Криптографія
Комп’ютерний практикум №1
ФБ-05 Чирков Андрій
варіант 10

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

Хід роботи: Спочатку потрібно уважно прочитати методичні вказівки, після чого приступимо до виконання завдань. Підраховуємо частоти літер, з цим проблем не було, після чого обчислюємо H1 і H2 для тексту з пробілами та без, формули використовував які були в лекції, трохи виникали складності, але в цілому все підрахувалося. Використовуючи програму CoolPinkProgram проблема була лише в тому що вона не дуже коректно показувала кнопки. Складності виникли під час обрахування надлишковості, а саме реалізувати формулу.

Я покращив таблиці, які додав до протоколу, там є всі частоти букв за спаданням. Ось найчастіші:

Для літер з пробілом

1	'	0.16870144486914324,			
2	'о':	0.09294082394813964,		H1	4.370687561
3	'е':	0.07304555320874961,		R	0.14089051896624727
4	'а':	0.06750213770472634,			
5	'н':	0.055647925512866424,			
6	'и':	0.05296209136951962,			
7	'т':	0.05234087803024213,			
8	'с':	0.04425048783518114,			
9	'в':	0.038663221977797105,			
10	'л':	0.03860658193803945,			

Для літер без пробіла:

1	'о':	0.11180197941461549,			
2	'е':	0.0878692170916276,		H1	4.470069077
3	'а':	0.08120083607519402,		R	0.11385411781383048
4	'н':	0.06694096262937296,			
5	'и':	0.06371007268403435,			
6	'т':	0.062962792016405,			
7	'с':	0.053230560262691136,			
8	'в':	0.04650943002266019,			
9	'л':	0.046441295608846925,			
10	'р':	0.03944103406061325,			

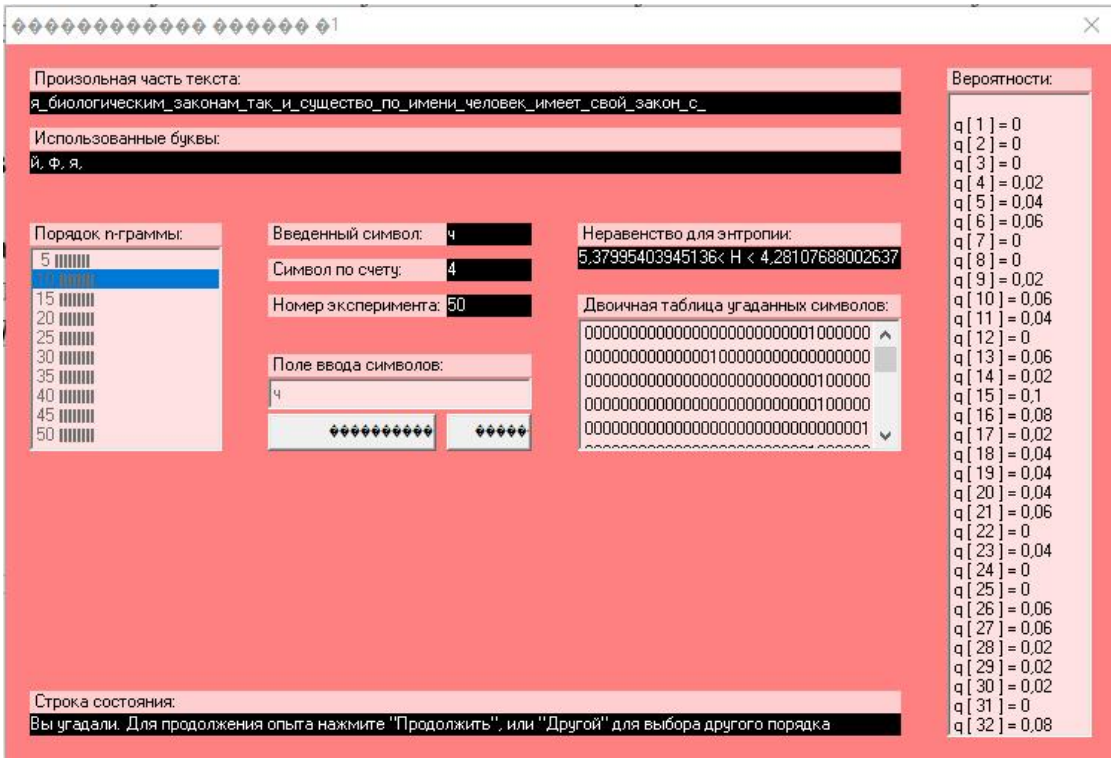
Для біграм з пробілами:

1	'о '	0.019739265			
2	' о'	0.017277064		H1	4.229839136
3	'е '	0.015161282		R	0.154507724
4	'и '	0.014711815			
5	'а '	0.014599996			
6	' н'	0.012902985			
7	' с'	0.011302445			
8	' е'	0.011164316			
9	' а'	0.01101961			
10	' в'	0.010912176			

Для біграм без пробілів:

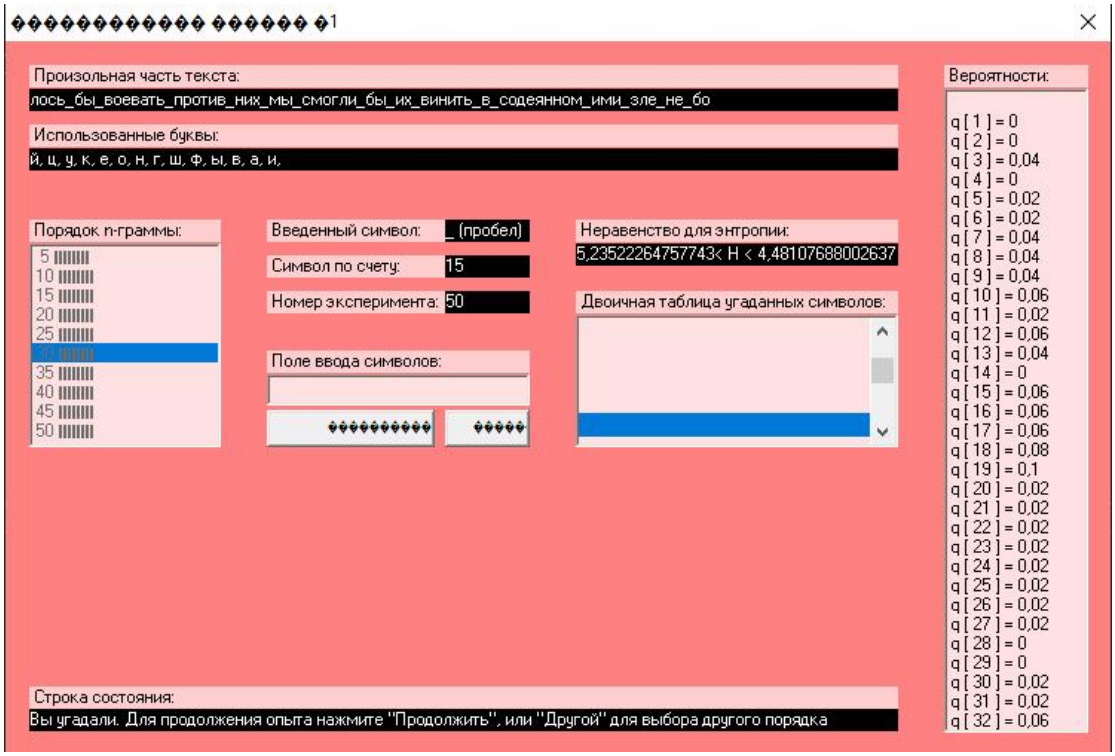
1	'то'	0.011995189			
2	'не'	0.00970587		H1	4.36571937
3	'ен'	0.009558172		R	0.122453185
4	'но'	0.009394649			
5	'от'	0.008788032			
6	'он'	0.008761658			
7	'оо'	0.008690446			
8	'ов'	0.008379225			
9	'по'	0.008046905			
10	'ст'	0.008004705			

H = 4.830515459769985
R = 0.6832290591478351



H = 4.650877618296385
R = 0.6804858059191587

H = 4.8581497638019
R = 0.73042967030258



Висновки: При виконанні лабораторної я навчився, та дізнався як обчислювати частоту букв, і підраховувати ентропію для літер та біграм. Помітно що без пробілів ентропія більша, ніж з ними, як в літерах так і в біграмах. В цілому

було корисно на практиці розробити програму, яка використовує трохи складні формули.