**СИМЕТРИЧНА КРИПТОГРАФІЯ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №1**

**Експериментальна оцінка ентропії на символ джерела відкритого тексту**

**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. А також успішне закриття предмету і успіх у житті.

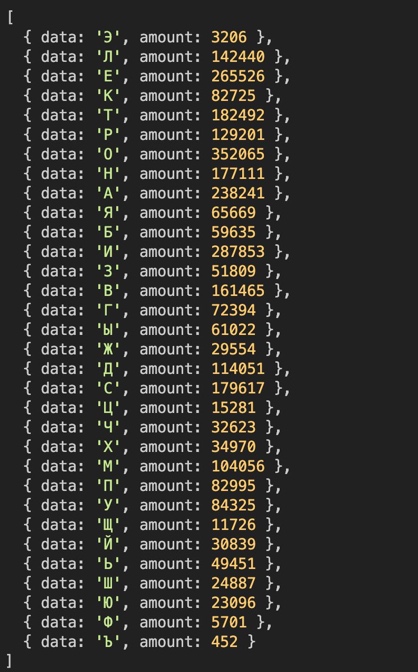
**Порядок виконання роботи**

1. Уважно прочитати методичні вказівки до виконання комп’ютерного практикуму.
2. Написати програми для підрахунку частот букв і частот біграм в тексті, а також підрахунку H1 та H2 за безпосереднім означенням. Підрахуватичастоти букв та біграм, а також значення H1 та H2 на довільно обраному тексті російською мовою достатньої довжини (щонайменше 1Мб), де імовірності замінити відповідними частотами. Також одержати значення H1 та H2 на тому ж тексті, в якому вилучено всі пробіли.
3. За допомогою програми CoolPinkProgram оцінити значення H (10) , H (20) , H (30)
4. Використовуючи отримані значення ентропії, оцінити надлишковість російської мови в різних моделях джерела

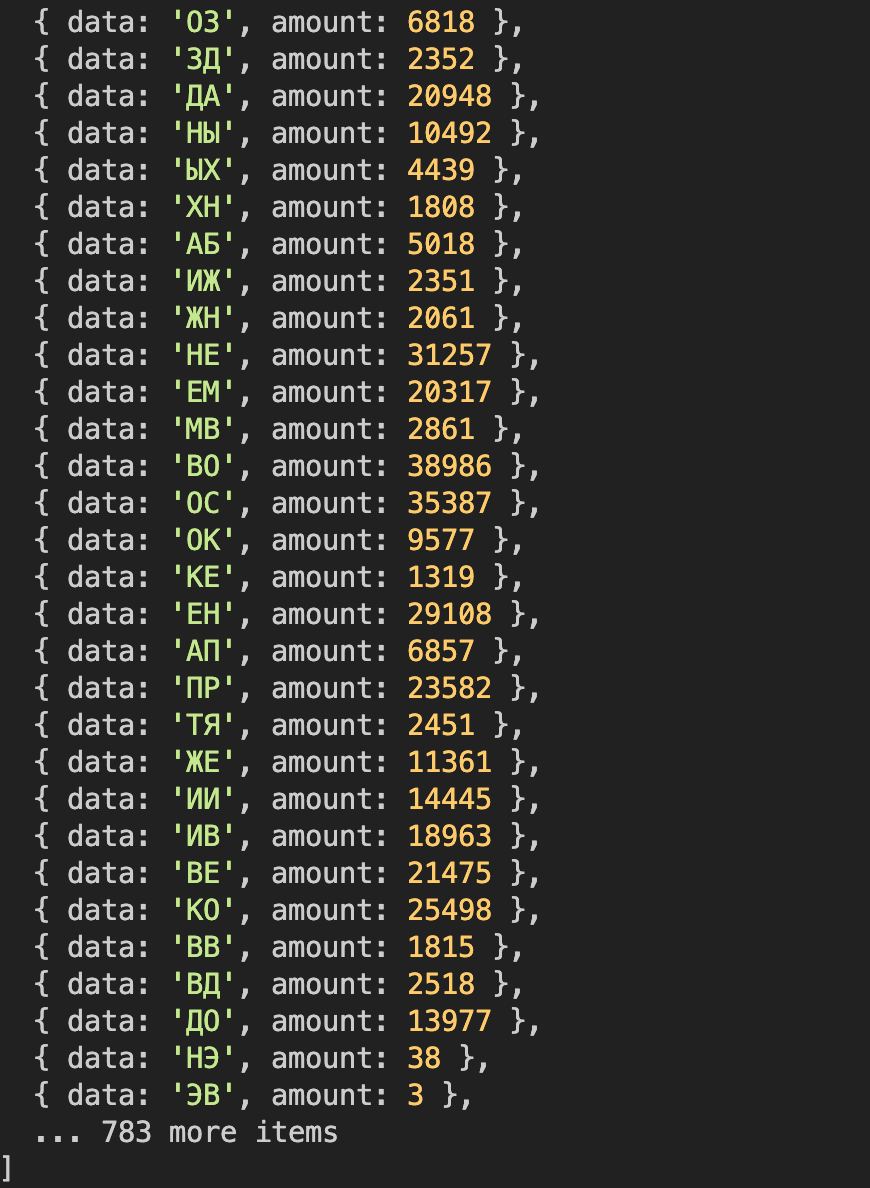
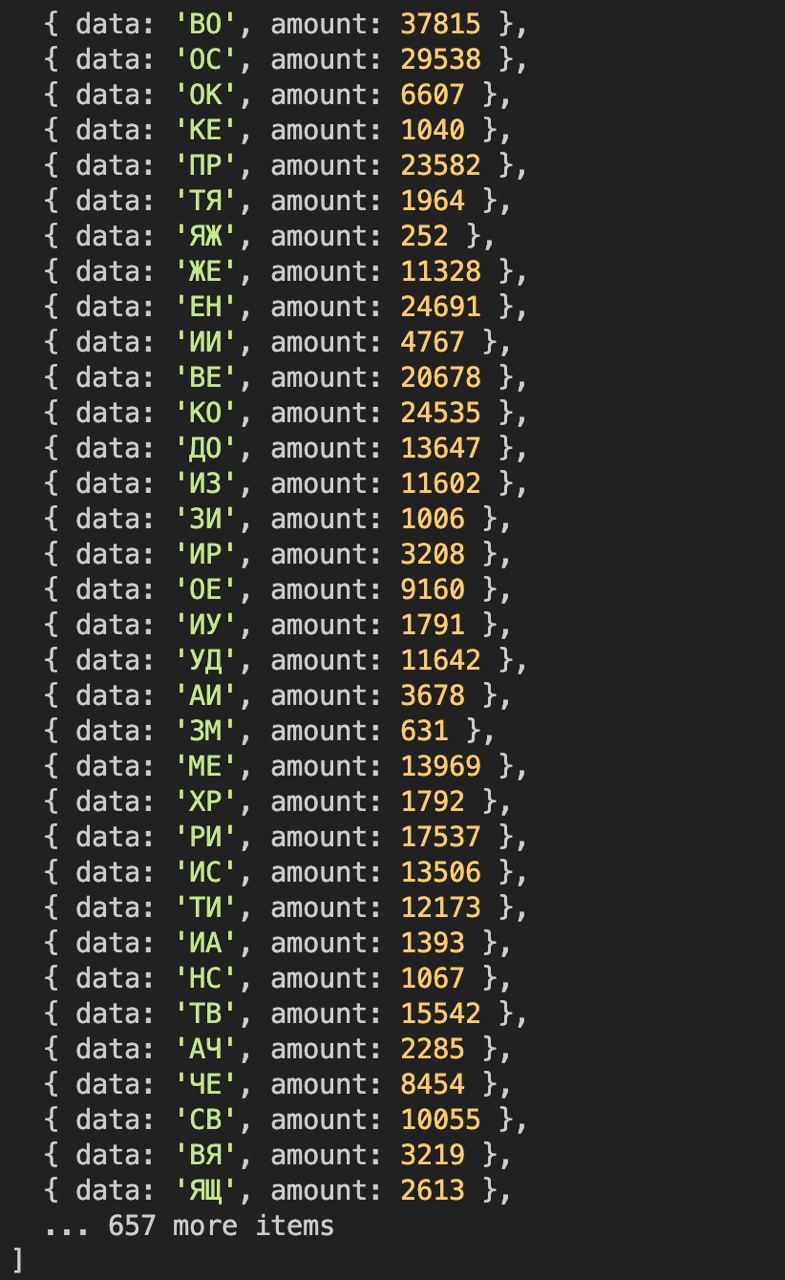
**Хід роботи**

Найбільші труднощі виникли з пошуком файлу через обмеження в його розмірі в 1Мб. Але рішення досить швидко було знайдено, було використано повне зібрання (Старий + Новий заповіт) розмірами 7.5Мб. Наступним випробуванням був запуск програми CoolPinkProgram.exe, через її недоступність на пристроях mac. При написанні програмної частини лабораторної роботи проблем не виникало. Мова виконання: typescript.

Таблиця частот входжень літер руснявого алфавіту в тексті:



Таблиця частот біграм з перетином та без:

****

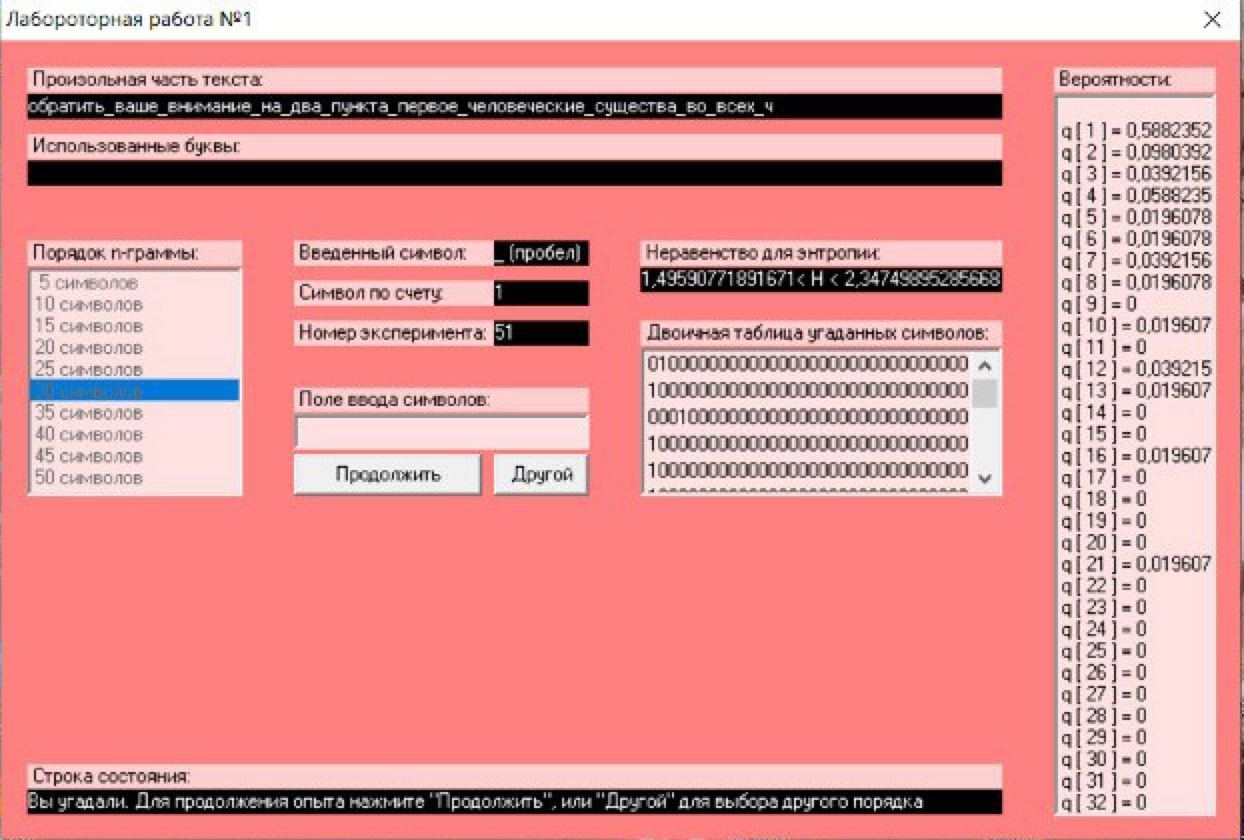
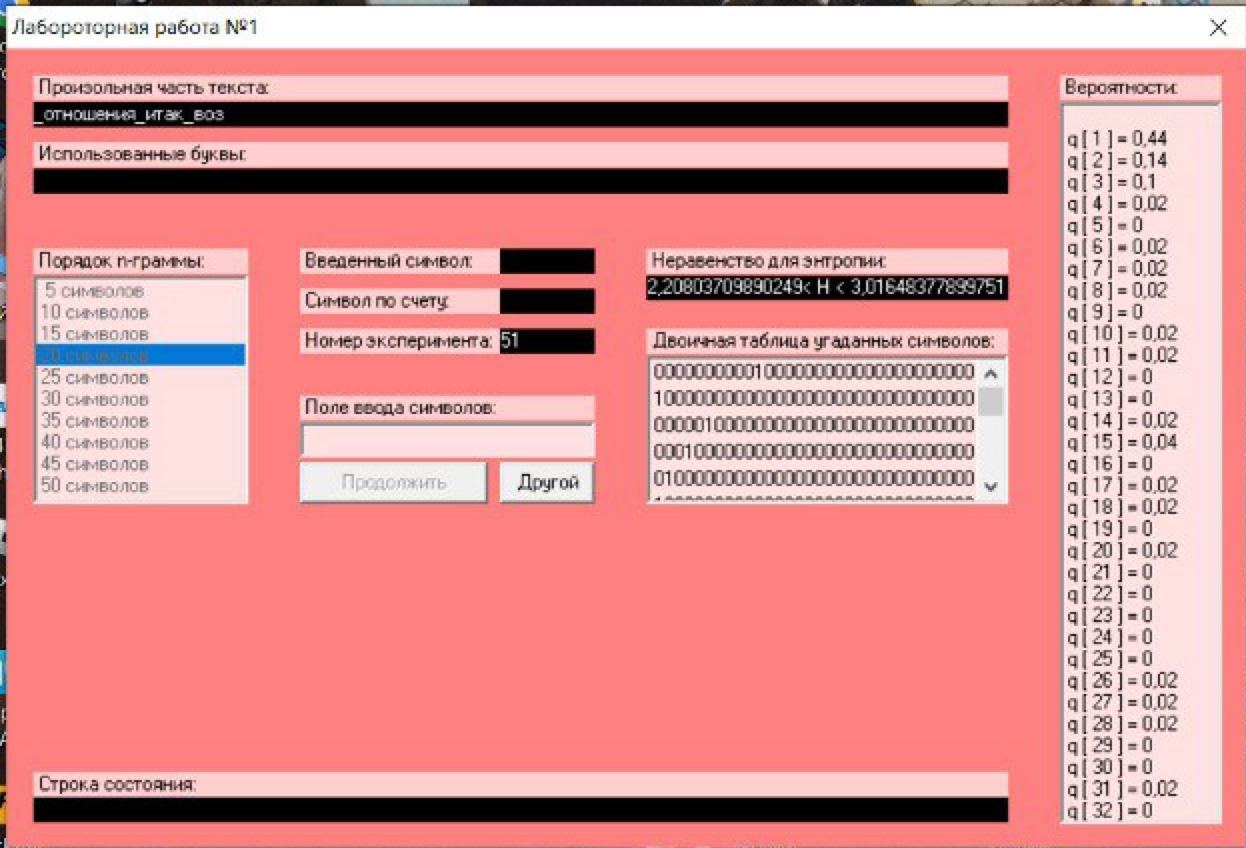
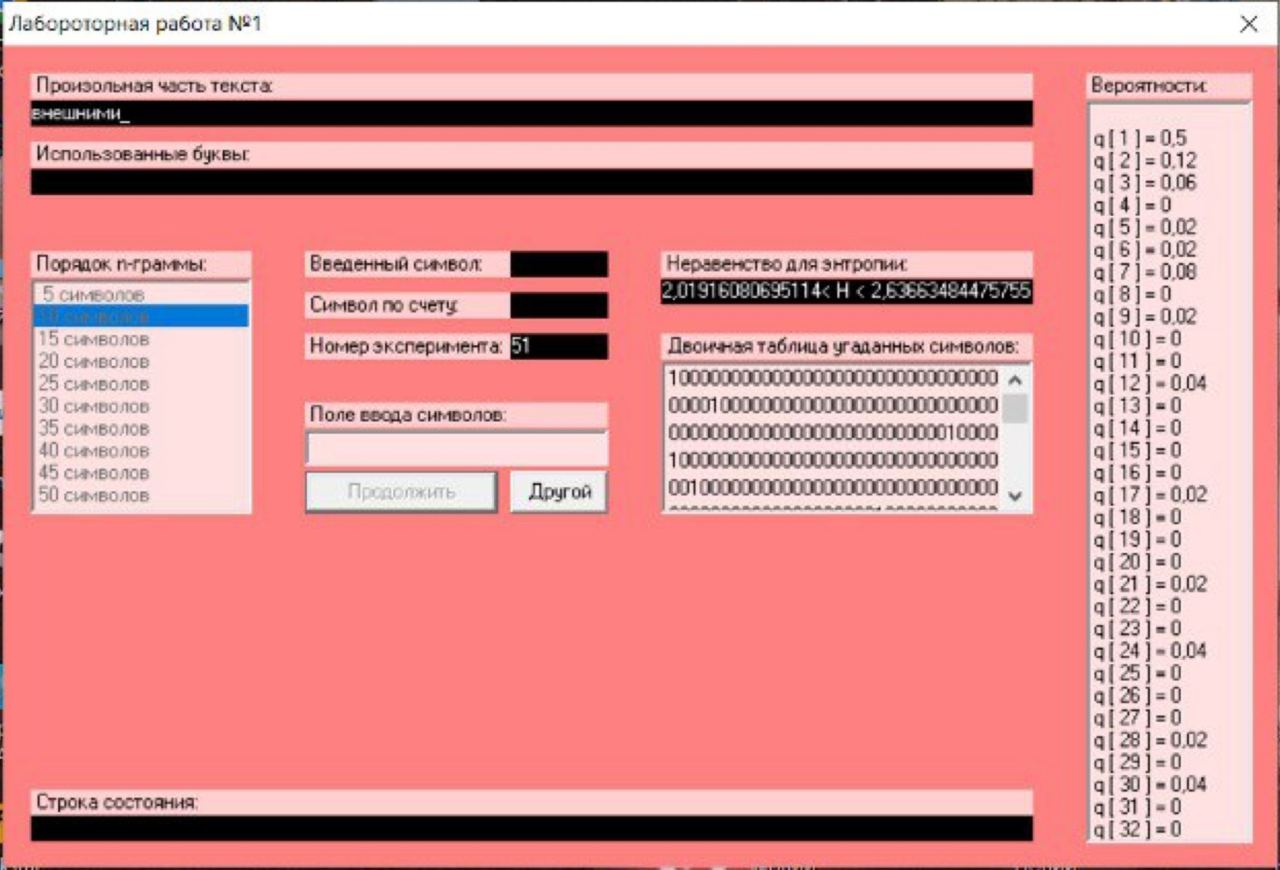
Ентропія H1



Ентропія H2 (з перетином та без)

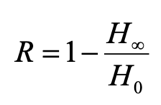


Оцінки для значень H (10) , H (20) , H (30)



Вибачте за якість, віндоус-ноутбук 2011 року народження)

Наочно побачили, як зі збільшенням кількості відображених символів у тексті (ми точно мали це отримати), ентропія буде знижуватись

Для знаходження оцінки надлишковості російської мови в різних моделях джерела, підставимо в формулу: , на місце Hoo отримані вище значення H1 , H2 , H (10) , H (20) , H (30)

R1=1-4.44/log(33)=0.12

R2=1-8.26/log(883)=0.16

R2\*=1-7.8/log(757)=0.14

R10=1-2.4/log(34)=0.59

R20=1-2.6/log(34)=0.69

R30=1-1.6/log(34)= 0.59

(\* - біграми без перетину)

Отримали значення надлишковості 0.12, 0.16, 0.14, 0.59, 0.69, 0.59

**Висновок:**

Під час виконання цього комп’ютерного практикуму, що віндоус-ноутбук є необхідною навичкою на 3 курсі, без якої виконання робіт унеможливлюється, або значно ускладнюється. Вивчили поняття ентропія, частота, pink, typescript, main, log та багато інших. Перечитали святе письмо. Перелічили символи з тексту, для перевірки показників програми. Визначили значення надлишковості для російської мови, зазначені вище. Втомилися