Polynomial encryption

Yeray Cachón Santana

May 20, 2018

This paper proposes a new method to encrypt and decrypt a message by special functions formed by Hermite, Laguerre, Tchebychev and Bessel The idea to encrypt a message will be by using base changes from the Taylor base to the bases of those special functions. The Hermite, Lagurrre, Tchebychev and Bessel polynomials are orthogonal, so they form a base set on a Hilbert space. The encryption will be using several sequences of those base changes according to a number sequence.

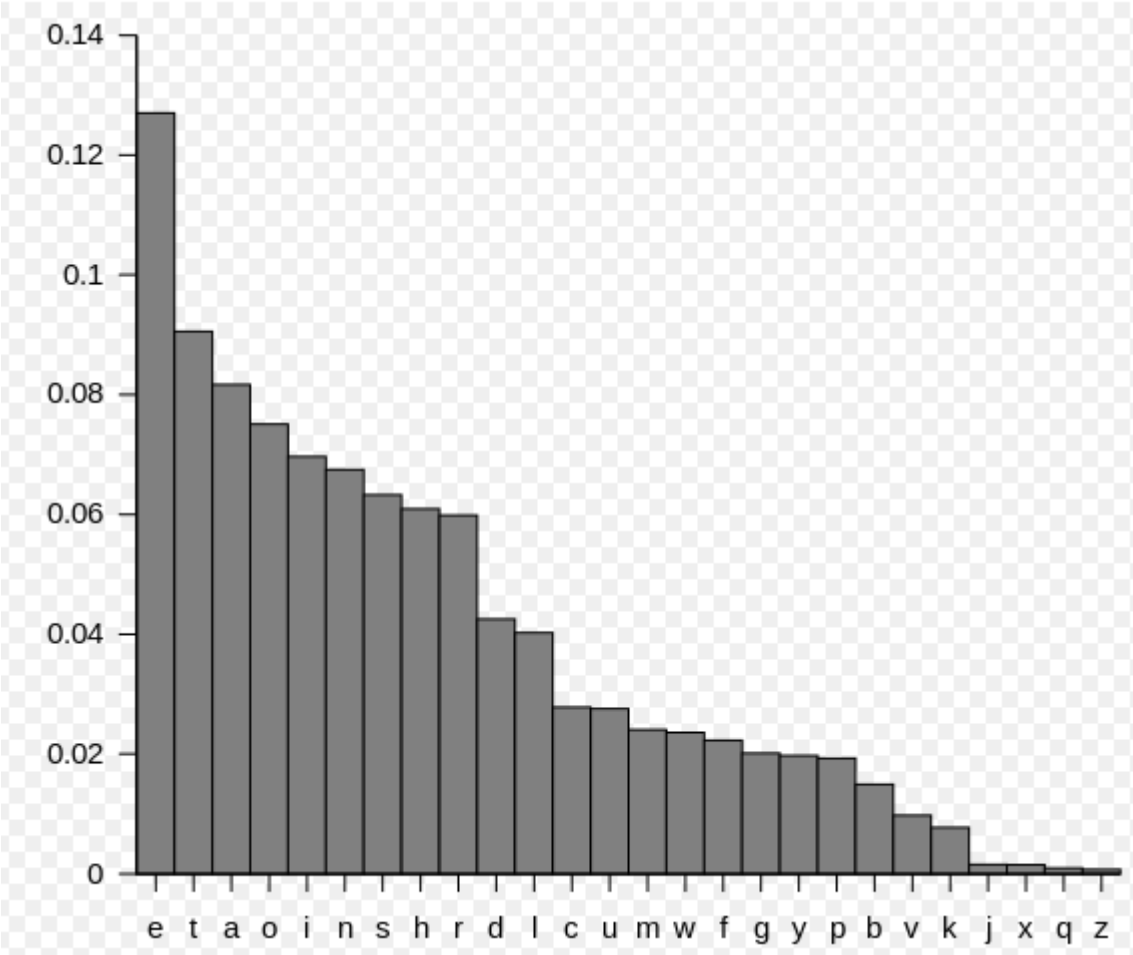
According to Hilbert space, as those are orthogonal polynomials, those functions form a orthogonal base. So, a change base can be done between a Taylor base and those bases - this is the method that will be used in order to encrypt a message.

Contents

1 Introduction

As far as I know, this work proposes a new method to encrypt a decrypt a message using several orthogonal polynomials. This could be interesting in order to extend the ways to encryption of files or any documents shared. As this are not known method, an attack would have more difficulties in order to decrypt the message. Also, the fact of combining the several method will make more difficult to attack because there are several patterns used in the encrypted message.

A way to attack an encrypted message is by the frequencies of the letters used on the alphabet (in this example, the relative frequencies of letters in the English language).



As it will be shown, the fact of sending a chain like "EEE", there will be differences on each sequence, so an attack by frequencies is much more difficult. Also, the Hermite method fails when all the letters of the block are the same but, in this case, other methods can be used (like Laguerre). Maybe, when there are sequences with the same code letter (like "AAAA"), the Bessel method encryption will give best results,as it's returning different numbers for the encryption of the same code letter.

But, as several methods are used when encrypting the message, an attack by frequencies cannot be easily applied on the whole message (I don't think that it could be possible), because the same letter will be decrypted by several numbers during the message. Also, the longer the message is, the more different numbers will be applied on the encrypted message. I think that other advantage of this method is that it can be parallelized. In this case, with a multi-processor system, each processor can encrypt a block independently the other blocks and, then, put the message together. Similarly, the decryption can be parallelized.

A disadvantage of this method is that it's slower than using AES, because there are system equations to be solved. But, as several methods are applied, it seems that it might be more secure. This can be used to encrypt text on a hard drive, and decrypt by a pass code as shown on the section 7.

This paper shows the method to encrypt and decrypt a message by the orthogonal functions Hermite, Laguerre, Tchebyscheff and Bessel. I think that it can be extended to other orthogonal functions. According to a Hilbert space, those functions formed a base set, so it can be used a change base from a Taylor base to those bases. Having said that, other orthogonal functions can be used in order to encrypt a message. In this paper, those orthogonal functions are used as example because their importance on physical-mathematical problems.

2 Hermite

In this section, let's define how to encrypt and decrypt using Hermite polynomial functions. Prior to this, let's see how the Hermite polynomials are defined:

$H_{n+1}(x) = 2xH_n(x) - 2nH_{n-1}(x)$

$H'_n(x) = 2nH_{n-1}$

The Hermite functions are the eigenvalues of the Fourier transform (see reference Eigenfunctions of the Fourier transform). As the Fourier transform is a linear, self-adjoint and compact operator, its eigenvalues formed a base (see spectral theorem). The orthogonality is given by:

$\int_{-\infty}^{+\infty} H_n(x)H_m(x)e^{-x^2}dx = 0$,m≠n

So, let's see how to the n-power of x can be set according to the Hermite polynomials:

$H_0 = 1$

$H_1 = 2xH_0 = 2x$, so $x = \frac{H_1}{2}$

$H_2 = 2xH_1 - 2*1*H_0 = 4x^2 - 2H_0$, so $x^2 = \frac{H_2+2H_0}{4}$

$H_3 = 2xH_2 - 2*2*H_1 = 2x(4x^2-2) - 4*2x = 8x^3 - 12x$, so $x^3 = \frac{H_3+6H_1}{8}$

$H_4 = 2xH_3 - 2*3*H_2 = 2x\left(8x^3-12x\right) - 6\left(4x^2-2\right) = 16x^4 - 48x^2 + 12 = 16x^4 - 12\left(H_2+2H_0\right) + 12H_0 = 16x^4 - 12H_2 - 12H_0$, so $x^4 = \frac{H_4+12H_2+12H_0}{16}$

$H_5 = 2xH_4 - 2*4*H_3 = 32x^5 - 96x^3 + 24x - 8*\left(8x^3-12x\right) = 32x^5 - 160x^3 + 120x = 32x^5 - 160\left(\frac{H_3+6H_1}{8}\right) - 120\left(\frac{H_1}{2}\right) = 32x^5 - 20H_3 - 60H_1$, so $x^5 = \frac{H_5+20H_3+60H_2}{32}$

$H_6 = 2xH_5 - 10H_4 = 64x^6 - 320x^4 + 240x^2 - 10H_4 = 64x^6 - 30H_4 - 60H_2 - 120H_0$, so $x^6 = \frac{H_6+30H_4+60H_2+120H_0}{64}$

It seems that it cannot be a general formula to set x^n in function of H_n. But, even this general formula, the n-power of x can be in function of H_n. With this idea, let's see how a polynomial may be encrypted. As the even-power of x is set according to even-nth term of Hermite polynomial (and the same for the odd), let's use a polynomial on even-power of x:

$P(x) = A + Bx^2 + Cx^4$

In this way, let's use linear equations of Hermite polynomials:

$H'_0 = A$

$H'_2 = 4Bx^2 - 2A$

$H'_4 = 16Cx^4 - 12H'_2 - 12H'_0 = 16Cx^4 - 12\left(4Bx^2-2A\right) - 12A = 16Cx^4 - 48Bx^2 + 12A$

So, let's calculate the coefficients of each term:

$Mx^0 = \frac{H_0}{2^0} = A$, M=A

$Mx^2 = \frac{H_2+2H_0}{4} = \frac{4Bx^2-2A+2A}{4} = Bx^2$,M=B

$Mx^4 = \frac{H'_4+12H'_2+4*3*2H_0}{16} = \frac{16Cx^4-48Bx^2+12A+48Bx^2-24A+12A}{16} = Cx^4$,M=C

In order to see this, the idea is putting the coefficients H'_nas linear combinations of H_n:

$H'_0 = AH_0$

$H'_2 = 4Bx^2 - 2AH_0 = 4B\left(\frac{H_2+2H_0}{4}\right) - 2AH_0 = BH_2 + (2B-2A)H_0$

$H'_4 = 16Cx^4 - 48Bx^2 + 12AH_0 = 16C\left(\frac{H_4+12H_2+12H_0}{16}\right) - 48B\left(\frac{H_2+2H_0}{4}\right) + 12AH_0 = CH_4 + 12(C-B)H_2 + 12(C-2B+A)H_0$

So, in those bases, let's see how it's the base change:

$B\left\{1, x^2, x^4....\right\} \longrightarrow B'\left\{H_0, H_2, H_4.....\right\}$

The change of base in Hermite base, it's according to the equations above:

$$\begin{cases} H'_0 = AH_0 \\ H'_2 = BH_2 + 2(B-A)H_0 \\ H'_4 = CH_4 + 12(C-B)H_2 + 12(C-2B+A)H_0 \end{cases}$$

$$\begin{pmatrix} H'_0 \\ H'_2 \\ H'_4 \end{pmatrix} = \begin{pmatrix} A & 0 & 0 \\ 2(B-A) & B & 0 \\ 12(C-2B+A) & 12(C-B) & C \end{pmatrix} \begin{pmatrix} H_0 \\ H_2 \\ H_4 \end{pmatrix}$$

The polynomial coefficients $P(x) = A + Bx^2 + Cx^4$has been transformed on a linear combinations of Hermite polynomials H_n.

2.1 Encryption and decryption

Let's see how to decrypt a message given by the Hermite polynomials. Firstly, the chain $\{H_0', H_2', H_4'....\}$ is received. Now, the decrypting system needs to find the coefficient A,B,C in order to decrypt the message. As the system is using a base of Hermite, the change base is:

$$\begin{cases} H_0' = AH_0 \\ H_2' = BH_2 + 2(B-A)H_0 \\ H_4' = CH_4 + 12(C-B)H_2 + 12(C-2B+A)H_0 \end{cases}$$

So,

$A = \frac{H_0'}{H_0}$

$B = \frac{H_2' + 2AH_0}{H_2 + 2H_0}$

$C = \frac{H_4' + 12BH_2 + 24BH_0 - 12AH_0}{H_4 + 12H_2 + 12H_0}$

Example. Let's encrypt and decrypt the chain "ABC". Associating, a number to each letter(A–>1,B–>2 and so on), the polynomial will be like this:

$P(x) = 1 + 2x^2 + 3x^4$

Then, the encryption message on Hermite base, will be:

$$\begin{pmatrix} H_0' \\ H_2' \\ H_4' \end{pmatrix} = \begin{pmatrix} A & 0 & 0 \\ 2(B-A) & B & 0 \\ 12(C-2B+A) & 12(C-B) & C \end{pmatrix} \begin{pmatrix} H_0 \\ H_2 \\ H_4 \end{pmatrix}$$

$$\begin{pmatrix} H_0' \\ H_2' \\ H_4' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 2 & 0 \\ 0 & 12 & 3 \end{pmatrix} \begin{pmatrix} H_0 \\ H_2 \\ H_4 \end{pmatrix}$$

Let's see if, with the numbers $\{2, 0, 12\}$ as the encrypted message of "ABC", is enough to decrypt the system.

Now, having those numbers, as the system knows that it's encrypted via Hermite polynomials, the system needs to solve the equations:

$$\begin{cases} 2(B-A) = 2 \\ 12(C-2B+A) = 0 \\ 12(C-B) = 12 \end{cases}$$

$$\begin{cases} B - A = 1 \\ C - 2B + A = 0 \\ C - B = 1 \end{cases}$$

$$\begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & -2 & 1 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$$

But, as $\begin{vmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & .2 & 1 \end{vmatrix} = 0$, the equation cannot be solved. So, let's adding the trace of the matrix on the encrypted message: $\{2, 0, 12, 6\}$. Now:

$$\begin{cases} B - A = 1 \\ C - 2B + A = 0 \\ C - B = 1 \\ A + B + C = 6 \end{cases}$$

$\begin{pmatrix} 1 & -2 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 6 \end{pmatrix}$, whence

$$'A = \frac{\begin{vmatrix} 0 & -2 & 1 \\ 2 & 0 & 1 \\ 6 & 1 & 1 \end{vmatrix}}{\begin{vmatrix} 1 & -2 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix}} = \frac{-6}{-6} = 1$$

$$B = \frac{\begin{vmatrix} 1 & 0 & 1 \\ -1 & 2 & 1 \\ 1 & 6 & 1 \end{vmatrix}}{\begin{vmatrix} 1 & -2 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix}} = \frac{-12}{-6} = 2$$

$$C = \frac{\begin{vmatrix} 1 & -2 & 0 \\ -1 & 0 & 2 \\ 1 & 1 & 6 \end{vmatrix}}{\begin{vmatrix} 1 & -2 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix}} = \frac{-18}{-6} = 3$$

Let's see, what happens if a message with the same letter is sent. For example, a message like "AAA". As shown previously, the trace of the matrix will be sent:

$$\begin{cases} B - A = 0 \\ C - 2B + A = 0 \\ C - B = 0 \\ A + B + C = 3 \end{cases}$$

$$\begin{pmatrix} 1 & -2 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 3 \end{pmatrix}, \text{ whence}$$

$$A = \frac{\begin{vmatrix} 0 & -2 & 1 \\ 0 & 0 & 1 \\ 3 & 1 & 1 \end{vmatrix}}{\begin{vmatrix} 1 & -2 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix}} = \frac{-6}{-6} = 1$$

$$B = \frac{\begin{vmatrix} 1 & 0 & 1 \\ -1 & 0 & 1 \\ 1 & 3 & 1 \end{vmatrix}}{\begin{vmatrix} 1 & -2 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix}} = \frac{-6}{-6} = 1$$

$$C = \frac{\begin{vmatrix} 1 & -2 & 0 \\ -1 & 0 & 0 \\ 1 & 1 & 3 \end{vmatrix}}{\begin{vmatrix} 1 & -2 & 1 \\ -1 & 0 & 1 \\ 1 & 1 & 1 \end{vmatrix}} = \frac{-6}{-6} = 1$$

3 Laguerre

The Laguere functions are the solutions for the differential equation:

xy"(x) + (1-x)y'(x) + ny(x) = 0

Where,

$L_n(x) = \frac{e^x}{2\pi i}\oint \frac{s^n e^{-s}}{(s-x)^{n+1}} ds$

Following the same method as for the Hermite polynomials, let's see how the Laguerre polynomials are defined:

$(n+1)\,L_{n+1}(x) = (2n+1-x)\,L_n(x) - nL_{n-1}(x)$

The first Laguerre polynomials are defined like this:

$L_0(x) = 1$

$L_1(x) = -x+1$

$2!L_2(x) = x^2 - 4x + 2$

$3!L_3(x) = -x^3 + 9x^2 - 18x + 6$

$4!L_4(x) = x^4 - 16x^3 + 72x^2 - 96x + 24$

Now, let's set how to set the n-th power on terms of Laguerre polynomials:

$L_1(x) = -x+1 = -x + L_o$, so $x = L_0 - L_1$

$L_2(x) = \frac{1}{2!}\left(x^2 - 4x + 2\right) = \frac{1}{2}x^2 - 2(L_0 - L_1) + L_0 = \frac{1}{2}x^2 + 2L_1 - L_0$, so $x^2 = 2(L_2 - 2L_1 + L_0)$

$L_3(x) = \frac{1}{3!}\left(-x^3 + 9x^2 - 18x + 6\right) = -\frac{x^3}{3!} + \frac{9}{3!}x^2 - 3x + 1 = -\frac{x^3}{3!} + 3\,(L_2 - 2L_1 + L_0) - 3\,(L_0 - L_1) + L_0 = -\frac{x^3}{3!} + 3\,(L_2 - L_1) + L_0$,whence $x^3 = 3!\,(L_0 - L_3 + 3\,(L_2 - L_1))$

$L_4(x) = \frac{1}{4!}\left(x^4 - 16x^3 + 72x^2 - 96x + 24\right) = \frac{x^4}{4!} + \frac{1}{4!}\left\{-16x^3 + 72x^2 - 96x + 24\right\}$

$L_4(x) = \frac{x^4}{4!} + \frac{1}{4!}\left\{-16\,(3!\,(L_0 - L_3 + 3\,(L_2 - L_1))) + 72 * 2\,(L_2 - 2L_1 + L_0) - 96\,(L_0 - L_1) + 24L_0\right\}$

$L_4(x) = \frac{x^4}{4!} + \frac{1}{4!}\,(96L_3 - 144L_2 + 96L_1 - 24L_0)$,whence $x^4 = 4!L_4 - 96L_3 + 144L_2 - 96L_1 + 24L_0$

In this case, it seems that it cannot be found a general formula to find x^n in terms of L_n. But, even without this general formula, we can follow the same procedure as shown on the section 1.

Let's use a general polynomial of 4th power

$L(x) = A + Bx + Cx^2 + Dx^3 + Ex^4$

In this way, let's use linear equations of Laguerre polynomials:

$L_0' = A$

$L_1' = Bx - A$

$2!L_2' = Cx^2 - 4Bx + 2A$

Let's calculate the coefficient of each term:

$Mx^0 = L_o' = A * L_0$

$L_1' = Bx - A = B * (L_0 - L_1) + A * L_0 = (A+B)\,L_0 - BL_1$

$2!L_2' = Cx^2 - 4Bx + 2A = 2C\,(L_2 - 2L_1 + L_0) - 4B\,(L_0 - L_1) + 2AL_0 = (2C - 4B + 2A)\,L_0 + (4B - 2C)\,L_1 + 2CL_2$

$$\begin{pmatrix} L_0' \\ L_1' \\ L_2' \end{pmatrix} = \begin{pmatrix} A & 0 & 0 \\ A+B & B & 0 \\ C-2B+A & B-C & C \end{pmatrix} \begin{pmatrix} L_0 \\ L_1 \\ L_2 \end{pmatrix}$$

Following the same method, let's encrypt the message "ABC" so A=1, B=2 and C=3

$$\begin{pmatrix} L_0' \\ L_1' \\ L_2' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 3 & 2 & 0 \\ 0 & -1 & 3 \end{pmatrix} \begin{pmatrix} L_0 \\ L_1 \\ L_2 \end{pmatrix}$$

Sending the numbers $\{3, 0, -1\}$as the encrypted message of "ABC".

$$\begin{cases} A + B = 3 \\ C - 2B + A = 0 \\ B - C = -1 \end{cases}$$

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & -2 & 1 \\ 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \end{pmatrix} = \begin{pmatrix} 3 \\ 0 \\ -1 \end{pmatrix},$$

Solving this system of linear equations, as shown previously,

$$\begin{cases} A = 1 \\ B = 2 \\ C = 3 \end{cases}$$

For example, in order to encrypt the message "AAA", the sequence {2,0,0} will be sent. In general, being x the position of the letter in the alphabet, if the sequence has the same letters, the encrypted sequence will be like {2x,0,0}.

4 Combining Hermite and Laguerre

In this section, let's see how those methods can be combined. In order to see this, let's put the equations like this:

$$\begin{cases} \begin{pmatrix} H'_0 \\ H'_2 \\ H'_4 \end{pmatrix} = \begin{pmatrix} H_A & 0 & 0 \\ 2(H_B - H_A) & H_B & 0 \\ 12(H_C - 2H_B + H_A) & 12(H_C - H_B) & H_C \end{pmatrix} \begin{pmatrix} H_0 \\ H_2 \\ H_4 \end{pmatrix} \\ \begin{pmatrix} L'_0 \\ L'_1 \\ L'_2 \end{pmatrix} = \begin{pmatrix} L_A & 0 & 0 \\ L_A + L_B & L_B & 0 \\ L_C - 2L_B + L_A & L_B - L_C & L_C \end{pmatrix} \begin{pmatrix} L_0 \\ L_1 \\ L_2 \end{pmatrix} \end{cases}$$

So, combining both of operators:

$$M_{HxL} = M_H x M_L = \begin{pmatrix} H_A & 0 & 0 \\ 2(H_B - H_A) & H_B & 0 \\ 12(H_C - 2H_B + H_A) & 12(H_C - H_B) & H_C \end{pmatrix} \begin{pmatrix} L_A & 0 & 0 \\ L_A + L_B & L_B & 0 \\ L_C - 2L_B + L_A & L_B - L_C & L_C \end{pmatrix}$$

$$M_{HxL} = \begin{pmatrix} H_A L_A & 0 & 0 \\ 2(H_B - H_A) L_A + H_B (L_A + L_B) & H_B L_B & 0 \\ 12(H_C - 2H_B + H_A) L_A + 12(H_C - H_B)(L_A + L_B) + H_C (L_C - 2L_B + L_A) & 12L_B (H_C - H_B) + H_C (L_B - L_C) & H_C L_C \end{pmatrix}$$

In order to encrypt the message "ABC", following the same method as previously, let's call:

$H_A = L_A = 1$

$H_B = L_{:B} = 2$

$H_C = L_C = 3$

So,

$$M_{HxL} = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 2 & 0 \\ 0 & 12 & 3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 3 & 2 & 0 \\ 0 & -1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 8 & 4 & 0 \\ 36 & 21 & 9 \end{pmatrix}$$

In this case, as $H_A = L_A$,$H_B = L_B$ and $H_C = L_C$, the numbers $\{8, 36, 21\}$can be sent.

In order to decrypt the message, knowing that the message is a combination of Hermite and Laguerre matrix, and $H_A = L_A = M_A$,$H_B = L_B = M_B$ and $H_C = L_C = M_C$,

$$M_{HxL} = \begin{pmatrix} M_A^2 & 0 & 0 \\ M_B^2 + 3M_A M_B - 2M_A^2 & M_B^2 & 0 \\ 12\left(M_A^2 - M_B^2\right) + M_C^2 + 25M_B M_C - 36M_A M_B + 25M_A M_C + 10M_B M_C & -M_C^2 - 12M_B^2 + 13M_B M_C & M_C^2 \end{pmatrix}$$

As the numbers $\{8, 36, 21\}$ are sent, in order to decrypt the message:

$$\begin{cases} M_B^2 + 3M_A M_B - 2M_A^2 = 8 \\ 12\left(M_A^2 - M_B^2\right) + M_C^2 - 36M_A M_B + 25M_A M_C + 10M_B M_C = 36 \\ -M_C^2 - 12M_B^2 + 13M_B M_C = 21 \end{cases}$$

Solving those equations,

$$\begin{cases} M_A = 1 \\ M_B = 2 \\ M_C = 3 \end{cases}$$

5 Tschebyscheff

The Tchebyscheff polynomials are given by this generating equation:

$\frac{1-t^2}{1-2xt-t^2} = T_0(x) + 2\sum_{n=1}^{\infty} T_n(x)t^n$

The first Tchebyscheff polynomials are defined by:

$T_0 = 1$

$T_1 = x$, whence $x = T_1$

$T_2 = 2x^2 - 1$, $x^2 = \frac{T_2+T_0}{2}$

$T_3 = 4x^3 - 3x$, $x^3 = \frac{T_3+3T_1}{4}$

$T_4 = 8x^4 - 8x^2 + 1$, $x^4 = \frac{T_4+8x^2-1}{8} = \frac{T_4+4T_2+3T_0}{8}$

$T_5 = 16x^5 - 20x^3 + 5x$, $x^5 = \frac{T_5+20x^3-5x}{16} = \frac{T_5+5(T_3+3T_1)-5T_1}{16} = \frac{T_5+5T_3+10T_1}{16}$

$T_6 = 32x^6 - 48x^4 + 18x^2 - 1$, $x^6 = \frac{T_6+6T_4+15T_2+10T_0}{32}$

Let's use a general polynomial of Tschebysheff:

$T(x)' = A + Bx + Cx^2 + Dx^3 + Ex^4$

$T_0' = A = AT_0$

$T_1' = Bx = BT_1$

$T_2' = 2Cx^2 - A = C(T_2 + T_0) - AT_0 = CT_2 + (C - A)T_0$

$T_3' = 4Dx^3 - 3Bx = D(T_3 + 3T_1) - 3BT_1 = DT_3 + 3(D - B)T_1$

$T_4' = 8Ex^4 - 8Cx^2 + A = E(T_4 + 4T_2 + 3T_0) - 4C(T_2 + T_0) + AT_0 = ET_4 + 4(E - C)T_2 + (3E - 4C + A)T_0$

$$\begin{pmatrix} T_0' \\ T_1' \\ T_2' \\ T_3' \\ T_4' \end{pmatrix} = \begin{pmatrix} A & 0 & 0 & 0 & 0 \\ 0 & B & 0 & 0 & 0 \\ C-A & 0 & C & 0 & 0 \\ 0 & 3(D-B) & 0 & D & 0 \\ 3E-4C+A & 0 & 4(E-C) & 0 & E \end{pmatrix} \begin{pmatrix} T_0 \\ T_1 \\ T_2 \\ T_3 \\ T_4 \end{pmatrix}$$

As shown on the matrix, there are 5 unknown quantities, but the system needs to send 5 numbers in order to decrypt the message. So, let's send this chain of number, adding the trace of the matrix:

{A+B+C+D+E,C-A,3(D-B),3E-4C+A,4(E-C)}

Following this, let's encrypt the message "ABCDE", so

$$\begin{pmatrix} T_0' \\ T_1' \\ T_2' \\ T_3' \\ T_4' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 \\ 2 & 0 & 3 & 0 & 0 \\ 0 & 6 & 0 & 4 & 0 \\ 4 & 0 & 8 & 0 & 5 \end{pmatrix} \begin{pmatrix} T_0 \\ T_1 \\ T_2 \\ T_3 \\ T_4 \end{pmatrix}$$

Sending the numbers {15,2,6,4,8} as the encrypted message of "ABCDE".

$$\begin{cases} A + B + C + D + E = 15 \\ C - A = 2 \\ 3(D - B) = 6 \\ 3E - 4C + A = 4 \\ 4(E - C) = 8 \end{cases}$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ -1 & 0 & 1 & 0 & 0 \\ 0 & -3 & 0 & 3 & 0 \\ 1 & 0 & -4 & 0 & 3 \\ 0 & 0 & -4 & 0 & 4 \end{pmatrix} \begin{pmatrix} A \\ B \\ C \\ D \\ E \end{pmatrix} = \begin{pmatrix} 15 \\ 2 \\ 6 \\ 4 \\ 8 \end{pmatrix}$$

Solving those equations:

$$\begin{cases} A = 1 \\ B = 2 \\ C = 3 \\ D = 4 \\ E = 5 \end{cases}$$

6 Bessel

In order to introduce the Bessel functions, let's introduce a function of two variables:

$g(x,t) = e^{(x/2)(t-1/t)}$

Expanding this function in a Laurent series:

$g(x,t) = e^{(x/2)(t-1/t)} = \sum_{n=-\infty}^{\infty} J_n(x)t^n$

The coefficient of t^n is then:

$J_n(x) = \sum_{s=0}^{\infty} \frac{(-1)^s}{s!(n+s)!}\left(\frac{x}{2}\right)^{n+2s}$

Taking the particular cases J_0 and J_1:

$J_0(x) = 1 - \frac{x^2}{2^2} + \frac{x^4}{2^2 4^2} - \frac{x^6}{2^2 4^2 6^2} + ...$

$J_1(x) = \frac{x}{2} - \frac{x^3}{2^2 4} + \frac{x^5}{2^2 4^2 6} + \frac{x^7}{2^2 4^2 6^2 8} + ...$

Let's write it in this way:

$J_n(x) = \sum_{s=0}^{\infty} \frac{(-1)^s}{s!(n+s)!}\left(\frac{x}{2}\right)^{n+2s}$

So, taking the first terms of the Bessel function for J_0:

$J_{0,0}(x) = 1$

$J_{0,2}(x) = -\frac{x^2}{2^2}$

$J_{0,4}(x) = \frac{x^4}{2^2 4^2}$

$J_{0,6}(x) = -\frac{x^6}{2^2 4^2 6^2}$

The n-th term of the series will be given by: $J_{0,2n} = (-1)^n \prod_{m=1}^{n} \frac{1}{(2m)^2}$. Following the same procedure as seen previously,

$x^2 = -2^2 J_{0,2}$

$x^4 = 2^2 4^2 J_{0,4}$

$x^6 = -2^2 4^2 6^2 J_{0,6}$

Using a general polynomial:

$J(x)' = A + Bx^2 + Cx^4 + Dx^6 = AJ_{0,0} - 2^2 BJ_{0,2} + 2^2 4^2 CJ_{0,4} - 2^2 4^2 6^2 DJ_{0,6} + ...$

For the several terms:

$J'_0 = AJ_{0,0}$

$J'_2 = -2^2 BJ_{0,2}$

$J'_4 = 2^2 4^2 CJ_{0,4}$

$J'_6 = -2^2 4^2 6^2 DJ_{0,6}$

In this case, as there are no crossed-terms, the matrix will be diagonal:

$$\begin{pmatrix} J'_0 \\ J'_2 \\ J'_4 \\ J'_6 \end{pmatrix} = \begin{pmatrix} A & & & \\ & -2^2 B & & \\ & & 2^2 4^2 C & \\ & & & -2^2 4^2 6^2 D \end{pmatrix} \begin{pmatrix} J_{0,0} \\ J_{0,2} \\ J_{0,4} \\ J_{0,6} \end{pmatrix}$$

Example. Let's encrypt and decrypt the chain "ABCD". Associating, a number to each letter(A–>1,B–>2 and so on), so the encryption will be:

$\{A, -2^2 B, 2^2 4^2 C, -2^2 4^2 6^2 D\}$

Taking A=1,B=2,C=3,D=4, the encrypted message will be {1,-8,192,-9216}. In this case, for decrypt the message, as the numbers are calculated via Bessel polynomials,

$A = \frac{J'_0}{J_0} = 1$

$B = -\frac{J'_2}{2^2 J_{0,2}} = -\frac{-8}{2^2} = 2$

$C = \frac{J_3}{2^2 4^2} = \frac{192}{2^2 4^2} = 3$

$D = \frac{J_4}{-2^2 4^2 6^2} = \frac{-9216}{-2^2 4^2 6^2} = 4$

In this case, it was used the expansion of the function J_0.But, this can be extended to others Bessel functions $(J_1, J_2...)$. This allows to extend the method to other orthogonal functions.

7 A way to combine those methods

Having seen Hermite, Laguerre, Tchebyscheff and Bessel as ways to encrypt and decrypt messages by base changing, let's see how those method can be combined. As it as shown 4 methods, a possible way could be by generating a pseudo-random number base 4, like.

$r_{(4} = 412433211....$

Then, the message will be separate into several blocks so, according to the digit, each block will be encrypted/decrypted. For example,

Hermite = 1

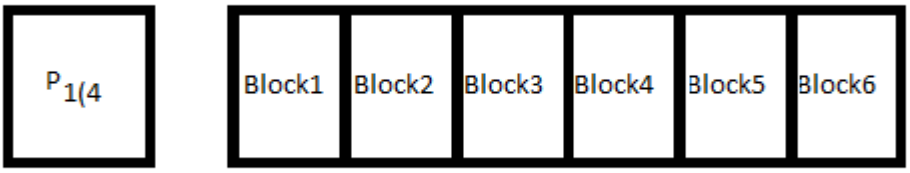
Laguerre = 2

Tchebyscheff = 3

Bessel = 4

As shown on the section "Combining Hermite and Laguerre", the matrices are combined in order to send a sequence that will be decrypted. In this section this will be reviewed and it will be extended to the other combinations.

Let's consider a pseudo-random number as a product of 2 prime random numbers. Seeing this in this schema:



The pseudo-random number will be as a product of numbers prime numbers:

$r_{(4} = p_{1(4} * p_{2(4}$

One of the prime number will be included on the first block. Then, in order to decrypt the message, the second prime number p_2 (private key) will be needed in order to find the random number $r_{(4}$. Once the pseudo-random number is calculated, following the sentence of the numbers, the system can decrypt the block message according to the previous methods (Hermite, Legendre, Tchebysheff and Bessel). So, to decrypt the message, knowing the $p_{1(4}$, the pseudo-random number will be calculated and, then, the message can be decrypted.

Each block can be, either a single block (Hermite, Laguerre, Tchebysheff or Bessel), or a combined block (as shown on "Combining Hermite and Laguerre"). So, let's consider those cases:

Hermite = 0

Laguerre = 1

Tschebyscheff= 2

Bessel = 3

Hermite-Laguerre = 4

Hermite-Bessel = 5

Hermite-Tschebyscheff = 6

Laguerre-Bessel = 7

Laguerre-Tschebyscheff = 8

Tschebyscheff-Bessel = 9

As the Bessel matrix is diagonal, the cases Bessel-Hermite, Bessel-Laguerre and Bessel-Tschebyscheff won't be considered because of the commutation of the matrix Bessel with the others. So, following the same procedure,

$r = p_1 * p_2$

Once the number r is calculated as a product of 2 numbers (one of them random), the blocks will be decrypted following the sequence of r.Let's see this with an example:

1) $p_1 = 199$(random key sent on the first block) and $p_2 = 137$(private key)

2) The sequence of encryption will be $r = p_1 * p_2 = 27263$

3) The blocks will be encrypted according the cyclic sequence 27263..... according to the cases considered previously.

In order to decrypt:

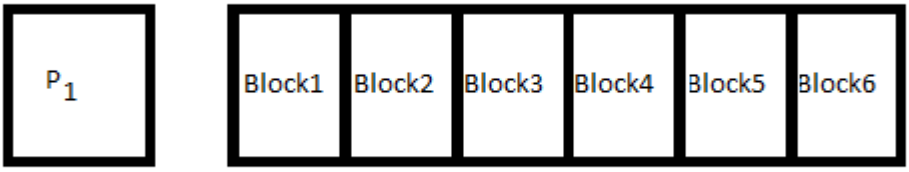
1) The random key is sent on the first block (p_1)

2) Private key: p_2

3) The random number is calculated $r = p_1 * p_2$

4) The blocks will be decrypted according to the sequence generated by r

So, the encrypted chain sent will be like this:



Knowing the random number p_1,the sequence of encryption will be calculated and, then, the message will be decrypted according the sequence, as shown previously.

8 Conclusions

This paper proposes a method to encrypt and decrypt a message using orthogonal polynomials. It has been shown as examples the Hermite, Laguerre, Bessel and Tschebyscheff, as well as combinations of those polynomials. It has also been shown that an attack by frequencies will be difficult as the same letter will be encrypted differently on each block. Those functions have been used because their importance on physical-mathematical problems, but it can be extended to whatever orthogonal functions.

Theorem. Suppose A is a compact self-adjoint operator on a (real or complex) Hilbert space V. Then there is an orthonormal basis of V consisting of eigenvectors of A. Each eigenvalue is real.

As the Hermite, Laguerre, Bessel and Tschebyscheff are compact self-adjoint operator, their eigenvectors formed an orthonormal basis, so they can be used in order to find a change base from a Taylor base $\{1, x, x^2..\}$to those bases (and vice-versa). This idea is used in order to encrypt and decrypt a message. Using several blocks of strings, each block can be encrypted by a specific method, following a cyclic sequence number which seed is calculated as a product of 2 primes. Feel free to send me any comments to ycachon@gmail.com about this paper.

9 References

https://en.wikipedia.org/wiki/Letter_frequency

Mathematical Methods for Physicists (Arfken and Weber)

http://mathworld.wolfram.com/BesselFunctionoftheFirstKind.html

Eigenfunctions of the Fourier transform : https://www2.bc.edu/mark-reeder/FourierEvecs.pdf