МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ 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:

Орлов Дмитро ФБ-14

Макуха Андрій ФБ-14

Перевірила

Селюх П. В.

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:

- 1. Написати програми для підрахунку частот букв і частот біграм в тексті, а також підрахунку H(1) та H(2) за безпосереднім означенням. Підрахувати частоти букв та біграм, а також значення H(1) та H(2) на довільно обраному тексті російською мовою достатньої довжини (щонайменше 1Мб), де імовірності замінити відповідними частотами. Також одержати значення H(1) та H(2) на тому ж тексті, в якому вилучено всі пробіли.
- 2. За допомогою програми CoolPinkProgram оцінити значення H(10), H(20), H(30)
- 3. Використовуючи отримані значення ентропії, оцінити надлишковість російської мови в різних моделях джерела

Хід роботи:

При обрахуванні будь-якого з варіантів значень ентропії та частоти літер необхідно очистити текст від зайвих символів, а також для зручності відображення замінити пробіл на нижнє підкреслення.

Наступним етапом ϵ обрахування ентропії для окремих літер (монограм), тому завдяки через проходження тексту рахуємо кількість літер та відповідно їх частоту для випадку з пробілом та без:

	Letter	Frequency		Letter	Frequency
0	_	0,1648470828	0	О	0,11446910168
1	О	0,0955992042	1	е	0,07871920031
2	е	0,0657425697	2	а	0,07678398187
3	a	0,0641263664	3	и	0,06957643604
4	И	0,0581069635	4	н	0,06737201399
5	н	0,0562659340	5	т	0,05542377558
6	Т	0,0462873278	6	Л	0,05317702592
7	Л	0,0444109483	7	С	0,05216624254
8	С	0,0435667896	8	р	0,04763888112
9	р	0,0397857505	9	В	0,04134222551
10	В	0,0345270802	10	Д	0,03460536273
11	Д	0,0289007696	11	м	0,03145618838
12	м	0,0262707274	12	к	0,03122253996
13	К	0,0260755953	13	у	0,02836288647
14	У	0,0236873473	14	'n	0,02826468641
15	П	0,0236053353	15	ь	0,02190877214
16	ь	0,0182971749	16	ы	0,02021736075
17	Ы	0,0168845878	17	Я	0,01996339508
18 19	Я	0,0166724876	18	Г	0,01977038116
20	Г	0,0165112915	19	6	0.01962816039
21	б	0,0163925154	20	3	0,01833632166
22	3	0,0153136325	21	4	0.01326039439
23	4	0,0110744570	22	x	0,01047693060
24	х	0,0087498391	23	й	0,01041089952
25		0,0086946931	24	ж	0,00920710223
26	ж	0,0076893382	25	ш	0.00799483941
27	Ш	0,0066769134	26	ю	0.00486090300
28	ю	0,0040595973	27	Э	0.00418704741
29	ф	0,0034968248	28	ф	0,00329816755
30	 	0,0027344742	29	ц	0,00329810733
31	ц	0,0024900360	30	<u> </u>	0,00298133701
	Щ	0,0024363239	30	Щ	0,00291721904

H1 entropy:4.472479351355553 Redundancy:0.09723412817157906

H1 entropy:4.380984409948693 З пробілами: Redundancy:0.12380311801026134

Наступним кроком рахуємо ті ж значення для 4 можливих випадків біграм (повні результати збережено в репозиторії):

3 перетином та пробілами

	_	а	б	В	Г	Д	е	ж	3	И	й	К	Л
_	0	0,00275023	0,0065652	0,01477067	0,0047948	0,00698376	0,00313060	0,00147763	0,00589780	0,01106174	0,0000212	0,00778974	0,00264418
а	0,01512134	0,00000424	0,00052742	0,00297930	0,00128674	0,00284780	0,00096570	0,00110575	0,00339502	0,00016263	0,00073386	0,00370893	0,00919520
6	0,0003322	0,00067872	0,00096570	0,00002262	0,00000424	0,00001555	0,00210403	0,00001414	0	0,00244056	0	0,00010463	0,00069710
В	0,00524312	0,00476803	0,00000848	0,00006504	0,0000155	0,00047793	0,00544532	0	0,0003747	0,00236986	0	0,00014422	0,00064619
Г	0,00091344	0,00113263	0,0000056!	0,00000707	0	0,00099263	0,00020644	0	0,0000014	0,00092900	0	0,00010322	0,0018085
Д	0,00153560	0,00561359	0,00002680	0,00080739	0,0000480	0,00005514	0,00414444	0,00003535	0,00002403	0,00227373	0	0,00023613	0,00050762
е	0,0173795	0,00005514	0,00124850	0,00181275	0,00277710	0,00270640	0,00088799	0,00072823	0,0012174	0,00012443	0,0015610	0,00094455	0,0049490
ж	0,0003775	0,00095162	0,00004242	0	0,00002262	0,00071124	0,00267670	0,00001414	0	0,00139986	0	0,00011453	0,00000848
3	0,0015129	0,00576489	0,00013574	0,00100535	0,0003492	0,00109726	0,0007041	0,00005938	0,0000127	0,00029835	0	0,00019654	0,0004397!
И	0,0204846	0,00005090	0,00054863	0,00183396	0,00065044	0,00139703	0,00155683	0,00019089	0,0020361	0,00041147	0,0011057	0,00228644	0,00610000
й	0,0069781	0,00001272	0,00000989	0,00000141	0,00001272	0,00023472	0,0000056	0	0	0	0	0,00011170	0,00002262
К	0,0041119	0,00591477	0	0,00009898	0	0	0,00036622	0,00000707	0,0000070	0,00295950	0	0,00000989	0,00082719
Л	0,0081404	0,00428584	0,00003252	0,00005514	0,0002036	0,00012160	0,00389840	0,00014564	0,00008059	0,00842323	0	0,00048783	0,0001696
M	0,0084430	0,00217473	0,00009750	0,00000282	0,0001428	0	0,00335684	0	0,00000282	0,00270640	0	0,00016119	0,00036764
н	0,00396062	0,00971420	0,00001838	0,00001272	0,00010463	0,00127684	0,00960390	0,00003110	0,0000212	0,00785763	0	0,00028845	0,00000282
0	0,02286018	0,00000282	0,00425473	0,00544249	0,00440603	0,00630645	0,0016515!	0,00176467	0,0012810	0,00069286	0,00329038	0,00216342	0,0058454
п	0,0000678	0,00149035	0	0	0	0	0,00223129	0	0	0,00113827	0	0,00010322	0,00080450
р	0,0012089	0,00785478	0,00023189	0,00032097	0,00013150	0,00037329	0,0058242	0,00022058	0,00005373	0,00418544	0	0,00049490	0,0002813
С	0,00270640	0,00151863	0,00004242	0,00131360	0,00007070	0,00015836	0,0033200	0,00001696	0,00001414	0,00134473	0	0,00362833	0,0027417!
Т	0,0052897	0,00505930	0,00004242	0,00189052	0,00001414	0,00015978	0,0043395	0,00000143	0,00000989	0,00309242	0	0,00048924	0,00024320
у	0,00595012	0	0,0005429	0,00057125	0,00112978	0,00190749	0,00015978	0,00131078	0,00035208	0,00015412	0,00016820	0,00055004	0,0018028
ф	0,0005882	0,00018664	0	0	0	0	0,00005650	0	0	0,00013715	0	0	0,00001979
х	0,0037414	0,00038178	0	0,00022341	0	0	0,00003110	0	0	0,00019513	0	0	0,00022624

Без перетину та пробілів

	а	6	В	г	А	е	ж	3	И	й
а	0.00029798	0.0012732	0.0052283	0.00236019		0,00154072	0.00143230	0.00477794	0.00150680	0.00092783
6						0,0025125				
В			_			0,00656248				
г						0,00023364				
Д		-	-	-	-	0,00493032	-	-	-	
е		-	-	-	-	0,0013138!	-	-	-	-
ж		-	-	-	-	0,0031356	-			
3		-	-	-		0,00085332	-	-	-	
И						0,0023872				
й		-	-	-	-	0,00008804	-	-	-	-
К						0,0005214				
Л						0,00509280				
M	0,0027360	0,00049438	0,0008804:	0,00043682	0,00055872	0,00423954	0,00007788	0,00031830	0,00391440	0
н						0,01157069				
0	0,00032169	0,00631529	0,0093696!	0,00587169	0,0086280	0,0024482	0,00240082	0,00255659	0,00250579	0,0038907
П	0,00184210	0	0,0000101!	0,00000338	0	0,00257013	0	0,00000338	0,00136464	0
р	0,00962023	0,00033523	0,0004977	0,0001760	0,0004740	0,00712459	0,0003047!	0,00011174	0,00496080	0
С	0,00186919	0,0001828!	0,00194030	0,0002167	0,00031830	0,00404314	0,00006433	0,00011174	0,00178114	0
T	0,00630513	0,00026753	0,0027868!	0,00018962	0,0004740	0,00550259	0,0001049	0,00021673	0,00424633	0
у	0,00017940	0,00091089	0,0011208	0,00152379	0,0025125	0,0002505	0,00156104	0,00055533	0,00088380	0,00019978
ф	0,0002505	0,0000101!	0,0000778	0,00001354	0,00002370	0,0000711:	0,00000338	0,00001693	0,00022349	0
X	0,0004977	0,0001930	0,00063999	0,00014899	0,00022349	0,0000778	0,00003724	0,0001828	0,0005959	0
ц	0,0008668	0,00001693	0,00013883	0,00000338	0,00001693	0,00056549	0	0,00001693	0,00009483	0
ч	0,00217394	0,0000067	0,0000203	0	0,0000067	0,0037790	0	0	0,00174390	0
Ш	0,0010666!	0,00000338	0,00003724	0,00000338	0,0000067	0,0022213!	0	0,0000067	0,00180140	0
щ	0,00043682	0	0,0000101!	0	0	0,0014526	0	0	0,0007754	0
ы	0,0001083	0,0004232	0,0016490	0,00028444	0,00030814	0,0020215	0,0001049	0,0002912	0,00051809	0,0020588

3 перетином та без пробілів:

	а	б	В	Г	Д	е	ж	3	И	й
а	0,00028105	0,00124443	0,00513688	0,00216379	0,00417858	0,0015779	0,00144929	0,00472038	0,00147469	0,00088380
б	0,00082285	0,0011614	0,00004571	0,00001354	0,00002370	0,00252780	0,00002033	0,0000118	0,00296124	0
В	0,00580227	0,00022518	0,00026751	0,00029968	0,00087702	0,0066132	0,00004063	0,00064846	0,0031068	0,00000169
Г	0,00136972	0,00003210	0,00011851	0,00001354	0,00126644	0,00026073	0,00000338	0,0000457	0,00120549	0
А	0,00678258	0,0000795	0,00112083	0,0001286	0,00013375	0,00498283	0,00004740	0,0001286	0,00285288	0,00000169
е	0,00032338	0,0024634	0,00404314	0,0038196	0,00410070	0,0013341	0,00115808	0,00245163	0,00144593	0,0018708
ж	0,00113946	0,00007113	0,00004232	0,00003894	0,00086856	0,00321859	0,00001693	0,00000846	0,0016998	0
3	0,00692142	0,00020480	0,00132062	0,00048592	0,00141035	0,0008702	0,00007957	0,00012359	0,00041142	0
И	0,00041819	0,00158130	0,00471191	0,00146963	0,00270558	0,00235849	0,00038602	0,00338452	0,00184718	0,00132908
й	0,00015237	0,00027428	0,00069756	0,0003047	0,00071787	0,00008634	0,00008465	0,00024550	0,00065184	0
К	0,00716353	0,00029290	0,00055195	0,00009989	0,00021673	0,0004977	0,00009650	0,00019640	0,00385183	0
Л	0,00532990	0,0004977	0,00080422	0,00088380	0,00038602	0,00506239	0,00020486	0,00028444	0,01073599	0
M	0,00280547	0,00050454	0,00094983	0,00044528	0,00048930	0,0041582	0,00008465	0,00033184	0,00400589	0
н	0,01174847	0,0002776	0,00044020	0,00022687	0,00171173	0,0115808	0,00007449	0,00020486	0,00977092	0
0	0,00030645	0,00631359	0,00914616	0,0058310	0,00859759	0,00250410	0,00245331	0,0025650	0,0024279	0,00394494
П	0,00178453	0,00000169	0,00000677	0,00000338	0,00000169	0,00267510	0	0,00000338	0,0013714	0
р	0,00944076	0,0003301!	0,00050285	0,00018454	0,00049100	0,00700269	0,00027089	0,0001083	0,00513013	0
С	0,00186580	0,00018962	0,00187088	0,00022010	0,00033354	0,0040346	0,00006433	0,00009820	0,00174390	0
т	0,00621539	0,00028952	0,00281902	0,00019470	0,00044528	0,0053620	0,00009483	0,0002031	0,00421414	0
У	0,00020147	0,00092274	0,00124443	0,00149840	0,00257690	0,00026243	0,00164062	0,00059089	0,0008076	0,0002014
ф	0,00024211	0,00000840	0,00006941	0,00000846	0,00002033	0,0000812	0,00000169	0,00001693	0,00022518	0
х	0,00052317	0,00018793	0,00066200	0,00017439	0,00021502	0,0000795	0,00003216	0,0001794	0,00056549	0
ц	0,00085163	0,00001523	0,00013036	0,00000846	0,00002539	0,00064338	0	0,0000101	0,00009312	0
Ч	0,00215532	0,00000840	0,00002033	0,00000169	0,00000338	0,0037891	0	0	0,0017151	0
Ш	0,00105988	0,0000050	0,00003216	0,00000338	0,00000507	0,00208929	0	0,00000338	0,0017557	0
щ	0,00043174	0	0,00000677	0	0,00000169	0,0014306	0,00000169	0	0,0007483	0
ы	0,00009483	0,0004385	0,0015830	0,00028274	0,0003047	0,0021180	0,00007618	0,0002912	0,00054348	0,0021079:

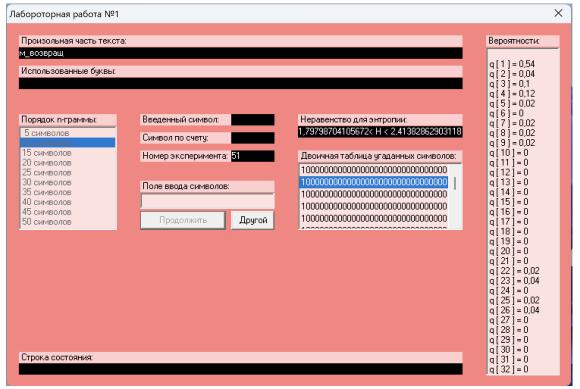
Без перетину та з пробілами:

		а	6	В	Г	Д	е	ж	3	И	й
	- 0	0.0028647	0,00649593	0.01471128	0.00476801		0.00315605	0.00145642	0.00604062	0.0110348	0.0000169
а		•	0,00053166	•						-	-
6		-	0,00091910	-			0,00211534		-	0,0024999!	-
В	0,00525160	0,00486699	0,00001133	0,00006504	0,00001696	0,0005062	0,00545522	0	0,00037612	0,00240380	0
Г	0,00090779	0,00117079	0,00000565	0,00000282	0	0,0010067	0,00020078	0	0,00000282	0,00095586	0
д	0,0014903	0,00566160	0,00003676	0,00076350	0,00005373	0,00007070	0,00414020	0,00004242	0,00003110	0,00240663	0
е	0,01750535	0,00005090	0,00126413	0,00175053	0,00277993	0,0027686	0,00089082	0,0007550	0,00119907	0,00013574	0,0014818
ж	0,00034784	0,00090779	0,00005090	0	0,00002262	0,0006617!	0,00265266	0,00001414	0	0,00138289	0
3	0,0015101	0,00568429	0,00013574	0,00099263	0,00035632	0,00108312	0,00068154	0,0000678	0,00001133	0,00031673	0
И	0,02057940	0,0000480	0,00054580	0,00177598	0,00068437	0,00133764	0,00141117	0,00016402	0,00207575	0,00040440	0,0010293
й	0,00712940	0,00001414	0,00001414	0,00000282	0,00001696	0,00025169	0,00000565	0	0	0	0
к	0,00416282	0,00589350	0	0,00011029	0	0	0,00041288	0,0000056!	0,00001133	0,00303162	0
Л	0,00810506	0,0042985	0,00003676	0,00005938	0,00018664	0,0001385	0,00380084	0,00014988	0,00008203	0,00840200	0
M	0,00845856	0,00222564	0,00009898	0	0,00013857	0	0,00327483	0	0,00000565	0,0026611	0
н	0,00394789	0,00959542	0,00001696	0,00001979	0,00010746	0,0012782	0,00952189	0,00002828	0,00002262	0,00792690	0
0	0,02280221	0,0000056	0,00439189	0,0054297	0,00436926	0,0062781	0,00167700	0,00178164	0,00134613	0,0007041	0,0032550
п	0,00005938	0,00151298	0	0	0	0	0,00218039	0	0	0,0011170	0
р	0,00123583	0,00785620	0,00024603	0,00032804	0,00013857	0,00032804	0,00578610	0,0002177!	0,00005656	0,00431270	0
С	0,00273468	0,00155540	0,00004242	0,00138000	0,00007070	0,00014422	0,00341340	0,00001979	0,00001133	0,0012952	0
T	0,00533927	0,00499143	0,00004807	0,0018636!	0,00001696	0,00015830	0,00417696	0	0,00000282	0,0029354	0
y	0,00583134	0	0,00055146	0,00053449	0,00113403	0,00185234	0,00014988	0,0013404	0,00032522	0,00015554	0,0001187
ф	0,00054297	0,0001979	0	0	0	0	0,00007070	0	0	0,0001470	0
X	0,00364247	0,0004213	0	0,00024038	0	0	0,00004524	0	0	0,0001781	0
ц	0,00031950	0,00063630	0	0,00009049	0	0	0,00055713	0	0	0,00004242	0
ч	0,00008766	0,00178729	0	0,0000113	0	0	0,00321263	0	0	0,00144793	0
ш	0,00006221	0,00083708	0	0,00001979	0	0	0,00181840	0	0	0,00142814	0
щ	0,00005373	0,00031673	0	0	0	0	0,00119341	0	0	0,0006221	0
ы	0,0049235	0	0,00022343	0,00081440	0,00011594	0,00005090	0,00166003	0,00001690	0,00005938	0,0000056	0,00179863

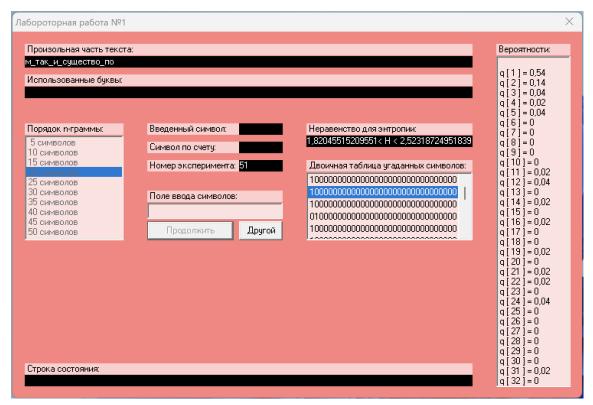
Ентропія для біграм та надлишковість

```
Bigram entropy ( without intersection with spaces): 3.976958387342564
Bigram reduancy:0.2046083225314872
Bigram entropy ( without intersection without spaces): 4.1563698389408525
Bigram reduancy:0.16104054451239935
Bigram entropy ( with intersection with spaces): 3.9771460295440533
Bigram reduancy:0.2045707940911894
Bigram entropy ( with intersection without spaces): 4.157481800042511
Bigram reduancy:0.16081609617971482
```

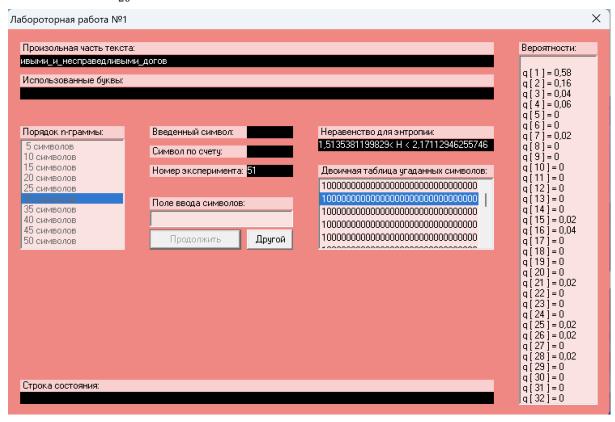
Далі обрахуємо H(10), H(20), H(30) за допомогою CoolPinkProgmar:



1,797987041<H₁₀<2,41382862



1,8204551520<H₂₀<2,52318724



1,51353811<H₃₀<2,17112946

Останнім кроком обрахуємо надлишковість рос мови за формулою

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

H(10):

$$R1 = 1 - \frac{1,797987041}{5} = 0,6404025918$$

$$R2 = 1 - \frac{2,41382862}{5} = 0,517234276$$

H(20):

$$R1 = 1 - \frac{1,8204551520}{5} = 0,6359089696$$

$$R2 = 1 - \frac{2,52318724}{5} = 0,495362552$$

$$R2 = 1 - \frac{2,52318724}{5} = 0,495362552$$

H(30):

$$R1 = 1 - \frac{1,51353811}{5} = 0,697292378$$

$$R2 = 1 - \frac{2,17112946}{5} = 0,565774108$$

Висновки:

Практично змогли порахувати ентропію на символ джерела та надлишковість. Також засвоїли поняття частот монограм та біграм, та знайшли їх на практиці.

За допомогою наведеної програми CoolPinkProgram змогли також обрахувати значення H10, H20, H30.