Resource-bounded randomness and computable Dowd-type generic sets

Dec. 15–20, 2011.

12th ASIAN LOGIC CONFERENCE,

Victoria University of Wellington

Masahiro Kumabe[(1)] and Toshio Suzuki[(2)]

(1) The Open University of Japan,

(2) Tokyo Metropolitan University (the speaker)

1 Abstract

The relationship between resource-bounded randomness (in the sense of Lutz, Ambos-Spies et al.) and Dowd-type genericity has been not clear so far. We show that there exists a primitive recursive function $t(n)$ such that every $t(n)$-random set (in the sense of Lutz) is r-Dowd (r-generic in the sense of Dowd) for each positive integer r. A proof is done by means of constructing resource-bounded martingales.

2 Introduction

Ambos-Spies et al. introduced the concept of resource-bounded random set by extending the works of Schnorr and Lutz. The concept of Dowd-type generic oracle, the main topic of this talk, is different from the resource-bounded genericity of Ambos-Spies et al.; while the former is based on an analogy of forcing theorem, the latter is based on time-bound of finite-extension strategy.

Def. [Dowd 1992] X is r-Dowd if every r-query tautology F with respect to X is forced by a forcing condition of polynomial-size in $|F|$.

We study the following property of an oracle X.
"For every positive integer r, X is r-Dowd."
In this talk, we denote the above property by the phrase "X is a Dowd-type generic oracle".

(1) [Dowd 1992] [S.2001] The class of all Dowd-type generic oracles has measure 1. ([Dowd 1992] asserts “they are not c.e.”)

(2) [S.2002] $\exists$ primitive recursive 1-Dowd oracle. And, $\forall$ Turing degree contains a 1-Dowd oracle.

(3) [S.&K.2009](*ALC10*) Martin-Löf 1-randomness implies Dowd-type genericity.

(4) [S.&K.2011](*ALC11*) (2) holds for “Dowd-type generic” in place of “1-Dowd”.

(1) [Dowd 1992] [S.2001] The class of all Dowd-type generic oracles has measure 1. ([Dowd 1992] asserts "they are not c.e.")

(2) [S.2002] $\exists$ primitive recursive 1-Dowd oracle. And, $\forall$ Turing degree contains a 1-Dowd oracle.

(3) [S.&K.2008](*ALC10*) Martin-Löf 1-randomness implies Dowd-type genericity.

(4) [S.&K.2010](*ALC11*) (2) holds for "Dowd-type generic" in place of "1-Dowd".

The result (4) gives an affirmative answer to a problem left open in the paper of the result (2).

Main result: There exists a primitive recursive function $t(n)$ such that every $t(n)$-random set is r-Dowd (r-generic in the sense of Dowd) for each positive integer r.

The main theorem of the current talk gives an alternative proof of the affirmative answer.

Contents of the talk

3 Def. of D.-type g.o. (sketch)

The definition of Dowd-type genericity is based on an analogy to *forcing theorem*.

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

cf. "A sentence in generic extension is forced by a finite-sized forcing condition. "

3 Def. of D.-type g.o. (sketch)

The definition of Dowd-type genericity is based on an analogy to *forcing theorem*.

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

cf. "A sentence in generic extension is forced by a finite-sized forcing condition."

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

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

(a set of connectives).

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.

Example: a formula of RPC, where each q_i is a propositional variable.

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

Given a formula F of RPC and an oracle X, truth of F is determined by

"a truth assignment $+$ a finite portion of X".

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

X is r-Dowd
$\Leftrightarrow_{\text{def.}}$ $\exists p$ (a polynomial depending on r)
$\forall F$ (an r-query tautology w. r. t. X)
$\exists S$ (a finite sub-function of X) such that
S forces F to be a tautology
(i.e., for every oracle Y extending S, F is a tautology with respect to Y)
and the size of S is at most $p(|F|)$, where the size denotes the cardinality of the domain of S.

4 Reviews of (2) and (4)

The result (4):

- *There exists a primitive recursive Dowd-type generic oracle.*
- *Every Turing degree contains a Dowd-type generic oracle.*

The result (2) is a special case where only 1-query formulas are considered.

We sketch our proof of the following result.

Lemma 1 *Suppose that r is a positive integer. Then, the followings hold.*

- *There exists a primitive recursive r-Dowd oracle.*
- *Every Turing degree contains an r-Dowd oracle.*

The result (4) is proved in a similar (but technically more complicated) manner.

Proof of Lemma 1 (sketch)

For an r-query formula F and a positive integer n, we say "*dimension of F $(\mathrm{dim}F)$ is n*" if every query symbol in F is of the form ξ^n.

For a forcing condition S, we say "*dimension of S $(\mathrm{dim}S)$ is n*" if the domain of S is the first 2^nth strings.

Example:

(1) $(q_0 \Leftrightarrow \xi^2(q_1, q_2)) \Rightarrow \neg q_0$ has dimension 2.

(2) If $\mathrm{dom}S = \{\lambda, 0, 1, 00\}$ then $\mathrm{dim}S = 2$.

Fix a polynomial p and a positive integer c (we assume that p and c satisfy a certain requirement). Suppose S is a forcing condition whose dimension is n.

We say "*S survives at dimension n*" if S is r-Dowd with respect to p and with respect to formulas whose length $\geq c$.

Suppose that X is an oracle. If for every dimension n, the initial segment of X survives, then X is r-Dowd.

Case 1, $r = 1$. This special case is proved in [Suzuki 2002].

Proposition 1 [Dowd 1992, Suzuki 2002]
Suppose that n is a positive integer and that S is a survivor at dimension n. Let p be the conditional probability of a randomly chosen extension S' of S at dimension $n+1$ being a survivor at dimension $n+1$. Then

$$p \geq 1 - \frac{1}{2^{n+2}} \ .$$

With Proposition 1, we know that there exists a binary tree such that for every n, each node S of height n is a survivor at dimension n, and each child of S is an extension of S.

The least infinite branch (its union) of the tree is a primitive recursive 1-Dowd oracle.
A given Turing degree $\mathbf{a}$ is recursively coded by an infinite branch of the tree, and the branch is a 1-Dowd oracle. Hence, every Turing degree contains a 1-Dowd oracle. (Case 1, proved.)

Case 2, otherwise ($r \geq 2$). In this case, we do not know whether every survivor at dimension n has surviving extensions at next stage.

Proposition 2 [Suzuki 1999] *Suppose that n is a positive integer. Let ρ be the conditional probability of a randomly chosen forcing condition S of dimension n being a survivor at dimension n. Then*

$$\rho \geq 1 - \frac{1}{2^{n+2}} \ .$$

Let $f(n) := 2^n + n + 1$. We say "*S survives at dimension n in the strong sense*" if the following (1) and (2) hold.

(1) S survives at dimension n.

(2) The probability of a randomly chosen forcing condition T (of the property (2a)) having property (2b) is high enough.

2a $\dim T = f(n)$, and T extends S.

2b $n + 1 \leq \forall i \leq f(n)$, the restriction of T at dimension i survives at dimension i.

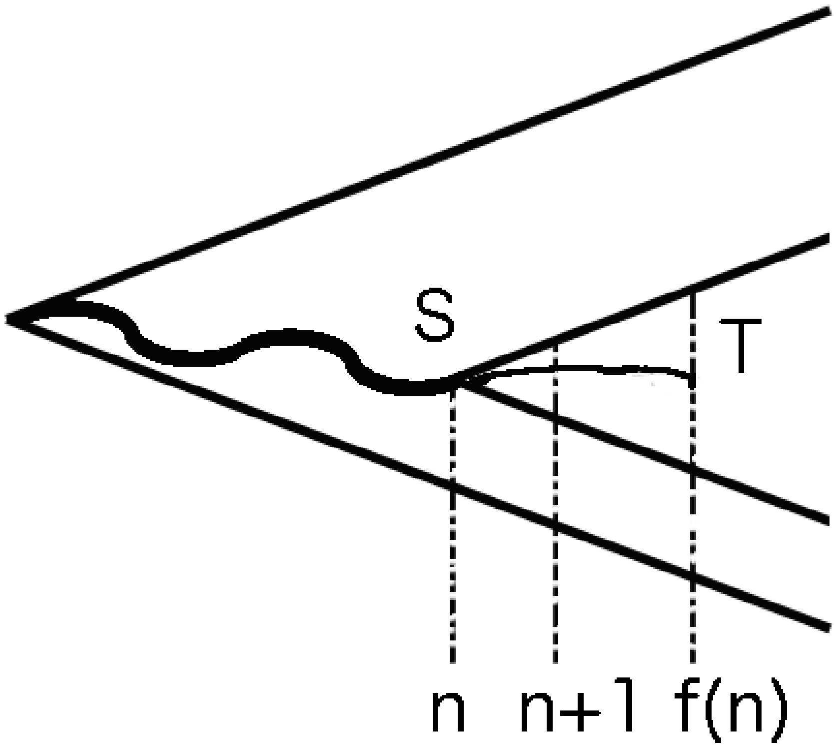

Fig.1 S survives in the strong sense at dim. n

Prob [a “far future” (i.e. at dimension $f(n)$) descendant T of S survives] is high enough.

By means of Proposition 2, we get a result similar to Proposition 1 for “a survivor in the strong sense” in place of “a survivor”. Thus we prove Lemma 1. Q.E.D.

The result (4) is proved in a similar manner.
The result (4):

- *There exists a primitive recursive Dowd-type generic oracle.*
- *Every Turing degree contains a Dowd-type generic oracle.*

5 Main result

Main result: There exists a primitive recursive function $t(n)$ such that every $t(n)$-random set is r-Dowd (r-generic in the sense of Dowd) for each positive integer r.

Proof (sketch): We construct a martingale that succeeds on every "non-Dowd" oracle. Suppose that 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 S.

In the two basic open sets given by $S0$ (S concatenated by 0) and $S1$, we investigate the conditional probabilities of a randomly chosen oracle T (to be more precise, its finite initial segment is chosen) fails to have property (2b) in the previous sub-section with respect to p.

2b $n+1 \leq \forall i \leq f(n)$, the restriction of T at dimension i survives at dimension i.

We denote them by $\varrho(S0)$ and $\varrho(S1)$.

Define the martingale values $d(S0)$, $d(S1)$ as:

$$\varrho(S0)/d(S0) = \varrho(S1)/d(S1)$$

If $\varrho(S) = 1$ (i.e., all extensions fail to have 2b) then let $d(S0) = d(S1) = d(S)$, and at a certain extension of S, we refresh the polynomial p. Under a certain assumption,

$$\varrho/d = \text{(constant)}$$

during the procedure of inductive definition.

And, an inequality on a certain infinite product

$$\prod_{n=1}^{\infty}(1+\frac{1}{2^n}) < 1+\sqrt{2}$$

helps us to control the convergence and divergence of the ratio along a given branch. By using this ratio, we get that our martingale succeeds on every "non-Dowd" oracle.

$\square$

Bibliography

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

[2] Kumabe, M. and Suzuki, T. : Computable Dowd-type generic oracles. *Proc. 11th ALC*, World Scientific, to appear.

[3] Suzuki, T. and Kumabe, M.: Weak randomness, genericity and Boolean decision trees. *Proc. 10th ALC*, World Scientific, 2009.

[4] Suzuki, T.: Degrees of Dowd-type generic oracles. *Inf. Comput.*, **176**, pp.66–87 (2002).

[5] Suzuki, T.: *Computational complexity of Boolean formulas with query symbols*. Doctoral dissertation, Institute of Mathematics, University of Tsukuba, Tsukuba-City, Japan (1999).

URL (Toshio Suzuki)

`http://www.ac.auone-net.jp/~bellp/`