

**Quiz 1 — 2023-01-24***Prof. Pediredla**Student: Amittai Siavava***Credit Statement**

I worked on these problems alone, with reference to class notes and the following books:

- (i) **Computer Vision: Algorithms and Applications** by **Richard Szeliski**

**Problems****Problem 1.**

The continuous convolution of two functions  $f(x)$  and  $g(x)$  is given as

$$(f * g)(x) = \int_{-\infty}^{+\infty} f(y) g(x - y) \, dy.$$

the Gaussian function at scale is defined as

$$G_s(x) = \frac{1}{\sqrt{2\pi s}} e^{-\frac{x^2}{2s}},$$

and has the property that

$$\int_{-\infty}^{+\infty} G_s(x) \, dx = 1.$$

Prove that this class of function satisfies the *semigroup property* — the convolution of one Gaussian function with another produces a third Gaussian function with scale equal to their sum, i.e.

$$(G_{s_1} * G_{s_2})(x) = G_{s_1+s_2}(x).$$

Let

$$G_\alpha(x) = \frac{1}{\sqrt{2\pi\alpha}} e^{(-\frac{x^2}{2\alpha})}, \quad G_\beta(x) = \frac{1}{\sqrt{2\pi\beta}} e^{(-\frac{x^2}{2\beta})}$$

be Gaussian functions of scale  $\alpha$  and  $\beta$  respectively.

Through direct construction, we see that:

$$\begin{aligned} (G_\alpha * G_\beta)(x) &= \int_{-\infty}^{+\infty} G_\alpha(y) G_\beta(x-y) dy \\ &= \left( \frac{1}{\sqrt{2\pi\alpha}} \cdot \frac{1}{\sqrt{2\pi\beta}} \right) \int_{-\infty}^{+\infty} e^{(-\frac{y^2}{2\alpha})} \cdot e^{(-\frac{(x-y)^2}{2\beta})} dy \\ &= \frac{1}{2\pi\sqrt{\alpha\beta}} \int_{-\infty}^{+\infty} e^{-\frac{y^2}{2\alpha} - \frac{(x-y)^2}{2\beta}} dy \end{aligned}$$

By integrating, we get:

$$= \frac{1}{\sqrt{2^3\pi(\alpha+\beta)}} \left[ e^{-\frac{x^2}{2(\alpha+\beta)}} \operatorname{erf} \frac{\frac{(\alpha+\beta)y-x}{\alpha\beta}}{\beta\sqrt{\frac{2(\alpha+\beta)}{\alpha\beta}}} \right]_{-\infty}^{\infty}$$

$\operatorname{erf} x$  is an *even* function, and  $\operatorname{erf} x = 1$  at  $x = \infty$ .

$$\begin{aligned} &= \frac{1}{\sqrt{2^3\pi(\alpha+\beta)}} \cdot 2e^{-\frac{x^2}{2(\alpha+\beta)}} \\ &= \frac{1}{\sqrt{2\pi(\alpha+\beta)}} \cdot e^{-\frac{x^2}{2(\alpha+\beta)}} \\ &= G_{\alpha+\beta}(x). \end{aligned}$$

**Problem 2.**

In class, we talked about finite-difference approximation to the derivative of the univariate function  $f(x)$ . Using Taylor polynomial approximations of  $f(x+h)$  and  $f(x-h)$ , we can easily show that

$$f'(x) = \frac{f(x+h) - f(x-h)}{2h} + O(h^2),$$

so that the derivative can be approximated by convolving a discrete version of  $f(x)$  — a vector of values  $(\dots, f(x_o - \Delta), f(x_o), f(x_o + \Delta), \dots)$  with kernel  $(1/2, 0, -1/2)$ . This is termed a central difference because its interval is symmetric about a sample point.

- (i) Derive a higher order central-difference approximation to  $f'(x)$  such that the truncation error tends to zero as  $h^4$  instead of  $h^2$ . *Hint: consider Taylor polynomial approximations of  $f(x \pm 2h)$  in addition to  $f(x \pm h)$ .* (7 points)

Let  $c_i$  denote the coefficient for each term containing  $h^i$  in the full Taylor polynomial expansion, then we may write the current estimation of  $f'(x)$  as

$$f'(x) = \frac{f(x+h) - f(x-h)}{2h} - [c_2h^2 + c_4h^4 + c_6h^6 + \dots]. \quad (0.1)$$

Our goal is to eliminate the  $h^2$  term. Consider the approximations using  $f(x \pm 2h)$  by plugging  $2h$  into the formula:

$$f'(x) = \frac{f(x+2h) - f(x-2h)}{4h} - [4c_2h^2 + 16c_4h^4 + 64c_6h^6 + \dots] \quad (0.2)$$

We notice that the  $h^2$  term in 0.2 is 4 times larger than the  $h^2$  term in 0.1. We can eliminate the  $h^2$  term in  $f'(x)$  by subtracting 0.2 from 4 times 0.1:

$$\begin{aligned} 3f'(x) &= 4 \frac{f(x+h) - f(x-h)}{2h} - \frac{f(x+2h) - f(x-2h)}{4h} - [0h^2 + O(h^4)] \\ 3f'(x) &= \frac{8(f(x+h) - f(x-h)) - (f(x+2h) - f(x-2h))}{4h} + O(h^4) \\ 3f'(x) &= \frac{-f(x+2h) + 8f(x+h) - 8f(x-h) + f(x-2h)}{4h} + O(h^4) \\ f'(x) &= \frac{-f(x+2h) + 8f(x+h) - 8f(x-h) + f(x-2h)}{12h} + O(h^4) \end{aligned} \quad (0.3)$$

We get equation 0.3 as a Taylor approximation of  $f'(x)$  with a truncation error of  $O(h^4)$ .

(ii) What is the corresponding convolution (not correlation!) kernel? (3 points)

The approximation has a correlation kernel of

$$\left(-\frac{1}{12}, \quad \frac{8}{12}, \quad -\frac{8}{12}, \quad \frac{1}{12}\right).$$

The convolution kernel is the same as the correlation kernel, but flipped.

$$\left(\frac{1}{12}, \quad -\frac{8}{12}, \quad \frac{8}{12}, \quad -\frac{1}{12}\right).$$

**Problem 3.**

In the Rijndael field  $F = \mathbb{F}_2[X]/(X^8 + X^4 + X^3 + X + 1)$ , where bytes are associated to polynomials modulo  $X^8 + X^4 + X^3 + X + 1$ , compute the product  $01010010 \cdot 10010010 \in F$ .

We can represent polynomials in  $F$  as binary numbers, where the state of each bit (whether 0 or 1) represents whether the corresponding power in the polynomial has a factor of 0 or 1.

Then:

$$X^8 + X^4 + X^3 + X + 1 = 100011011$$

Then, we can perform the multiplication modulo 2:

$$\begin{array}{r} 10010010 \\ 1010010 \\ \times 0010010 \\ \hline 10010010 \dots \\ 10010010 \dots \\ \hline 10110210200100 \end{array}$$

Shifting back to base 2, we get: 10110010000100

We then need to find this number mod 100011011

$$\begin{array}{r|l} \text{mod } 10110010000100, 100011011 & \\ 100011011 & 10110010000100 \\ 100000 & 100011011 \dots \\ & 111111100 \dots \\ 1000 & 100011011 \dots \\ & 111001111 \dots \\ 100 & 100011011 \dots \\ & 110101000 \dots \\ 10 & 100011011 \dots \\ & 101100110 \\ 1 & 100011011 \\ \hline 101111 & 1111101 \end{array}$$

Thus, the product in  $F$  is 1111101