

**Міністерство освіти і науки України  
Національний технічний університет України  
"Київський політехнічний інститут імені Ігоря Сікорського"  
Фізико-технічний інститут**

**Криптографія  
Лабораторна робота №1.**

Виконав:  
студент гр. ФБ-94  
Резніченко Н. І.  
Белоцький. Д. О.

Київ – 2021

**Мета:** 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.

## Entropy:

Letters with spaces entropy: 4.446592

Letters without spaces entropy: 8.893183

Entropy for crossed bgramms with spaces: 5.187000

Entropy for uncrossed bgramms with spaces: 4.629763

Entropy for crossed bgramms without spaces: 4.629763

Entropy for uncrossed bgramms without spaces: 4.844959

## Letters with spaces count:

п: 23449.000000      ч: 15073.000000

ю: 4672.000000      я: 17941.000000

ы: 13933.000000      о: 97745.000000

ж: 9531.000000      к: 28479.000000

б: 14863.000000      и: 61333.000000

ц: 2540.000000      г: 14090.000000

х: 7542.000000      а: 67791.000000

м: 26714.000000      с: 44101.000000

л: 39430.000000      р: 35509.000000

з: 13563.000000      д: 27316.000000

ь: 20115.000000      щ: 2600.000000

е: 72365.000000      ш: 7378.000000

т: 55096.000000      ф: 826.000000

в: 38403.000000      у: 25696.000000

н: 54457.000000      й: 8347.000000

э: 2739.000000

## Letters without spaces count:

щ: 2600.000000      н: 54457.000000

а: 67791.000000      э: 2739.000000

г: 14090.000000	х: 7542.000000
ы: 13933.000000	м: 26714.000000
ь: 20115.000000	ч: 15073.000000
о: 97745.000000	п: 23449.000000
т: 55096.000000	у: 25696.000000
ж: 9531.000000	ц: 2540.000000
б: 14863.000000	ф: 826.000000
ю: 4672.000000	р: 35509.000000
й: 8347.000000	к: 28479.000000
д: 27316.000000	с: 44101.000000
е: 72365.000000	я: 17941.000000
з: 13563.000000	в: 38403.000000
и: 61333.000000	л: 39430.000000
ш: 7378.000000	

### **Letters frequency with spaces:**

о: 0.114504	е: 0.084773
а: 0.079414	и: 0.071849
т: 0.064543	н: 0.063794
с: 0.051662	л: 0.046191
в: 0.044988	р: 0.041597
к: 0.033362	д: 0.032000
м: 0.031294	у: 0.030102
п: 0.027470	ь: 0.023564
я: 0.021017	ч: 0.017657
б: 0.017411	г: 0.016506
ы: 0.016322	з: 0.015888
ж: 0.011165	й: 0.009778
х: 0.008835	ш: 0.008643
ю: 0.005473	э: 0.003209
щ: 0.003046	ц: 0.002976
ф: 0.000968	

### Letters frequency without spaces:

о: 0.114504    е: 0.084773  
а: 0.079414    и: 0.071849  
т: 0.064543    н: 0.063794  
с: 0.051662    л: 0.046191  
в: 0.044988    р: 0.041597  
к: 0.033362    д: 0.032000  
м: 0.031294    у: 0.030102  
п: 0.027470    б: 0.023564  
я: 0.021017    ч: 0.017657  
б: 0.017411    г: 0.016506  
ы: 0.016322    з: 0.015888  
ж: 0.011165    й: 0.009778  
х: 0.008835    ш: 0.008643  
ю: 0.005473    э: 0.003209  
щ: 0.003046    ц: 0.002976  
ф: 0.000968

### CoolPinkProgram

<b>H(10)</b>	<b>0,636 &lt; R &lt; 0,746</b>
<b>H(20)</b>	<b>0,365 &lt; R &lt; 0,5</b>
<b>H(30)</b>	<b>0,357 &lt; R &lt; 0,484</b>

H(10)

Произвольная часть текста:  
а\_нарушение\_на\_кого\_то\_или\_на\_что\_то\_другое\_вы\_заметили\_что\_мы\_подыскиваем\_

Использованные буквы:

Порядок n-граммы:  
5 символов  
15 символов  
20 символов  
25 символов  
30 символов  
35 символов  
40 символов  
45 символов  
50 символов

Введенный символ: и

Символ по счету: 1

Номер эксперимента: 53

Поле ввода символов:  
и

Продолжить Другой

Неравенство для энтропии:  
3,18052615054133< H < 3,7302920964325

Двоичная таблица угаданных символов:  
00000000000000010000000000000000  
00000010000000000000000000000000  
00000010000000000000000000000000  
1000000000000000000000000000000000  
0010000000000000000000000000000000  
0000000000000000000000000000000000

Вероятности:  
q[ 1 ] = 0,3018867  
q[ 2 ] = 0,0566037  
q[ 3 ] = 0,0943396  
q[ 4 ] = 0,0188679  
q[ 5 ] = 0,0188679  
q[ 6 ] = 0,0566037  
q[ 7 ] = 0,0754716  
q[ 8 ] = 0,0188679  
q[ 9 ] = 0  
q[ 10 ] = 0,018867  
q[ 11 ] = 0,018867  
q[ 12 ] = 0  
q[ 13 ] = 0  
q[ 14 ] = 0  
q[ 15 ] = 0  
q[ 16 ] = 0,056603  
q[ 17 ] = 0,018867  
q[ 18 ] = 0  
q[ 19 ] = 0,037735  
q[ 20 ] = 0,018867  
q[ 21 ] = 0,018867  
q[ 22 ] = 0,037735  
q[ 23 ] = 0  
q[ 24 ] = 0  
q[ 25 ] = 0,018867  
q[ 26 ] = 0  
q[ 27 ] = 0,018867  
q[ 28 ] = 0,037735  
q[ 29 ] = 0,037735  
q[ 30 ] = 0,018867  
q[ 31 ] = 0  
q[ 32 ] = 0

Строка состояния:  
Вы угадали. Для продолжения опыта нажмите "Продолжить", или "Другой" для выбора другого порядка

H(20)

Произвольная часть текста:  
больной\_игрок\_допустил\_нарушение\_если\_бы\_не\_существовало\_определенного\_согл

Использованные буквы:  
к,

Порядок n-граммы:  
5 символов  
10 символов  
15 символов  
25 символов  
30 символов  
35 символов  
40 символов  
45 символов  
50 символов

Введенный символ: т

Символ по счету: 2

Номер эксперимента: 53

Поле ввода символов:  
т

Продолжить Другой

Неравенство для энтропии:  
1,82718760987134< H < 2,5012731003334

Двоичная таблица угаданных символов:  
00001000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00010000000000000000000000000000  
1000000000000000000000000000000000  
0000000000000000000000000000000000

Вероятности:  
q[ 1 ] = 0,5283018  
q[ 2 ] = 0,1320754  
q[ 3 ] = 0,0754716  
q[ 4 ] = 0,0188679  
q[ 5 ] = 0,0377358  
q[ 6 ] = 0  
q[ 7 ] = 0,0188679  
q[ 8 ] = 0  
q[ 9 ] = 0  
q[ 10 ] = 0,018867  
q[ 11 ] = 0  
q[ 12 ] = 0  
q[ 13 ] = 0  
q[ 14 ] = 0  
q[ 15 ] = 0,018867  
q[ 16 ] = 0  
q[ 17 ] = 0  
q[ 18 ] = 0  
q[ 19 ] = 0  
q[ 20 ] = 0,018867  
q[ 21 ] = 0,056603  
q[ 22 ] = 0  
q[ 23 ] = 0,037735  
q[ 24 ] = 0  
q[ 25 ] = 0,018867  
q[ 26 ] = 0  
q[ 27 ] = 0,018867  
q[ 28 ] = 0  
q[ 29 ] = 0  
q[ 30 ] = 0  
q[ 31 ] = 0  
q[ 32 ] = 0

Строка состояния:  
Вы угадали. Для продолжения опыта нажмите "Продолжить", или "Другой" для выбора другого порядка

**H(30)**

Произвольная часть текста:  
\_что\_брать\_каждую\_понравившуюся\_женщину\_вы\_не\_имеете\_права\_разного\_мнения\_д

Использованные буквы:

Порядок n-граммы:  
5 символов  
10 символов  
15 символов  
20 символов  
25 символов  
35 символов  
40 символов  
45 символов  
50 символов

Введенный символ: c

Символ по счету: 1

Номер эксперимента: 53

Поле ввода символов:  
c

Продолжить

Другой

Неравенство для энтропии:  
1,78641985725751 < H < 2,4243381785949

Двоичная таблица угаданных символов:  
01000000000000000000000000000000  
01000000000000000000000000000000  
00001000000000000000000000000000  
10000000000000000000000000000000  
10000000000000000000000000000000  
00000000000000000000000000000000

Вероятности:  
q[1] = 0,5849056  
q[2] = 0,1132075  
q[3] = 0,0188679  
q[4] = 0,0188679  
q[5] = 0,0188679  
q[6] = 0  
q[7] = 0  
q[8] = 0,0188679  
q[9] = 0  
q[10] = 0  
q[11] = 0,037735  
q[12] = 0  
q[13] = 0  
q[14] = 0,018867  
q[15] = 0  
q[16] = 0  
q[17] = 0  
q[18] = 0,037735  
q[19] = 0  
q[20] = 0  
q[21] = 0,018867  
q[22] = 0  
q[23] = 0,037735  
q[24] = 0  
q[25] = 0  
q[26] = 0  
q[27] = 0,018867  
q[28] = 0,018867  
q[29] = 0,018867  
q[30] = 0  
q[31] = 0,018867  
q[32] = 0

Строка состояния:  
Вы угадали. Для продолжения опыта нажмите "Продолжить", или "Другой" для выбора другого порядка

**Висновки:** При виконанні лабораторної роботи ми засвоїли поняття ентропії на символ джерела та надлишковості та навчилися їх вимірювати, набули навичок щодо їх оцінки.