Математические методы верификации схем и программ

mk.cs.msu.ru → Лекционные курсы
→ Математические методы верификации схем и программ

Блок 20

Двоичные решающие диаграммы:
BDD, OBDD, ROBDD

Лектор:
Подымов Владислав Васильевич
E-mail:
valdus@yandex.ru

ВМК МГУ, 2022/2023, осенний семестр

Вступление

Двоичная решающая диаграмма (Binary Decision Diagram; BDD) — это один из наиболее популярных способов эффективного представления булевых функций для тех задач, в которых требуется преобразование структур, отвечающих построению формул над функциями

Существует несколько широко применяющихся русских вариантов названия этой структуры данных:

- Вместо «двоичная» иногда пишут «бинарная»
- Вместо «решающая диаграмма» иногда пишут «разрешающая диаграмма» или «диаграмма решений»

Вступление

Символьные представления нередко основываются на BDD или аналогичных структурах, и поэтому считается, что для более полного понимания тонкостей эффективной работы с символьными представлениями следует иметь общие знания об устройстве BDD

В эти знания входит *как минимум* то,

- как устроены (синтаксис) BDD и какие булевы функции ими реализуются (семантика)
- как строить BDD по другим представлениям (например, формулам)
- какие операции можно выполнять над BDD и как устроены соответствующие алгоритмы

BDD: синтаксис

Двоичная решающая диаграмма над упорядоченным набором переменных $x_1, \ldots, x_n$ — это конечный ациклический ориентированный граф, устроенный так

Вершины BDD обычно называют узлами

В графе есть два выделенных узла: 0 и 1

Узлы 0, 1 называются терминальными, а остальные — внутренними

Каждый внутренний узел v помечен одной из переменных ($var(v)$)

Из каждого внутреннего узла исходят ровно две дуги́, одна помечена символом 0, другая — символом 1

Из терминального узла не исходит ни одной дуги́

Узел, достижимый из v по дуге с символом 0, называется младшим потомком ($low(v)$), а с символом 1 — старшим потомком ($high(v)$)

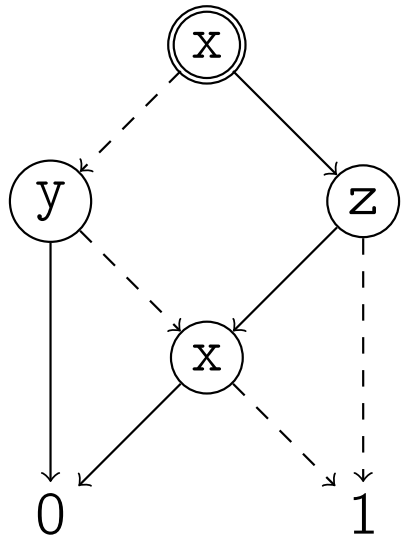
Вершины $low(v)$ и $high(v)$ также будем обозначать $v[0]$ и $v[1]$

Нередко ду́ги BDD изображаются так: метки 0 и 1 опускаются, и дуга с меткой 0 изображается пунктиром

Один (и только один) из узлов BDD объявлен корнем

BDD: синтаксис

Пример



Корень BDD изображён двойным контуром

Для внутреннего узла v, для которой $var(v) = \mathrm{y}$, верно

- $high(v) = v[1] = 0$ и
- $var(low(v)) = var(v[0]) = \mathrm{x}$

BDD: семантика

Каждому узлу v BDD $\mathcal{D}$ над переменными $x_1, \ldots, x_n$ сопоста́вим n-местную булеву формулу Φ_v^D:

- $\Phi_0^D = 0$
- $\Phi_1^D = 1$
- Для внутреннего узла v верно
  $\Phi_v^D = \neg var(v) \,\&\, \Phi_{low(v)}^D \vee var(v) \,\&\, \Phi_{high(v)}^D$
  - Формула вида $\neg x \,\&\, \varphi \vee x \,\&\, \psi$ называется разложением Шеннона

В узле v BDD $\mathcal{D}$ над переменными $x_1, \ldots, x_n$ реализуется n-местная булева функция $\mathfrak{f}_v^D$ — это функция, реализуемая формулой Φ_v^d

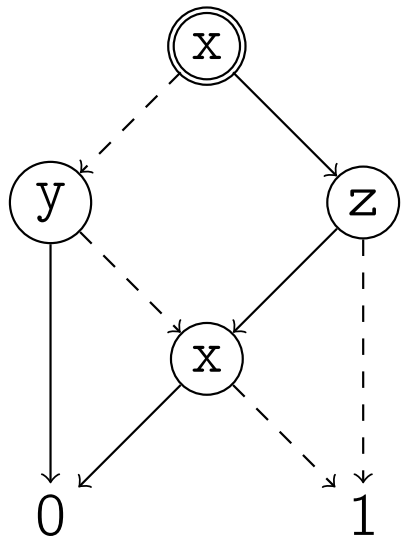
BDD $\mathcal{D}$ реализует булеву функцию $\mathfrak{f}^D$, реализуемую в её корне

Альтернативный способ определения значения $\mathfrak{f}^D(\alpha_1, \ldots, \alpha_n)$ (значения $\mathcal{D}$ на оценке переменных $\xi = [\mathrm{x}_1/\alpha_1, \ldots, \mathrm{x}_n/\alpha_n]$):

- Обойдём BDD как граф, начав в корне
- Если обход завершился в узле 0 или 1, то это значение объявляется значением $\mathfrak{f}^D(\alpha_1, \ldots, \alpha_n)$
- Если текущий узел v — внутренний, то следующим обходится узел $v[\xi(var(v))]$

BDD: семантика

Пример диаграммы $\mathcal{D}$:



Пронумеруем внутренние узлы по строчкам, во второй строке слева направо: v_0, v_1, v_2, v_3

$\Phi^{\mathcal{D}}_{v_3} = \neg \mathrm{x} \,\&\, 1 \vee \mathrm{x} \,\&\, 0 \sim \neg \mathrm{x}$

$\Phi^{\mathcal{D}}_{v_2} = \neg \mathrm{z} \,\&\, 1 \vee \mathrm{z} \,\&\, \Phi^{\mathcal{D}}_{v_3} \sim \neg \mathrm{z} \vee \neg \mathrm{x}$

$\Phi^{\mathcal{D}}_{v_1} = \neg \mathrm{y} \,\&\, \Phi^{\mathcal{D}}_{v_3} \vee \mathrm{y} \,\&\, 0 \sim \neg \mathrm{y} \,\&\, \neg \mathrm{x}$

$\Phi^{\mathcal{D}}_{v_0} = \neg \mathrm{x} \,\&\, \Phi^{\mathcal{D}}_{v_1} \vee \mathrm{x} \,\&\, \Phi^{\mathcal{D}}_{v_2} \sim \neg x \,\&\, \neg \mathrm{y} \vee \mathrm{x} \,\&\, \neg \mathrm{z}$

То есть диаграммой $\mathcal{D}$ реализуется та же функция, что и формулой $\neg x$

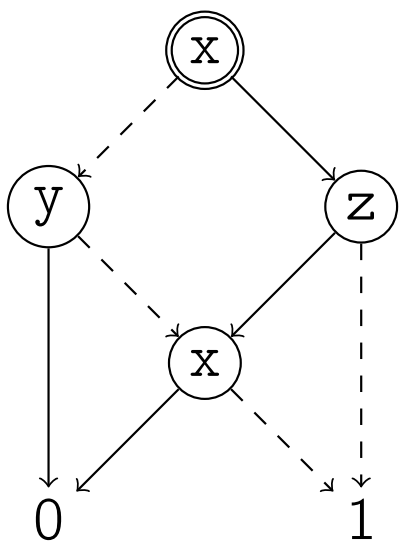
Это подтверждает и обход на оценке $[\mathrm{x}/1, \mathrm{y}/0, \mathrm{z}/1]$: $\textcircled{\textcircled{\mathrm{x}}} \xrightarrow{1} \textcircled{\mathrm{z}} \xrightarrow{1} \textcircled{\mathrm{x}} \xrightarrow{1} 0$

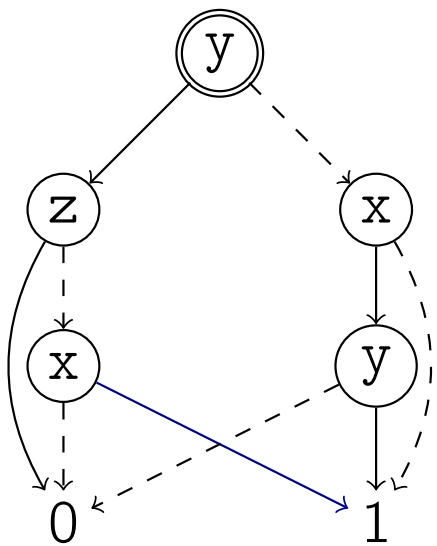
BDD: семантика

Две BDD $\mathcal{D}_1$, $\mathcal{D}_2$ (а также BDD $\mathcal{D}$ и формула φ) над переменными $x_1, \ldots, x_n$ называются эквивалентными ($\mathcal{D}_1 \sim \mathcal{D}_2$; $\mathcal{D} \sim \varphi$), если ими реализуются одинаковые функции над этим набором переменных

Проблема, присущая BDD: непросто проверить их эквивалентность, т.к. одна и та же функция может реализовываться существенно разными по структуре диаграммами

Например, такие две BDD эквивалентны:



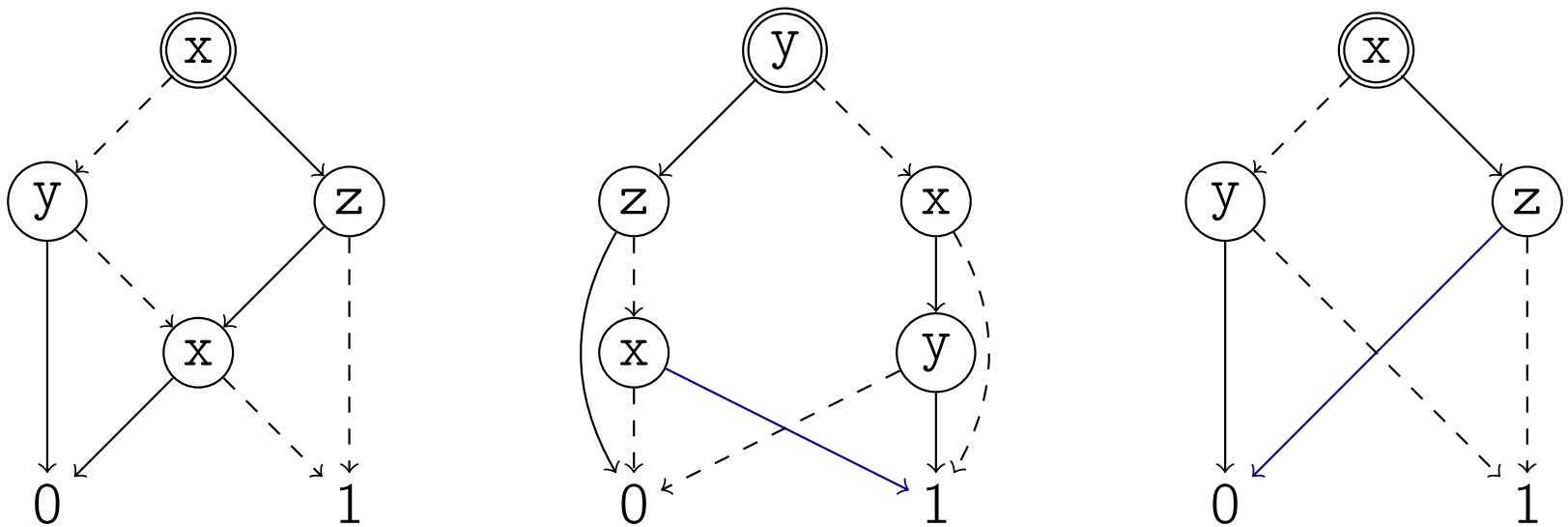


OBDD

Один из факторов, влияющих на трудность проверки эквивалентности BDD — это возможность записывать переменные в узлах «хаотично»

BDD $\mathcal{D}$ над набором переменных $x_1, \ldots, x_n$ называется упорядоченной (Ordered BDD; OBDD), если для любой дуги $v \to w$, ведущей во внутренний узел, верно $var(v) < var(w)$ для естественного порядка $<$ переменных: $x_i < x_j \Leftrightarrow i < j$

Например, среди изображённых ниже эквивалентных BDD над набором переменных $\mathtt{x}, \mathtt{y}, \mathtt{z}$ только самая правая упорядочена (является OBDD)

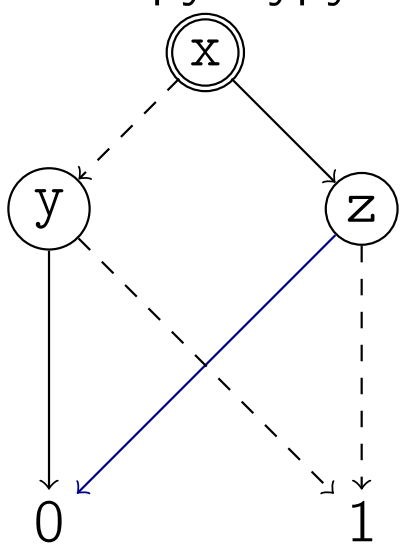


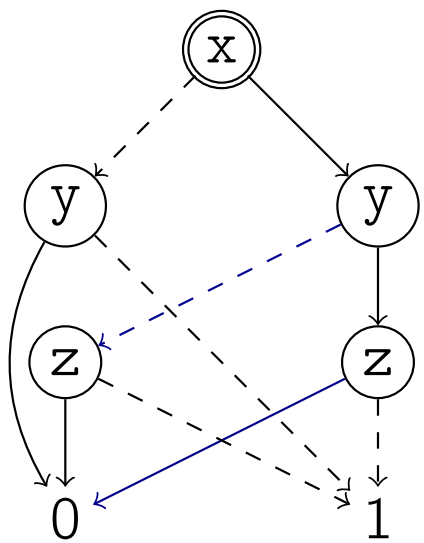
ROBDD

Для практических целей хотелось бы иметь **каноническое** представление булевых функций решающими диаграммами: единственное, и при этом такое, с которым было бы достаточно удобно работать (строить и преобразовывать)

Проблема, присущая OBDD: они не могут быть признаны каноническим представлением, т.к. бывают существенно различные эквивалентные OBDD

Например, следующие две OBDD над $\mathtt{x}, \mathtt{y}, \mathtt{z}$ эквивалентны, но имеют различное число узлов и хотя и не очень сильно, но всё же заметно различающуюся структуру



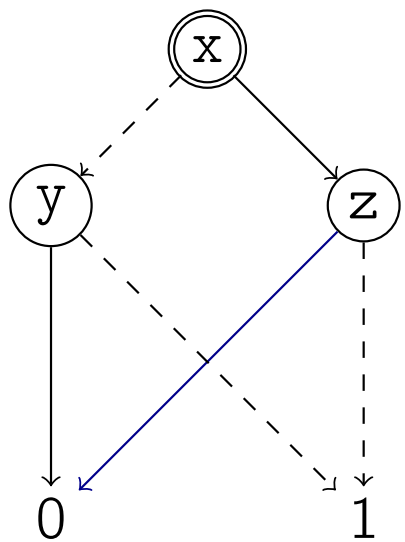


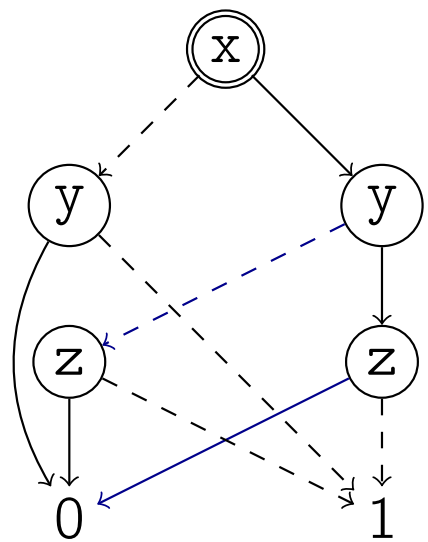
ROBDD

OBDD называется приведённой (или сокращённой, или редуцированной; Reduced OBDD; ROBDD), если для неё выполнены два условия:

1. Все узлы достижимы из корня
2. В любой паре различных узлов реализуются различные функции

Например, среди изображённых ниже диаграмм над $\mathtt{x}, \mathtt{y}, \mathtt{z}$ левая является приведённой, а правая — нет

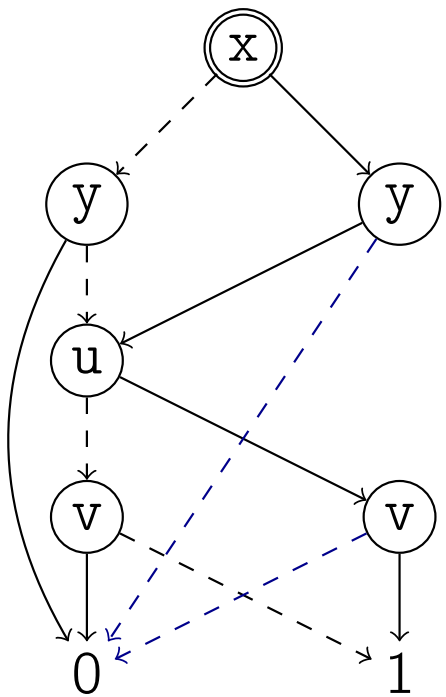


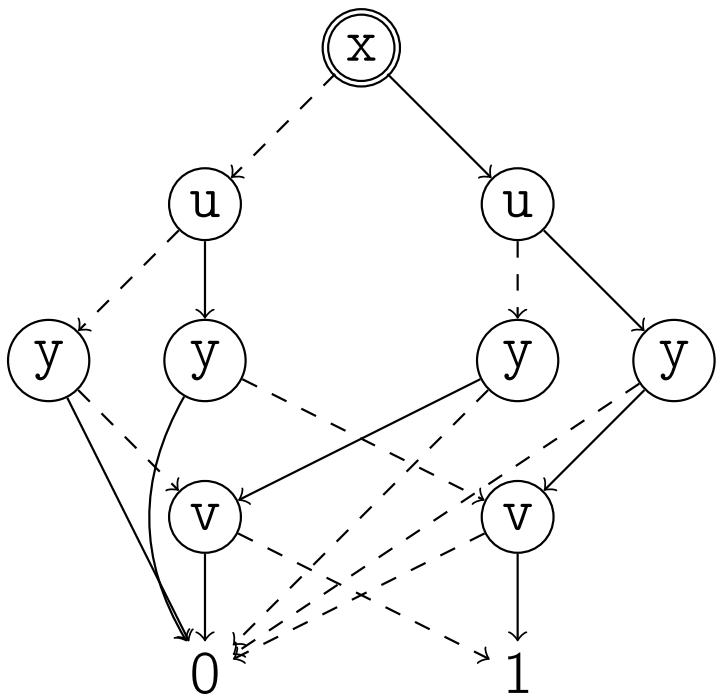


ROBDD

При использовании ROBDD очень важную роль играет выбор порядка переменных, над которой строится BDD

Например, ROBDD, эквивалентная формуле $(\mathtt{x} \leftrightarrow \mathtt{y}) \,\&\, (\mathtt{u} \leftrightarrow \mathtt{v})$ для порядка $\mathtt{x} < \mathtt{y} < \mathtt{u} < \mathtt{v}$ имеет заметно меньше вершин, чем для порядка $\mathtt{x} < \mathtt{u} < \mathtt{y} < \mathtt{v}$:





ROBDD

Так как решающие диаграммы не относятся напрямую к формулировке и решению рассматриваемых задач верификации и являются только вспомогательным «техническим» инструментом, то основные свойства диаграмм и алгоритмы будут приводиться без обоснования

Утверждение. **Если ROBDD D_1 и D_2 над общим набором переменных эквивалентны, то они изоморфны как размеченные графы**

Изоморфизм ROBDD проверить несложно, для этого можно:

- Однозначно построить соответствие вершин, начав с соответствия корней и продвигаясь по дугам с одинаковыми метками
  - Если в сопоставление входит пара (v, w), то должны входить и пары $(low(v), low(w))$ и $(high(v), high(w))$
- В случае успешного (взаимно однозначного) сопоставления — что друг другу сопоставлены ноли и единицы, и что сопоставленные вершины обязательно помечены одинаковыми переменными

ROBDD обеспечивают единственность представления функции с точностью до графового изоморфизма — а удобно ли с ними работать?

ROBDD: приведение OBDD

Дано: OBDD $\mathcal{D}$

Требуется: построить ROBDD $\mathcal{D}^*$, эквивалентную $\mathcal{D}$, над тем же набором переменных

Алгоритм устроен несложно — достаточно, пока это возможно, выполнять следующие три несложных преобразования:

- Если в диаграмме есть внутренний узел v, отличный от корня, в который не входит ни одной дуги́, то удалить v и исходящие ду́ги
- Если в диаграмме есть внутренний узел v, такой что $\mathit{low}(v) = \mathit{high}(v)$, то удалить v и все ду́ги, входившие в v, в $\mathit{low}(v)$; если v был корнем, то объявить $\mathit{low}(v)$ корнем
- Если в диаграмме есть различные внутренние узлы v, w, такие что $\mathit{low}(v) = \mathit{low}(w)$ и $\mathit{high}(v) = \mathit{high}(w)$ и w не корень, то удалить узел w и перенаправить все ду́ги, входившие в w, в v

ROBDD: простейшие диаграммы

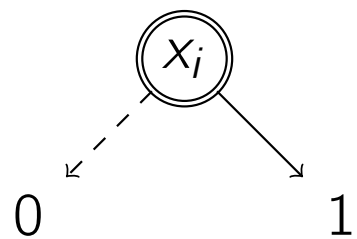
$\mathcal{D}^{\varphi}$ — так обозна́чим ROBDD, эквивалентную формуле φ

ROBDD для простейших функций устроены очень просто

$\mathcal{D}^{0}$:

$\mathcal{D}^{1}$:

$\mathcal{D}^{x_i}$:



ROBDD: отрицание

Дано: ROBDD $\mathcal{D}^{\varphi}$

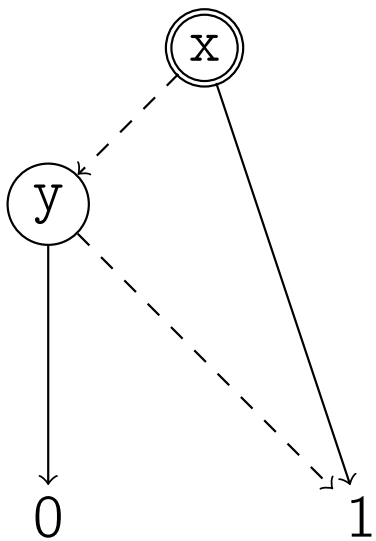
Требуется: построить ROBDD $\neg D^{\varphi} = \mathcal{D}^{\neg\varphi}$ над тем же набором переменных

Алгоритм устроен несложно:

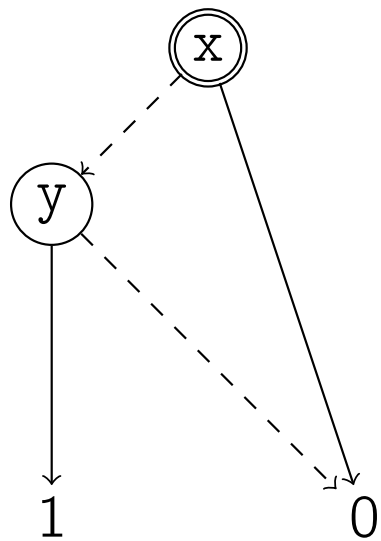
- Поменять местами терминальные вершины

Пример

$\mathcal{D}^{\mathrm{x}\,\&\,\neg\mathrm{y}}$:



$\mathcal{D}^{\neg(\mathrm{x}\,\&\,\neg\mathrm{y})}$:



ROBDD: подстановка константы

$\varphi[\mathrm{x}/e]$ — формула, получающаяся из φ подстановкой выражения e на место переменной x

Дано: ROBDD $\mathcal{D}^{\varphi}$, значение $b \in \{0, 1\}$

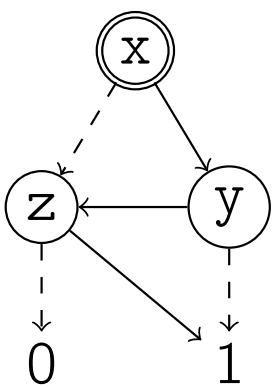
Требуется: построить ROBDD $\mathcal{D}^{\varphi}[\mathrm{x}/b] = \mathcal{D}^{\varphi[\mathrm{x}/b]}$ над тем же набором переменных

Алгоритм и тут устроен несложно:

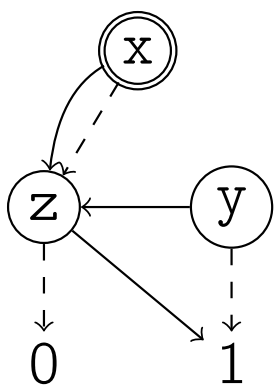
- Для каждой вершины v, такой что $var(v) = \mathrm{x}$, перенаправить входящие дуги в вершину $v[b]$
- Привести получившуюся OBDD

Пример $(\varphi = \mathrm{z}\,\&(\neg\mathrm{x} \vee \mathrm{y}) \vee \mathrm{x}\,\&\,\neg\mathrm{y})$

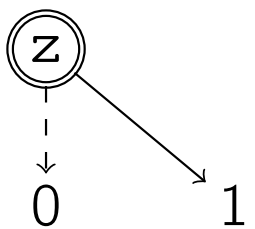
$\mathcal{D}^{\varphi}$:



OBDD $\mathcal{D} \sim \varphi[\mathrm{y}/1]$:



$\mathcal{D}^{\varphi[\mathrm{y}/1]}$:



ROBDD: применение двуместной операции

Дано: ROBDD $\mathcal{D}^{\varphi}$, $\mathcal{D}^{\psi}$ над набором переменных $x_1, \ldots, x_n$, двуместная булева операция $\circ$

Требуется: построить ROBDD $\mathcal{D}^{\varphi} \circ \mathcal{D}^{\psi} = \mathcal{D}^{\varphi \circ \psi}$ над тем же набором переменных

Алгоритм устроен сложнее всех предыдущих, но тоже достаточно просто:

- Если $n = 0$, то обе формулы φ, ψ — это константы 0, 1, и результат — простейшая диаграмма $\mathcal{D}^{\varphi \circ \psi}$
- Иначе:
  - Построить диаграммы $\mathcal{D}_{\varphi,0} = \mathcal{D}^{\varphi[\mathrm{x}_1/0]}$, $\mathcal{D}_{\varphi,1} = \mathcal{D}^{\varphi[\mathrm{x}_1/1]}$, $\mathcal{D}_{\psi,0} = \mathcal{D}^{\psi[\mathrm{x}_1/0]}$, $\mathcal{D}_{\psi,1} = \mathcal{D}^{\psi[\mathrm{x}_1/1]}$
  - *Рекурсивно* построить диаграммы $\mathcal{D}_0 = \mathcal{D}_{\varphi,0} \circ \mathcal{D}_{\psi,0}$ и $\mathcal{D}_1 = \mathcal{D}_{\varphi,1} \circ \mathcal{D}_{\psi,1}$
  - Объединить $\mathcal{D}_0$ и $\mathcal{D}_1$, считая все внутренние вершины попарно различными, добавить вершину x_1, объявить её корнем и направить дуги с метками 0, 1 в бывшие корни диаграмм $\mathcal{D}_0$, $\mathcal{D}_1$
  - Привести полученную OBDD

А почему это работает?

ROBDD: построение по формуле

Формулу φ (*над* $\neg$ *и двуместными операциями*) можно трактовать как схему применения операций к функциям, реализуемым простейшими формулами 0, 1, $\mathtt{x}_i$

Диаграмму $\mathcal{D}^{\varphi}$ можно получить как результат применения операций согласно той же схеме к соответствующим простейшим диаграммам $\mathcal{D}^{0}$, $\mathcal{D}^{1}$, $\mathcal{D}^{\mathtt{x}_i}$

Например, $\mathcal{D}^{\mathtt{x}\,\&\,\neg\mathtt{y}\vee\mathtt{z}} = \mathcal{D}^{\mathtt{x}}\,\&\,\neg\mathcal{D}^{\mathtt{y}} \vee \mathcal{D}^{\mathtt{z}}$

ROBDD: производные операции

На практике к ROBDD применяются и другие операции — выражающиеся через имеющиеся, но, быть может, имеющие специальную более эффективную реализацию:

- Для формулы φ: $\exists \mathrm{x}\ \varphi = \varphi[\mathrm{x}/0] \vee \varphi[\mathrm{x}/1]$
  Для диаграммы: $\exists \mathrm{x}\ \mathcal{D}^{\varphi} = \mathcal{D}^{\exists \mathrm{x}\ \varphi}$
- Для формулы φ: $\forall \mathrm{x}\ \varphi = \varphi[\mathrm{x}/0]\ \&\ \varphi[\mathrm{x}/1]$
  Для диаграммы: $\forall \mathrm{x}\ \mathcal{D}^{\varphi} = \mathcal{D}^{\forall \mathrm{x}\ \varphi}$
- Для формулы φ: $\mathit{relprod}(\varphi, \psi, \mathrm{x}_1, \ldots, \mathrm{x}_k) = \exists \mathrm{x}_1\ \ldots \exists \mathrm{x}_n\ (\varphi\ \&\ \psi)$
  Для диаграммы: $\mathit{relprod}(\mathcal{D}^{\varphi}, \mathcal{D}^{\psi}, \mathrm{x}_1, \ldots, \mathrm{x}_n) = \mathcal{D}^{\mathit{relprod}(\varphi, \psi, \mathrm{x}_1, \ldots, \mathrm{x}_n)}$
  - Пусть формулой φ задаётся двуместное отношение R_1 над комплектами переменных $\widetilde{x}$ и $\widetilde{y}$, а формулой ψ — одноместное отношение R_2 над комплектом $\widetilde{y}$ или двуместное над $\widetilde{y}$ и $\widetilde{z}$
    Тогда $\mathit{relprod}(\varphi, \psi, \widetilde{y})$ задаёт отношение
    - $\exists \widetilde{y}(R_1(\widetilde{x}, \widetilde{y})\ \&\ R_2(\widetilde{y}))$: множество всех $\widetilde{x}$, входящих в отношение R_1 с хотя бы одним $\widetilde{y}$ из R_2 — или
    - $\exists \widetilde{y}(R_1(\widetilde{x}, \widetilde{y})\ \&\ R_2(\widetilde{y}, \widetilde{z}))$: множество всех пар $(\widetilde{x}, \widetilde{z})$, соединяющихся посредством R_1 и R_2 через хотя бы один $\widetilde{y}$

ROBDD: производные операции

Задача QBF (выполнимости квантифицированных булевых формул): для заданной произвольной формулы вида $Q_1 x_1 \dots Q_n x_n(\varphi)$, где $Q_i \in \{\exists, \forall\}$ и φ — КНФ над $x_1, \dots, x_n$, проверить соотношение $Q_1 x_1 \dots Q_n x_n(\varphi) \not\sim 0$

Эта задача **весьма трудна**: является PSPACE-полной

Но её можно сравнительно «просто» с помощью ROBDD:

- Построить ROBDD по заданной формуле (с кванторами)
- Проверить изоморфизм полученной BDD и $\mathcal{D}^0$

Сложность работы с ROBDD «скрыта» в возрастании их размера при применении операций:

- При применении одной операции размер возрастает несильно (*полиномиально с низкой степенью*)
- При многократном применении операций размер может возрастать весьма существенно (*неполиномиально*)

Но хотя использование ROBDD и неэффективно в теории, оно всё же считается эффективным на практике: при должном выборе порядка переменных нередко получаются достаточно компактные диаграммы