2015.2.23

興味を持たれた人のために（期間限定）[1]

藪下小夜子の定理について

１９９６年藪下小夜子はＰ≠ＮＰ予想に関して次のような定理を証明した.

> 単純な構造の探索アルゴリズムだが，もしも一般の CNF-SAT-探索問題を $T(n)$ 時間で解くアルゴリズムが存在した場合，そのアルゴリズムも $T(n)^{O(1)}$ 時間で，CNF-SAT-探索問題を解く.

これはＰ≠ＮＰ予想の解決に向けて大きな前進と言われる定理であり，この探索アルゴリズムは「Yabushita Universarl Search」（略称，Y-Search）と呼ばれている．また，定理自身を「Yabushita Universal Search Theorem」と言う場合もある.

【解説】（渡辺研のウェブの Reseaerch Topics も参照）

- CNF-SAT とは，和積形 (conjunctive normal form) の命題論理式（CNF-論理式）の充足可能性問題のこと．決定問題は著名なＮＰ完全問題の 1 つである．つまり，この問題の多項式時間計算可能性（あるいは不可能性）がＰ＝ＮＰ（あるいはＰ≠ＮＰ）を決める．この定理では充足解探索型の問題を考えている.
- 正確には，ここでは promise problem を考える．つまり，充足解を持つ CNF-論理式が与えられるという前提でアルゴリズムを考える．充足可能でない式が与えられた場合，アルゴリズムは停止しなくてもよいこととする.
- 上のような想定で考えた場合，実は，このような万能性を持つアルゴリズムは本当に作ることも可能である．万能チューリング機械を用い，すべてのチューリング機械を列挙しながら，それらを並列に走らせ，解が求まりしかもその正しさを確認できたときに，それを出力するようなアルゴリズムを考えればよい．ここで「万能チューリング機械」と言っているが，これは要するにインタープリタのこと．たとえば `Ruby` のインタープリタを使えばよい.
- 藪下の定理の重要なところは，最初に曖昧に書かれている「単純な構造の」という点. Y-Search は，実は乱択アルゴリズムで，乱択分岐を持つのだが，その分岐が Basic Type I と Basic Type II という，比較的単純な分岐であり，その計算構造に関して，藪下が解析したことが重要なのである.（う〜ん，どう重要なのだろう...）
- では，この定理がＰ≠ＮＰ予想の解決にどうつながるのだろうか？　長い話を端折って言うと，この分岐構造を解析すると，このアルゴリズムが「異なる」充足解を出

---

[1] この資料は予告なく削除する可能性があります．もちろん，一部は渡辺の空想から生まれた話です.

力する確率が解析できそうなのである．しかも，Y-search が多項式時間で止まる場合，ランダムな充足可能な CNF-SAT 論理式に対し，ある乱択計算パスに注目してみると，それが他のパスと異なる解を出す確率が $2^{-o(n)}$ になりそうなのである．もしそうだとすると，ランダムな充足可能な CNF-SAT 論理式では，高い確率で解の個数が指数個になることとなる．ところが，これは森・渡辺らの CNF-SAT に対する相転移定理（そんな定理が証明できたのですかぁ，これまたすごい！）の解析に反する．よって Y-search は多項式時間に止まらない．つまりは，どんなアルゴリズムも CNF-SAT-探索問題を多項式時間に解くことができない．よって，Ｐ≠ＮＰが言えるのである．

さてさて，藪下依子は，この最後のステップを完成することができるのでしょうか？