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: ассистент кафедры ТП 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

1.1. Функциональное программирование

Функциональное программирование — парадигма программирования, в которой процесс вычисления трактуется как вычисление значений функций в математическом понимании последних (в отличие от функций как подпрограмм в процедурном программировании) [**wikiFP**]. В функциональном программировании избегается использование изменяемого глобального состояния и изменяемых данных.

1.1.1. Концепции

Функции высших порядков — это такие функции, которые могут принимать в качестве аргументов и возвращать другие функции [**SICP**]. *Чистые функции* — функции, которые не имеют побочных эффектов ввода-вывода и изменения памяти, они зависят только от своих параметров и возвращают только свой результат.

1.1.2. Сопоставление с образцом

Сопоставление с образцом — способ обработки структур данных, при котором аргументы функций сравниваются (по значению или по структуре) с образцом такого же типа.

1.2. Теория типов

Теория типов — какая-либо формальная система, являющаяся альтернативой наивной теории множеств, сопровождаемая классификацией элементов такой системы с помощью типов, образующих некоторую иерархию. Элементы теории типов — выражения, также называемые *термами*. Если терм M имеет тип A, то это записывают так: $M : A$. Например, $2 : \mathbb{N}$.

Теории типов также содержат правила для переписывания термов — замены подтермов формулы другими термами. Такие правила также называют правилами *редукции* или *конверсии* термов. Например, термы $2+1$ и 3 — разные термы, но первый редуцируется во второй: $2+1 \twoheadrightarrow 3$. Про терм, который не может быть редуцирован, говорят, что терм — в *нормальной форме*.

1.2.1. Отношение конвертабельности

Два терма называются *конвертабельными*, если существует терм, к которому они оба редуцируются. 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.

1.2.2. Интуиционистская теория типов

Интуиционистская теория типов основана на математическом конструктивизме [**MLTT**].

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 сумма (пара). Например, тип $\Sigma_{n:\mathbb{N}} \mathrm{Vec}(\mathbb{R}, n)$ — тип пары из числа n и кортежа из n вещественных чисел.

Конечные типы в ИТТ: $\bot$ или 0 — пустой тип, не содержащий ни одного элемента; $\top$ или 1 — единичный тип, содержащий единственный элемент. *Тип равенства*: для x и y выражение $x \equiv y$ обозначает тип доказательства равенства x и y. То есть, если тип $x \equiv y$ населен, то x и y называются равными. Есть только один каноничный элемент типа $x \equiv x$ — доказательство рефлексивности: $refl : \Pi_{a:A} a \equiv a$.

1.3. Унификация

Унификация — процесс и алгоритм решения уравнений над выражениями в теории типов. Алгоритм унификации находит подстановку, которая назначает значение каждой переменной в выражении, после применения которой, части уравнения становятся конвертабельными. Пример: равенство двух списков $cons(x, cons(x, nil)) \equiv cons(2, y)$ — уравнение с двумя переменными x и y. Решение: подстановка $x \mapsto 2, y \mapsto cons(2, nil)$.

1.4. Индуктивные семейства

Определение 1.1. *Индуктивное семейство* [**DybjerIndFam**]— это семейство типов данных, которые могут 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 [**OkasakiThesis**, **McBridePivotal**] приведены различные подходы к построению функциональных структур данных.

Пример задания структуры данных и инвариантов — тип данных AVL-дерева и для хранения баланса в AVL-дереве [**AVLTree**].
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
```

1.5. Agda

Agda [**AgdaLang**] — 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:

$\mathsf{head} : \forall\ \{A\}\ \{n\} \to \mathsf{Vec}\ A\ (\mathsf{succ}\ n) \to A$

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

$\mathsf{head}\ (\mathsf{cons}\ a\ as) = a$

1.6. Выводы по главе ??

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 [**DBLP:books/mg/CormenLRS01**] — 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

2.3. Реализация

2.3.1. Вспомогательные определения

Часть общеизвестных определений заимствована из стандартной библиотеки Agda [**AgdaSLib**].

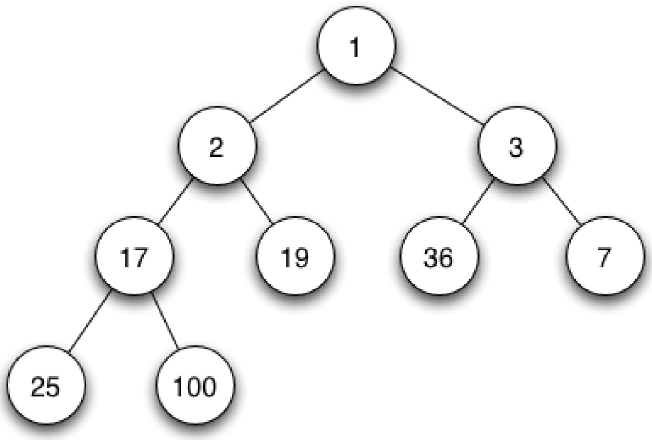

Рис. 2.1. Пример заполненной кучи для минимума

Тип данных для пустого типа из интуционистской теории типов.

```
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 ИТТ.

```
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 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
... | tri> ¬a ¬b  c = tri> (contraposition lemma-succ-≤ ¬a) (contraposition lemma-
... | tri= ¬a  b ¬c = tri= (contraposition lemma-succ-≤ ¬a) (cong succ b) (contrapo
```

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 _<_ _==
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 (min cmp b c))
```

Функция — минимум из трех элементов.

```
min3 : {A : Set} {_<_ : Rel₂ A} {_==_ : Rel₂ A} → (cmp : Cmp _<_ _==_)
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)
  → (_<=_ {_<_ = _<_} {_==_} 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
```

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

```
resp<= : {A : Set} {_<_ : Rel₂ A} {_==_ : Rel₂ A} → (resp : _<_ 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)
```

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 TryHeap (A : Set) (_<_ _==_ : Rel₂ A) (cmp : Cmp _<_ _==_)
  (sym== : Symmetric _==_) (resp : _<_ Respects₂ _==_) (trans< : Trans _<
  (trans== : Trans _==_)
  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
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.

$$\mathsf{data}\ \mathsf{Heap} : (\mathsf{expanded}\ A) \to (h : \mathbb{N}) \to \mathsf{HeapState} \to \mathsf{Set}\ \mathsf{where}$$

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

$$\mathsf{eh} : \mathsf{Heap}\ \mathsf{top}\ \mathsf{zero}\ \mathsf{full}$$

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 **??** 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.

```
nl : ∀ {n} {x y} → (p : A) → (i : (# p) ≤ x) → (j : (# p) ≤ y)
→ (a : Heap x (succ n) almost)
→ (b : Heap y n full)
→ Heap (# p) (succ (succ n)) almost
```

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 $n + 1$.

```
nr : ∀ {n} {x y} → (p : A) → (i : (# p) ≤ x) → (j : (# p) ≤ y)
→ (a : Heap x (succ n) full)
→ (b : Heap y (succ n) almost)
→ Heap (# p) (succ (succ n)) almost
```

Замечание: высота любой неполной кучи больше нуля.

```
lemma-almost-height : ∀ {m h} → Heap m h almost → h ℕ> 0
```

Функция — просмотр минимума в куче.

```
peekMin : ∀ {m h s} → Heap m h s → (expanded A)
peekMin eh = top
peekMin (nd p _ _ _ _) = # p
peekMin (nf p _ _ _ _) = # p
peekMin (nl p _ _ _ _) = # p
```

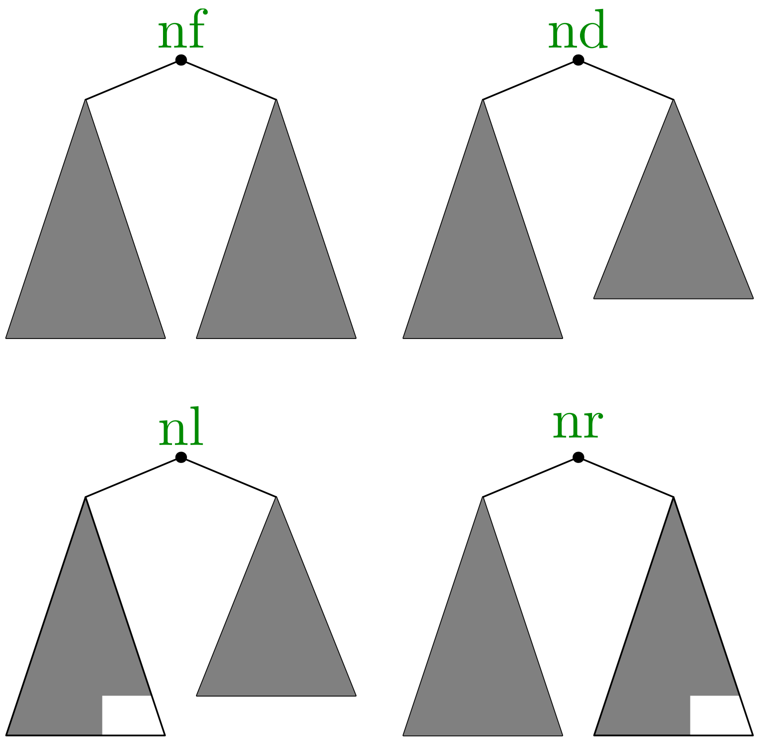

Рис. 2.2. Конструкторы типа данных Heap

```
peekMin (nr p _ _ _ _) = # p
```

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

```
min3E : (expanded A) → (expanded A) → (expanded A) → (expanded A)
min3E x y z = min3 cmpE x y z
```

Леммы для сравнения с минимумами для элементов расширенного типа.

```
lemma-<=minE : ∀ {a b c} → a ≤ b → a ≤ c → a ≤ (minE b c)
lemma-<=minE ab ac = lemma-<=min {expanded A}{_<E_}{_=E_}{cmpE} a
lemma-<=min3E : ∀ {x a b c} → x ≤ a → x ≤ b → x ≤ c → x ≤ (min3E a b c)
lemma-<=min3E = lemma-<=min3 {expanded A}{_<E_}{_=E_}{cmpE}
```

Функция вставки элемента в полную кучу.

```
finsert : ∀ {h m} → (z : A) → Heap m h full
  → Σ HeapState (Heap (minE m (# z)) (succ h))
```

Вставка элемента в неполную кучу.

```
ainsert : ∀ {h m} → (z : A) → Heap m h almost
  → Σ HeapState (Heap (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.

```
fmerge : ∀ {x y h} → Heap x h full → Heap y h full
→ OR (Heap x zero full × (x ≡ y) × (h ≡ zero))
  (Heap (minE x y) (succ h) almost)
```

Извлечение минимума из полной кучи.

```
fpop : ∀ {m h} → Heap m (succ h) full
  → OR (Σ (expanded A)
    (λ x → (Heap x (succ h) almost) × (m ≤ x)))
(Heap top h full)
fpop (nf _ _ _ eh eh) = orB eh
fpop (nf _ i j (nf x i₁ j₁ a b) (nf y i₂ c d)) with fmerge (nf x i₁ j₁ a b) (nf y i₂ j₂
... | orA (() , _ , _)
... | orB res = orA ((minE (# x) (# y)) , res , lemma-<=minE i j)
```

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

```
makeH : ∀ {x y h} → (p : A) → Heap x h full → Heap y h full → Heap (min3E x
```

Вспомогательные леммы, использующие lemma-<=minE.

lemma-resp : ∀ $\{x\ y\ a\ b\}$ → $x == y$ → (# x) ≤ a → (# x) ≤ b
  → (# y) ≤ minE a b
lemma-resp $x{=}y$ i j = lemma-<=minE (snd resp≤ (base $x{=}y$) i)
  (snd resp≤ (base $x{=}y$) j)
lemma-trans : ∀ $\{x\ y\ a\ b\}$ → $y < x$ → (# x) ≤ a → (# x) ≤ b
  → (# y) ≤ minE a b
lemma-trans $y{<}x$ i j = lemma-<=minE (trans≤ (le (base $y{<}x$)) i)
  (trans≤ (le (base $y{<}x$)) j)

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

ndmerge : ∀ $\{x\ y\ h\}$ → Heap x (succ (succ h)) full → Heap y (succ h) full
→ Heap (minE x y) (succ (succ (succ h))) almost

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

afmerge : ∀ $\{h\ x\ y\}$ → Heap x (succ (succ h)) almost
  → OR (Heap y (succ h) full) (Heap y (succ (succ h)) full)
  → OR (Heap (minE x y) (succ (succ h)) full) (Heap (minE x y) (succ (succ (succ

Извлечение минимума из неполной кучи.

apop : ∀ $\{m\ h\}$ → Heap m (succ h) almost
  → OR (Σ (expanded A) (λ x → (Heap x (succ h) almost) × (m ≤ x)))
    (Σ (expanded A) (λ x → (Heap x h full) × (m ≤ x)))

2.4. Выводы по главе ??

Разработаны типы данных для представления структуры данных двоичная куча.