計算機ソフトウェア
第十三回

電気電子工学科
黒橋禎夫

計算できない問題がある

- クラスNP(nondeterministic polynomial): ちょっとやそっとじゃ解けない
- 難問対策 = 厳密解をあきらめて近似解を探す

例: 巡回セールスルマン問題

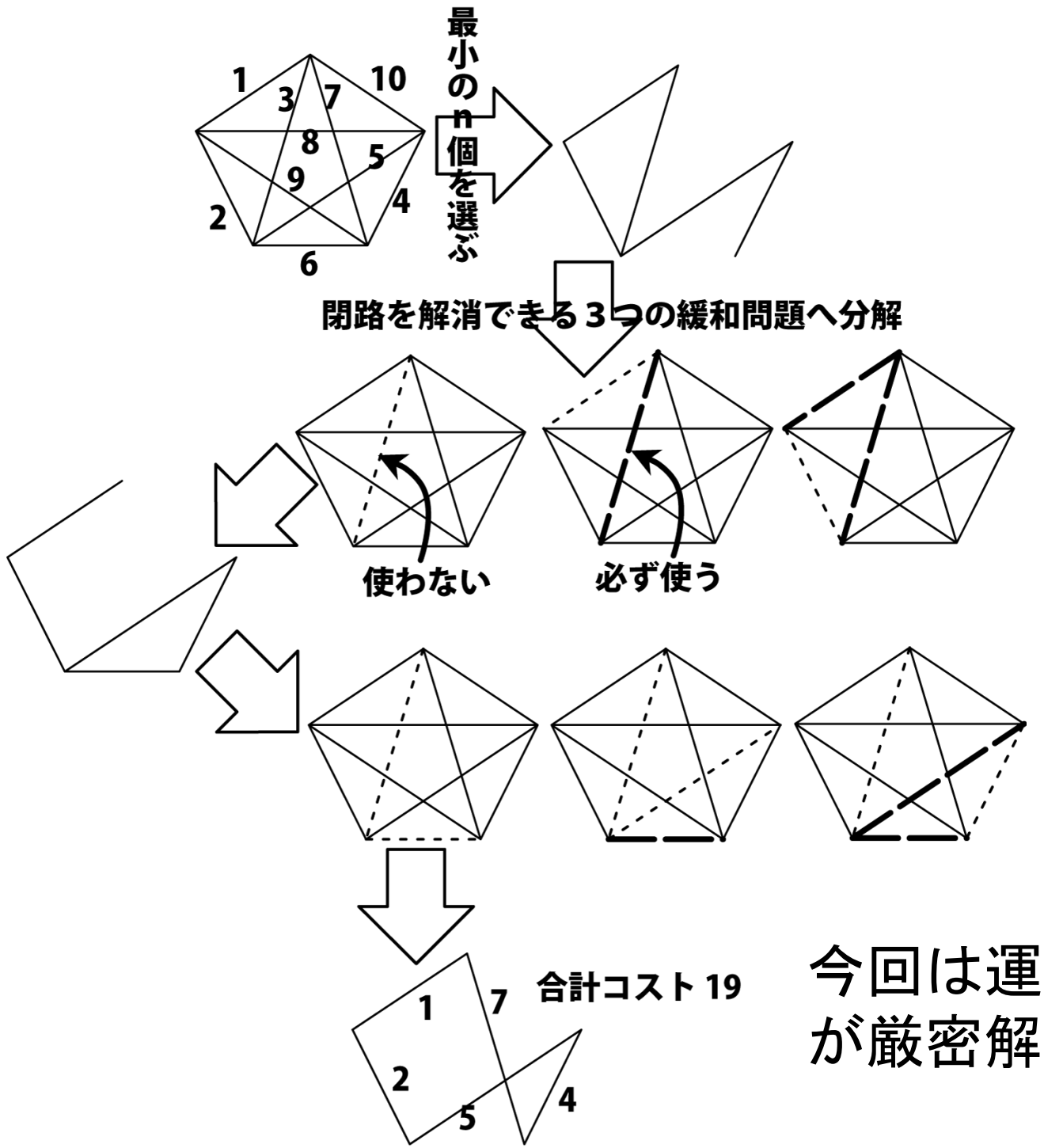
- G=(V,E), |V|=n のとき、目的関数 $\Sigma c(v_i, v_j)x_{ij}$ を最小にする
- ただし、条件 x [x_{ij}=0 or 1 であって x_{ij}=1なる辺を集めるとGのハミルトン閉路である] を満たすものとする
- ハミルトン閉路を求めることはできないので条件を緩めて解ける問題をつくる

緩和問題 relaxed problem

- 緩和した条件 $\Sigma x_{ij}=n$ である経路をもとめる
- ハミルトン閉路ではないが、いったん解いておいてから徐々にハミルトン閉路へ近づけてゆく

分枝限定法
branch-and-bound method

- 緩和問題 R を解く → 解 X
- Rの条件を少し強める
- いくつかの緩和問題に分解



深さ優先探索でとりあえず解を求めて安心

後は時間の許す限り探索を続ける

今回は運良く1つ目の解が厳密解になってます

山登り法 hill-climbing method

- 緩和と他の方法を組み合わせる
- ある近似解から1箇所の変更で辿り着ける他の解（たくさんある）をその解の近傍という
- 近傍の中でより良い解を探索することを局所改良という
- 緩和で解がひとつ求まったら近傍で改良をすこしやってみる価値があります

ナップザック問題 knapsack problem

- NP困難　2^n のしらみつぶし以外手がない

  正数集合 $X=\{a_1\ a_2\ \ldots\ a_n\}$ と S について
  $\Sigma a_i \leqq S$ を最大にする X の部分集合を探す

- $\Sigma a_i = S$ の判定問題はNP完全

やさしいナップザック問題

- $a_1 + a_2 + \ldots + a_{i-1} < a_i$ である場合 O(n)

- Ex. 日本の硬貨・紙幣

  ￥６１６ → 500 + 100 + 10 + 5 + 1

ナップザック問題を利用した公開暗号系

- 設計手順
  1. 十分大きい n
  2. $a_1 + a_2 + \ldots a_{i-1} < a_i$
  3. $a_1 + a_2 + \ldots a_n < m$
  4. m と互いに素な w
  5. $v \cdot w \equiv 1 \pmod{m}$ である v
  6. $b_i \equiv w \cdot a_i \pmod{m}$

  公開 n, $\{b_i\}$　秘密 m, v, $\{a_i\}$

ナップザック問題を利用した公開暗号系

- 暗号化
  nビット列 (x_i | 0 または 1, i = 1…n)
  → $C = \Sigma b_i \cdot x_i$
- 解読
  $C = \Sigma b_i$ をみたす$\{b_i\}$の部分列を探す＝ナップザック問題 $O(2^n)$
- 複合化
  $S \equiv v \cdot C \pmod m$ とすれば $S = \Sigma a_i \cdot x_i$ となり
  $S = \Sigma a_i$ をみたす$\{a_i\}$の部分列を探す＝やさしいナップザック問題 O(n)