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$\mathbf{N} \to \mathbf{R}$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$\mathbf{N} \to \mathbf{R}$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、

$N \le n$なる任意の自然数nについて

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

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

$$f(x) \quad is \quad polynomially-boubded$$

$$iff$$

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

Asymptotic notation $O(*)$

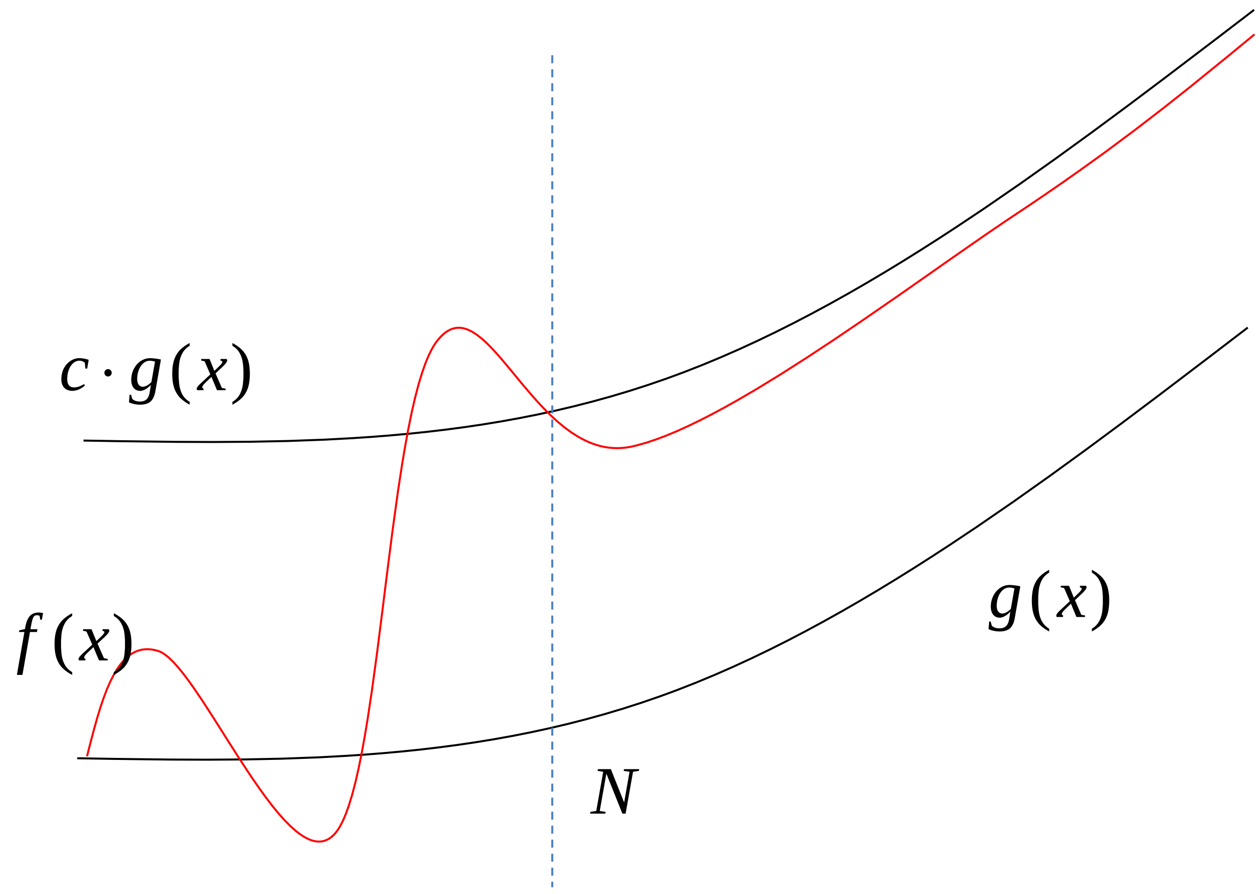
$$f \in O(g)$$

$$iff$$

$$\Big({}^{\exists} c, N \ s.t.\ 0 < c \ \&$$

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

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

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

```
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

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

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

```
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 <= n holds
  2 to_power n <= c * ( n to_power x);
```

Related article in MML
Monomial sequence

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

```
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 =<5,4,3>; (c.0=5,c.1=4,c.2=3);

c (#) seq_a^(x,1,0)

=<(c.0)*x^0, (c.1)*x^1, (c.2)*x^2>

=<5*x^0, 4*x^1, 3*x^2>

(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 $\mathrm{Re}\,al$.

$\mu(n)$ is negligible function iff

exists N be a natural number s.t.,

$\forall n$ be a nutural number st $\mathrm{N} \leq n$ 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 <=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 to_power x)
holds  f is negligible
```

binary operations on negligible functions

```
theorem
for  f,g be Function of NAT,REAL  st f is negligible & g is negligible
    holds  f+g is negligible;

theorem
for  f be Function of NAT,REAL,     a be Real
  st f is negligible holds
a(#)f is negligible;

theorem
for  f,g,h be Function of NAT,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

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

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

```
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 <= n holds
  2 to_power n <= c * ( n 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○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、

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

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：

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

$C(\in \mathbb{R}_{\geq 0})$ 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

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

であり、次が成り立つ。
Lemma 2

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

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、

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

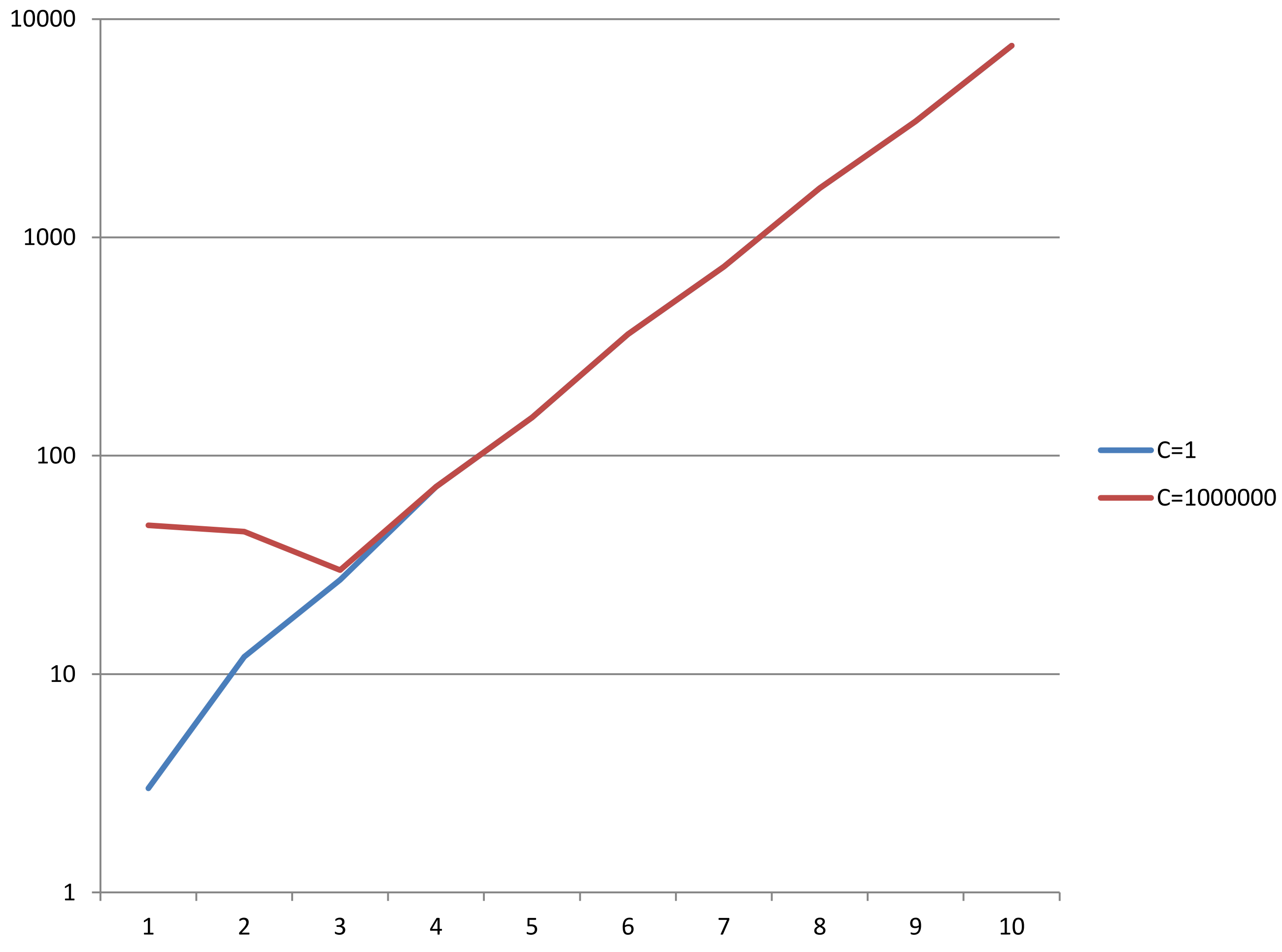
であり、**Lemma 2** より、

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

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

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

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 <= n & 3*n*(max (Newton_Coeff n)) <= t
holds
 (1 + 1/t) to_power n <= 4/3;
```

悔しいのでMizarで証明

```
Lemma2:
for n be Nat,t0, t1,C be Real st 0 < C & 1 <= n &
 t0 = 3*n*(max (Newton_Coeff n)) &
  t1 = max(0,log(4/3, C*(t0 to_power n)
                                       /(2 to_power (t0 -1))))
holds   C*(t0 to_power n)/(2 to_power (t0 -1))
<= (4/3) to_power t1
```

悔しいのでMizarで証明

```
Theorem:
for n be Nat,t0, t1,t,C be Real st 0 < C &1 <= n &
 t0 = 3*n*(max (Newton_Coeff n)) &
  t1 = max(0,log(4/3, C*(t0 to_power n)/(2
to_power (t0 -1))))
 & t0 + t1 < t holds
 C *(t to_power n) < 2 to_power t;
```

まとめ

- 多項式オーダーの形式定義
- 2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冪がnegligible であることの形式証明
  （Negligible function の存在証明）
- （おまけ）2冪>> 多項式の構成的な形式証明

```
theorem
 for n being Nat st 1 <= n holds
1 <= max (Newton_Coeff n );

theorem
for n being Nat,
 t being Real st 1 <= n & 3*n*(max (Newton_Coeff
n)) <= t
holds  (1 + 1/t) to_power n <= 4/3;
```

```
theorem
for k,n be Nat, T,t,c be Real st 0 < c & T <= t &
   for s be Real st T <= s holds (s+1) to_power n <= c*( s
to_power n)
holds (t + k) to_power n <= (c to_power k)*(t to_power n);

theorem
for n be Nat,t0, t1,C be Real st 0 < C & 1 <= n &
 t0 = 3*n*(max (Newton_Coeff n)) &
  t1 = max(0,log(4/3, C*(t0 to_power n)/(2 to_power (t0 -1))))
holds   C*(t0 to_power n)/(2 to_power (t0 -1)) <= (4/3)
to_power t1;
```

```
theorem
for n be Nat,t0, t1,t,C be Real st 0 < C &1 <= n &
 t0 = 3*n*(max (Newton_Coeff n)) &
  t1 = max(0,log(4/3, C*(t0 to_power n)/(2
to_power (t0 -1))))
 & t0+ t1 < t holds
 C *(t to_power n) < 2 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 <= n holds
  2 to_power n  <=  c * ( n to_power x);
```