negligible functionの形式定義について

岡崎 裕之(信州大学)
布田 裕一(JAIST)

モチベーション

- 定理証明系Mizar（でなくてもよいけれど）を用いて安全性証明がやりたい
- （ついでに他にも工学的なものができればうれしい）
- 暗号理論に使えるライブラリが全然足りない
- 必要なモノを作らないといけない

必要なモノ

- 数論関連のライブラリ
- 計算量
- アルゴリズム
- 確率

確率ができたので

- 暗号理論の形式化に適用する！
- 識別不能性を形式化したい
- 無視できるほど小さい（negligible）を形式化しなければいけない

Mizarについて

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

negligible

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

$$\varepsilon < \frac{1}{\left|p(n)\right|}$$

であるときεは無視できるほど小さい

negligible function

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、

$N \le n$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

negligible (function)の定義

- 定義は美しい（数学では良い）
- 我々のやりたい場合ではどうか？
- コンピュータサイエンスの場合、有限，かつ離散の場合を扱いたい
- （有理数）
- 自明な0以外にこんなものはあるのか？

negligible function

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、

$N \le n$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

negligible function（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

多項式オーダーの定義（Mizar）

```
definition
let p be Real_Sequence;
attr p is polynomial_order means
 ex k be Element of NAT st p in
   Big_Oh(seq_n^(k));
end;
```

O-表記

```
definition
  let f be eventually-nonnegative Real_Sequence;
  func Big_Oh(f)
       -> FUNCTION_DOMAIN of  NAT, REAL
   equals
  { 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;
```

多項式オーダーの定義（Mizar）

```
definition
let p be Real_Sequence;
attr p is polynomial_order means
 ex k be Element of NAT st p in
   Big_Oh(seq_n^(k));
end;
```

negligible functionの定義（Mizar）

```
definition
let mu be Element of Funcs(NAT,REAL);
attr mu is negligible means
 ex f be Real_Sequence
     st f is non polynomial_order
&    ex N being Nat st
       for n being Nat st n >= N holds
      mu. n <= (seq_const 1 /" f ).n;
end;
```

```
definition
let f1, f2 be complex-valued Function;
func f1 (#) f2 -> Function means
( dom it = (dom f1) /¥ (dom f2) &
 ( for c being object st c in dom it holds
it . c = (f1 . c) * (f2 . c) ) );

func f1 /" f2 -> Function equals
  f1 (#) (f2");
End;
```

negligible functionの定義（Mizar）

```
definition
let mu be Element of Funcs(NAT,REAL);
attr mu is negligible means
 ex f be Real_Sequence
     st f is non polynomial_order
&    ex N being Nat st
       for n being Nat st n >= N holds
      mu. n <= (seq_const 1 /" f ).n;
end;
```

negligible functionの存在（Mizar）

theorem

for f be Real_Sequence st f is

non　polynomial_order holds

ex mu be Element of Funcs(NAT,REAL) st

mu = (seq_const 1 /“ f) & mu is negligible;

まとめ(SCISのときまで)

- negligibleの定義について考察した
- 暗号理論に適するようにオーダーを使った定義を提案した（離散、有限の場合）
- 直観とも一致する定義となる
- 非自明なnegligible functionの存在を容易に示すことが出来る

現在進めていること

- non polynomial_order Real_Sequenceについて
- negligible functionの定義は本当にこんなのなので良いのか？
  - 多項式オーダーと任意の多項式の関係
  - 普通のnegligible functionの定義と新たな定義の関係

現在証明作業進行中のもの

theorem

for a be Element of NAT st 1 < a holds

seq_a^(a,1,0) is non polynomial_order;

ただし let a,b,c be Real;

  func seq_a^(a,b,c) -> Real_Sequence means

  it.n = a to_power (b*n+c);

negligible functionの定義（Mizar）

```
definition
let mu be Element of Funcs(NAT,REAL);
attr mu is negligible means
 ex f be Real_Sequence
     st f is non polynomial_order
&    ex N being Nat st
       for n being Nat st n >= N holds
      mu. n <= (seq_const 1 /" f ).n;
end;
```

Cnegligible (仮)の定義

```
definition
let mu be Element of Funcs(NAT,REAL);
attr mu is Cnegligible means
 ex f be Real_Sequence
     st f is non polynomial_order
&    ex N being Nat st
       for n being Nat st n >= N holds
      mu. n <= (seq_const 1 /" f ).n;
end;
```

Cnegligible の評価方針

よく知られたnegligibleも定義してしまって、negligibleとCnegligibleのＧａｐについて評価する。

negligibleとCnegligibleの識別不能性を考えてみる…….でも向かくいくかどうかは今後の課題。

結局何を考えるのか？

- 多項式オーダーと任意の多項式の関係
- O（n^k） (kは任意の自然数)　と多項式全体の集合の関係がどうなっているのか考えてみる？

（実）多項式（数列）の定義

```
definition
let c be Real_Sequence;
func seq_p(c) -> Real_Sequence
means
for x be Element of NAT holds
it.x =  Sum(c (#) seq_a^(x,1,0) );
```

n次多項式の集合

definition

let n be Element of NAT;

func n th_degree_sequenses -> Subset of (n+1)-tuples_on REAL means

for c be Element of (n+1)-tuples_on REAL holds seq_p(c) in it;

これとBig_Oh(seq_n^(n))を比べる！