Resource-bounded Forcing Theorem and Randomness

Toshio Suzuki[1]* and Masahiro Kumabe[2]

[1]Tokyo Metropolitan University, toshio-suzuki•tmu.ac.jp

[2]The Open University of Japan, kumabe•ouj.ac.jp (•=atmark)

CTFM 2014, Tokyo Institute of Technology

17 Feb. 2014

*This work was partially supported by Japan Society for the Promotion of Science (JSPS) KAKENHI (C) 22540146 and (B) 23340020.

Abstract

- Forcing complexity (of a given formula)
  $=$ Min. size of forcing conditions (its domain) which force it.
  $\neq$ Time-bound of extension strategy.

- Resource-bounded forcing theorem holds almost everywhere.

[Dowd, 1992] For almost all inifinite binary sequnece X:
Every tautology with respect to $X \upharpoonright \{0,1\}^{\leq n}$ is forced by a sub-function S of X such that $|\mathrm{dom} S|$ is polynomial in n.
(The poly. depends on $\sharp$ of occurrences of query symbols.)

Resource-bounded randomness implies r.-b. forcing theorem.

Main Theorem: $\exists$ An elementary recursive function $t(n)$ s.t.
[X is $t(n)$-random $\Rightarrow$ Resource-bounded forcing thm. holds for X].

Outline

§1 Forcing Complexity

Forcing complexity
= The minimum size of a forcing condition

Forcing complexity is the minimum size of a forcing condition that forces a given propositional formula. The origin of forcing complexity is in Dowd's study on NP=? coNP question.

M. Dowd: Generic oracles, uniform machines, and codes.
Inf. Comput., **96**, pp. 65–76 (1992).

§1 Forcing Complexity

Forcing complexity
$\neq$ Time-bound of extension strategy

Ambos-Spies et al. introduced the concept of resource-bounded random sets by extending the works of Schnorr and Lutz. They show that resource-bounded randomness implies resource-bounded genericity. While the genericity of Ambos-Spies is based on time-bound of finite-extension strategy, the genericity of Dowd, the main topic of this talk, is based on an analogy of forcing theorem.

K. Ambos-Spies and E. Mayordomo:
Resource-bounded measure and randomness.
Lecture Notes in Pure and Appl. Math., **187**, pp. 1–47,1997.

§1 Forcing Complexity

To be more precise:

Def. Resource-bounded randomness (Ambos-Spies et al.)

$t(n)$-random
$\simeq$ random for $O(t(n))$-time computable martingales.

Time-bound of finite-extension strategy.

[Ambos-Spies and Mayordomo 1997],
[Ambos-Spies, Terwijn, and Zheng 1997]:

$$t(n)\text{-random} \Rightarrow t(n)\text{-stochastic} \Rightarrow t(n)\text{-generic.}$$

§1 Forcing Complexity

On the other hand, the detail of forcing complexity is as follows.

Def. of Dowd-generic sets (sketch)

"A certain property* of an exponential-sized portion of an oracle X is forced by a polynomial-sized portion of X. "

"A certain property" is described with *the relativized propositional calculus* (RPC).

$$\mathrm{RPC} = (\text{ propositional caluculus }) \\ + \{\xi^1(-), \xi^2(-,-), \xi^3(-,-,-), \cdots\}$$

For each n, the n-ary connective ξ^n (a *query symbol*) is interpreted to the initial segment of a given oracle up to 2^nth string.

§1 Forcing Complexity

Example of a formula of RPC

$(q_0 \Leftrightarrow \xi^3(q_1, q_2, q_3)) \Rightarrow [q_0 \vee (q_1 \wedge q_4)]$

Given a formula F of RPC and an oracle X, truth of F is determined by "a truth assignment + a finite portion of X".

Interpretation:

ξ^n(ith of $\{0,1\}^n$) is interpreted as to be X(ith of $\{0,1\}^*$),

where "ith" is that of length-lexicographic order.

§1 Forcing Complexity

ξ^n(ith of $\{0,1\}^n$) is interepreted as to be X(ith of $\{0,1\}^*$).
Examples ($n = 2$ and $n = 3$)

$\xi^2(0,0)$	$\xi^2(0,1)$	$\xi^2(1,0)$	$\xi^2(1,1)$
X(empty string)	$X(0)$	$X(1)$	$X(00)$

$\xi^3(0,0,0)$	$\xi^3(0,0,1)$	$\xi^3(0,1,0)$	$\xi^3(0,1,1)$
X(empty string)	$X(0)$	$X(1)$	$X(00)$
$\xi^3(1,0,0)$	$\xi^3(1,0,1)$	$\xi^3(1,1,0)$	$\xi^3(1,1,1)$
$X(01)$	$X(10)$	$X(11)$	$X(000)$

Thus, $\xi^2(q_2, q_1)$ and $\xi^3(0, q_2, q_1)$ are interpreted as to be the same.

§1 Forcing Complexity

Def. Force

A finite portion σ (a finite sub-function) of an oracle X is called a *forcing condition*.

σ *forces* F if for any Y extending σ, F is a tautology w. r. t. Y.

Example of force

Let F be: $(q_0 \Leftrightarrow \xi^3(q_1, q_2, q_3)) \Rightarrow \neg q_0$

F is a tautology w. r. t. the characteristic func. of the empty set.
If σ forces F then the size of σ (its domain) $\geq 2^3$.
(And, the first 2^3 bits of σ should be 0.)

§2 Non-Existence

The case of unbounded occurrences of query symbols

Definition. t-generic sets [Dowd 1992]

X is t-generic if every tautology F with respect to X is forced by a forcing condition of polynomial-size in $|F|$.

Thm. Non-existence of t-generic sets [Dowd, 1992], [S. 2001]

There are no t-generic sets.

M. Dowd: Generic oracles, uniform machines, and codes.
Inf. Comput., **96**, pp. 65–76 (1992).

S.: Forcing complexity: minimum sizes of forcing conditions.
Notre Dame J. Formal Logic, **42**, pp. 117–120 (2001).

§3 Existence

Resource-bounded forcing theorem holds almost everywhere.

It is widely known that 1-randomness and 1-genericity are incompatible.

Interestingly, Dowd found that the following holds for a randomly chosen $X : \omega \to \{0, 1\}$.

"A property of an exponential-sized portion of X is forced by a polynomial-sized portion of X".

M. Dowd: *Inf. Comput.* (1992).
S.: *Notre Dame J. Formal Logic* (2001).
S.: *Inf. Comput.* (2002).

§3 Existence

The case of bounded occurrences of query symbols:
Here, r-query denotes "the ♯ of occurrences of query symbols is r."

Def. Dowd-generic sets [Dowd, 1992]

- Let r be a positive integer.
  X is r-Dowd
  if every r-query tautology F w. r. t. X
  is forced by a forcing condition of polynomial-size in $|F|$.

- X is Dowd-generic
  if X is r-Dowd for every positive integer r.
  (Polynomial bound depends on each r, unlike t-genericity)

§3 Existence

Thm. Existence of Dowd-generic sets

- [Dowd, 1992], [S.2001], [S.2002]
  The class of all Dowd-generic sets has Lebesgue measure 1.
- [S. and Kumabe, 2009] Schnorr random $\Rightarrow$ Dowd-generic.

S.: Degrees of Dowd-type generic oracles.
Inf. Comput., **176**, pp.66–87 (2002).

S. and M. Kumabe: Weak randomness, genericity and Boolean decision trees.
Proc. 10th Asian Logic Conference, pp.322–344, 2009.

§3 Existence

[Dowd 1992] asserts "Any 1-Dowd set is not c.e." (false)

Thm. Degrees of Dowd-generic sets

- [S. 2002] There exists a primitive recursive 1-Dowd set.
  And, every Turing degree contains a 1-Dowd set.
- [Kumabe and S. 2012]
  The same holds for "Dowd-generic" in place of "1-Dowd".

M. Kumabe and S.:
Computable Dowd-generic oracles.
Proc. 11th Asian Logic Conference, pp.128–146, 2012.

§4 Main Theorem

Main Theorem

There exists an elementary recursive function $t(n)$ s.t.
$t(n)$-random $\Rightarrow$ Dowd-generic.

Gives an alt. proof: $\exists$ a primitive recursive Dowd-generic set.

M. Kumabe and S.:
Resource-bounded martingales and computable Dowd-type generic sets. submitted to a journal (2010).

§4 Main Theorem (Sketch of Proof)

The key to our proof is a construction of a martingale that succeeds on every "non-Dowd" set. A basic idea is as follows.

Suppose a forcing condition S is given and we want to define the value $d(S)$ of the martingale. Assume that a polynomial p is given at the node S. In the two basic open sets given by $S0$ (S concatenated by 0) and $S1$, we investigate the following conditional probabilities.

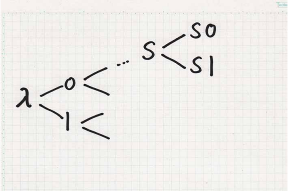

Figure 1: Martingale

§4 Main Theorem (Sketch of Proof)

We randomly chose an oracle T. Then we investigate a prob. of T having the following property $(*)$, under the condition that T extends $S0$ (or $S1$, respectively). Here, $f(n) >> n$.

$(*)$

Somewhere between $n+1$ and $f(n)$, T fails the test for "the forcing theorem at stage i with respect to r and p".

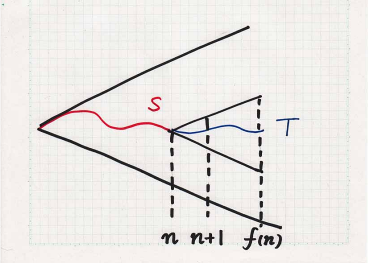

Figure 2:

We denote these conditional probabilities by $\varrho(S0)$ and $\varrho(S1)$.

§4 Main Theorem (Sketch of Proof)

We define the martingale values $d(S0)$ and $d(S1)$ in proportion to $\varrho(S0)$ and $\varrho(S1)$. In other words, we shall define them so that the following equation holds.

The ratio of the martingale value to rho

$$\frac{d(S0)}{\varrho(S0)} = \frac{d(S1)}{\varrho(S1)}$$

§4 Main Theorem (Sketch of Proof)

Then, in many nodes, the ratio of d to ϱ shall be the same as that of the parent node. For example, the following holds.

$$\frac{d(S0)}{\varrho(S0)} = \frac{d(S)}{\varrho(S)}$$

By means of this property, we show that d succeeds on every "non-Dowd" oracle. In other words, for every "non-Dowd" oracle X, it holds that lim sup of $d(X \upharpoonright n)$ is infinite.

Summary

§2 Results on Non-Existence (Thm. [Dowd 1992], [S. 2001])

No t-generic sets (No poly.-bound on forcing complexity when unbounded occurrences of query symbols).

§3 Results on Existence (Def.)

(1) r-Dowd
$\leftrightarrow$ poly.-bound on forcing comp. for r-query tautologies
(It satisfies the resource-bounded forcing theorem).
(2) Dowd-generic $\leftrightarrow \forall r \geq 1 \quad r$-Dowd

§4 Main Theorem

There exists an elementary recursive function $t(n)$ s.t.
$t(n)$-random $\Rightarrow$ Dowd-generic.

References

- K. Ambos-Spies and E. Mayordomo: Resource-bounded measure and randomness. In: *Lecture Notes in Pure and Appl. Math.*, 187, 1–47 Dekker, 1997.
- K. Ambos-Spies, S. A. Terwijn and X. Zheng: Resource bounded randomness and weakly complete problems. *Theoret. Comput. Sci.*, 172 (1997) 195–207.
- M. Dowd: Generic oracles, uniform machines, and codes. *Inf. Comput.*, **96**, pp. 65–76 (1992).
- M. Kumabe and T. Suzuki: Computable Dowd-generic oracles. *Proc. 11th Asian Logic Conference*, pp.128–146, World Scientific, 2012.
- M. Kumabe and T. Suzuki: Resource-bounded martingales and computable Dowd-type generic sets, submitted to a journal (2010).

- M. Kumabe, T. Suzuki and T. Yamazaki: Does truth-table of linear norm reduce the one-query tautologies to a random oracle? *Arch. Math. Logic*, **47**, pp.159–180 (2008).
- T. Suzuki: Recognizing tautology by a deterministic algorithm whose while-loop's execution time is bounded by forcing. *Kobe Journal of Mathematics*, **15**, pp. 91–102 (1998).
- T. Suzuki: *Computational complexity of Boolean formulas with query symbols*. Doctoral dissertation, Institute of Math., Univ. of Tsukuba, Japan (1999).
- T. Suzuki: Complexity of the r-query tantologies in the presense of a generic oracle. *Notre Dame J. Formal Logic*, **41**, pp. 142–151 (2000).
- T. Suzuki: Forcing complexity: minimum sizes of forcing conditions. *Notre Dame J. Formal Logic*, **42**, pp. 117–120 (2001).

- T. Suzuki: Degrees of Dowd-type generic oracles. *Inf. Comput.*, **176**, pp.66–87 (2002).
- T. Suzuki: Bounded truth table does not reduce the one-query tautologies to a random oracle. *Arch. Math. Logic*, **44**, pp.751–762 (2005).
- T. Suzuki and M. Kumabe: Weak randomness, genericity and Boolean decision trees. *Proc. 10th Asian Logic Conference*, pp.322–344, World Scientific, 2009.

Toshio Suzuki URI:
`http://researchmap.jp/read0021048/?lang=english`

Appendix: Jump and a Problem

Let $1\mathrm{TAUT}^X$ denote the set of all 1-query tautologies w. r. t. X.

Question: Does $1\mathrm{TAUT}^X$ has a degree strictly higher than X?

Given a reduction concept $\leq_r$ (e.g., poly.-time Turing $\leq_T^P$),
we introduce the following statement, and we call it
"One-query jump hypothesis w. r. t. $\leq_r$" (1QJH(r), for short).

Def. One-query Jump Hypothesis w. r. t. $\leq_r$ [S. 2002]

"The class $\{X : X <_r 1\mathrm{TAUT}^X\}$ has Lebesgue measure 1 in the Cantor space".

Jump and a Problem

Thm. [S. 1998]

1QJH(poly.-time Turing) $\Leftrightarrow$ RP $\neq$ NP.

Here, RP is the one-sided version of BPP.

Thm. [S. 2002]

1QJH(poly.-time truth table) $\Rightarrow$ P $\neq$ NP.

S.: Recognizing tautology by a deterministic algorithm whose while-loop's execution time is bounded by forcing.
Kobe Journal of Mathematics, **15**, pp. 91–102 (1998).

Jump and a Problem

Examples of 1QJH [Kumabe, S. and Yamazaki 2008]

(1) 1QJH(monotone reductions) holds.
(tt-reductions s.t. truth tables are monotone Boolean formulas.)

(2) $c < 1 \Rightarrow$ 1QJH(tt-reductions s.t. norm $\leq c \times |F|$) holds.
(F is an input formula and $|F| = \sharp$ of occurrences of symbols.)

Problem

In (2), can we relax the assumption of "$c < 1$"?

M. Kumabe, S. and T. Yamazaki: Does truth-table of linear norm reduce the one-query tautologies to a random oracle?
Arch. Math. Logic, **47**, pp.159–180 (2008).