The Fisher–Yates shuffle

Manuel Eberl

April 19, 2020

Abstract

This work defines and proves the correctness of the Fisher–Yates shuffle [1, 2, 3] for shuffling – i.e. producing a random permutation – of a list. The algorithm proceeds by traversing the list and in each step swapping the current element with a random element from the remaining list.

Contents

1 Fisher–Yates shuffle 2
  1.1 Swapping elements in a list .................. 2
  1.2 Random Permutations .......................... 3
  1.3 Shuffling Lists ................................ 3
  1.4 Forward Fisher-Yates Shuffle .................. 4
  1.5 Backwards Fisher-Yates Shuffle .............. 4
  1.6 Code generation test .......................... 5
1 Fisher–Yates shuffle

theory Fisher-Yates
  imports HOL−Probability.Probability
begin

lemma integral-pmf-of-multiset:
  \( A \neq \{\#\} \Rightarrow (\int x. (f x :: real) \, \text{measure-pmf} (\text{pmf-of-multiset} A)) = \\
  (\sum x \in \text{set-mset} A. \text{of-nat} (\text{count} A x) \times f x) / \text{of-nat} (\text{size} A) \)
⟨proof⟩

lemma pmf-bind-pmf-of-multiset:
  \( A \neq \{\#\} \Rightarrow \text{pmf} (\text{pmf-of-multiset} A \gg f) = \)
  (\sum x \in \text{set-mset} A. \text{real} (\text{count} A x) \times \text{pmf} (f x) y) / \text{real} (\text{size} A)
⟨proof⟩

lemma pmf-map-inj-inv:
  assumes inj-on f (set-pmf p)
  assumes \( \forall x. f' (f x) = x \)
  shows \( \text{pmf} (\text{map-pmf} f p) x = \) (if \( x \in \text{range} f \) then \( \text{pmf} p (f' x) \) else 0)
⟨proof⟩

1.1 Swapping elements in a list

definition swap where swap xs i j = xs[i := xs!j, j := xs ! i]

lemma length-swap [simp]: length (swap xs i j) = length xs
⟨proof⟩

lemma swap-eq-Nil-iff [simp]: swap xs i j = [] \iff xs = []
⟨proof⟩

lemma nth-swap: i < length xs \implies j < length xs \implies
  swap xs ! j ! k = (if k = i then xs ! j else if k = j then xs ! i else xs ! k)
⟨proof⟩

lemma map-swap: i < length xs \implies j < length xs \implies map f (swap xs i j) =
  swap (map f xs) i j
⟨proof⟩

lemma swap-swap: i < length xs \implies j < length xs \implies swap (swap xs i j) ! j i = xs
⟨proof⟩

lemma mset-swap: i < length xs \implies j < length xs \implies mset (swap xs i j) = mset xs
⟨proof⟩

2
lemma \(hd\text{-}swap\): \(i < \text{length } xs \implies hd (\text{swap } xs \ 0 \ i) = xs \ ! i\)

\(⟨\text{proof}⟩\)

1.2 Random Permutations

First, we prove the intuitively obvious fact that choosing a random permutation of a multiset can be done by first randomly choosing the first element and then randomly choosing the rest of the list.

lemma pmf-of-set-permutations-of-multiset-nonempty:
assumes \((A :: 'a \text{ multiset}) \neq \{\#\}\)
shows \(\text{pmf-of-set } (\text{permutations-of-multiset } A) =\)
\(\begin{cases} x \leftarrow \text{pmf-of-multiset } A; \\
xzs \leftarrow \text{pmf-of-set } (\text{permutations-of-multiset } (A - \{\#x\#\})); \\
\text{return-pmf } (x\#xzs) \\
\end{cases}\)
\(\text{is } \&\& \text{lhs } = \&\& \text{rhs} \)

\(⟨\text{proof}⟩\)

1.3 Shuffling Lists

We define shuffling of a list as choosing from the set of all lists that correspond to the same multiset uniformly at random.

definition shuffle :: 'a list \Rightarrow 'a list pmf where
shuffle xs = \text{pmf-of-set } (\text{permutations-of-multiset } (mset xs))

lemma shuffle-empty [simp]: shuffle [] = \text{return-pmf } []

\(⟨\text{proof}⟩\)

lemma shuffle-singleton [simp]: shuffle [x] = \text{return-pmf } [x]

\(⟨\text{proof}⟩\)

The crucial ingredient of the Fisher–Yates shuffle is the following lemma, which decomposes a shuffle into swapping the first element of the list with a random element of the remaining list and shuffling the new remaining list.

With a random-access implementation of a list – such as an array – all of the required operations are cheap and the resulting algorithm runs in linear time.

lemma shuffle-fisher-gates-step:
assumes \(xs\text{-nonempty } [\text{simp}]: \text{xs } \neq []\)
shows \(\text{shuffle } xs =\)
\(\begin{cases} i \leftarrow \text{pmf-of-set } \{..<\text{length } xs\}; \\
\text{let } ys = \text{swap } xs \ 0 \ i; \\
zs \leftarrow \text{shuffle } (\text{tl } ys); \\
\text{return-pmf } (\text{hd } ys \ # \ zs) \\
\end{cases}\)

\(⟨\text{proof}⟩\)
1.4 Forward Fisher-Yates Shuffle

The actual Fisher–Yates shuffle is now merely a kind of tail-recursive version of decomposition described above. Note that unlike the traditional Fisher–Yates shuffle, we shuffle the list from front to back, which is the more natural way to do it when working with linked lists.

```plaintext
function fisher-yates-aux where
  fisher-yates-aux i xs = (if i + 1 ≥ length xs then return-pmf xs else
do {j ← pmf-of-set {i..<length xs};
  fisher-yates-aux (i + 1) (swap xs i j)})
⟨proof⟩
termination ⟨proof⟩
declare fisher-yates-aux.simps [simp del]

lemma fisher-yates-aux-correct: fisher-yates-aux i xs = map-pmf (λys. take i xs @ ys) (shuffle (drop i xs))
⟨proof⟩

definition fisher-yates where
  fisher-yates = fisher-yates-aux 0

lemma fisher-yates-correct: fisher-yates xs = shuffle xs
⟨proof⟩
```

1.5 Backwards Fisher-Yates Shuffle

We can now easily derive the classical Fisher–Yates shuffle, which goes through the list from back to front and show its equivalence to the forward Fisher–Yates shuffle.

```plaintext
fun fisher-yates-alt-aux where
  fisher-yates-alt-aux i xs = (if i = 0 then return-pmf xs else
do {j ← pmf-of-set {..i};
  fisher-yates-alt-aux (i - 1) (swap xs i j)})

declare fisher-yates-alt-aux.simps [simp del]

lemma fisher-yates-alt-aux-altdef: i < length xs ⇒ fisher-yates-alt-aux i xs = map-pmf rev (fisher-yates-alt-aux (length xs - i - 1) (rev xs))
⟨proof⟩

definition fisher-yates-alt where
  fisher-yates-alt xs = fisher-yates-alt-aux (length xs - 1) xs

lemma fisher-yates-alt-aux-correct: fisher-yates-alt xs = shuffle xs
⟨proof⟩
```
1.6 Code generation test

Isabelle's code generator allows us to produce executable code both for shuffle and for fisher-yates and fisher-yates-alt. However, this code does not produce a random sample (i.e. a single randomly permuted list) – which is, in fact, the only purpose of the Fisher–Yates algorithm – but the entire probability distribution consisting of $n!$ lists, each with probability $1/n!$.

In the future, it would be nice if Isabelle also had some code generation facility that supports generating sampling code.

```
value [code] shuffle "abcd"
value [code] fisher-yates "abcd"
value [code] fisher-yates-alt "abcd"
```

end

References

