# Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Фізико-технічний інститут

# КРИПТОГРАФІЯ КОМП'ЮТЕРНИЙ ПРАКТИКУМ №1

Експериментальна оцінка ентропії на символ джерела відкритого тексту

Виконали: ФБ-31 Аль-Фітурі Асія ФБ-31 Гриб Вероніка

## 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.

## Порядок виконання роботи

- 1. Написати програми для підрахунку а) частот букв і b) частот біграм в тексті, а також підрахунку с) H1 та H2 за безпосереднім означенням. Підрахувати частоти 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.
- А) частота букв
- 1. Частота літер

Частота окремої літери обчислюється як відношення кількості появ цієї літери до загальної кількості літер у тексті

$$P(l) = \frac{f(l)}{n}$$

Дані збереглись а табличці

Розмір: 1.07 МБ

Готово: створено 5 таблиць у crypto\_5tables.xlsx

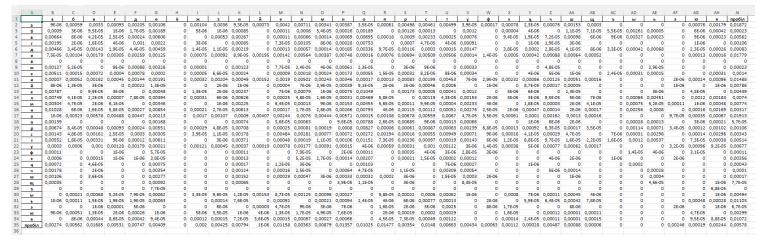
Частота літери з пробілами

	Α	В		С	
1	Літера	Кількість	L	łастота	
2	пробіл	172157	0	,166875	
3	О	95774	0	,092835	
4	a	74368	0	,072086	
5	e	73361		0,07111	
6	И	53873		0,05222	
7	н	52690	0	,051073	
8	Т	51049	0	,049483	
9	С	44734	0	,043361	
10	Л	43373	0	,042042	
11	p	43076	0	,041754	
12	В	41001	0	,039743	
13	К	31695	0	,030723	
14	M	27873	0	,027018	
15	Д	25559	0	,024775	
16	у	24698		0,02394	
17	п	21472	0	,020813	
18	Г	18252	0	,017692	
19	Ь	16945	0	,016425	
20	я	16841	0	,016324	
21	ы	14150	0	,013716	
22	3	13902	0	,013475	
23	б	13350		0,01294	
24	ч	11986	0	,011618	
25	й	10369	0	,010051	
26	ж	837	1	0,008114	1
27	ш	812	1	0,007872	2
28	x	737	9	0,007153	3
29	ю	522	3	0,005063	3
30	ц	375	3	0,003638	3
31	э	282	7	0,00274	ļ
32	щ	223	3	0,002164	ļ
33	ф	105	0	0,001018	3
34	ъ	14	9	0,000144	ļ
25					

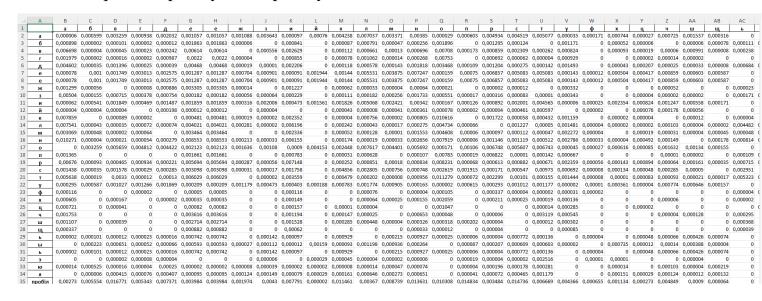
Частота літерів без пробілів

4	Α	В	С	
1	Літера	Кількість	Частота	
2	0	95774	0,11143	
3	a	74368	0,086525	
4	e	73361	0,085353	
5	И	53873	0,06268	
6	н	52690	0,061303	
7	Т	51049	0,059394	
8	С	44734	0,052047	
9	Л	43373	0,050463	
10	р	43076	0,050118	
11	В	41001	0,047703	
12	К	31695	0,036876	
13	M	27873	0,032429	
14	Д	25559	0,029737	
15	у	24698	0,028735	
16	п	21472	0,024982	
17	Γ	18252	0,021236	
18	ь	16945	0,019715	
19	я	16841	0,019594	
20	ы	14150	0,016463	
21	3	13902	0,016175	
22	б	13350	0,015532	
23	ч	11986	0,013945	
24	й	10369	0,012064	
25	ж	8371	0,009739	
26	ш	8121	0,009449	
27	x	7379	0,008585	
28	ю	5223	0,006077	
29	ц	3753	0,004367	
30	э	2827	0,003289	
31	щ	2233	0,002598	
32	ф	1050	0,001222	
33	ъ	149	0,000173	
34				

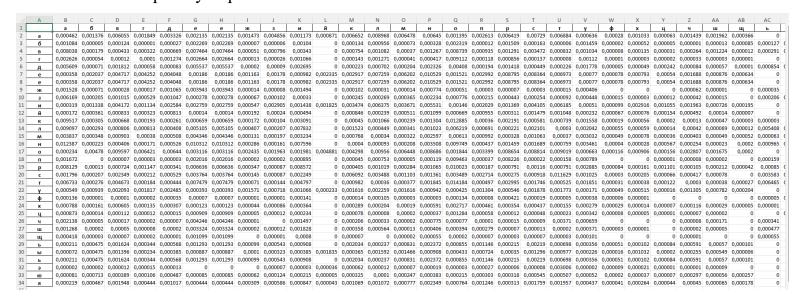
Біграми які перетинаются з пробілом



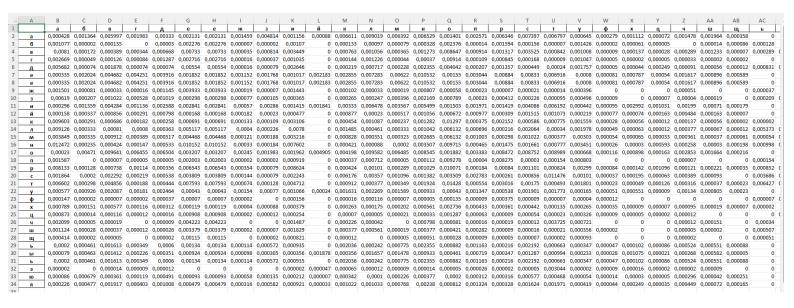
#### біграма з пробілу без перетену



#### без пробілу перетин



# без пробілу без перетену



$$H(Z) = -\sum_{i=1}^{n} p_i \log p_i.$$

Обчислюємо ентропію символів за формулою:

$$R = 1 - \frac{H_{\infty}}{H_0}$$

## Надлишковість:

A	ט	C	
Метрика	пробілам	ез пробілі	В
H1	4,452091	4,452091	
R1	0,117418	0,109582	
Н2 (перети	3,96747	4,138175	
R2 (перети	0,213489	0,172365	
Н2 (без пе	3,967347	4,138428	
R2 (без пе	0,213514	0,172314	

2. За допомогою програми CoolPinkProgram оцінити значення H (10), H (20) , H (30)

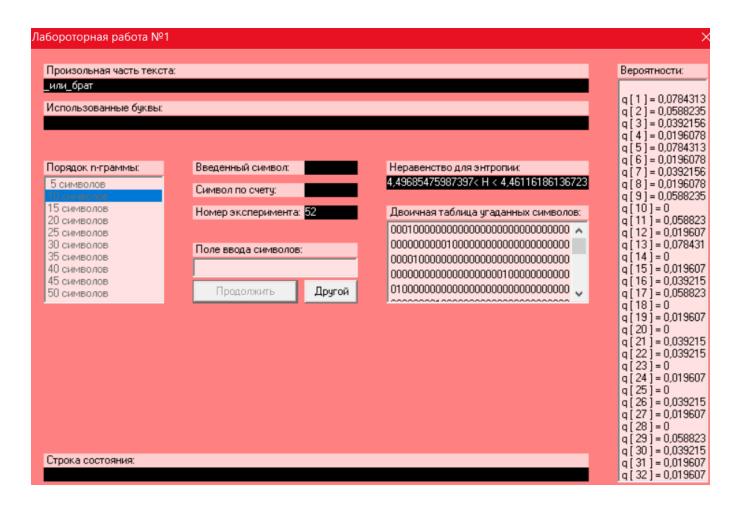
Hадлишковість джерела відкритого тексту (мови) дорівнює  $R=1-\frac{H_{\infty}}{H_0}$  і характеризує величину можливого ущільнення тексту деякою схемою кодування символів без втрати його змісту.

 $H\infty$  — це ентропія «нескінченного порядку» (умовна ентропія, яку оцінюють через експеримент з n-грамами, наприклад H(10),H(20),H(30)

H0=log2m, де m — кількість символів в алфавіті (для російської мови без пробілу  $\approx 32$ , з пробілом  $\approx 33$ ).

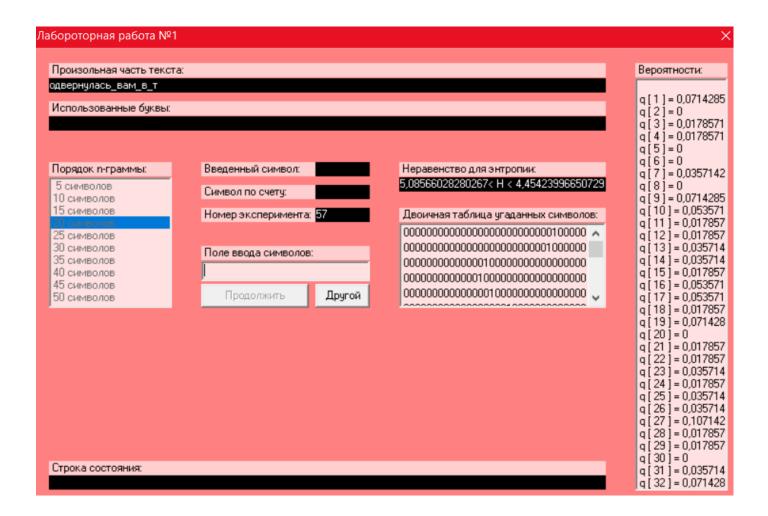
H(10)

Ентропія 4,4968 < H < 4,4611

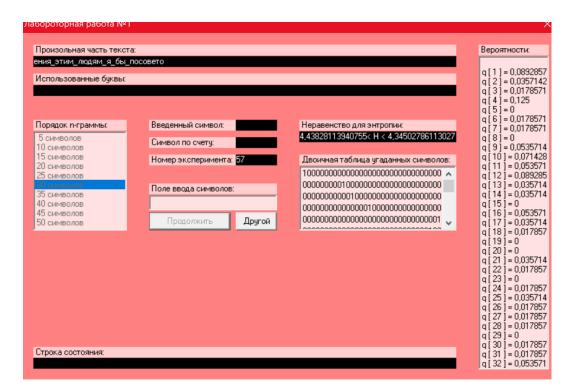


H(20)

Ентропія 5,0856 < H < 4,4542



H(30) Ентропія 4,4382 < H < 4,3450



Порядок п-грам	Ентропія (Н)	Надлишковість (R)
10 символів	4.4611 < H < 4.4968	0.110 < R < 0.116
20 символів	4.4542 < H < 5.0856	0.000 < R < 0.117
30 символів	4.3450 < H < 4.4382	0.120 < R < 0.138

#### Висновок

У роботі на основі книги російською мовою підраховано частоти літер і біграм для двох варіантів (з пробілом/без пробілу) та побудовано матриці біграм з перетином і без, що загалом дало 7 таблиць результатів. За програмою *CoolPinkProgram* отримано оцінки умовної ентропії H(n) та на їх основі обчислено надлишковість за формулою R=1–H\H0

H0= log2 33 це приблизно 5.044