

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		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		

$$H = 4.830515459769985$$
$$R = 0.6832290591478351$$

$H = 4.650877618296385$   
 $R = 0.6804858059191587$

Произвольная часть текста:  
ояснения\_дело\_в\_том\_что\_они\_лишь\_еще\_одно\_доказательство\_того\_как\_глубоко\_н

Использованные буквы:  
й, ц, у, к, е, н, г, ш, щ, э, х, ж, д, л, о, р, п, а, э, ю, б, т, и,

Порядок n-граммы:  
5 ██████████  
10 ██████████  
15 ██████████  
20 ██████████  
25 ██████████  
30 ██████████  
35 ██████████  
40 ██████████  
45 ██████████  
50 ██████████

Введенный символ: \_ (пробел)  
Символ по счету: 24  
Номер эксперимента: 50

Неравенство для энтропии:  
 $5.04358329712093 < H < 4.25817193947184$

Двоичная таблица угаданных символов:

Поле ввода символов:

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

Вероятности:

$q[1]$	= 0.04
$q[2]$	= 0
$q[3]$	= 0.02
$q[4]$	= 0.06
$q[5]$	= 0.06
$q[6]$	= 0.04
$q[7]$	= 0
$q[8]$	= 0.02
$q[9]$	= 0
$q[10]$	= 0
$q[11]$	= 0
$q[12]$	= 0.02
$q[13]$	= 0.06
$q[14]$	= 0.04
$q[15]$	= 0.06
$q[16]$	= 0.08
$q[17]$	= 0.06
$q[18]$	= 0.06
$q[19]$	= 0
$q[20]$	= 0.08
$q[21]$	= 0
$q[22]$	= 0.06
$q[23]$	= 0.02
$q[24]$	= 0.04
$q[25]$	= 0
$q[26]$	= 0.04
$q[27]$	= 0
$q[28]$	= 0
$q[29]$	= 0
$q[30]$	= 0.02
$q[31]$	= 0.04
$q[32]$	= 0.08

$H = 4.8581497638019$   
 $R = 0.73042967030258$

Произвольная часть текста:  
лось\_бы\_воевать\_против\_них\_мы\_смогли\_бы\_их\_винить\_в\_содеянном\_ими\_эле\_не\_бо

Использованные буквы:  
й, ц, у, к, е, о, н, г, ш, ф, ы, в, а, и,

Порядок n-граммы:  
5 ██████████  
10 ██████████  
15 ██████████  
20 ██████████  
25 ██████████  
30 ██████████  
35 ██████████  
40 ██████████  
45 ██████████  
50 ██████████

Введенный символ: \_ (пробел)  
Символ по счету: 15  
Номер эксперимента: 50

Неравенство для энтропии:  
 $5.23522264757743 < H < 4.48107688002637$

Двоичная таблица угаданных символов:

Поле ввода символов:

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

Вероятности:

$q[1]$	= 0
$q[2]$	= 0
$q[3]$	= 0.04
$q[4]$	= 0
$q[5]$	= 0.02
$q[6]$	= 0.02
$q[7]$	= 0.04
$q[8]$	= 0.04
$q[9]$	= 0.04
$q[10]$	= 0.06
$q[11]$	= 0.02
$q[12]$	= 0.06
$q[13]$	= 0.04
$q[14]$	= 0
$q[15]$	= 0.06
$q[16]$	= 0.06
$q[17]$	= 0.06
$q[18]$	= 0.08
$q[19]$	= 0.1
$q[20]$	= 0.02
$q[21]$	= 0.02
$q[22]$	= 0.02
$q[23]$	= 0.02
$q[24]$	= 0.02
$q[25]$	= 0.02
$q[26]$	= 0.02
$q[27]$	= 0.02
$q[28]$	= 0
$q[29]$	= 0
$q[30]$	= 0.02
$q[31]$	= 0.02
$q[32]$	= 0.06

**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.