

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  $H_1$  і  $H_2$  для тексту з пробілами та без, формули використовував які були в лекції, трохи виникали складності, але в цілому все підраховалося. 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	'o'	0.019739265			
2	'o'	0.017277064		H1	4.229839136
3	'e'	0.015161282		R	0.154507724
4	'и'	0.014711815			
5	'a'	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		4.36571937
3	'ен'	0.009558172		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		

The screenshot shows a software interface with a pink background and a black top bar containing a row of 26 diamond-shaped icons. The interface is divided into several sections:

- Top Section:**
  - Label: "Произвольная часть текста:" (Arbitrary part of the text:)
  - Input field: "ошению\_к\_"
  - Label: "Использованные буквы:" (Used letters:)
  - Empty input field.
- Left Panel:**
  - Label: "Порядок n-граммы:" (Order of n-gram:)
  - List of values with corresponding bar charts:
    - 5
    - 15
    - 20
    - 25
    - 30
    - 35
    - 40
    - 45
    - 50
- Center Section:**
  - Label: "Введенный символ:" (Entered symbol:)
  - Input field: "Символ по счету:" (Symbol by number:)
  - Label: "Номер эксперимента:" (Experiment number:)
  - Input field: "50"
  - Label: "Поле ввода символов:" (Symbol input field:)
  - Input field: "☐☐☐☐☐"
  - Input field: "☐☐☐☐☐"
- Right Section:**
  - Label: "Неравенство для энтропии:" (Entropy inequality:)
  - Text: "2.07951543314719 < H < 2.83840168049668"
  - Label: "Двоичная таблица угаданных символов:" (Binary table of guessed symbols:)
  - Table with 10 columns and 10 rows of binary data.
- Far Right Panel:**
  - Label: "Вероятности:" (Probabilities:)
  - List of probabilities:
    - q[1] = 0.4897959
    - q[2] = 0.0816326
    - q[3] = 0.0816326
    - q[4] = 0.0408163
    - q[5] = 0
    - q[6] = 0.0204081
    - q[7] = 0
    - q[8] = 0.0204081
    - q[9] = 0.0204081
    - q[10] = 0
    - q[11] = 0.040816
    - q[12] = 0
    - q[13] = 0.040816
    - q[14] = 0.040816
    - q[15] = 0
    - q[16] = 0.040816
    - q[17] = 0.020408
    - q[18] = 0.020408
    - q[19] = 0.020408
    - q[20] = 0
    - q[21] = 0
    - q[22] = 0.020408
    - q[23] = 0
    - q[24] = 0
    - q[25] = 0
    - q[26] = 0
    - q[27] = 0
    - q[28] = 0
    - q[29] = 0
    - q[30] = 0
    - q[31] = 0
    - q[32] = 0
- Bottom Section:**
  - Label: "Строка состояния:" (Status bar:)
  - Empty input field.

$$0.591247052207243 < R < 0.442079132749186$$

