情報論理学
(第３回)

基礎工学部情報科学科　泉 泰介

恒真性の判定法

- 前回の授業で，与えられた式の恒真性の判定が知識獲得や自動証明において核となる役割を果たすことを述べた
- コンピュータサイエンス的には，当然「自動で恒真性」を判定する方法が欲しい
  - 命題論理に関してはしらみつぶしが可能…だが，もちろん効率は悪い
- 今回は恒真性を判定するもう少しマシな方法を検討する
  - コンセンサス法
  - リゾルベント法(**導出原理**)

Part1：標準形・コンセンサス・リゾルベント

論理式の標準形

- リテラル：単一の命題記号Pならびにその否定$\neg P$
  - Pと$\neg P$は**互いに相補的なリテラル**とも呼ぶ

- 積和(標準)形(disjunctive normal form：**DNF**)　加法標準形，選言標準形とも呼ばれる
  - 積項(複数のリテラルを$\wedge$で結合したもの)を$\vee$で結合したもの

例：$(P \wedge \neg Q \wedge R) \vee (\neg P \wedge \neg R) \vee (Q \wedge R)$

- 和積(標準)形(conjunctive normal form：**CNF**)　乗法標準形，連言標準形とも呼ばれる
  - 和項(複数のリテラルを$\vee$で結合したもの)を$\wedge$で結合したもの

例：$(\neg P \vee Q \vee R) \wedge (P \vee Q) \wedge (Q \vee \neg R)$

  - 和項は節(clause)と呼ばれるときもある

標準形への変換

論理記号の優先順位：$\neg > \wedge > \vee > \rightarrow > \leftrightarrow$

- 任意の論理式は積和/和積形のいずれ[illegible]も(論理的同値変形で)変換可能
  - 例：$(P \wedge \neg Q) \rightarrow (\neg P \rightarrow \neg R) \wedge S$を変換してみる

$$
\begin{aligned}
&(P \wedge \neg Q) \rightarrow (\neg P \rightarrow \neg R) \wedge S \\
\Leftrightarrow\ &(P \wedge \neg Q) \rightarrow (P \vee \neg R) \wedge S \\
\Leftrightarrow\ &\neg(P \wedge \neg Q) \vee (P \vee \neg R) \wedge S \\
\Leftrightarrow\ &(\neg P \vee Q) \vee (P \vee \neg R) \wedge S
\end{aligned}
$$

積和形

$$
\begin{aligned}
\Leftrightarrow\ &(\neg P \vee Q) \vee (P \vee \neg R) \wedge S \\
\Leftrightarrow\ &\neg P \vee Q \vee (P \wedge S) \vee (\neg R \wedge S)
\end{aligned}
$$

(分配則$(A \vee B) \wedge C \Leftrightarrow (A \wedge C) \vee (B \wedge C)$を利用)

和積形

$$
\begin{aligned}
\Leftrightarrow\ &(\neg P \vee Q) \vee (P \vee \neg R) \wedge S \\
\Leftrightarrow\ &(\neg P \vee Q \vee P \vee \neg R) \wedge (\neg P \vee Q \vee S)
\end{aligned}
$$

(分配則$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$を利用)

標準形への変換手続き

- 変換$P \rightarrow Q \Leftrightarrow \neg P \vee Q$ または $\mathrm{P} \rightarrow Q \Leftrightarrow \neg(P \wedge \neg Q)$を用いて→を除去する
- 変換$\neg(P \vee Q) \Leftrightarrow (\neg P \wedge \neg Q)$ または $\neg(P \wedge Q) \Leftrightarrow (\neg P \vee \neg Q)$を用いてリテラルに付随しない¬を除去する
- 変換$\neg\neg P \Leftrightarrow P$ で不要な¬を除去する
- 積和形の場合
  - $(A \vee B) \wedge C \Leftrightarrow (A \wedge C) \vee (B \wedge C)$を利用して外側の∧を中に入れる
- 和積形の場合
  - $(A \wedge B) \vee C \Leftrightarrow (A \vee C) \wedge (B \vee C)$を利用して外側のvを中に入れる

この流れで処理

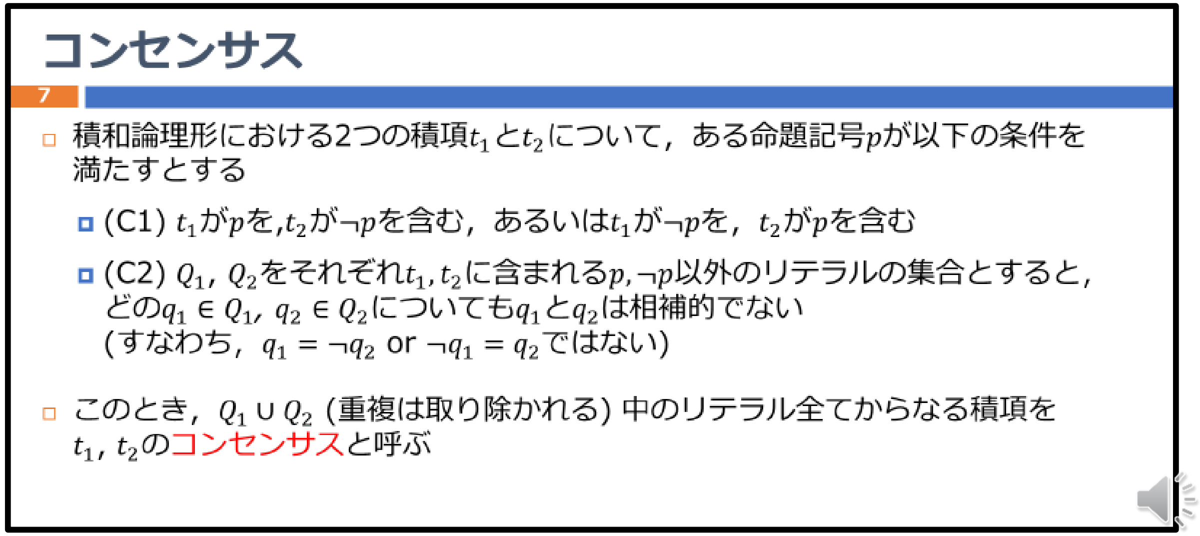
- 注) ここで標準形は，最簡な式まで変形することは要求していない
- 他の方法でも出すことは可能

コンセンサス

- 積和論理式における2つの積項t_1とt_2について，ある命題記号pが以下の条件を満たすとする
  - t_1がpを,t_2が$\neg p$を含む，あるいはt_1が$\neg p$を，t_2がpを含む
- $t_1 = Q_1 \wedge p_1$, $t_2 = Q_2 \wedge p_2$ $((p_1, p_2) = (p, \neg p)$ あるいは$(\neg p, p))$とする
- 積項$Q_1 \wedge Q_2$をt_1, t_2のコンセンサスと呼ぶ
  - Q_1, Q_2は空集合かもしれないことに注意
  - Q_1, Q_2が共に空のときはT(真の値)がコンセンサスとなる (Tは含まれるリテラルがゼロ個の積項とみなす)

コンセンサスの例

- $t_1 = \neg u \wedge w \wedge x \wedge \neg y$ ， $t_2 = \neg u \wedge w \wedge x \wedge y \wedge z$, $t_3 = \neg u \wedge w \wedge z$, $t_4 = \neg w \wedge x \wedge y$とする
  - t_1とt_2はコンセンサス$\neg u \wedge w \wedge x \wedge z$を持つ($y, \neg y$が相補的)
  - t_1とt_3はコンセンサスを持たない(相補的なリテラルがない)
  - t_1とt_4はコンセンサス$\neg u \wedge x \wedge \neg y \wedge y$ および $\neg u \wedge w \wedge \neg w \wedge x$を持つ($y, \neg y$, $w, \neg w$がどちらも相補的)



リゾルベント

違いはここだけ

- 和積論理式における2つの和項c_1とc_2について，ある命題記号pが以下の条件を満たすとする
  - c_1がpを,c_2が$\neg p$を含む，あるいはc_1が$\neg p$を，c_2がpを含む
- $c_1 = Q_1 \vee p_1$, $c_2 = Q_2 \vee p_2$ $((p_1, p_2) = (p, \neg p)$ あるいは$(\neg p, p))$とする
- 和項$Q_1 \vee Q_2$をc_1, c_2のリゾルベントと呼ぶ
  - Q_1, Q_2は空集合かもしれないことに注意
  - Q_1, Q_2が共に空のときはF(真の値)がリゾルベントとなる (Fは含まれるリテラルがゼロ個の和項とみなす)
- 例は前述のコンセンサスの例において∧を∨に変えるだけなので，略

注) テキストでは上のようなpがちょうどひとつである，という条件をつけているが(一種の流儀で，本質的ではない)，ここでは後の議論のわかりやすさためそのようなpが一つでなくてもよいものとする(p.32参照)

コンセンサス法

- 以下のようなステップに基づいて論理式fの恒真性を示す
  - fを積和標準形に変換する(f_0とする)
  - while (f_iが積項Tを持たない or ある積項対(t_1, t_2) がコンセンサスtを持ち，f_iはtを含まない)
    - f_iに積項tを追加し，f_{i+1}とする

    ((t_1, t_2)の候補が複数あるときは好きなものを選ぶ)
  - 終了時のf_*が積項Tを含めば恒真であると判定，そうでなければ恒真でないと判定

コンセンサス法：動作例

- $f = (A \land B) \lor (A \land \neg B) \lor \neg A$ の恒真性を示す

$$f_0 = (A \land B) \lor (A \land \neg B) \lor \neg A$$
$$f_1 = (A \land B) \lor (A \land \neg B) \lor \neg A \lor A$$
$$f_2 = (A \land B) \lor (A \land \neg B) \lor \neg A \lor A \lor T$$

- $f = (A \land B) \lor (\neg A \land C) \lor \neg C$が恒真でないことを示す

$$f_0 = (A \land B) \lor (\neg A \land C) \lor \neg C$$
$$f_1 = (A \land B) \lor (\neg A \land C) \lor \neg C \lor (B \land C)$$
$$f_2 = (A \land B) \lor (\neg A \land C) \lor \neg C \lor (B \land C) \lor \neg A$$
$$f_3 = (A \land B) \lor (\neg A \land C) \lor \neg C \lor (B \land C) \lor \neg A \lor B$$

ここまでくると，どの2項のコンセンサスを取っても
新たな積項が生じない→恒真でない

リゾルベント法

- 以下のようなステップに基づいて論理式fの**恒偽性**(すなわち$\neg f$の恒真性)を示す
  - fを和積標準形に変換する(f_0とする)
  - while (f_iが和項Fを持たない or ある和項対(c_1, c_2) がリゾルベントcを持ち，f_iはcを含まない)
    - f_iに積項cを追加し，f_{i+1}とする

    ((c_1, c_2)の候補が複数あるときは好きなものを選ぶ)
  - 終了時のf_*がFであればfは恒偽であると判定，項が残れば恒偽でないと判定

リゾルベント法：動作例

- $f = (A \lor B) \land (A \lor \neg B) \land \neg A$ の恒偽性を示す

$$f_0 = (A \lor B) \land (A \lor \neg B) \land \neg A$$
$$f_1 = (A \lor B) \land (A \lor \neg B) \land \neg A \land A$$
$$f_2 = (A \lor B) \land (A \lor \neg B) \land \neg A \land A \lor F$$

- $f = (A \lor B) \land (\neg A \lor C) \land \neg C$が恒偽でないことを示す

$$f_0 = (A \lor B) \land (\neg A \lor C) \land \neg C$$
$$f_1 = (A \lor B) \land (\neg A \lor C) \land \neg C \land (B \lor C)$$
$$f_2 = (A \lor B) \land (\neg A \lor C) \land \neg C \land (B \lor C) \land \neg A$$
$$f_3 = (A \lor B) \land (\neg A \lor C) \land C \land (B \lor C) \land \neg A \lor B$$

ここまでくると，どの2項のリゾルベントを取っても
新たな和項が生じない→恒偽でない

Part2：正当性と導出原理

コンセンサス法=ド・モルガン+リゾルベント法(1)

(一般の)ド・モルガン則

$$\neg(A_1 \vee A_2 \vee \cdots \vee A_n) \Leftrightarrow (\neg A_1) \wedge (\neg A_2) \wedge \cdots \wedge (\neg A_n)$$
$$\neg(A_1 \wedge A_2 \wedge \cdots \wedge A_n) \Leftrightarrow (\neg A_1) \vee (\neg A_2) \vee \cdots \vee (\neg A_n)$$

- 積和形論理関数$f = t_1 \vee t_2 \vee \cdots \vee t_m$を考える
- 積項$t_i = a_{i,1} \wedge a_{i,2} \wedge \cdots \wedge a_{i,k}$に対して$\neg t_i$を考えると，
  ド・モルガン則より$\neg t_i$は和項$\neg a_{i,1} \vee \neg a_{i,2} \vee \cdots \vee \neg a_{i,k}$ となる．これをc_iとする
- 和積形論理関数$g = c_1 \wedge c_2 \wedge \cdots \wedge c_m$を考えると，ド・モルガン則より
  $$\neg f = \neg(t_1 \vee t_2 \vee \cdots \vee t_m) = (\neg t_1) \wedge (\neg t_2) \wedge \cdots \wedge (\neg t_m) = c_1 \wedge c_2 \wedge \cdots \wedge c_m = g$$
- fが恒真$\Leftrightarrow$ $\neg f$が恒偽 なので，結局fの恒真性の判定はgの恒偽性の判定と同じ

コンセンサス法=ド・モルガン+リゾルベント法(2)

- fにコンセンサス法を適用することとgにリゾルベント法を適用することは本質的に同じ
- fへのコンセンサス法の導出系列$f_0, f_1, \ldots$を以下のように書き換える
  1. 各リテラルの否定・肯定を反転する (TとFも入れ替える)
  2. $\vee$と$\wedge$を入れ替える

  このようにして得られる系列は，gへのリゾルベント法の導出系列になる

$$f_0 = (A \wedge B) \vee (A \wedge \neg B) \vee \neg A$$
$$f_1 = (A \wedge B) \vee (A \wedge \neg B) \vee \neg A \vee A$$
$$f_2 = (A \wedge B) \vee (A \wedge \neg B) \vee \neg A \vee A \vee T$$

$$g_0 = (\neg A \vee \neg B) \wedge (\neg A \vee B) \wedge A$$
$$g_1 = (\neg A \vee \neg B) \wedge (\neg A \vee B) \wedge A \wedge \neg A$$
$$g_2 = (\neg A \vee \neg B) \wedge (\neg A \vee B) \vee A \wedge \neg A \wedge F$$

結局のところ，コンセンサス法かリゾルベント法どちらかだけ正当性を示せばOK

リゾルベント法の正当性

- 正当性のために示す必要があること
  1. アルゴリズムは停止する
  2. アルゴリズムが停止するとき，答えは正しい
- それぞれについて証明していく

1. の証明

- リゾルベントが有限回しか新たに生成されないことを示す
  - 節cに含まれるリテラルの集合を$\ell(c)$で表すとする

- リゾルベントの定義より，c_1，c_2から生成されたリゾルベントcは
$$\ell(c) \subseteq \ell(c_1) \cup \ell(c_2)$$
を満たすので，リゾルベントを生成することで元の論理式になかったリテラルが生まれることはない

- 元の論理式fにn個の命題変数 (=高々$2n$個のリテラル)が含まれているとすると可能な異なる節の個数は高々2^{2n}種類
  - =$2n$個の要素からなる集合から取り出せる異なる部分集合の総数
(リゾルベント生成時に重複するリテラルは除去されることに注意)
  - 最悪でも$f_{2^{2n}}$で終わる

2. の証明(1)

- まず，f とf_iが論理的同値であることを示す

補題1

任意のiについて，$f \Leftrightarrow f_i$

- 証明はiについての数学的帰納法で示す
  - (基底) $i = 0$のとき：$f = f_0$なので明らか
  - (帰納段階) f_iについて$f \Leftrightarrow f_i$であると仮定して，f_{i+1}を検討する
    - f_i中の節$(Q_1 \vee p)$および$(Q_2 \vee \neg p)$よりリゾルベント$(Q_1 \vee Q_2)$が追加されたとする
  - f_iから$(Q_1 \vee p)$および$(Q_2 \vee \neg p)$を取り除いた残りの部分をf'とすると

$$f_i = f' \wedge (Q_1 \vee p) \wedge (Q_2 \vee \neg p)$$
$$f_{i+1} = f' \wedge (Q_1 \vee p) \wedge (Q_2 \vee \neg p) \wedge (Q_1 \vee Q_2) = f_i \wedge (Q_1 \vee Q_2)$$

2. の証明(2)

$$f_i = f' \wedge (Q_1 \vee p) \wedge (Q_2 \vee \neg p), \qquad f_{i+1} = f_i \wedge (Q_1 \vee Q_2)$$

- この2つの論理的同値性を示す．すなわち「任意の解釈Iに対して，$[\![f_i]\!]^I$が真⇔$[\![f_{i+1}]\!]^I$が真」を示す
  - そのとき$f_i \Leftrightarrow f_{i+1}$であり，帰納法の仮定$f_i \Leftrightarrow f$と併せて$f \Leftrightarrow f_{i+1}$が得られる
- ⇒の証明
  - $[\![f_i]\!]^I$が真であるとする．Iにおいてpが真であれば$[\![Q_2]\!]^I$は真であり，偽であれば$[\![Q_1]\!]^I$は真である．よって$[\![Q_1 \vee Q_2]\!]^I$は真であり，$[\![f_{i+1}]\!]^I$は真
- ⇐の証明
  - $[\![f_{i+1}]\!]^I$が真であるとすると，Iにおいてf_{i+1}中のすべての和項は真になる．f_iの和項はすべてf_{i+1}の和項でもあるので，Iにおいてf_iの和項はすべて真になる(終)

2. の証明(3)

- 正しさの証明：「fが恒偽⇔ f_*がFを含む」を示せばよい
  - ⇐は簡単(f_*がFを含むとき当然恒偽であり，$f_* \Leftrightarrow f$なので，fも恒偽)
  - ⇒が手ごわい(次スライドから．証明方針はテキストとは異なる)

2. の証明(4)

- Vをf (すなわち，f_*)に現れる命題変数の集合とする
- Vの要素のみを命題変数として持つ論理式gに対して，それを真にするすべての(Vに対する)解釈の集合を$M(g)$で表すとする
- 2つの論理式f, gについて，$M(f) \subseteq M(g)$であるとき「gはfをカバーする」という

2. の証明(4)

$M(c)$:cを真にする解釈の集合
$\ell(c)$:cに含まれるリテラルの集合

- まず先立って以下の補題を証明しよう

補題2

A) c_1, c_2 を節とすると, $\ell(c_1) \subseteq \ell(c_2) \Rightarrow M(c_1) \subseteq M(c_2)$

B) c_1, c_2を恒真でない節とすると, $\ell(c_1) \subset \ell(c_2) \Rightarrow M(c_1) \subset M(c_2)$

- Aの証明) c_1のあるリテラルを真にする解釈はc_2も真にするので, 明らかに $M(c_1) \subseteq M(c_2)$
- Bの証明) A)が成り立つので, $M(c_1) \neq M(c_2)$を言えばいい. 詳細は略(MR課題)

(終)

2. の証明(5)

- メインディッシュ

補題3

fが恒偽ならば，f_*に含まれる節の集合をSとすると，$F \in S$

2. の証明(6)

$M(c)$:cを真にする解釈の集合
$\ell(c)$:cに含まれるリテラルの集合

- 背理法の仮定：節FがSに含まれないとする
- 節集合Tを以下の2条件を満たす節xの集合とする
  1. xは恒真ではない
  2. いかなる$x' \in S$についても$M(x') \not\subseteq M(x)$
- $M(c') \subseteq M(F)$であるようなc'は明らかに$c' = F$のみであり，背理法の仮定より$F \notin S$．よってFはTへと含まれるので，Tは空ではない
  - τを，Tに含まれるもののなかで，$M(\tau)$が極大であるようなものとする
    - すなわち，すべての$x' \in T$ について，$M(\tau) \not\subset M(x')$が成り立つようなもの

2. の証明(7)

$M(c)$:cを真にする解釈の集合
$\ell(c)$:cに含まれるリテラルの集合

- ケース１： τがV中のすべての変数を含んでいる
  - c'をS中の任意の節とすると，$\tau \in T$なので$M(c') \not\subseteq M(\tau)$
  - τはすべての変数を含んでいるので，c'中の変数もすべて含む
  - 一方で補題2A(の対偶)により，$M(c') \not\subseteq M(\tau)$から$\ell(c') \not\subseteq \ell(\tau)$が成立
  - このとき，ある命題変数pが存在し，c'がp，τが$\neg p$を含む，あるいはc'が$\neg p$，τがpを含む
  - τのリテラルを全て偽にするような解釈は，すべての$c' \in S$を真にする($\tau \in T$よりτは恒真ではないので，そのような解釈は必ず存在)
  - すなわち，f_*は充足可能であり，補題1より$f \Leftrightarrow f_*$なのでfの恒偽性に矛盾

2. の証明(8)

$M(c)$:cを真にする解釈の集合
$\ell(c)$:cに含まれるリテラルの集合

- ケース2：τがある変数xを含んでいない
  - $\tau_1 = \tau \vee x$, $\tau_2 = \tau \vee \neg x$とする．このとき$\tau_1$, τ_2は恒真ではない　(略．MR課題)
  - 補題2Bより$M(\tau) \subset M(\tau_1)$, $M(\tau) \subset M(\tau_2)$を得る
  - τがT中の極大元であるという事実から，τ_1, τ_2はTに入らない
    $\Rightarrow M(\tau'_1) \subseteq M(\tau_1)$, $M(\tau'_2) \subseteq M(\tau_2)$である$\tau'_1, \tau'_2 \in S$が存在
  - τ'_1はxを，τ'_2は$\neg x$を必ず含まないといけない
    (そうでなければ$\ell(\tau'_1) \subseteq \ell(\tau)$ or $\ell(\tau'_2) \subseteq \ell(\tau)$ なので補題2Aより
    $M(\tau'_1) \subseteq M(\tau)$ or $M(\tau'_2) \subseteq M(\tau)$ $(\tau'_1, \tau'_2 \in S)$が成立して$\tau \in T$に矛盾)
  - このとき，和項対(τ'_1, τ'_2)はリゾルベントを持つ(rとする)
    f_*からは新たなリゾルベントを生成できないので，$r \in S$でないといけない
  - $\ell(r) \subseteq \left(\ell(\tau'_1) \cup \ell(\tau'_2)\right) \setminus \{x, \neg x\}$なので$\ell(r) \subseteq \ell(\tau)$．補題2Aより
    $M(r) \subseteq M(\tau)$となり，これは$\tau \in T$に矛盾

(終)

導出原理

- リゾルベント法は導出原理(resolution principle)とも呼ばれる
  - もとは述語論理の恒真性判定アルゴリズム(の一部)として示された
- 導出原理は人口知能分野における恒真性判定アルゴリズムとして有名
  - 前回の説明の通り，同分野では$Q_1 \wedge Q_2 \wedge \cdots \wedge Q_k \rightarrow P$の形式の恒真性判定問題が良く表れる．この形式は，同値変形により

$$Q_1 \wedge Q_2 \wedge \cdots \wedge Q_k \rightarrow P$$
$$\Leftrightarrow \neg((Q_1 \wedge Q_2 \wedge \cdots \wedge Q_k) \wedge \neg P)$$

と変形できる．このときQ_*,Pが和項のとき，導出原理を用いて$(Q_1 \wedge Q_2 \wedge \cdots \wedge Q_k) \wedge \neg P$の恒偽性を示すのが筋のよいやりかたになる

導出原理

- 実際には，Q_i, Pは以下の形式をとることが多い
  - Q_i, Pが単一のリテラル
    - 和項の特殊ケースなので気にしないでよい
  - Q_i, Pが積項
    - そのままでOK
  - Q_i, Pが因果律，すなわち，それら自身も$R_1 \wedge R_2 \wedge \cdots \wedge R_j \rightarrow S$の形式
    - このときは$\neg(R_1 \wedge R_2 \wedge \cdots \wedge R_j) \vee S \Leftrightarrow (\neg R_1 \vee \neg R_2 \vee \cdots \vee \neg R_j \vee S)$と和項に変形できる

実行時間について

- 導出原理の実行時間は最悪時は真理値表の総当たりと変わらない
(か，それ以上に遅い)
  - 命題変数の個数がn個のとき，nの指数時間を必要とするかもしれない
  - が，そもそも和積標準形の恒偽性判定は最悪時高速なアルゴリズムが
期待できない
    - 恒偽性判定はNP完全問題であり，多項式時間アルゴリズムを持たないと予想されている
(データ構造とアルゴリズムの授業参照)
  - 実用的な時間で判定するには，どの対に対してリゾルベントを取るかどうかの
選択(導出戦略と呼ばれる)が重要
    - 高速化のためのさまざまな戦略が研究されている