(v)) $\mid\mid$ pref(w) (Cor. 1)

$\Rightarrow$ pref$(x) \subseteq$ pref$(u \mid\mid v) \mid\mid$ pref(w) (Thm. 2)

Now $x \in (u \mid\mid v) \mid\mid w$ by Thm. 5(2) since $u \mid\mid v$ and $\{w\}$ are limit-closed!
The converse inclusion follows from the above and commutativity

Discussion and future work

- Our proof of the associativity of shuffling is fully self-contained (it does not rely on the sometimes vague or not substantiated claims made in the literature for related operations)

Associativity is of interest not only from mathematical point of view:

- Associativity of shuffling as considered here is the basis for proofs of the associativity of some variants of ‘synchronized’ shuffling in my Ph.D. thesis (ter Beek, 2003)
- Associativity of these variants, in their turn, is crucial to prove that several types of team automata satisfy compositionality

  $\Rightarrow$ to be addressed in a forthcoming paper!

(M.H. ter Beek, C. Martín-Vide and V. Mitrana, Synchronized Shuffles TCS 341, 1-3 (2005), 263–275)