НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Навчально-науковий фізико-технічний інститут КАФЕДРА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

«Криптографія»

Комп'ютерний практикум №1

Студенти: Маврикін Едуард

Слобода Ірина

Група: ФБ-25

Варіант 2

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.

При написанні коду особливих проблем не виникло, єдине - вивести таблицю частот біграм повністю неможливо через її розмір, тому вона додатково зберігається у CSV файл. Також після виконання основного коду можна вводити букви, щоб отримати найімовірнішу наступну літеру; для цього використовуються частоти біграм, які перетинаються, та алфавіт із пробілом.

Таблиця з отриманими значеннями ентропії:

	3 пробілами	Без пробілів
Н₁ (ентропія одиночних букв)	4.340	4.451
H ₂ (біграми без перекриття)	3.970	4.127
H ₂ (біграми з перекриттям)	3.970	4.127

Таблиці з оцінками надлишковості російської мови (R):

	3 пробілами	Без пробілів
R₁ (на основі H₁)	13.95%	10.99%
R ₂ (біграми без перекриття)	21.29%	17.45%
R ₂ (біграми з перекриттям)	21.30%	17.45%

3 пробілами (Но = 5.044):

$$R_1 = 1 - 4.3401/5.044 = 0.1395 = 13.95\%$$

$$R_2$$
 (без перекриття) = 1 - 3.9701/5.044 = 0.2129 = 21.29%

$$R_2$$
 (3 перекриттям) = 1 - 3.9697/5.044 = 0.2130 = 21.30%

Без пробілів ($H_0 = 5.000$):

```
R_1=1 - 4.4507/5.000 = 0.1099 = 10.99% R_2 \ (\text{без перекриття}) = 1 \ - 4.1275/5.000 = 0.1745 = 17.45\% R_2 \ (\text{3 перекриттям}) = 1 \ - 4.1274/5.000 = 0.1745 = 17.45\%
```

Приклад роботи програми

```
Sorted letter frequency with spaces:
(letter, count, frequency)
  179144 0.1753391406479397
o 96681 0.09462758148184398
e 73380 0.0718214740138984
a 67115 0.06568953704609964
н 54835 0.053670353332680824
и 54644 0.053483410002936285
т 54553 0.05339434276206323
c 44600 0.04365273563668396
в 38984 0.03815601448566115
л 38734 0.037911324263482434
p 35246 0.03449740628364491
к 27833 0.02724185181560145
д 26983 0.026409905060193795
м 26495 0.02593226974650093
y 24993 0.024462170891651168
п 23121 0.0226299305079769
ь 19362 0.01895076832729764
я 18000 0.017617695996867966
ч 15249 0.01492512479201331
6 14655 0.014343740824116668
г 14232 0.013929724968190272
ы 13912 0.013616521483801507
в 12975 0.012699422531075658
ж 9615 0.009410785944993639
й 8437 0.008257805618087501
x 7171 0.007018694332974454
ш 6937 0.006789664285015171
ю 4733 0.00463247528628756
э 2971 0.002907898600371929
щ 2521 0.00246745620045023
ц 2336 0.002286385436037976
ф 1049 0.0010267201722619164
ъ 204 0.00019966722129783693
```

H1 (entropy of single letters): 4.340109159286999
H2 (entropy of bigrams without overlapping): 3.9700541960289835
H2 (entropy of bigrams with overlapping): 3.9697042983305573

		6											N N		9	10	
0.001740	a 0.002435		8 0.015537	0.002699	A 007779	e 00274E	A 002044		0.005724	0.000400	0.000051	0.000002	0.000000	0.000000	0.002664	0.000045	0.00258
0.015572		0.000550	0.002649		0.001779			0.003414		0.000455	0.000031	0.000002	0.000000	0.000000	0.002004	0.000873	0.0019
0.015572	0.000037	0.000000	0.002049	0.000000			0.000006	0.003414		0.000010	0.000200	0.000149	0.003602	0.000000	0.000014	0.000008	0.0019
0.000413	0.005540	0.000002	0.000043	0.000000	0.000844		0.000008	0.000507		0.000574	0.000143	0.000004	0.003002	0.000147	0.000012	0.000000	0.0000
A STATE OF THE STA	0.000959	0.000023	0.000039	0.000043			0.000000	0.000004	0.000192	0.000374	0.000000	0.000004	0.002703	0.000147	0.000020	0.000000	0.0001
0.000312	0.005129	0.000035	0.000020	0.000000			0.000002		0.000023	0.000069	0.000000	0.000000	0.000427	0.001092	0.000000	0.000000	0.0004
0.016915		0.001298	0.000310	0.003351	0.002672			0.001221		0.000009	0.000000	0.000000	0.000000	0.000000	0.000000	0.000014	0.0002
0.000671	0.0001198	0.000238	0.001247	0.000002			0.000733	0.001221	0.0001188	0.000000	0.000949	0.000000	0.000000	0.000000	0.000010	0.000211	0.0002
0.001073	0.001138	0.000123	0.000000	0.000002			0.000010	0.000000	0.0000031	0.000006	0.000000	0.000000	0.000000	0.000047	0.000002	0.000000	0.0004
0.015864	0.000078	0.000123	0.000583	0.000548	0.001734				0.001482		0.000135	0.000041	0.000227	0.000114	0.000000	0.000301	0.0016
0.005458	0.000078	0.000033	0.002384	0.000031	0.001754	0.000000	0.000213	0.001032	0.001482	0.000178	0.000133	0.000000	0.000000	0.000000	0.000020	0.000000	0.0000
0.003436	0.006734	0.000033	0.000037	0.000031	0.000200	0.000362	0.000010	0.000010	0.000200	0.000178	0.000002	0.000000	0.000000	0.000000	0.000000	0.000000	0.000
0.006503	0.005311	0.000027	0.000230	0.000145	0.000012	0.003565	0.000319	0.000018	0.000012	0.000014	0.000000	0.000000	0.000609	0.004659	0.000000	0.000681	0.001
0.006763	0.002834	0.000031	0.000045	0.000245	0.000033	0.003923	0.000015	0.000015	0.000254	0.000008	0.000000	0.000000	0.000783	0.000065	0.000002	0.000001	0.001
0.003999	0.002034	0.000018	0.000043	0.000031	0.000043	0.009976	0.000000	0.000025	0.000031	0.000000	0.000000	0.000000	0.002463	0.001214	0.000000	0.000003	0.000
0.003535	0.000012	0.003447	0.000041	0.004099	0.005041	0.001824	0.002089	0.000013	0.002296	0.000000	0.000035	0.000000	0.000000	0.000000	0.000000	0.000587	0.000
0.000031	0.000011	0.000000	0.007010	0.000000	0.000000	0.002805	0.002003	0.000000	0.002230	0.000303	0.000243	0.000000	0.000192	0.000143	0.000010	0.000000	0.000
0.000681	0.007225	0.000106	0.000380	0.000149	0.000315	0.005095	0.000258	0.000053	0.000072	0.000207	0.000008	0.000000	0.000806	0.000902	0.000000	0.000184	0.000
0.003338	0.001715	0.000112	0.001368	0.000037	0.000198	0.004414	0.000043	0.000022	0.000352	0.000072	0.000000	0.000010	0.000219	0.002968	0.000002	0.000225	0.003
0.005379	0.005599	0.000035	0.002036	0.000018	0.000088	0.005763	0.000006	0.000016	0.000341	0.000012	0.000022	0.000012	0.001357	0.006509	0.000016	0.000084	0.000
0.006325	0.000033	0.000791	0.000666	0.001482	0.002022	0.000184	0.001676	0.000251	0.000812	0.000562	0.000321	0.000000	0.000000	0.000000	0.000008	0.000734	0.000
0.000016	0.000198	0.000000	0.000000	0.000000	0.000000	0.000057	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000020	0.000112	0.000000	0.000000	0.000
0.002449	0.000374	0.000012	0.000206	0.000004	0.000016	0.000319	0.000008	0.000016	0.000002	0.000012	0.000002	0.000000	0.000000	0.000000	0.000010	0.000000	0.000
0.000325	0.000491	0.000000	0.000039	0.000002	0.000004	0.000738	0.000000	0.000000	0.000000	0.000002	0.000000	0.000000	0.000133	0.000000	0.000000	0.000000	0.000
0.000431	0.002468	0.000002	0.000002	0.000000	0.000004	0.003792	0.000000	0.000000	0.000000	0.000151	0.000000	0.000000	0.000000	0.000229	0.000000	0.000000	0.000
0.000059	0.000906	0.000000	0.000004	0.000000	0.000000	0.002151	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000638	0.000000	0.000000	0.000
0.000006	0.000325	0.000000	0.000000	0.000000	0.000000	0.001366	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000033	0.000000	0.000000	0.000
0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000037	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000
0.004048	0.000006	0.000159	0.000816	0.000104	0.000200	0.000675	0.000018	0.000063	0.000170	0.000417	0.000004	0.000000	0.000000	0.000000	0.000002	0.000000	0.000
0.011117	0.000008	0.000090	0.000108	0.000129	0.000055	0.000450	0.000004	0.000168	0.000088	0.000278	0.000029	0.000000	0.000000	0.000000	0.000008	0.000364	0.000
0.000010	0.000000	0.000000	0.000000	0.000004	0.000004	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000000	0.000008	0.000000	0.000
0.002602	0.000000	0.000335	0.000022	0.000002	0.000327	0.000002	0.000016	0.000016	0.000110	0.000063	0.000162	0.000000	0.000000	0.000000	0.000000	0.000045	0.000
0.010490	0.000025	0.000051	0.000333	0.000084	0.000527	0.000100			0.000168	0.000016	0.000125	0.000000	0.000000	0.000000	0.000006	0.000125	0.000

[33 rows x 33 co	lumns]												
Bigram frequency	matrix wi	th overlapping											
2.159834e-02	0.002395	6.260161e-03	0.015523	2.657338e-03	0.007375	0.003878	5.774695e-05	9.787618e-07	0.000000	0.000000	2.731724e-03	4.110800e-05	2.546738e-03
a 1.567879e-02	0.000040	5.383190e-04	0.002684	6.714306e-04	0.001860	0.001193	2.378391e-04	0.000000e+00	0.000000	0.000000	1.957524e-05	8.466290e-04	1.928161e-03
6 4.052074e-04	0.000608	9.787618e-07	0.000049	0.000000e+00	0.000020	0.002103	1.624745e-04	1.301753e-04	0.003664	0.000053	8.808857e-06	7.830095e-06	6.029173e-04
в 5.124797е-03	0.005615	2.055400e-05	0.000055	3.719295e-05	0.000849	0.004937	1.957524e-06	3.915047e-06	0.002662	0.000152	1.566019e-05	9.787618e-07	1.849860e-04
г 9.366751e-04	0.000985	2.936286e-06	0.000016	9.787618e-07	0.001099	0.000178	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000e+00	0.00000e+00	0.000000e+00
д 7.810520е-04	0.005102	3.034162e-05	0.000898	8.808857e-06	0.000042	0.004193	1.957524e-06	0.000000e+00	0.000422	0.001053	9.787618e-07	1.076638e-05	4.238039e-04
e 1.721740e-02	0.000019	1.379075e-03	0.001221	3.292555e-03	0.002745	0.001743	9.356963e-04	0.000000e+00	0.000000	0.000000	1.468143e-05	2.280515e-04	2.172851e-04
ж 6.567492e-04	0.001204	2.446905e-05	0.000006	4.893809e-06	0.000699	0.004359	0.000000e+00	0.000000e+00	0.000000	0.000049	2.936286e-06	0.000000e+00	0.000000e+00
	0.004441	1.184302e-04	0.000865	3.415879e-04	0.000688	0.000174	0.000000e+00	3.817171e-05	0.000255	0.000103	9.787618e-07	1.957524e-06	4.189101e-04
и 1.584420е-02	0.000079	7.017722e-04	0.002549	5.539792e-04	0.001763	0.001667	1.282178e-04	0.000000e+00	0.000000	0.000000	1.272390e-05	2.985224e-04	1.095235e-03
й 5.469321е-03	0.000004	3.229914e-05	0.000028	2.349028e-05	0.000298	0.000005	9.787618e-07	0.000000e+00	0.000000	0.000000		0.000000e+00	1.957524e-06
Control of the last of the las	0.006789		0.000261		0.000021	0.000376	0.000000e+00	0.000000e+00	0.000000	0.000000			3.915047e-06
	0.005364		0.000050	1.321328e-04	0.000035	0.003660	9.787618e-07	0.000000e+00	0.000593	0.004613	2.936286e-06	7.311351e-04	1.230304e-03
	0.002866	3.621419e-05	0.000055	9.298238e-05	0.000038	0.003880	0.000000e+00	0.000000e+00	0.000797	0.000078	6.851333e-06	4.893809e-06	3.406091e-04
	0.009930	2.349028e-05	0.000040	3.132038e-05	0.000291	0.010016	8.319476e-05	0.000000e+00	0.002453	0.001186	0.000000e+00	2.074975e-04	1.773516e-03
	0.000018	3.501031e-03	0.007910	4.091225e-03	0.004924	0.001714	2.251152e-04	0.000000e+00	0.000000	0.000000	1.566019e-05	5.715969e-04	6.195562e-04
	0.000785	0.000000e+00	0.000000	0.000000e+00	0.000000	0.002805	0.000000e+00	0.000000e+00	0.000215	0.000152	0.000000e+00	0.000000e+00	5.686606e-04
	0.007221	1.106001e-04	0.000361	1.507293e-04		0.005034	1.272390e-05	0.000000e+00	0.000804	0.000947	0.000000e+00	1.986887e-04	9.572291e-04
	0.001673	1.008125e-04	0.001344	3.425666e-05		0.004340	9.787618e-07	1.370267e-05	0.000197	0.003035	1.957524e-06	2.456692e-04	3.537245e-03
	0.005625	3.034162e-05	0.002087	1.957524e-05		0.005799	2.544781e-05	1.272390e-05	0.001376	0.006529	1.761771e-05	8.025847e-05	3.905260e-04
	0.000032	7.360289e-04	0.000688	1.441716e-03	0.001972		2.740533e-04	0.000000e+00	0.000000	0.000000	5.872571e-06	7.144961e-04	5.970447e-05
	0.000219	0.000000e+00	0.000000	0.000000e+00	0.000000	0.000047	0.000000e+00	0.000000e+00	0.000022	0.000105	0.000000e+00	0.000000e+00	0.000000e+00
	0.000401	8.808857e-06	0.000201	1.957524e-06		0.000317	9.787618e-07	0.000000e+00	0.000000	0.000000	5.872571e-06	0.000000e+00	2.936286e-06
	0.000505	0.000000e+00	0.000027	9.787618e-07	0.000002		0.000000e+00	0.000000e+00	0.000157	0.000000	0.000000e+00	0.000000e+00	9.787618e-07
	0.002482	1.957524e-06	0.000006	0.000000e+00	0.000003	0.003789	0.000000e+00	0.000000e+00	0.000000	0.000240	0.000000e+00	0.000000e+00	0.000000e+00
	0.000886	0.000000e+00	0.000007	0.000000e+00	0.000000	0.002102	0.000000e+00	0.000000e+00	0.000000	0.000618	0.000000e+00	0.000000e+00	0.000000e+00
7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7	0.000359	0.000000e+00	0.000000	0.000000e+00	0.000000	0.001344	0.000000e+00	0.000000e+00	0.000000	0.000038	0.000000e+00	0.000000e+00	0.000000e+00
ъ 9.787618е-07	0.000000	0.000000e+00	0.000000	0.000000e+00	0.000000	0.000031	0.000000e+00	0.000000e+00	0.000000	0.000000	0.000000e+00	0.000000e+00	1.673683e-04
	0.000004	1.634532e-04	0.000784	1.096213e-04	0.000179	0.000706	6.851333e-06	0.000000e+00	0.000000	0.000000	9.787618e-07	0.000000e+00	3.915047e-06
	0.000008	9.689742e-05	0.000098	1.389842e-04	0.000052	0.000419	2.936286e-05	0.000000e+00	0.000000	0.000000	1.174514e-05	3.151613e-04	4.531667e-04
	0.000000	0.000000e+00	0.000004	5.872571e-06	0.000006	0.000000	0.000000e+00	0.000000e+00	0.000000	0.000000	1.272390e-05	0.000000e+00	0.000000e+00
	0.000004	3.102675e-04	0.000018	2.936286e-06	0.000297	0.000003	1.624745e-04	0.000000e+00	0.000000	0.000000	2.936286e-06	3.621419e-05	0.000000e+00
я 1.054322е-02	0.000028	4.110800e-05	0.000322	7.634342e-05	0.000518	0.000089	 1.184302e-04	0.000000e+00	0.000000	0.000000	5.872571e-06	9.102485e-05	8.808857e-05

```
[33 rows x 33 columns]
Sorted letter frequency without spaces:
(letter, count, frequency)
o 96681 0.11474726902425476
e 73380 0.08709213393531112
a 67115 0.0796564263977706
н 54835 0.06508172750535277
и 54644 0.06485503634179805
T 54553 0.06474703165130864
c 44600 0.05293416698712015
в 38984 0.04626873465977335
л 38734 0.045972018477110126
p 35246 0.041832234296592746
к 27833 0.03303400604826267
д 26983 0.032025171027207686
м 26495 0.03144598103864906
y 24993 0.02966331021320838
п 23121 0.027441499437426117
ь 19362 0.0229800749149018
я 18000 0.021363565151752525
ч 15249 0.018098500277726345
6 14655 0.017393502627718514
г 14232 0.01689145884665233
ы 13912 0.016511662132843396
в 12975 0.015399569880221611
ж 9615 0.011411704385227806
й 8437 0.01001357773251867
x 7171 0.008511006983512075
ш 6937 0.008233280636539293
ю 4733 0.005617430770180261
э 2971 0.0035261751147698194
щ 2521 0.0029920859859760064
ц 2336 0.0027725160108052166
φ 1049 0.0012450211024549111
ъ 204 0.00024212040505319527
```

H1 (entropy of single letters without spaces): 4.450720785464344 H2 (entropy of bigrams without overlapping without spaces): 4.127474285221844 H2 (entropy of bigrams with overlapping without spaces): 4.127369564159534

Bigram frequency matrix with overlapping (no spaces):

8. 0.000315 0.001278 0.0005178 0.0005171 0.001371 0.

```
Enter a letter: a

Possible letters after 'a': , л, к, с, т, м, з, н, в, я, д, р, ж, е, ч, х, п, ш, й, ю, г, б, щ, и, о, у, ф, ц, а, э

Enter a letter: т

Possible letters after 'т': о, ь, е, а, , и, р, в, у, ы, н, с, я, к, ч, л, п, т, д, ю, ц, м, б, щ, г, х, э, з, ъ, ш, ж

Enter a letter: в

Possible letters after 'в': о, а, , е, с, и, ы, н, д, ш, у, з, р, л, п, т, ч, я, ь, к, м, х, в, г, б, ц, э, ж, ъ, й, щ, ф, ю

Enter a letter: 0

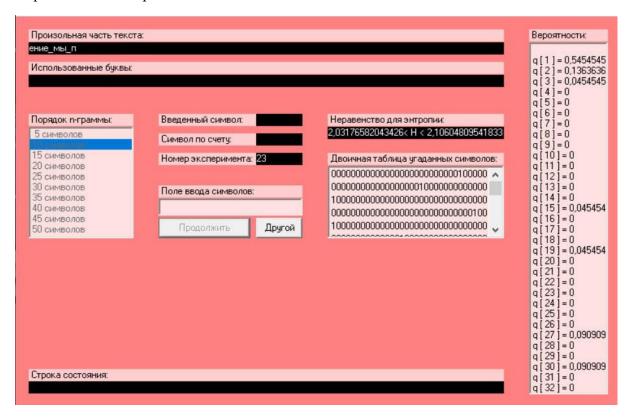
Possible letters after 'o': , в, т, н, с, л, м, д, р, г, б, й, ч, ж, е, п, к, ш, з, и, я, ю, х, о, щ, ф, у, ц, а, э

Enter a letter:
```

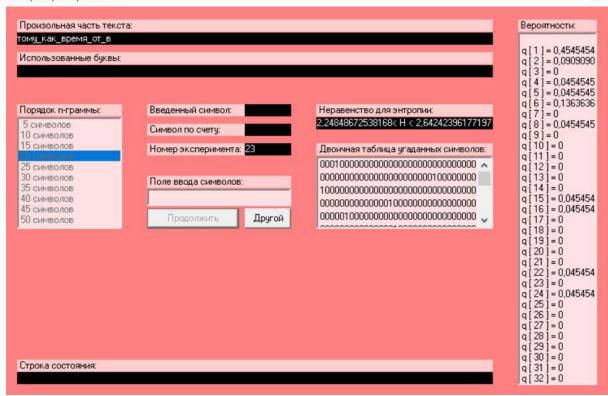
CoolPinkProgram

H1

Нерівність для ентропії: 2.03176582043426 < H < 2.10604809541833



Лабороторная работа №1



H3

Лабороторная работа №1 X Произольная часть текста: Вероятности: делающий_их_не_просто_заявляет_что_ему_не_нравится_поведение_другого_челов q[1]=0,6086956 q[2]=0,1304347 q[3]=0,0434782 q[4]=0 q[5]=0 Использованные буквы: q[5] = 0 q[6] = 0,0434782 q[7] = 0 q[8] = 0 q[9] = 0 q[10] = 0 q[11] = 0 q[12] = 0 q[13] = 0 q[14] = 0,043478 q[15] = 0,043478 q[16] = 0 q[17] = 0 Порядок п-граммы: Введенный символ: Неравенство для энтропии: 1,54239602903911< H < 1,9993073294931 5 символов Символ по счету: 10 символов 15 символов Номер эксперимента: 23 Двоичная таблица угаданных символов: 20 символов 5 символо Поле ввода символов: 35 символов 40 символов 45 символов 0000000000000000000000100000000 Продолжить Другой 50 символов q[18] = 0 q[19] = 0 q[20] = 0 q[21] = 0 q[22] = 0 q[23] = 0 q[24] = 0,043478 q[25] = 0 q[26] = 0 q[27] = 0 q[28] = 0 q[29] = 0 q[30] = 0,043478 q[31] = 0 q[32] = 0 q[18]=0 Строка состояния: Вы угадали. Для продолжения опыта нажмите "Продолжить", или "Другой" для выбора другого порядка

Модель	Ентропія	Надлишковість
H10	2.0689	58.99%
H20	2.4455	51.52%
Н30	1.7709	64.89%
H(30) до R = 64. <u>8</u> 9%		

Висновки

Під час виконання лабораторної роботи ми навчалися визначати частоту літер і біграм у тексті, а також обчислювати значення його ентропії та надлишковості. На практиці використовували частоту біграм для прогнозування наступної літери.