Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики

Факультет информационных технологий и программирования
Кафедра компьютерных технологий

Рыбак Андрей Викторович

Представление структур данных индуктивными семействами и доказательства их свойств

Научный руководитель: Я. М. Малаховски

Санкт-Петербург
2014

Содержание

Введение

Структуры данных используются в программировании повсеместно для упрощения хранения и обработки данных. Свойства структур данных происходят из инвариантов, которые эта структура данных соблюдает.

Практика показывает, что тривиальные структуры и их инварианты данных хорошо выражаются в форме индуктивных семейств. Мы хотим узнать насколько хорошо эта практика работает и для более сложных структур.

В данной работе рассматривается представление в форме индуктивных семейств структуры данных приоритетная очередь типа «двоичная куча».

Глава 1. Обзор

В данной главе производится обзор предметной области и даются определения используемых терминов.

1.1. Лямбда-исчисление

Лямбда-исчисление (λ-calculus) — вычислительный формализм с тремя синтаксическим конструкциями, называемыми *пре-лямбда-термами*:

- *вхождение переменной*: v. При этом $v \in V$, где V — некоторое множество имён переменных;
- *лямбда-абстракция*: $\lambda x.A$, где x — имя переменной, а A — пре-лямбда-терм. При этом терм A называют *телом абстракции*, а x перед точкой — *связыванием.*
- *лямбда-аппликация*: BC;

и одной операцией *бета-редукции.* При этом говорят, что вхождение переменной является *свободным*, если оно не связано какой-либо абстракцией. *Лямбда-термы* — это пре-лямбда-термы, факторизованные по отношению *альфа-эквивалентности.*

Альфа-эквивалентность (α-equality) отождествляет два пре-лямбда-терма, если один из них может быть получен из другого путём некоторого *корректного* переименовывания переменных — переименования не нарушающего отношение связанности.

Бета-редукция (β-reduction) для лямбда-терма A выбирает в нём некоторую лямбда-аппликацию BC, содержащую лямбда-абстракцию в левой части A, и заменяет свободные вхождения переменной, связанной A, в теле самой A на терм C.[1]

[1] В терминах пре-лямбда-термов это означает замену свободных вхождений в теле A на пре-терм C так, чтобы ни для каких переменных не нарушилось отношение связанности. То есть, в пре-терме A следует корректно переименовать все связанные переменные, имена которых совпадают с именами свободных переменных в C.

Два лямбда-терма A и B называются *конвертабельными*, когда существует две последовательности бета-редукций, приводящих их к общему терму C. Или, эквивалентно, когда термы A и B состоят с друг с другом в рефлексивно-симметрично-транзитивном замыкании отношения бета-редукции, также называемом отношением *бета-эквивалентности.*

За более подробной информацией об этом формализме следует обращаться к [1] и [2].

1.2. Функциональное программирование

Функциональное программирование — парадигма программирования, являющаяся разновидностью декларативного программирования, в которой программу представляют в виде функций (математическом смысле этого слова, а не в смысле, используемом в процедурном программировании), а выполнением программы считают вычисление значений применения этих функций к заданным значениям. Большинство функциональных языков программирования используют в своём основании лямбда-исчисление (например, Haskell [3], Curry [4], Agda [5], диалекты LISP [6–8], SML [9], OCaml[10]), но существуют и функциональные языки явно не основанные на этом формализме (например, препроцессор языка C и шаблоны в C++).

1.3. Алгебраические типы данных и сопоставление с образцом

Алгебраический тип данных — вид составного типа, то есть типа, сформированного комбинированием других типов. Комбинирование осуществляется с помощью алгебраических операций — сложения и умножения.

Сумма типов A и B — дизъюнктное объединение исходных типов. Значения типа-суммы обычно создаются с помощью *конструкторов.*

Произведение типов A и B — прямое произведение исходных типов, кортеж типов.

1.3.1. Сопоставление с образцом

Сопоставление с образцом — способ обработки объектов алгебраических типов данных, который идентифицирует значения по конструктору и извлекает данные в соответствии с представленным образцом.

1.4. Теория типов

Теория типов — раздел математики изучающий отношения типизации вида $M : \tau$ и их свойства. M называется *термом* или *выражением*, а τ — типом терма M.

Теория типов также изучает правила для *переписывания* термов — замены подтермов в выражениях другими термами. Такие правила также называют правилами *редукции* или *конверсии* термов. Редукцию терма x в терм y записывают: $x \to y$. Также рассматривают транзитивное замыкание отношения редукции: $\xrightarrow{*}$. Например, термы $2+1$ и 3 — разные термы, но первый редуцируется во второй: $2+1 \xrightarrow{*} 3$. Если для терма x не существует терма y, для которого $x \to y$, то говорят, что терм x — в *нормальной форме*.

1.4.1. Отношение конвертабельности

Два терма x и y называются *конвертабельными*, если существует терм z такой, что $x \xrightarrow{*} z$ и $y \xrightarrow{*} z$. Обозначают $x \overset{*}{\leftrightarrow} y$. Например, $1+2$ и $2+1$ — конвертабельны, как и термы $x+(1+1)$ и $x+2$. Однако, $x+1$ и $1+x$ (где x — свободная переменная) — не конвертабельны, так как оба представлены в нормальной форме. Конвертабельность — рефлексивно-транзитивно-симметричное замыкание отношения редукции.

1.4.2. Интуиционистская теория типов

Интуиционистская теория типов основана на математическом конструктивизме [11].

Операторы для типов в ИТТ:

- Π-тип (пи-тип) — зависимое произведение. Например, если $\mathrm{Vec}(\mathbb{R}, n)$ — тип кортежей из n вещественных чисел, $\mathbb{N}$ — тип натуральных чисел, то $\Pi_{n:\mathbb{N}} \mathrm{Vec}(\mathbb{R}, n)$ — тип функции, которая по натуральному числу n возвращает кортеж из n вещественных чисел.
- Σ-тип — зависимая пара. Например, тип $\Sigma_{n:\mathbb{N}} \mathrm{Vec}(\mathbb{R}, n)$ — тип пары из числа n и кортежа из n вещественных чисел.

Базовые типы в ИТТ: $\perp$ или 0 — пустой тип, не содержащий ни одного элемента; $\top$ или 1 — единичный тип, содержащий единственный элемент.

Индуктивный или *рекурсивный* тип — тип данных, который может содержать значения своего типа.

1.5. Унификация

Унификатор для термов A и — подстановка S, действующая на их свободные переменные, такая что $S(A) \equiv S(B)$.

Унификация — процесс поиска унификатора.

1.6. Индуктивные семейства

Определение 1.1. *Индуктивное семейство* [12, 13] — это индуктивный тип данных, который может зависеть от других типов и значений.

Тип или значение, от которого зависит зависимый тип, называют *индексом.*

Одной из областей применения индуктивных семейств являются системы интерактивного доказательства теорем.

Индуктивные семейства позволяют формализовать математические структуры, кодируя утверждения о структурах в них самих, тем самым перенося сложность из доказательств в определения.

В работах [14, 15] приведены различные подходы в использовании индуктивных семейств в реализации структур данных и доказательстве их свойств.

Пример задания структуры данных и инвариантов — тип данных AVL-дерева и для хранения баланса в AVL-дереве [16].
Если $m \sim n$, то разница между m и n не больше чем один:

```
data _∼_ : ℕ → ℕ → Set where
  ∼+ : ∀ {n} →   n ∼ 1 + n
  ∼0 : ∀ {n} →   n ∼ n
  ∼- : ∀ {n} → 1 + n ∼ n
```

1.7. Agda

Agda [5] — чистый функциональный язык программирования с зависимыми типами. В Agda есть поддержка модулей:

```
module AgdaDescription where
```

В коде на Agda широко используются символы Unicode. Тип натуральных чисел — ℕ.

```
data ℕ : Set where
  zero : ℕ
  succ : ℕ → ℕ
```

В Agda функции можно определять как mixfix операторы. Пример — сложение натуральных чисел:

```
_+_ : ℕ → ℕ → ℕ
zero + b = b
succ a + b = succ (a + b)
```

Символы подчеркивания обозначают места для аргументов.

Зависимые типы позволяют определять типы, зависящие (индексированные) от значений других типов. Пример — список, индексированный своей длиной:

```
data Vec (A : Set) : ℕ → Set where
  nil  : Vec A zero
  cons : ∀ {n} → A → Vec A n → Vec A (succ n)
```

В фигурные скобки заключаются неявные аргументы.

Такое определение позволяет нам описать функцию head для такого списка, которая не может бросить исключение:

```
head : ∀ {A} {n} → Vec A (succ n) → A
```

У аргумента функции head тип Vec A (succ n), то есть вектор, в котором есть хотя бы один элемент. Это позволяет произвести сопоставление с образцом только по конструктору cons:

```
head (cons a as) = a
```

1.8. Выводы по главе 1

Рассмотрены некоторые существующие подходы к построению структур данных с использованием индуктивных семейств. Кратко описаны особенности языка программирования *Agda*.

Глава 2. Описание реализованной структуры данных

В данной главе описывается разработанная функциональная структура данных приоритетная очередь типа «двоичная куча».

2.1. Постановка задачи

Целью данной работы является разработка типов данных для представления структуры данных и инвариантов.

Требования к данной работе:

- Разработать типы данных для представления структуры данных
- Реализовать функции по работе со структурой данных
- Используя разработанные типы данных доказать выполнение инвариантов.

2.2. Структура данных «двоичная куча»

Определение 2.1. Двоичная куча или пирамида [17] — такое двоичное подвешенное дерево, для которого выполнены следующие три условия:

- Значение в любой вершине не больше (если куча для минимума), чем значения её потомков.
- На i-ом слое 2^i вершин, кроме последнего. Слои нумеруются с нуля.
- Последний слой заполнен слева направо

На рисунке 2.1 изображен пример кучи.

2.3. Реализация

2.3.1. Вспомогательные определения

Часть общеизвестных определений заимствована из стандартной библиотеки Agda [18].

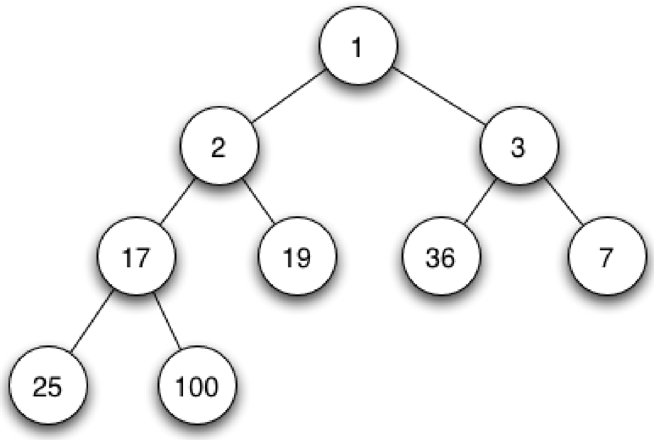

Рис. 2.1. Пример заполненной кучи для минимума

Тип данных для пустого типа. У этого типа нет конструкторов, и, как следствие, нет термов, населяющих этот тип.

```
data ⊥ : Set where
```

Из элемента пустого типа следует что-угодно.

```
⊥-elim : ∀ {a} {Whatever : Set a} → ⊥ → Whatever
⊥-elim ()
```

Логическое отрицание.

```
¬ : ∀ {a} → Set a → Set a
¬ P = P → ⊥
```

Контрадикция, противоречие: из A и $\neg A$ можно получить любое B.

```
contradiction : A → ¬ A → B
contradiction a ¬a = ⊥-elim (¬a a)
```

Контрапозиция

```
contraposition : (A → B) → (¬ B → ¬ A)
```

```
contraposition = flip _∘_
```

Пропозициональное равенство из интуционистской теории типов.

```
data _≡_ {a} {A : Set a} (x : A) : A → Set a where
  refl : x ≡ x
```

Тип-сумма — зависимая пара.

```
record Σ {a b} (A : Set a) (B : A → Set b) : Set (a ⊔ b) where
  constructor _,_
  field fst : A ; snd : B fst
```

Декартово произведение — частный случай зависимой пары, Второй индекс игнорирует передаваемое ему значение.

```
_×_ : ∀ {a b} (A : Set a) → (B : Set b) → Set (a ⊔ b)
A × B = Σ A (λ _ → B)
```

Конгруэнтность пропозиционального равенства.

```
cong : ∀ (f : A → B) {x y} → x ≡ y → f x ≡ f y
cong f refl = refl
```

2.3.2. Определение отношений и доказательство их свойств

Для сравнения элементов нужно задать отношения на этих элементах.

```
Rel₂ : Set → Set₁
Rel₂ A = A → A → Set
```

Трихотомичность отношений меньше, равно и больше: одновременно два элемента могут принадлежать только одному отношению из трех.

```
data Tri {A : Set} (_<_ _==_ _>_ : Rel₂ A) (a b : A) : Set where
  tri< :   (a < b) → ¬ (a == b) → ¬ (a > b) → Tri _<_ _==_ _>_ a b
  tri= : ¬ (a < b) →   (a == b) → ¬ (a > b) → Tri _<_ _==_ _>_ a b
  tri> : ¬ (a < b) → ¬ (a == b) →   (a > b) → Tri _<_ _==_ _>_ a b
```

Введем упрощенный предикат, использующий только два отношения — меньше и равенство. Отношение больше заменяется отношением меньше с переставленными аргументами.

```
flip₁ : ∀ {A B : Set} {C : Set₁} → (A → B → C) → B → A → C
flip₁ f a b = f b a
```

```
Cmp : {A : Set} → Rel₂ A → Rel₂ A → Set
Cmp {A} _<_ _==_ = ∀ (x y : A) → Tri (_<_) (_==_) (flip₁ _<_) x y
```

Тип данных для отношения меньше или равно на натуральных числах.

```
data _ℕ≤_ : Rel₂ ℕ where
  z≤n : ∀ {n} → zero ℕ≤ n
  s≤s : ∀ {n m} → n ℕ≤ m → succ n ℕ≤ succ m
```

Все остальные отношения определяются через _ℕ≤_ .

```
_ℕ<_ _ℕ≥_ _ℕ>_ : Rel₂ ℕ
n ℕ< m = succ n ℕ≤ m
n ℕ> m = m ℕ< n
n ℕ≥ m = m ℕ≤ n
```

В качестве примера компаратора — доказательство трихотомичности для отношения меньше для натуральных чисел.

```
lemma-succ-≡ : ∀ {n} {m} → succ n ≡ succ m → n ≡ m
lemma-succ-≡ refl = refl
lemma-succ-≤ : ∀ {n} {m} → succ (succ n) ℕ≤ succ m → succ n ℕ≤ m
lemma-succ-≤ (s≤s r) = r

cmpℕ : Cmp {ℕ} _ℕ<_ _≡_
cmpℕ zero (zero) = tri= (λ ()) refl (λ ())
cmpℕ zero (succ y) = tri< (s≤s z≤n) (λ ()) (λ ())
cmpℕ (succ x) zero = tri> (λ ()) (λ ()) (s≤s z≤n)
cmpℕ (succ x) (succ y) with cmpℕ x y
... | tri<  a ¬b ¬c = tri< (s≤s a) (contraposition lemma-succ-≡ ¬b)
  (contraposition lemma-succ-≤ ¬c)
... | tri> ¬a ¬b  c = tri> (contraposition lemma-succ-≤ ¬a)
  (contraposition lemma-succ-≡ ¬b) (s≤s c)
... | tri= ¬a  b ¬c = tri= (contraposition lemma-succ-≤ ¬a)
  (cong succ b) (contraposition lemma-succ-≤ ¬c)
```

Транзитивность отношения

```
Trans : {A : Set} → Rel₂ A → Set
Trans {A} _rel_ = {a b c : A} → (a rel b) → (b rel c) → (a rel c)
```

Симметричность отношения.

```
Symmetric : ∀ {A : Set} → Rel₂ A → Set
Symmetric _rel_ = ∀ {a b} → a rel b → b rel a
```

Предикат P учитывает (соблюдает) отношение _rel_ .

```
_Respects_ : ∀ {ℓ} {A : Set} → (A → Set ℓ) → Rel₂ A → Set _
P Respects _rel_ = ∀ {x y} → x rel y → P x → P y
```

Отношение P соблюдает отношение _rel_ .

```
_Respects₂_ : ∀ {A : Set} → Rel₂ A → Rel₂ A → Set
P Respects₂ _rel_ =
  (∀ {x} → P x  Respects _rel_) ×
  (∀ {y} → flip P y Respects _rel_)
```

Тип данных для обобщенного отношения меньше или равно.

```
data _<=_ {A : Set} {_<_ : Rel₂ A} {_==_ : Rel₂ A} : Rel₂ A where
  le : ∀ {x y} → x < y → x <= y
  eq : ∀ {x y} → x == y → x <= y
```

Обобщенные функции минимум и максимум.

```
min max : {A : Set} {_<_ : Rel₂ A} {_==_ : Rel₂ A}
  → (cmp : Cmp _<_ _==_) → A → A → A
min cmp x y with cmp x y
... | tri< _ _ _ = x
... | _ = y
max cmp x y with cmp x y
... | tri> _ _ _ = x
... | _ = y
```

Лемма: элемент меньше или равный двух других элементов меньше или равен минимума из них.

```
lemma-<=min : {A : Set} {_<_ : Rel₂ A} {_==_ : Rel₂ A}
  {cmp : Cmp _<_ _==_} {a b c : A}
  → (_<=_ {_<_ = _<_} {_==_} a b)
  → (_<=_ {_<_ = _<_} {_==_} a c)
  → (_<=_ {_<_ = _<_} {_==_} a (min cmp b c))
```

Функция — минимум из трех элементов.

```
min3 : {A : Set} {_<_ : Rel₂ A} {_==_ : Rel₂ A}
  → (cmp : Cmp _<_ _==_) → A → A → A → A
min3 cmp x y z with cmp x y
... | tri< _ _ _ = min cmp x z
... | _ = min cmp y z
```

Аналогичная предыдущей лемма для минимума из трех элементов.

```
lemma-<=min3 : {A : Set} {_<_ : Rel₂ A} {_==_ : Rel₂ A}
  {cmp : Cmp _<_ _==_} {x a b c : A}
  → (_<=_ {_<_ = _<_} {_==_} x a)
  → (_<=_ {_<_ = _<_} {_==_} x b)
  → (_<=_ {_<_ = _<_} {_==_} x c)
  → (_<=_ {_<_ = _<_} {_==_} x (min3 cmp a b c))
lemma-<=min3 {cmp = cmp} {x} {a} {b} {c} xa xb xc with cmp a b
... | tri< _ _ _ = lemma-<=min {cmp = cmp} xa xc
... | tri= _ _ _ = lemma-<=min {cmp = cmp} xb xc
... | tri> _ _ _ = lemma-<=min {cmp = cmp} xb xc
```

Леммы lemma-<=min и lemma-<=min3 понадобятся при доказательстве соотношений между элементами, из котороых составляются новые кучи при их обработке.

Отношение _<=_ соблюдает отношение равенства _==_, с помощью которого оно определено.

```
resp<= : {A : Set} {_<_ : Rel₂ A} {_==_ : Rel₂ A}
  → (resp : _<_ Respects₂ _==_) → (trans== : Trans _==_)
  → (sym== : Symmetric _==_) → (_<=_ {A}{_<_}{_==_}) Respects₂ _=
resp<= {A}{_<_}{_==_} resp trans sym = left , right where
  left : ∀ {a b c : A} → b == c → a <= b → a <= c
  left b=c (le a<b) = le (fst resp b=c a<b)
  left b=c (eq a=b) = eq (trans a=b b=c)
  right : ∀ {a b c : A} → b == c → b <= a → c <= a
  right b=c (le a<b) = le (snd resp b=c a<b)
  right b=c (eq a=b) = eq (trans (sym b=c) a=b)
```

Транзитивность отношения _<=_.

```
trans<= : {A : Set} {_<_ : Rel₂ A} {_==_ : Rel₂ A}
  → _<_ Respects₂ _==_ → Symmetric _==_ → Trans _==_ → Trans _<_
  → Trans (_<=_ {A}{_<_}{_==_})
trans<= r s t== t< (le a<b) (le b<c) = le (t< a<b b<c)
trans<= r s t== t< (le a<b) (eq b=c) = le (fst r b=c a<b)
trans<= r s t== t< (eq a=b) (le b<c) = le (snd r (s a=b) b<c)
trans<= r s t== t< (eq a=b) (eq b=c) = eq (t== a=b b=c)
```

2.3.3. Куча

Модуль, в котором мы определим структуру данных куча, параметризован исходным типом, двумя отношениями, определенными для этого типа, _<_ и _==_. Также требуется симметричность и транзитивность _==_, транзитивность _<_, соблюдение отношением _<_ отношения _==_ и

```
module Heap (A : Set) (_<_ _==_ : Rel₂ A) (cmp : Cmp _<_ _==_)
  (sym== : Symmetric _==_) (trans== : Trans _==_)
  (trans< : Trans _<_) (resp : _<_ Respects₂ _==_)
  where
```

Будем индексировать кучу минимальным элементом в ней, для того, чтобы можно было строить инварианты порядка на куче исходя из этих индексов. Так как в пустой куче нет элементов, то мы не можем выбрать элемент, который нужно указать в индексе. Чтобы решить эту проблему, расширим исходный тип данных, добавив элемент, больший всех остальных. Тип данных для расширения исходного типа.

```
  data expanded (A : Set) : Set where
    # : A → expanded A -- (# x) - элемент исходного типа
    top : expanded A -- элемент расширение
```

Теперь нам нужно аналогичным образом расширить отношения заданные на множестве исходного типа. Тип данных для расширения отношения меньше.

```
  data _<E_ : Rel₂ (expanded A) where
  base : ∀ {x y : A} → x < y → (# x) <E (# y)
  ext  : ∀ {x : A} → (# x) <E top
```

Вспомогательная лемма, извлекающая доказательство для отношения элементов исходного типа из отношения для элементов расширенного типа.

```
  lemma-<E : ∀ {x} {y} → (# x) <E (# y) → x < y
  lemma-<E (base r) = r
```

Расширенное отношение меньше — транзитивно.

```
trans<E : Trans _<E_
trans<E {# _} {# _} {# _} a<b b<c =
  base (trans< (lemma-<E a<b) (lemma-<E b<c))
trans<E {# _} {# _} {top} _  _  = ext
```

Тип данных расширенного отношения равенства.

```
data _=E_ : Rel₂ (expanded A) where
  base : ∀ {x y} → x == y → (# x) =E (# y)
  ext  : top =E top
```

Расширенное отношение равенства — симметрично и транзитивно.

```
sym=E  : Symmetric _=E_
sym=E (base a=b) = base (sym== a=b)
sym=E ext = ext
trans=E : Trans _=E_
trans=E (base a=b) (base b=c) = base (trans== a=b b=c)
trans=E ext ext = ext
```

Отношение _<E_ соблюдает отношение _=E_.

```
respE : _<E_ Respects₂ _=E_
respE = left , right where
  left : ∀ {a b c : expanded A} → b =E c → a <E b → a <E c
  left {# _} {# _} {# _} (base r1) (base r2) = base (fst resp r1 r2)
  left {# _} {top} {top} ext ext = ext
```

```
right : ∀ {a b c : expanded A} → b =E c → b <E a → c <E a
right {# _} {# _} {# _} (base r1) (base r2) = base (snd resp r1 r2)
right {top} {# _} {# _} _ ext = ext
```

Отношение меньше-равно для расширенного типа.

```
_≤_ : Rel₂ (expanded A)
_≤_ = _<=_ {expanded A} {_<E_} {_=E_}
```

Транзитивность меньше-равно следует из свойств отношений `_=E_` и `_<E_`:

```
trans≤ : Trans _≤_
trans≤ = trans<= respE sym=E trans=E trans<E
resp≤ : _≤_ Respects₂ _=E_
resp≤ = resp<= respE trans=E sym=E
```

Вспомогательная лемма, извлекающая доказательство равенства элементов исходного типа из равенства элементов расширенного типа.

```
lemma-=E : ∀ {x} {y} → (# x) =E (# y) → x == y
lemma-=E (base r) = r
```

Трихотомичность для `_<E_` и `_=E_`.

```
cmpE : Cmp {expanded A} _<E_ _=E_
cmpE (# x) (# y) with cmp x y
cmpE (# x) (# y) | tri< a b c =
  tri< (base a) (contraposition lemma-=E b) (contraposition lemma-<E c)
cmpE (# x) (# y) | tri= a b c =
  tri= (contraposition lemma-<E a) (base b) (contraposition lemma-<E c)
```

```
cmpE (# x) (# y) | tri> a b c =
  tri> (contraposition lemma-<E a) (contraposition lemma-=E b) (base c)
cmpE (# x) top = tri< ext (λ ()) (λ ())
cmpE top (# y) = tri> (λ ()) (λ ()) ext
cmpE top top   = tri= (λ ()) ext (λ ())
```

Функция — минимум для расширенного типа.

```
minE : (x y : expanded A) → expanded A
minE = min cmpE
```

Вспомогательный тип данных для индексации кучи — куча полная или почти заполненная.

```
data HeapState : Set where
  full almost : HeapState
```

Тип данных для кучи, проиндексированный минимальным элементом кучи, натуральным числом — высотой — и заполненностью.

```
data Heap : (expanded A) → (h : ℕ) → HeapState → Set where
```

У пустой кучи минимальный элемент — top, высота — ноль. Пустая куча — полная.

```
eh : Heap top zero full
```

Полная куча высотой $n + 1$ состоит из корня и двух куч высотой n. Мы хотим в непустых кучах задавать порядок на элементах — элемент в узле меньше либо равен элементов в поддеревьях. Мы можем упростить этот инвариант, сравнивая элемент в узле только с корнями поддеревьев. Порядок кучи задается с помощью двух элементов отношения

$\_\leq\_$: i и j, которые говорят от том, что значение в корне меньше-равно значений в корнях левого и правого поддеревьев соответственно. На рисунке 2.2 схематичное изображены конструкторы типа данных Heap.

$$
\begin{aligned}
&\mathsf{nf} : \forall\ \{n\}\ \{x\ y\} \to (p : A) \to (i : (\#\ p) \leq x) \to (j : (\#\ p) \leq y)\\
&\quad \to (a : \mathsf{Heap}\ x\ n\ \mathsf{full})\\
&\quad \to (b : \mathsf{Heap}\ y\ n\ \mathsf{full})\\
&\quad \to \mathsf{Heap}\ (\#\ p)\ (\mathsf{succ}\ n)\ \mathsf{full}
\end{aligned}
$$

Куча высотой $n+2$, у которой нижний ряд заполнен до середины, состоит из корня и двух полных куч: левая высотой $n+1$ и правая высотой n.

$$
\begin{aligned}
&\mathsf{nd} : \forall\ \{n\}\ \{x\ y\} \to (p : A) \to (i : (\#\ p) \leq x) \to (j : (\#\ p) \leq y)\\
&\to (a : \mathsf{Heap}\ x\ (\mathsf{succ}\ n)\ \mathsf{full})\\
&\to (b : \mathsf{Heap}\ y\ n\ \mathsf{full})\\
&\to \mathsf{Heap}\ (\#\ p)\ (\mathsf{succ}\ (\mathsf{succ}\ n))\ \mathsf{almost}
\end{aligned}
$$

Куча высотой $n + 2$, у которой нижний ряд заполнен меньше, чем до середины, состоит из корня и двух куч: левая неполная высотой $n + 1$ и правая полная высотой n.

$$
\begin{aligned}
&\mathsf{nl} : \forall\ \{n\}\ \{x\ y\} \to (p : A) \to (i : (\#\ p) \leq x) \to (j : (\#\ p) \leq y)\\
&\to (a : \mathsf{Heap}\ x\ (\mathsf{succ}\ n)\ \mathsf{almost})\\
&\to (b : \mathsf{Heap}\ y\ n\ \mathsf{full})\\
&\to \mathsf{Heap}\ (\#\ p)\ (\mathsf{succ}\ (\mathsf{succ}\ n))\ \mathsf{almost}
\end{aligned}
$$

Неполная куча высотой $n + 2$, у которой нижний ряд заполнен больше, чем до середины, состоит из корня и двух куч: левая полная высотой $n + 1$ и правая неполная высотой $n + 1$.

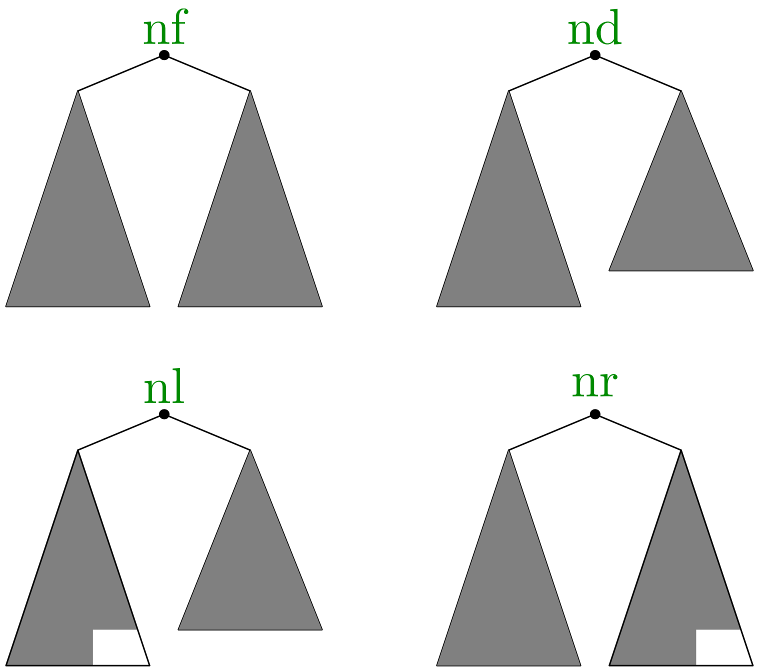

Рис. 2.2. Конструкторы типа данных Heap

$$\mathsf{nr} : \forall\ \{n\}\ \{x\ y\} \to (p : A) \to (i : (\#\ p) \leq x) \to (j : (\#\ p) \leq y)$$
$$\to (a : \mathsf{Heap}\ x\ (\mathsf{succ}\ n)\ \mathsf{full})$$
$$\to (b : \mathsf{Heap}\ y\ (\mathsf{succ}\ n)\ \mathsf{almost})$$
$$\to \mathsf{Heap}\ (\#\ p)\ (\mathsf{succ}\ (\mathsf{succ}\ n))\ \mathsf{almost}$$

Замечание: высота любой неполной кучи больше нуля.

$$\mathsf{lemma\text{-}almost\text{-}height} : \forall\ \{m\ h\} \to \mathsf{Heap}\ m\ h\ \mathsf{almost} \to h\ \mathbb{N}\!>\ 0$$

Функция — просмотр минимума в куче.

$$\mathsf{peekMin} : \forall\ \{m\ h\ s\} \to \mathsf{Heap}\ m\ h\ s \to (\mathsf{expanded}\ A)$$
$$\mathsf{peekMin}\ \mathsf{eh} = \mathsf{top}$$
$$\mathsf{peekMin}\ (\mathsf{nd}\ p\ \_\ \_\ \_\ \_) = \#\ p$$
$$\mathsf{peekMin}\ (\mathsf{nf}\ p\ \_\ \_\ \_\ \_) = \#\ p$$
$$\mathsf{peekMin}\ (\mathsf{nl}\ p\ \_\ \_\ \_\ \_) = \#\ p$$
$$\mathsf{peekMin}\ (\mathsf{nr}\ p\ \_\ \_\ \_\ \_) = \#\ p$$

Функция — минимум из трех элементов расширенного типа — частный случай ранее определенной общей функции.

$$\mathsf{min3E} : (\mathsf{expanded}\ A) \to (\mathsf{expanded}\ A) \to (\mathsf{expanded}\ A) \to (\mathsf{expanded}\ A)$$
$$\mathsf{min3E}\ x\ y\ z = \mathsf{min3}\ \mathsf{cmpE}\ x\ y\ z$$

Леммы для сравнения с минимумами для элементов расширенного типа.

$$\mathsf{lemma\text{-}{<}{=}minE} : \forall\ \{a\ b\ c\} \to a \le b \to a \le c \to a \le (\mathsf{minE}\ b\ c)$$
$$\mathsf{lemma\text{-}{<}{=}minE} = \mathsf{lemma\text{-}{<}{=}min}\ \{\mathsf{expanded}\ A\}\{\_{<}\mathsf{E}\_\}\{\_{=}\mathsf{E}\_\}\{\mathsf{cmpE}\}$$
$$\mathsf{lemma\text{-}{<}{=}min3E} : \forall\ \{x\ a\ b\ c\} \to x \le a \to x \le b \to x \le c \to x \le (\mathsf{min3E}\ a\ b\ c)$$
$$\mathsf{lemma\text{-}{<}{=}min3E} = \mathsf{lemma\text{-}{<}{=}min3}\ \{\mathsf{expanded}\ A\}\{\_{<}\mathsf{E}\_\}\{\_{=}\mathsf{E}\_\}\{\mathsf{cmpE}\}$$

Функция вставки элемента в полную кучу.

$$\mathsf{finsert} : \forall\ \{h\ m\} \to (z : A) \to \mathsf{Heap}\ m\ h\ \mathsf{full}$$
$$\to \Sigma\ \mathsf{HeapState}\ (\mathsf{Heap}\ (\mathsf{minE}\ m\ (\#\ z))\ (\mathsf{succ}\ h))$$

Вставка элемента в неполную кучу.

$$\mathsf{ainsert} : \forall\ \{h\ m\} \to (z : A) \to \mathsf{Heap}\ m\ h\ \mathsf{almost}$$
$$\to \Sigma\ \mathsf{HeapState}\ (\mathsf{Heap}\ (\mathsf{minE}\ m\ (\#\ z))\ h)$$

Вспомогательный тип данных.

```
data OR (A B : Set) : Set where
  orA : A → OR A B
  orB : B → OR A B
```

Слияние двух полных куч одной высоты.

$$\mathsf{fmerge} : \forall\ \{x\ y\ h\} \to \mathsf{Heap}\ x\ h\ \mathsf{full} \to \mathsf{Heap}\ y\ h\ \mathsf{full}$$
$$\to \mathsf{OR}\ (\mathsf{Heap}\ x\ \mathsf{zero}\ \mathsf{full} \times (x \equiv y) \times (h \equiv \mathsf{zero}))$$

$(\mathsf{Heap}\ (\mathsf{minE}\ x\ y)\ (\mathsf{succ}\ h)\ \mathsf{almost})$

Извлечение минимума из полной кучи.

$\mathsf{fpop} : \forall\ \{m\ h\} \to \mathsf{Heap}\ m\ (\mathsf{succ}\ h)\ \mathsf{full}$
$\to \mathsf{OR}\ (\Sigma\ (\mathsf{expanded}\ A)$
$(\lambda\ x \to (\mathsf{Heap}\ x\ (\mathsf{succ}\ h)\ \mathsf{almost}) \times (m \leq x)))$
$(\mathsf{Heap}\ \mathsf{top}\ h\ \mathsf{full})$

Составление полной кучи высотой $h + 1$ из двух куч высотой h и одного элемента.

$\mathsf{makeH} : \forall\ \{x\ y\ h\} \to (p : A) \to \mathsf{Heap}\ x\ h\ \mathsf{full} \to \mathsf{Heap}\ y\ h\ \mathsf{full}$
$\to \mathsf{Heap}\ (\mathsf{min3E}\ x\ y\ (\#\ p))\ (\mathsf{succ}\ h)\ \mathsf{full}$

Вспомогательные леммы, использующие lemma-<=minE.

$\mathsf{lemma\text{-}resp} : \forall\ \{x\ y\ a\ b\} \to x == y \to (\#\ x) \leq a \to (\#\ x) \leq b$
$\to (\#\ y) \leq \mathsf{minE}\ a\ b$
$\mathsf{lemma\text{-}resp}\ x{=}y\ i\ j = \mathsf{lemma\text{-}{<}{=}minE}\ (\mathsf{snd}\ \mathsf{resp}{\leq}\ (\mathsf{base}\ x{=}y)\ i)$
$(\mathsf{snd}\ \mathsf{resp}{\leq}\ (\mathsf{base}\ x{=}y)\ j)$
$\mathsf{lemma\text{-}trans} : \forall\ \{x\ y\ a\ b\} \to y < x \to (\#\ x) \leq a \to (\#\ x) \leq b$
$\to (\#\ y) \leq \mathsf{minE}\ a\ b$
$\mathsf{lemma\text{-}trans}\ y{<}x\ i\ j = \mathsf{lemma\text{-}{<}{=}minE}\ (\mathsf{trans}{\leq}\ (\mathsf{le}\ (\mathsf{base}\ y{<}x))\ i)$
$(\mathsf{trans}{\leq}\ (\mathsf{le}\ (\mathsf{base}\ y{<}x))\ j)$

Слияние поддеревьев из кучи, у которой последний ряд заполнен до середины, определенной конструктором nd.

$\mathsf{ndmerge} : \forall\ \{x\ y\ h\} \to \mathsf{Heap}\ x\ (\mathsf{succ}\ (\mathsf{succ}\ h))\ \mathsf{full} \to \mathsf{Heap}\ y\ (\mathsf{succ}\ h)\ \mathsf{full}$
$\to \mathsf{Heap}\ (\mathsf{minE}\ x\ y)\ (\mathsf{succ}\ (\mathsf{succ}\ (\mathsf{succ}\ h)))\ \mathsf{almost}$

Слияние неполной кучи высотой $h + 2$ и полной кучи высотой $h + 1$ или $h + 2$.

$$\begin{aligned}
&\mathsf{afmerge} : \forall\ \{h\ x\ y\} \to \mathsf{Heap}\ x\ (\mathsf{succ}\ (\mathsf{succ}\ h))\ \mathsf{almost} \\
&\quad \to \mathsf{OR}\ (\mathsf{Heap}\ y\ (\mathsf{succ}\ h)\ \mathsf{full})\ (\mathsf{Heap}\ y\ (\mathsf{succ}\ (\mathsf{succ}\ h))\ \mathsf{full}) \\
&\quad \to \mathsf{OR}\ (\mathsf{Heap}\ (\mathsf{minE}\ x\ y)\ (\mathsf{succ}\ (\mathsf{succ}\ h))\ \mathsf{full}) \\
&\qquad (\mathsf{Heap}\ (\mathsf{minE}\ x\ y)\ (\mathsf{succ}\ (\mathsf{succ}\ (\mathsf{succ}\ h)))\ \mathsf{almost})
\end{aligned}$$

Извлечение минимума из неполной кучи.

$$\begin{aligned}
&\mathsf{apop} : \forall\ \{m\ h\} \to \mathsf{Heap}\ m\ (\mathsf{succ}\ h)\ \mathsf{almost} \\
&\quad \to \mathsf{OR}\ (\Sigma\ (\mathsf{expanded}\ A)\ (\lambda\ x \to (\mathsf{Heap}\ x\ (\mathsf{succ}\ h)\ \mathsf{almost}) \times (m \leq x))) \\
&\qquad (\Sigma\ (\mathsf{expanded}\ A)\ (\lambda\ x \to (\mathsf{Heap}\ x\ h\ \mathsf{full}) \times (m \leq x)))
\end{aligned}$$

2.4. Выводы по главе 2

Разработаны типы данных для представления структуры данных двоичная куча.

Список литературы

1. *Thompson S.* Type theory and functional programming. International computer science series. Addison-Wesley, 1991. С. I–XV, 1–372. ISBN: 978-0-201-41667-1.
2. *Sørensen M. H. B.*, *Urzyczyn P.* Lectures on the Curry-Howard Isomorphism. 1998.
3. The Haskell Programming Language. http://www.haskell.org/haskellwiki/Haskell.
4. A Truly Integrated Functional Logic Languageu. http://www-ps.informatik.uni-kiel.de/currywiki/.
5. Agda language. http://wiki.portal.chalmers.se/agda/pmwiki.php.
6. *IEEE.* IEEE Std 1178-1990, IEEE Standard for the Scheme Programming Language. 1991. С. 52. ISBN: 1-55937-125-0. http://standards.ieee.org/reading/ieee/std_public/description/busarch/1178-1990_desc.html.
7. *Hickey R.* The Clojure programming language / DLS. Под ред. Johan Brichau. ACM, 2008. С. 1. ISBN: 978-1-60558-270-2.
8. *Abelson H.*, *Sussman G. J.* Structure and Interpretation of Computer Programs. MIT Press, 1985. ISBN: 0-262-51036-7.
9. *Milner R.*, *Tofte M.*, *Macqueen D.* The Definition of Standard ML. Cambridge, MA, USA: MIT Press, 1997. ISBN: 0262631814.
10. OCaml. http://ocaml.org/.
11. *Martin-Löf P.* Intuitionistic Type Theory. Bibliopolis, 1984. ISBN: 88-7088-105-9.
12. *Dybjer P.* Inductive Families // Formal Asp. Comput. 1994. №4. С. 440–465.
13. *Atkey R.*, *Johann P.*, *Ghani N.* Refining Inductive Types // Logical Methods in Computer Science. 2012. №2.
14. *Xi H.*, *Pfenning F.* Dependent Types in Practical Programming / POPL. Под ред. Andrew W. Appel и Alex Aiken. ACM, 1999. С. 214–227. ISBN: 1-58113-095-3.
15. *McBride C.* How to Keep Your Neighbours in Order. https://personal.cis.strath.ac.uk/conor.mcbride/Pivotal
16. *McBride C.*, *Norell U.*, *Danielsson N. A.* The Agda standard library — AVL trees. http://agda.github.io/agda-stdlib/html/Data.AVL.html.
17. *Cormen T. H.*, *Leiserson C. E.*, *Rivest R. L.*, *Stein C.* Introduction to Algorithms, Second Edition. The MIT Press и McGraw-Hill Book Company, 2001. ISBN: 0-262-03293-7, 0-07-013151-1.
18. The Agda standard library. http://agda.github.io/agda-stdlib/html/README.html.