МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ» ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №1

З дисципліни «Криптографія» Експериментальна оцінка ентропії на символ джерела відкритого тексту

Виконали: Правдива Тамара ФБ-02 Бобер Наталія ФБ-05

Перевірила: Селюх П. В.

Мета роботи

Засвоєння понять ентропії на символ джерела та його надлишковості, вивчення та порівняння різних моделей джерела відкритого тексту для наближеного визначення ентропії, набуття практичних навичок щодо оцінки ентропії на символ джерела.

Хід роботи

Для виконання цієї лабораторної роботи в якості експериментального тексту було використано декілька глав «Стив Джобс -Уолтер Айзексон».

Перш за все, була створена програма, яка очищує текст від непотрібних символів (цифри, знаки пунктуації, тощо). Лише після цього була створена програма для обробки тексту та виконання завдання. Так як необхідно працювати як з пробілом, так і без нього, робота програми відбувається в два етапи, які відрізняються один від одного лише алфавітом.

Якщо говорити про труднощі, то найбільше їх виникло при роботі з біграмами, де потрібно було враховувати перетин (або його відсутність) букв, який впливав на підрахунок частот та ентропії, вивід результатів в таблиці, де так і не вдалося вивести числа з пробілами в текстовику, напевно, зручніше було б вивести в таблицю excel, але і з цим були певні проблеми.

Результати

1. Написати програми для підрахунку частот букв і частот біграм в тексті, а також підрахунку Н1 та Н2 за безпосереднім означенням. Підрахувати частоти букв та біграм, а також значення Н1 та Н2 на довільно обраному тексті російською мовою достатньої довжини (щонайменше 1Мб), де імовірності замінити відповідними частотами. Також одержати значення Н1 та Н2 на тому ж тексті, в якому вилучено всі пробіли.

Результати з пробілами:

H letter: 4.381850329932886

H cross bigrams: 4.000506233421664 H non-cross bigrams: 4.000363326572691

Результати без пробілів:

H letter: 4.45483115391814

H cross bigrams: 4.137830453960522 H non-cross bigrams: 4.137314968244347 Результати з пробілами "":0.157350 o:0.096570 e:0.066070 a:0.065950 и:0.060730 н:0.054390 т:0.051820 c:0.047590 л:0.043950 p:0.039790 в:0.036190 д:0.028340 к:0.028270 м:0.027250 п:0.024990 y:0.021090 б:0.017080 ь:0.015470 я:0.015460 ы:0.014840

3:0.013860

г:0.013570

ч:0.012050

ж:0.010260

й:0.008380

x:0.006470

ш:0.005380

ю:0.005110

ц:0.003620

э:0.003360 ф:0.002370

щ:0.002130

ъ:0.000260

ë:0.000000

Результати без пробілів o:0.114600 e:0.078400 a:0.078270 и:0.072070 н:0.064540 т:0.061490 c:0.056480 л:0.052150 p:0.047220 в:0.042940 д:0.033630 к:0.033550 м:0.032340 п:0.029650 y:0.025030 б:0.020270 ь:0.018360 я:0.018340 ы:0.017610 3:0.016450 г:0.016110 ч:0.014310 ж:0.012170 й:0.009940 x:0.007670 ш:0.006380 ю:0.006060 ц:0.004300 э:0.003990 ф:0.002820 щ:0.002530

ъ:0.000310

ë:0.000000

Результати з пробілами (cross)

 $a\ 0.00001\ 0.00137\ 0.00304\ 0.00059\ 0.00142\ 0.00103\ 0.00005\ 0.00012\ 0.00013\ 0.00005\ 0.000005\ 0.00005\ 0.00005\ 0.00005\ 0.00005\ 0.00005\ 0.00005\ 0.0000$ $\texttt{B} \ \ 0.00593 \ \ 0.00001 \ \ 0.00003 \ \ 0.00001 \ \ 0.00003 \ \ 0.00001 \ \ 0.00002 \ \ 0.00001 \ \ 0.00001 \ \ 0.00002 \ \ 0.00001 \ \ 0.00001 \ \ 0.00002 \ \ 0.00001 \ \ 0.00001 \ \ 0.00001 \ \ 0.00001 \ \ 0.00001 \ \ 0.00001 \ \ 0.000001 \ \ 0.000$ ϵ 0.00000 0.0000 0.0000 0.0000 0.0000 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 0.000 \times 0.00076 0.00004 0.00000 0 3 0.00440 0.00012 0.00097 0.00022 0.00083 0.00040 0.00000 0.00006 0.00010 0.00006 0.00010 0.00006 0.00010 0.00001 0.00001 0.00001 0.00000 0.00001 0.00000 0.00001 0.00000 0.00001 0.00001 0.00001 0.00001 0.00010 0 $\text{ \ensuremath{\pi}\ 0.00045\ 0.00033\ 0.00294\ 0.00064\ 0.00126\ 0.00244\ 0.00000\ 0.00016\ 0.00278\ 0.00127\ 0.00041\ 0.00270\ 0.0032\ 0.00027\ 0.00125\ 0.00032\ 0.00017\ 0.00127\ 0.00045\ 0.00122\ 0.00049\ 0.0015\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.000000\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.0000000\ 0.00000\ 0.00000\ 0.00000\ 0.000000\ 0.00000\ 0.00000\ 0.00$ $\ddot{\text{H}}$ 0.00000 0.00000 0.00002 0.00001 0.00017 0.00002 0.00000 0.0 $\kappa\ 0.00582\ 0.00000\ 0.00014\ 0.00000\ 0.00001\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.0000$ $\pi\ 0.00572\ 0.00001\ 0.00006\ 0.00008\ 0.00003\ 0.00406\ 0.00000\ 0.00001\ 0.00000\ 0.00001\ 0.00000\ 0.00001\ 0.00000\ 0.00001\ 0.00000\ 0.00001\ 0.00000\ 0.00001\ 0.00000\ 0.00000\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.000000\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.000000\ 0.0$ $o. 0.00015\ 0.00731\ 0.00732\ 0.00459\ 0.00524\ 0.00184\ 0.00000\ 0.00018\ 0.00731\ 0.00732\ 0.00459\ 0.00569\ 0.00023\ 0.00040\ 0.00003\ 0.000003\ 0.000003\ 0.000003\ 0.000003\ 0.000003\ 0.00003\ 0.00003\ 0$ $\pi\ 0.00172\ 0.00002\ 0.000000\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.000$ $\begin{array}{c} \textbf{p} \ \ 0.00870 \ \ 0.000870 \ \ 0.$ $\texttt{T} \ \ 0.00571 \ \ 0.00030 \ \ 0.00232 \ \ 0.00001 \ \ 0.00030 \ \ 0.00232 \ \ 0.00001 \ \ 0.0000$ $\sqrt{0.00009\,0.00038\,0.00054\,0.00085\,0.00165\,0.00019\,0.00000\,0.00009\,0.00009\,0.00009\,0.00000\,0.00000\,0.00001\,0.00002\,0.00000\,0.00001\,0.00012\,0.00000\,0.00001\,0.00012\,0.00000\,0.00000\,0.00000\,0.00001\,0.00015\,0.00004\,0.00094\,0.00091}$ $\overset{\leftarrow}{\Phi}$ 0.00011 0.00000 0.0000 0.0000 0.0000 0.0000 0.00000 0.00000 0.00000 0.00000 0.00000 0.00000 $\hat{\mathbf{x}}$ 0.00053 0.00000 0.00012 0.00001 0.00001 0.00000 0.0 $\pm 0.00033 \ 0.00000 \ 0.00009 \ 0.00000 \ 0.00009 \ 0.00000 \ 0$ $\frac{1}{4}, 0.00164, 0.00000, 0.00001, 0.00000, 0$ $\pm 0.00046\ 0.00000\ 0.00001\ 0.0000000\ 0.00000\ 0.000000\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.0$ $_{\rm III}$ 0.00042 0.00000 0. $\ \, \mathbf{b}, 0.00000, 0.00007, 0.00005, 0.00009, 0.00025, 0.00009, 0.00025, 0.00023, 0.00000, 0.00004, 0.00000, 0.00004, 0.00000, 0.00004, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.000000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.000000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.000000, 0.00001, 0.00000, 0.000000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.000000, 0.00001, 0.00000, 0.00001, 0.00000, 0.00001, 0.00000, 0.000000, 0.00000, 0.00000, 0.00000, 0.00000, 0.00000, 0.00000, 0.000000, 0.00000,$ f 60.000000.00032.0.00001.0.00001.0.00001.0.00001.0.00001.0.00001.0.00001.0. $^{\circ\circ\circ}0.00180\ 0.00542\ 0.01365\ 0.00304\ 0.0093\ 0.00309\ 0.00000\ 0.00116\ 0.00339\ 0.00953\ 0.00003\ 0.00951\ 0.00214\ 0.00525\ 0.01309\ 0.0191\ 0.01638\ 0.00516\ 0.01472\ 0.00530\ 0.00381\ 0.00084\ 0.00154\ 0.00043\ 0.00083\ 0.00003\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00245\ 0.00006\ 0.00135\ 0.00793$

Результати з пробілами (non-cross)

вг деё ж з и й к л м н о п р с т у ф $a \quad 0.000010.001380.003020.000630.001430.000990.000000.001160.003250.000230.000730.003450.010460.002700.00550.000040.000890.002540.003630.004980.000360.000220.000610.000490.000760.000530.000130.000000.000000.000000.000000.000000.000470.001290.014630.0004980.000360.0004980.0000490.0004980.0004980.0004980.0004980.00004980.0000400.000490.000490.000490.00040$ 0.005780.000010.000030.000010.0000180.003840.0000010.0000180.003840.000000.000010.0000180.003840.000000.000010.0000110. $0.004590\ 0.00050\ 0.00460\ 0.00020\ 0.00120\ 0.00120\ 0.004320\ 0.000000\ 0.003590\ 0.00090\ 0.002710\ 0.000000\ 0.001650\ 0.00040\ 0.00120\ 0.00160\ 0.00640\ 0.00110\ 0.01500\ 0.00040\ 0.00110\ 0.00010\ 0.0$ $0.000230\ 0.01070\ 0.01090\ 0.02600\ 0.02810\ 0.01140\ 0.000000\ 0.000550\ 0.01020\ 0.00090\ 0.01140\ 0.00090\ 0.01020\ 0.000590\ 0.0059$ $0.000470\ 0.00340\ 0.02870\ 0.00640\ 0.01320\ 0.02500\ 0.000040\ 0.001320\ 0.02500\ 0.00000\ 0.00140\ 0.001320\ 0.02500\ 0.000140\ 0.001310\ 0.002500\ 0.00140\ 0.001310\ 0.002500\ 0.00140\ 0.001310\ 0.002500\ 0.00140\ 0.001310\ 0.002500\ 0.00140\ 0.001310\ 0.002500\ 0.00140\ 0.001310\ 0.002500\ 0.00140\ 0.001310\ 0.00140\ 0$ $0.002970\ 0.00040\ 0.00040\ 0.00010\ 0.00030\ 0.03390\ 0.000000\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.000000\ 0.0$ $0.009570\ 000090\ 000110\ 000210\ 000810\ 007400\ 000000\ 000020\ 000090\ 000820\ 000090\ 000820\ 000090\ 000890\ 001590\ 000200\ 000040\ 0000570\ 0000570\ 0000570\ 000040\ 000000\ 000320\ 000090\ 000890\ 001480\ 004230\ 000910\ 000090\ 0001480\ 0004230\ 000910\ 000090\ 0001480\$ $0.008730\ 0.00060\ 0.00570\ 0.00270\ 0.00270\ 0.00280\ 0.06720\ 0.000000\ 0.00360\ 0.000360\ 0.00440\ 0.000000\ 0.00440\ 0.00070\ 0.00870\ 0.00180\ 0.00180\ 0.00480\ 0.00630\ 0.00280\ 0.00090\ 0.000210\ 0.00070\ 0.00280\ 0.00070\ 0.00280\ 0.00070\ 0.00080\ 0.000$ $0.000000 \ 0.00070 \ 0.00050 \ 0.00070 \ 0.00050 \ 0.00070 \ 0.00050 \ 0.0$

Результати без пробілів (cross)

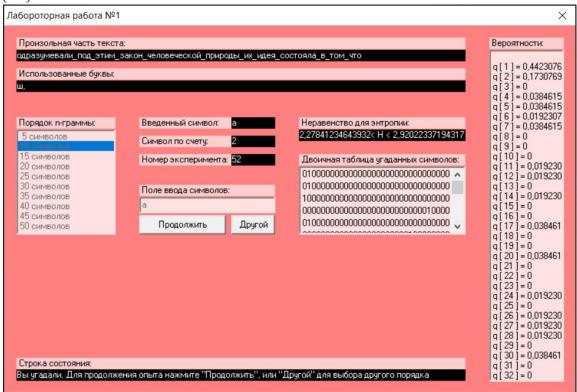
б в г д е ё ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь 0.007200.000300.000540.000440.000770.004750.000000.000070.000480.003680.000000.001250.001130.000680.001100.0001110.003720.000880.001010.000060.000080.000100.000280.000690.000020.0000110.0002520.000130.000170.000010.00035 $\pi = 0.005360.000090.000670.000060.000250.005260.000000.004340.000100.003420.000000.00300.001320.000090.00260.004090.00300.001270.000940.000160.001990.000010.000070.000140.000120.000060.000000.000140.000120.000090.000140.0001270.000940.000140.0001270.000940.000140.0001270.000940.000140.0$ 0.005240.000200.001310.000290.001600.000530.000000.0000160.0000530.000000.0000160.000760.000000.0000160.000760.0000210.00001-0.000120.000260.000600.000190.000750.000090.000170.0000580.000000.0000850.000170.000580.0000150.000370.001080.000590.000850.000320.001260.000720.000190.000110.0000590.000070.000200.000110.00000110.0000110.0000110.0000110.0000110.0000110.0000110.0000110.0000110.0000110.0000110.0000110.006930.000310.001200.000280.000800.005270.000000.000410.000170.009930.000000.000930.001850.000440.001140.000890.000230.003340.000340.001540.000050.000120.000020.001140.000020.000000.000000.000430.004920.000170.001180.00216 $0.003740\ 0.00320\ 0.00770\ 0.00220\ 0.00680\ 0.04270\ 0.000000\ 0.00020\ 0.0004270\ 0.000000\ 0.0004380\ 0.000000\ 0.00660\ 0.00270\ 0.00660\ 0.002280\ 0.004090\ 0.00260\ 0.001120\ 0.00250\ 0.002610\ 0.00070\ 0.00090\ 0.00030\ 0.000400\ 0.00020\ 0.0004000\ 0.0004000\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.0004000\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.000400\ 0.00$ $0.011410\ 0.00480\ 0.00540\ 0.00350\ 0.01210\ 0.09930\ 0.000000\ 0.00280\ 0.00230\ 0.010300\ 0.00000\ 0.000730\ 0.00080\ 0.0018$ $0.010350\ 000120\ 000710\ 000380\ 000420\ 008040\ 000000\ 000450\ 000000\ 000690\ 000000\ 000690\ 000040\ 000120\ 000690\ 000780\ 002830\ 000100\ 000010\ 0000250\ 000110\ 0000230\ 000010\ 000000\ 001700\ 000340\ 000110\ 0000250\ 0000250\ 00000250\ 00000250\ 0000250\ 0000250\ 00$ 0.002600.000270.001670.000120.000750.003600.000000.000050.000140.002320.000000.004910.002520.000930.001690.004630.003330.000600.001870.013740.001130.000080.000370.000140.000490.000110.000000.00030.000360.002980.000230.000090.004730.006830.000210.003210.000110.000520.007020.000000.000070.000140.005560.000000.001210.000460.000330.001720.015480.000670.003790.001880.000530.001480.000080.000100.000020.000310.000040.0000110.000000.001350.007010.000150.000060.000550.000130.000480.001820.000280.001110.000340.000000.000160.000500.000650.000010.001220.001270.000940.001740.000770.001270.000460.001640.000230.000050.000310.000160.000520.000030.000210.0000000.000000.000000.0000170.000060.000130.000160.0000160.000160.000160.000160.00

Результати без пробілів (non-cross)

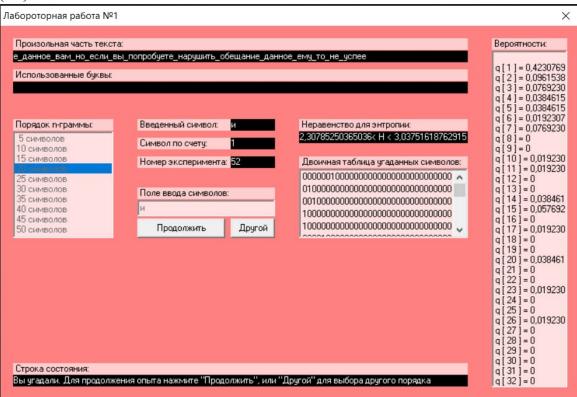
бвгдеёжзийклмнопрстуфхцч ш щ ъ ы ь $a \quad 0.000200.002220.005290.001010.003050.001650.000000.001590.004350.001410.000810.005470.012490.003970.007180.001170.002770.003570.005960.006740.000830.000360.000840.000650.001190.000670.000200.000000.000000.000000.000000.0000420.000580.001810.000400.000810.$ 0.006950.000270.000570.000470.000760.004800.000000.000060.000460.003670.000000.001190.000750.001160.001100.003820.000840.001050.000040.000100.000090.000250.000620.000030.000010.002470.000090.000160.0000020.00032 $0.005450\ 0.00100\ 0.00680\ 0.00090\ 0.00230\ 0.05210\ 0.000000\ 0.004350\ 0.00110\ 0.003500\ 0.00020\ 0.001390\ 0.00290\ 0.001160\ 0.00290\ 0.01160\ 0.00910\ 0.00150\ 0.01960\ 0.00000\ 0.00050\ 0.00140\ 0.00110\ 0.00080\ 0.00000\ 0.00020\ 0.00140\ 0.00110\ 0.00080\ 0.00$ 0.000790.001101.005490.001110.002740.003160.000000.000300.003550.002720.001210.003630.007800.00380.006370.002120.002840.002180.005810.005710.000490.000360.001830.000610.001840.000590.000180.0000000.000000.000000.000000.000370.000850.002390.007020.000300.001220.000330.000800.005420.0000300.00170.008960.000000.000900.001860.000450.001130.006750.000870.000250.003260.000310.001590.000070.000130.000011.001160.000020.000000.000000.000430.004890.000150.001170.00209 $0.003630\ 0.00350\ 0.00730\ 0.00210\ 0.00620\ 0.04150\ 0.000000\ 0.00010\ 0.0004150\ 0.000000\ 0.00180\ 0.001$ $0.011480\ 0.00540\ 0.00530\ 0.00350\ 0.01200\ 0.00980\ 0.000000\ 0.00320\ 0.00250\ 0.01420\ 0.000000\ 0.001470\ 0.01040\ 0.00060\ 0.00180\ 0.00370\ 0.01950\ 0.02040\ 0.00270\ 0.00070\ 0.000640\ 0.000330\ 0.00070\ 0.000640\ 0.00070\ 0.00070\ 0.00070\ 0.00070\ 0.0000$ $0.002050\ 0.00040\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.000000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.00000\ 0.000000\ 0.00$ 0.006740.000200.003210.000110.000520.007160.000000.000050.000190.00630.000000.001220.000470.000310.001750.015330.000650.003820.001880.000550.001410.000070.000100.000220.000320.000030.000010.000000.001330.006860.000120.0000550.000570.00000570.000570.000570.000570.000570.0000570.000570.000570.000570.00 $\pi = 0.000150.000460.001780.000250.001030.000350.000000.000150.000490.0000490.000180.0001310.000980.001130.000450.001630.0001630.000250.000100.000350.000160.000470.000020.000000.000000.000000.000000.000160.000050.00012$

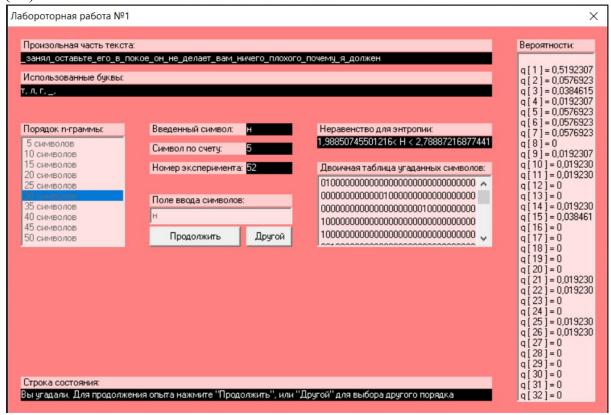
2. За допомогою програми CoolPinkProgram оцінити значення (10) Н, (20) Н, (30) Н.

(10)H



(20)H





3. Використовуючи отримані значення ентропії, оцінити надлишковість російської мови в різних моделях джерела.

Результати з пробілами:

R letter: 0.13869634694845956

R cross bigrams: 0.2136539650010565 R non-cross bigrams: 0.21368205500454784

Результати без пробілів:

R letter: 0.11687488159931758

R cross bigrams: 0.17971705698388785 R non-cross bigrams: 0.17981924680172867

Результати for CoolPinkProgramm:

0,4259961275 < R(10) < 0,5521515503 0,4029408602 < R(20) < 0,5463647449

0,4518147344 < R(30) < 0,6091357289

Висновки:

В результаті виконання даної лабораторної роботи ми отримали такі навички:

- о Підрахунку частоти монограм і біграм у тексті
- о Знаходження ентропії для монограм і біграм
- о Визначення надлишковості мови
- о Робота з CoolPinkProgram

При виконанні першого завдання, ми практично переконалися у тому, що літерами з найбільшими частотами ε 'о', 'а' та 'e'. В той час як літерами з найменшою частотою ε 'ъ' та 'ë'. В третьому пункті лабораторної роботи ми вирахували надлишковість російської мови, побачили її залежність від ентропії та кількості символів в алфавіті.