

SOLUTION OF EXERCISESHEET 2

Exercise 2-1

Test

Exercise 2-2

Exercise 2-3

f and q are negligible functions and q be a positive polynomial.

- (a) Is e^{-x} negligible? For any polynomial x^c , choose ${\cal N}=c$, then for all $x>{\cal N}$ holds: $e^{-x}<\frac{1}{x^c}$, because $e^x>x^c$ for all x>N=c. $\Rightarrow e^{-x}$ is negligible.
- (b) Is $\frac{1}{x^{2021}+1}$ negligible? For the polynomial x^{2022} there is no N, that for all x>N holds: $\frac{1}{x^{2021}+1}<\frac{1}{x^{2022}}$, because $x^{2021}+1$ is smaller than x^{2022} for x>1. $\Rightarrow \frac{1}{x^{2021}+1}$ is not negligible.
- (c) Is h(x) negligible, when h(x) is a positive function such that h(x) < f(x) for all x? For f(x) holds: $f(x) < \frac{1}{p(x)}$ (Definition 0.1). Because of $h(x) < f(x) < \frac{1}{p(x)}$ for all x, h(x) is also negligible.
- (d) Is f(x) + g(x) negligible? f(x) negligible $\Rightarrow f(x) < \frac{1}{p(x)}$ (Definition 0.1). g(x) negligible $\Rightarrow g(x) < \frac{1}{p'(x)}$ (Definition 0.1).

$$\Rightarrow f(x) + g(x) < \frac{1}{p(x)} + \frac{1}{p'(x)}$$

$$= \frac{p'(x) + p(x)}{p(x) \cdot p'(x)}$$

$$= \frac{1}{\frac{p(x) \cdot p'(x)}{p'(x) + p(x)}}$$

Addition, multiplication and division of two polynomials results in another polynomial. p(x)and p'(x) can be any polynomials. Because of that the denominator $(\frac{p(x) \cdot p'(x)}{p'(x) + p(x)})$ can also be any polynomial.

 $\Rightarrow f(x) + g(x)$ is negligible.

(e) Is $f(x) \cdot q(x)$ negligible? f(x) negligible $\Rightarrow f(x) < \frac{1}{p(x)}$ (Definition 0.1).



Solution of Exercisesheet 2

q(x) is a positive polynomial.

$$\Rightarrow f(x) < \frac{1}{p(x)} \qquad | \cdot q(x), q(x) positive$$

$$f(x) \cdot q(x) < \frac{q(x)}{p(x)}$$

$$f(x) \cdot q(x) < \frac{1}{\frac{p(x)}{q(x)}}$$

Division of two polynomials results in another polynomial. p(x) can be any polynomial. So the denominator $(\frac{p(x)}{q(x)})$ can also be any polynomial.

$$\Rightarrow f(x) \cdot q(x)$$
 is negligible.

(f) Is $\frac{f(x)}{g(x)}$ negligible?

$$f(x)$$
 negligible $\Rightarrow f(x) < \frac{1}{p(x)}$ (Definition 0.1). $g(x)$ negligible $\Rightarrow g(x) < \frac{1}{p'(x)}$ (Definition 0.1).

$$g(x)$$
 negligible $\Rightarrow g(x) < \frac{1}{p'(x)}$ (Definition 0.1).

$$\Rightarrow \frac{f(x)}{g(x)} < \frac{\frac{1}{p(x)}}{\frac{1}{p'(x)}}$$
$$\frac{f(x)}{g(x)} < \frac{1}{\frac{p(x)}{p'(x)}}$$

Division of two polynomials results in another polynomial. p(x) and p'(x) can be any polynomials. So the denominator $(\frac{p(x)}{p'(x)})$ can also be any polynomial.

$$\Rightarrow \frac{f(x)}{g(x)}$$
 is negligible.

(g) Is $2^{-1024} = \frac{1}{2^{1024}}$ negligible?

For the polynomial x^{1025} there is no N, that for all x>N holds: $\frac{1}{2^{1024}}<\frac{1}{x^{1025}}$, because 2^{1024} is always smaller than x^{1025} for all x>1. $\Rightarrow 2^{-1024}$ is not negligible.

(h) Is
$$(f(x))^{\frac{1}{q(x)}}$$
 negligible?

$$f(x) = e^{-x}$$
 is negligible (see (a))

$$q(x)=x$$
 is a positive polynomial for all $x>0$

$$\Rightarrow (e^{-x})^{\frac{1}{x}} = e^{-1} = \frac{1}{e}$$

For the polynomial $\overset{e}{x^2}$ there is no N, that for all x>N holds:

 $\frac{1}{e}<\frac{1}{x^2},$ because e is always smaller than x^2 for all $x\geq 2.$

$$\Rightarrow e^{-1}$$
 is not negligible. $\Rightarrow (f(x))^{\frac{1}{q(x)}}$ is not negligible.

(i) Is $x^{-\log\log\log x}$ negligible?

For any polynomial x^c , choose $N=e^{e^{e^c}}$, then for all x>N holds: $x^{-\log\log\log x} < \frac{1}{x^c}$, because $x^{\log\log\log x} > x^c$ and $\log\log\log x > c$ for all $x > N = e^{e^{e^c}}$. $\Rightarrow x^{-\log\log\log x}$ is negligible.

Introduction to Modern Cryptography Theresa, Celine, Prisca, Saibaba

November 1, 2022





SOLUTION OF EXERCISESHEET 2

Exercise 2-4

Exercise 2-5