

# negligible function の 形式定義について

岡崎裕之(信州大学)

布田裕一(北陸先端技術大学院大学)

# 去年の話

ある  $\mathbf{N} \rightarrow \mathbf{R}$  である関数  $\mu(\cdot)$  について

任意の多項式  $p(\cdot)$  に対して、

ある自然数  $N$  が存在し、

$N \leq n$  なる任意の自然数  $n$  について

$$\mu(n) < \frac{1}{|p(n)|}$$

であるとき  $\mu(\cdot)$  は無視できるほど小さい関数である

多項式オーダーの  
話で置き換える

# 去年の話(提案)

ある  $\mathbf{N} \rightarrow \mathbf{R}$  である関数  $\mu(\cdot)$  について

ある多項式オーダーでない関数  $f(\cdot)$  が存在し、

ある自然数  $N$  が存在し、

$N \leq n$  なる任意の自然数  $n$  について

$$\mu(n) \leq \frac{1}{|f(n)|}$$

であるとき  $\mu(\cdot)$  は無視できるほど小さい関数である

去年はそう言いましたが

あれはうそ

今回の発表内容

普通の定義でうまくいきましたので  
訂正と、うまくいった経緯の説明

# 経緯

- negligible functionの定義自体は簡単
- しかし、negligible functionの存在をうまく証明できるのか？
- とりあえず多項式オーダーを書いてみよう
- 2冪が多項式オーダーでないことが証明できてしまった
- $1/2$ 冪がnegligibleであることも証明できてしまった

# Mizarについて

- 数学の証明を計算機で検証する  
(自動検証)
- 数学定理の形式的証明
- 数学っぽい文法

<http://markun.cs.shinshu-u.ac.jp/kiso/projects/proofchecker/mizar/index-j.html>

# motivation

## **Our Aim:**

- Proving security of cryptographic protocols
- Formalizing and evaluating cryptographic primitives
- Formalizing performance evaluation of cryptographic algorithms

# Related Topics

we must formalize for cryptology

- Probability
  - Computational Complexity
  - Algorithms
  - Number Theory
  - Information Theory
- etc.



# Class P

- Problem X is in class P  
if it takes **polynomially bounded**  
computation time to solve problem X
- There are feasible algorithms to  
solve X efficiently  
if problem X in P

# Polynomially-bounded Functions

*$f(x)$  is polynomially – boubded  
iff*

$$\exists n \in \mathbf{N} \text{ s.t. } f(x) \in O(x^n)$$

# Asymptotic notation $O(^*)$

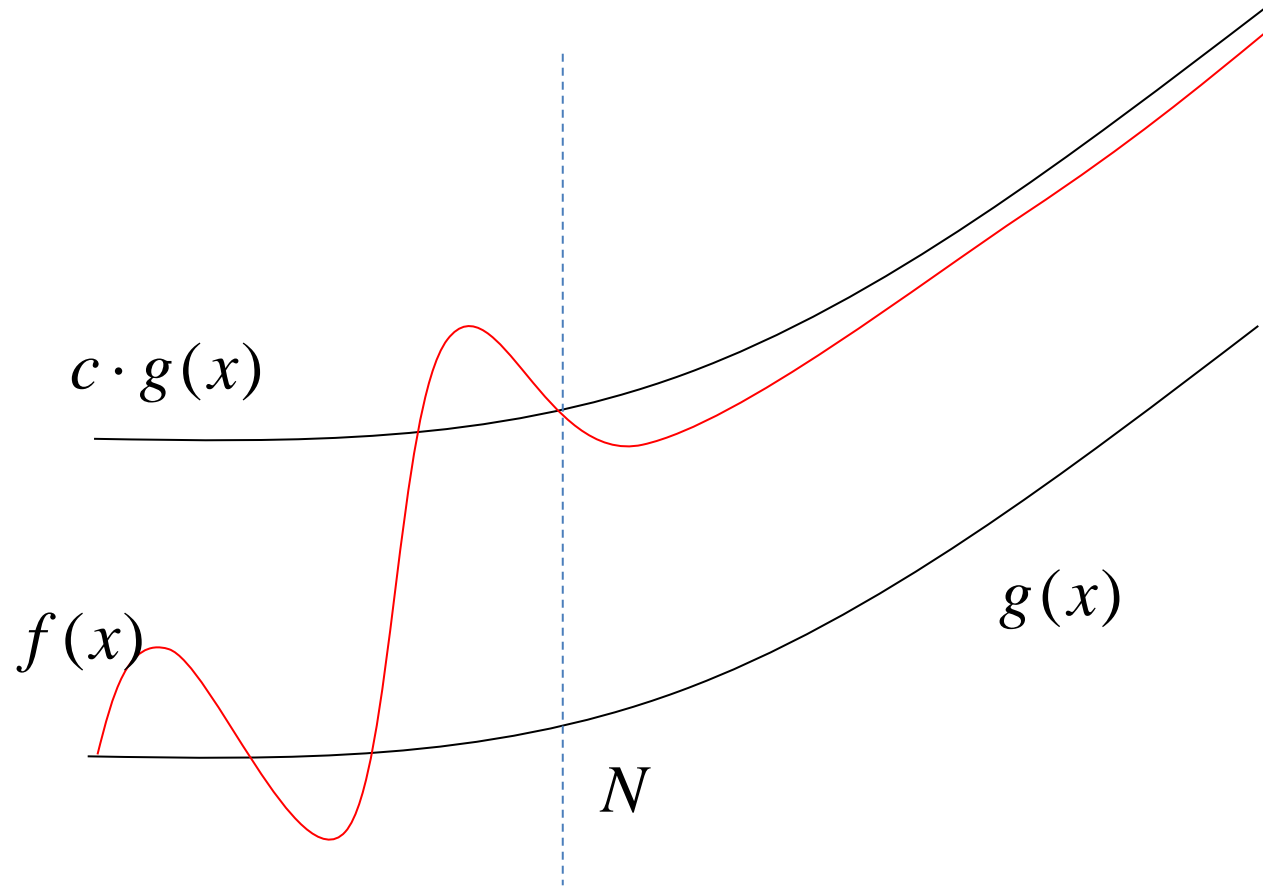
$$f \in O(g)$$

*iff*

$$\left( \exists c, N \text{ s.t. } 0 < c \ \&$$

$$\forall x \text{ s.t. } N \leq x \text{ holds } f(x) \leq c \cdot g(x) \right)$$

# Asymptotic notation $O(^*)$



# Related article in MML

## Asymptotic notation $O(*)$

definition

```
let f be eventually-nonnegative Real_Sequence;  
func Big_Oh(f) -> FUNCTION_DOMAIN of NAT,  
    REAL equals  
:: ASYMPT_0: def 9  
  { t where t is Element of Funcs(NAT, REAL) :  
    ex c, N st c > 0 & for n st n >= N holds t.n <= c*f.n  
    & t.n >= 0 };  
end;
```

# Related article in MML

## Monomial sequence

$$0, 1^a, 2^a, \dots, n^a, \dots$$

definition

let a be Real;

func seq\_n^(a) -> Real\_Sequence means

:: ASYMPT\_1: def 3

it.0 = 0 & for n st n > 0 holds it.n = n to\_power a;

end;

# Polynomially-bounded Functions in Mizar

definition

let p be Real\_Sequence;

attr p is polynomially-bounded means

:: ASYMPT\_2:def 1

ex k be Element of NAT st p in

Big\_Oh(seq\_n^(k));

end;

# Algebraic structure

definition

```
func R_Algebra_of_PolynomialOrderSeqs -> strict AlgebraStr
means
the carrier of it = PolynomialOrderSeqs
& the multF of it
= (RealFuncMult(NAT)) || PolynomialOrderSeqs
& the addF of it = (RealFuncAdd(NAT)) || PolynomialOrderSeqs
& the Mult of it
= (RealFuncExtMult(NAT)) | [:REAL,PolynomialOrderSeqs:]
& the OneF of it = RealFuncUnit(NAT)
& the ZeroF of it = RealFuncZero(NAT);
end;
```



# Theorem

$2^n$  is non polynomially-bounded

$\forall x \in \mathbf{N}$  s.t.  $1 < x$  holds

$\neg \left( \exists c, N \in \mathbf{N}$  s.t.  $\forall n \in \mathbf{N}$  s.t.  $N \leq n$  holds  $2^n \leq c \cdot n^x$  )

theorem

for  $x$  be Element of NAT st  $1 < x$  holds

not ex  $N, c$  be Element of NAT st

for  $n$  be Element of NAT st  $N \leq n$  holds

$2 \text{ to\_power } n \leq c * (n \text{ to\_power } x);$

# Related article in MML

## Monomial sequence

$$0, 1^a, 2^a, \dots, n^a, \dots$$

definition

let a be Real;

func seq\_n^(a) -> Real\_Sequence means

:: ASYMPT\_1: def 3

it.0 = 0 & for n st n > 0 holds it.n = n to\_power a;

end;

# Univariate Polynomial sequence

definition

let c be XFinSequence of REAL;  
func seq\_p(c) -> Real\_Sequence  
means

:: ASYMPT\_2:def 2

for x be Element of NAT holds

it.x = Sum(c (#) seq\_a^(x,1,0));

end;

# EXAMPLE

$$f(x) = 5 + 4x^1 + 3x^2$$

$$c = \langle 5, 4, 3 \rangle; \quad (c.0=5, c.1=4, c.2=3);$$

$$c \text{ (\#) } \text{seq\_a}^{\wedge}(x, 1, 0)$$

$$= \langle (c.0) * x^0, (c.1) * x^1, (c.2) * x^2 \rangle$$

$$= \langle 5 * x^0, 4 * x^1, 3 * x^2 \rangle$$

$$(\text{seq\_p}(c)).x = 5 + 4 * x^1 + 3 * x^2;$$

# Polynomial is Polynomially-bounded

theorem :: ASYMPT\_2:54

for k be Nat,

c be XFinSequence of REAL

st len c = k+1 & 0 < c.k

holds seq\_p(c) in Big\_Oh( seq\_n^(k) );

# Negligible Functions

Let  $\mu(n)$  be a function from *Natural* to *Real*.

$\mu(n)$  is negligible function iff

exists  $N$  be a natural number s.t.,

$\forall n$  be a natural number st  $N \leq n$  holds

$\forall p(*)$  be a polynomial holds

$$\mu(n) < \frac{1}{|p(n)|}$$

# Negligible Functions

definition

let  $f$  be Function of NAT,REAL;

attr  $f$  is negligible

means

:defneg:

for  $c$  be non empty positive-yielding XFinSequence of REAL

holds

ex  $N$  be Element of NAT

st

for  $x$  be Element of NAT

st  $N \leq x$  holds  $|f.x| < 1/((seq\_p(c)).x)$  ;

end;

$\frac{1}{2^x}$  is negligible

theorem

for  $f$  be Function of NAT, REAL st

for  $x$  be Element of NAT holds

$$f.x = 1 / (2 \text{ to\_power } x)$$

holds  $f$  is negligible



# binary operations on negligible functions

theorem

for  $f, g$  be Function of  $\text{NAT}, \text{REAL}$  st  $f$  is negligible &  $g$  is negligible  
holds  $f+g$  is negligible;

theorem

for  $f$  be Function of  $\text{NAT}, \text{REAL}$ ,  $a$  be Real  
st  $f$  is negligible holds  
 $a(\#)f$  is negligible;

theorem

for  $f, g, h$  be Function of  $\text{NAT}, \text{REAL}$  st  $f$  is negligible &  $g$  is negligible &  
 $h = f(\#)g$   
holds  $h$  is negligible;

# Future Work using negligibility

- Roughly saying, a cryptosystem is secure if the "probability of attack against the cryptosystem succeeds" is negligible.
- “indistinguishability” is defined using negligibility

# Theorem

$2^n$  is non polynomially-bounded

$\forall x \in \mathbf{N}$  s.t.  $1 < x$  holds

$\neg \left( \exists c, N \in \mathbf{N}$  s.t.  $\forall n \in \mathbf{N}$  s.t.  $N \leq n$  holds  $2^n \leq c \cdot n^x$  )

theorem

for  $x$  be Element of NAT st  $1 < x$  holds

not ex  $N, c$  be Element of NAT st

for  $n$  be Element of NAT st  $N \leq n$  holds

$2 \text{ to\_power } n \leq c * (n \text{ to\_power } x);$

2冪が多項式オーダーでないことの  
証明、背理法でうまくいったよ！



と某東学院大学の長〇先生  
←に言ったところ悔しがって  
「構成的な証明」  
を考えていただきました。

$n(\in \mathbb{Z}_{\geq 0})$  とする。また、

$$T_0(n) := \max_{1 \leq k \leq n} \{ {}_n C_k \times 3n \}$$

と置く。このとき次が成り立つ。

**Lemma 1**  $\forall t > T_0(n) (t \in \mathbb{R})$  に対して、 $(t+1)^n < \frac{4}{3}t^n$  が成り立つ。

証明：

$$\frac{(t+1)^n}{t^n} = 1 + \sum_{k=1}^n {}_n C_k (1/t)^k \leq 1 + \sum_{k=1}^n {}_n C_k (1/t) \leq 1 + \sum_{k=1}^n \frac{1}{3n} = \frac{4}{3}.$$

$C(\in \mathbb{R}_{\geq 0})$  とする。また、

$$T_1(n, C) := \max\{0, \lceil \log_{4/3} \frac{CT_0(n)^n}{2^{T_0(n)-1}} \rceil\}$$

と置く。定義より

$$\left(\frac{4}{3}\right)^{T_1(n, C)} \geq \frac{CT_0(n)^n}{2^{T_0(n)-1}}$$

であり、次が成り立つ。

**Lemma 2**

$$T_0(n)^n \leq \frac{1}{C} \cdot \left(\frac{4}{3}\right)^{T_1(n, C)} \cdot 2^{T_0(n)-1}.$$

**Theorem**  $\forall t > T_0(n) + T_1(n, C) (t \in \mathbb{R})$  に対して、 $Ct^n < 2^t$  が成り立つ。

証明: 上の条件を満たす  $t$  に対して、 $\exists m_t \geq T_1(n, C) (m_t \in \mathbb{Z}), 0 \leq \exists s_t < 1 (s_t \in \mathbb{R})$  で、 $t = T_0(n) + m_t + s_t$  を満たすものが存在する。したがって、**Lemma 1** より、

$$t^n \leq \left(\frac{4}{3}\right)^{m_t} (T_0(n) + s_t)^n < \left(\frac{4}{3}\right)^{m_t} (T_0(n) + 1)^n \leq \left(\frac{4}{3}\right)^{m_t+1} T_0(n)^n$$

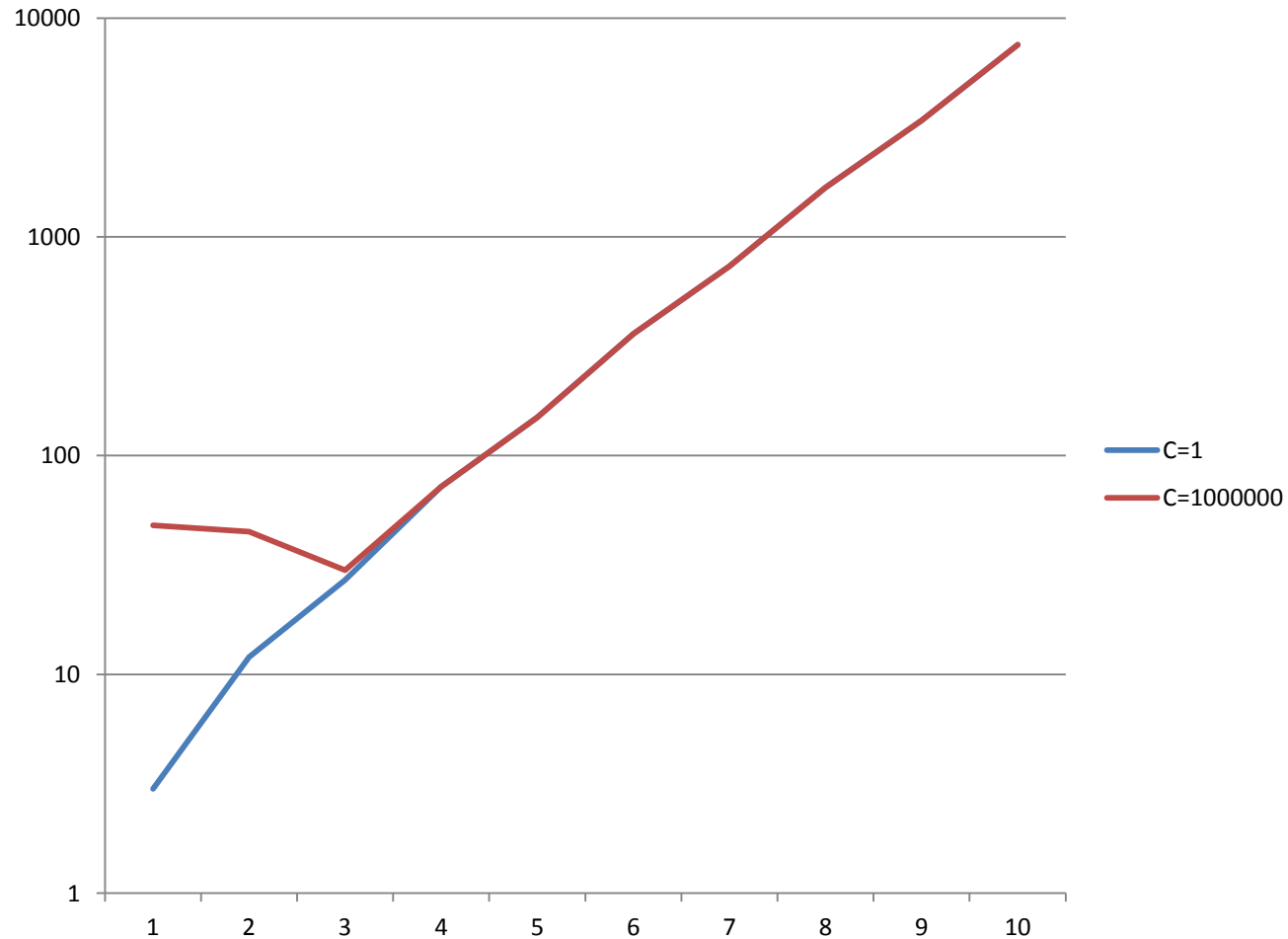
であり、**Lemma 2** より、

$$\leq \frac{1}{C} \cdot \left(\frac{4}{3}\right)^{m_t+1} \cdot \left(\frac{4}{3}\right)^{T_1(n, C)} \cdot 2^{T_0(n)-1}$$

$m_t \geq T_1(n, C), \left(\frac{4}{3}\right)^2 < 2$  より、

$$\leq \frac{2}{3} \cdot \frac{1}{C} \cdot \left(\frac{4}{3}\right)^{2m_t} \cdot 2^{T_0(n)} \leq \frac{2}{3} \cdot \frac{1}{C} \cdot 2^{T_0(n)+m_t} \leq \frac{1}{C} \cdot 2^{T_0(n)+m_t+s_t} = \frac{1}{C} \cdot 2^t$$

# 数値例 (n=10まで、C=1,1000000)



# 悔しいのでMizarで証明

Lemma1:

for n being Nat,

t being Real

st  $1 \leq n \ \& \ 3 * n * (\max (\text{Newton\_Coeff } n)) \leq t$

holds

$(1 + 1/t) \text{ to\_power } n \leq 4/3;$



# 悔しいのでMizarで証明

Lemma2:

for  $n$  be Nat,  $t_0, t_1, C$  be Real st  $0 < C$  &  $1 \leq n$  &

$t_0 = 3 * n * (\max(\text{Newton\_Coeff } n))$  &

$t_1 = \max(0, \log(4/3, C * (t_0 \text{ to\_power } n)$

$/(2 \text{ to\_power } (t_0 - 1))))$

holds  $C * (t_0 \text{ to\_power } n) / (2 \text{ to\_power } (t_0 - 1))$

$\leq (4/3) \text{ to\_power } t_1$

# 悔しいのでMizarで証明

Theorem:

for n be Nat, t0, t1, t, C be Real st  $0 < C \ \& \ 1 \leq n \ \&$

$t_0 = 3 * n * (\max (\text{Newton\_Coeff } n)) \ \&$

$t_1 = \max(0, \log(4/3, C * (t_0 \text{ to\_power } n) / (2 \text{ to\_power } (t_0 - 1))))$

$\ \& \ t_0 + t_1 < t$  holds

$C * (t \text{ to\_power } n) < 2 \text{ to\_power } t;$

# まとめ

- 多項式オーダーの形式定義
- $2^{\text{冪}}$ が多項式オーダーでないことを形式証明  
(多項式オーダーでない関数の存在証明)
- Negligible function の形式定義
- $1/2^{\text{冪}}$ がnegligible であることの形式証明  
(Negligible function の存在証明)
- (おまけ)  $2^{\text{冪}} \gg$  多項式の構成的な形式証明

theorem

for n being Nat st  $1 \leq n$  holds  
 $1 \leq \max(\text{Newton\_Coeff } n)$ ;

theorem

for n being Nat,

t being Real st  $1 \leq n$  &  $3 \cdot n \cdot (\max(\text{Newton\_Coeff } n)) \leq t$

holds  $(1 + 1/t)^n \leq 4/3$ ;

theorem

for  $k, n$  be Nat,  $T, t, c$  be Real st  $0 < c$  &  $T \leq t$  &

for  $s$  be Real st  $T \leq s$  holds  $(s+1)$  to\_power  $n \leq c * (s$   
to\_power  $n)$

holds  $(t + k)$  to\_power  $n \leq (c$  to\_power  $k) * (t$  to\_power  $n)$ ;

theorem

for  $n$  be Nat,  $t_0, t_1, C$  be Real st  $0 < C$  &  $1 \leq n$  &

$t_0 = 3 * n * (\max (\text{Newton\_Coeff } n))$  &

$t_1 = \max(0, \log(4/3, C * (t_0$  to\_power  $n) / (2$  to\_power  $(t_0 - 1))))$

holds  $C * (t_0$  to\_power  $n) / (2$  to\_power  $(t_0 - 1)) \leq (4/3)$   
to\_power  $t_1$ ;

theorem

for  $n$  be Nat,  $t_0, t_1, t, C$  be Real st  $0 < C \ \& \ 1 \leq n \ \&$

$t_0 = 3 * n * (\max (\text{Newton\_Coeff } n)) \ \&$

$t_1 = \max(0, \log(4/3, C * (t_0 \text{ to\_power } n) / (2$   
 $\text{to\_power } (t_0 - 1))))$

$\ \& \ t_0 + t_1 < t$  holds

$C * (t \text{ to\_power } n) < 2 \text{ to\_power } t;$

theorem

for  $x$  be Element of NAT st  $1 < x$  holds

not ex  $N, c$  be Element of NAT st

for  $n$  be Element of NAT st  $N \leq n$  holds

$2 \text{ to\_power } n \leq c * (n \text{ to\_power } x);$