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

Фізико-технічний інститут

Криптографія

Лабораторна робота No 1

Виконали: студенти групи ФБ-13

Клименко Д. О. Стягайло Д. А.

Київ 2023

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.

Letters with spaces count:

	0		0
	173034	**ь**	19477
о	96341	**я**	17896
е	72144	**ч**	15201
а	66806	**б**	14598
н	54575	**г**	14150
и	54412	**ы**	13848
т	54321	**з**	12918
с	44418	**ж**	9580
в	38802	**й**	8372
л	38580	**х**	7147
р	35006	**ш**	6900
к	27691	**ю**	4729
д	26876	**э**	2969
м	26396	**щ**	2512
у	24911	**ц**	2311
п	23038	**ф**	988

Letters without spaces count:

	0		0

о	96341	**я**	17896
е	72144	**ч**	15201
а	66806	**б**	14598
н	54575	**г**	14150
и	54412	**ы**	13848
т	54321	**з**	12918
с	44418	**ж**	9580
в	38802	**й**	8372
л	38580	**х**	7147
р	35006	**ш**	6900
к	27691	**ю**	4729
д	26876	**э**	2969
м	26396	**щ**	2512
у	24911	**ц**	2311
п	23038	**ф**	988
ь	19477		0

Crossed bgram with spaces:

	0		
о	24772	**но**	9716
е	18726	**ст**	9441
и	17827	**по**	9161
а	17454	**ко**	8662
в	16997	**к**	8269
н	16496	**д**	8192
с	16485	**ов**	7803
п	16204	**м**	7679
то	14828	**го**	7632
ь	12261	**ни**	7577

и	11811	**ра**	7347
я	11683	**ро**	7157
о	11634	**ал**	7153
т	10515	**л**	7087
не	10206	**у**	7079
на	10100	**б**	6970

Unrossed bgram with spaces:

	0		
о	12418	**но**	4958
е	9310	**ст**	4729
и	8835	**по**	4613
а	8780	**ко**	4291
в	8556	**д**	4237
с	8314	**к**	4029
н	8200	**ов**	3888
п	8185	**го**	3874
то	7375	**м**	3841
ь	6145	**ни**	3772
о	5885	**ра**	3692
и	5856	**ро**	3613
я	5822	**ал**	3583
т	5280	**у**	3489
не	5182	**ка**	3488
на	5038	**л**	3483

Crossed bgram without spaces:

	0		
то	15206	ро	7206
ов	10558	ка	6942
не	10288	пр	6725
на	10150	ть	6656
но	9990	ет	6607
ст	9786	во	6579
по	9163	ак	6466
ко	8958	ер	6351
он	8726	ло	6289
от	8184	ас	6273
ен	8005	ес	6220
ос	7867	ол	6166
ни	7844	те	6035
го	7754	ом	6033
ал	7423	од	6010
ра	7364	ел	5907

Unrossed bgram without spaces:

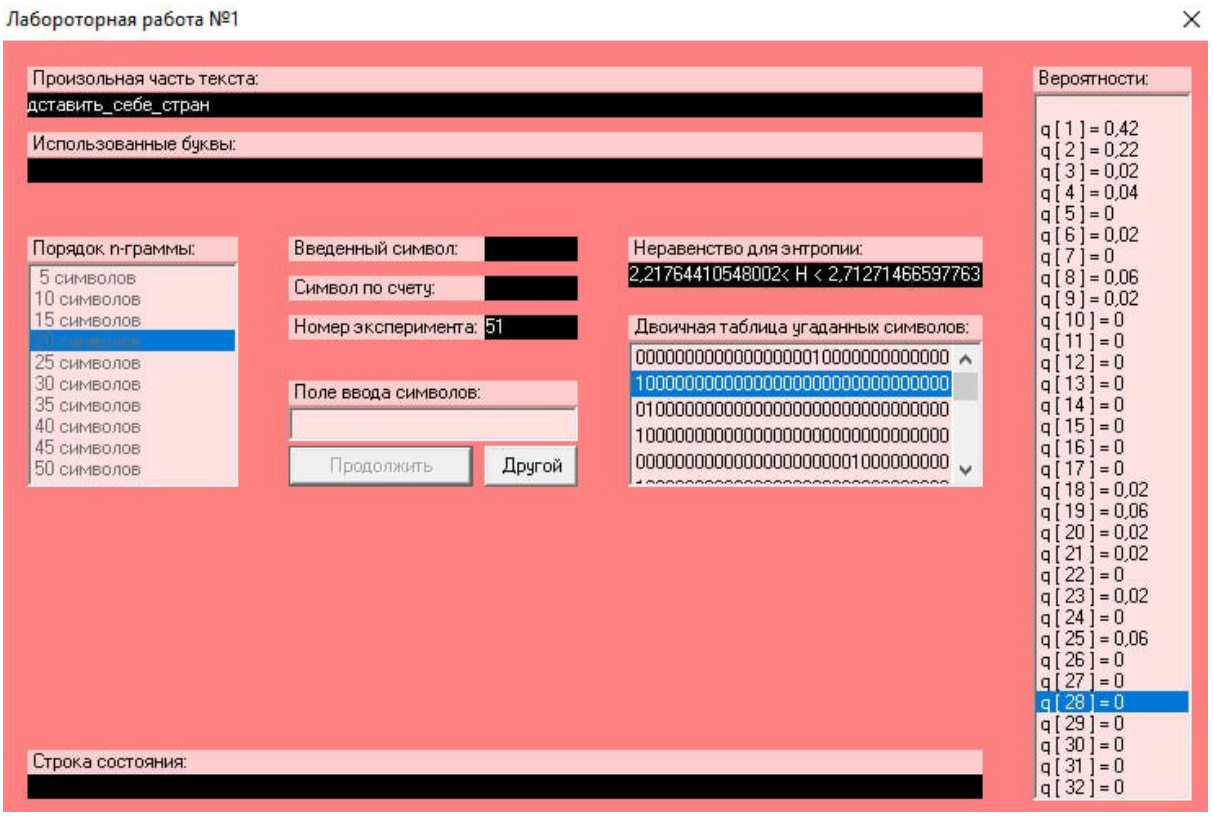
	0		
то	7625	ро	3611
ов	5329	ка	3487
на	5106	ет	3379
не	5082	пр	3355
ст	4954	ть	3340

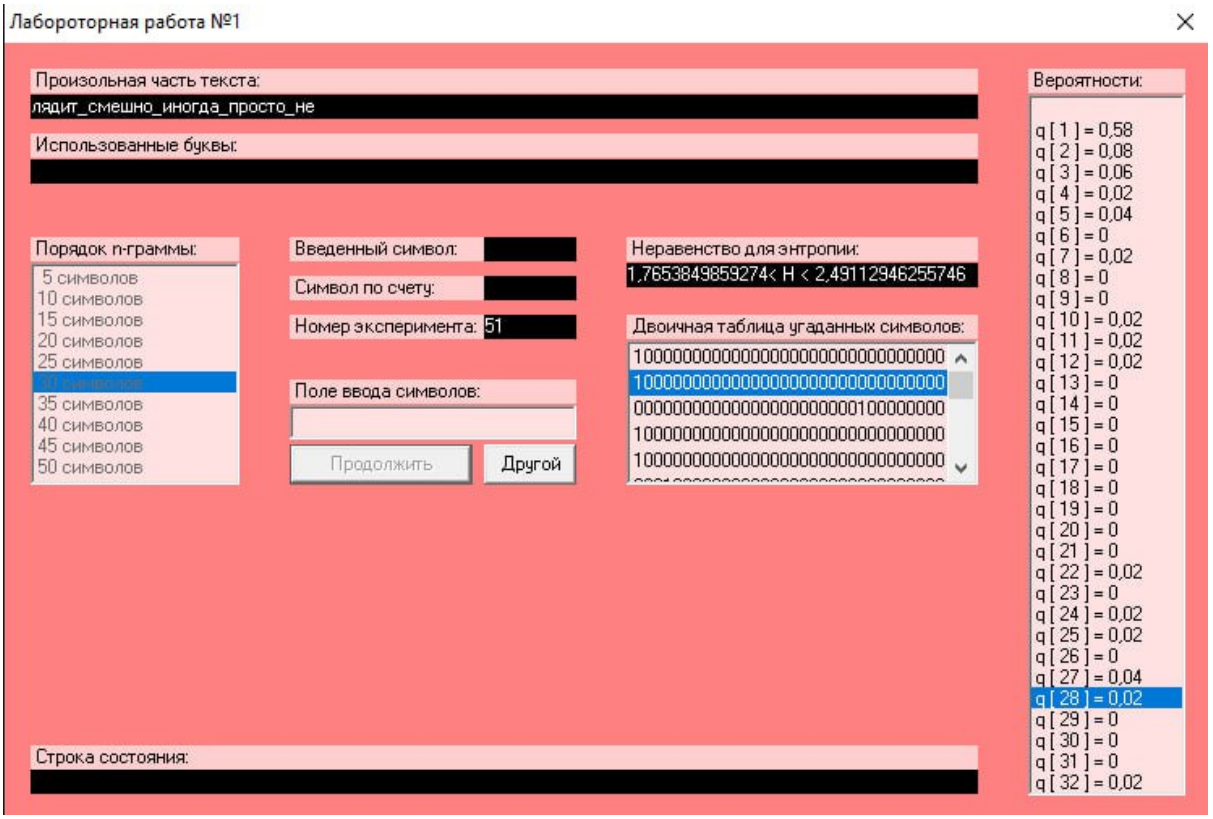
но	4952	**во**	3224
по	4634	**ак**	3221
ко	4509	**ер**	3167
он	4365	**ло**	3137
ен	4030	**ас**	3125
от	4020	**од**	3087
ни	3918	**ес**	3053
ос	3870	**ом**	3033
го	3813	**те**	3020
ал	3707	**ол**	3018
ра	3639	**ли**	2960

	Entropy	R
with space	4,348109	0,130378
without space	4,4493	0,11014
crossed b-gram w spaces	3,935584	0,212883
uncrossed b-gram w spaces	3,934698	0,21306
crossed b-gram w/o spaces	4,12658	0,174684
uncrossed b-gram w/o spaces	4,125616	0,174877

Cool Pink Program

H(10)	2.5365443<H<3.0030177	0.409722<R<0.501412
H(20)	2.2176441<H<2.7127147	0.466784<R<0.564096
H(30)	1.7653850<H<2.4911295	0.510339<R<0.652993


Лабороторная работа №1
Произольная часть текста:
дставить_себе_стран
Использованные буквы:
Порядок n-граммы:
5 символов
10 символов
15 символов
20 символов
25 символов
30 символов
35 символов
40 символов
45 символов
50 символов
Введенный символ:
Символ по счету:
Номер эксперимента: 51
Поле ввода символов:
Продолжить
Другой
Неравенство для энтропии:
2,21764410548002< H < 2,71271466597763
Двоичная таблица угаданных символов:
Вероятности:
q [1] = 0,42
q [2] = 0,22
q [3] = 0,02
q [4] = 0,04
q [5] = 0
q [6] = 0,02
q [7] = 0
q [8] = 0,06
q [9] = 0,02
q [10] = 0
q [11] = 0
q [12] = 0
q [13] = 0
q [14] = 0
q [15] = 0
q [16] = 0
q [17] = 0
q [18] = 0,02
q [19] = 0,06
q [20] = 0,02
q [21] = 0,02
q [22] = 0
q [23] = 0,02
q [24] = 0
q [25] = 0,06
q [26] = 0
q [27] = 0
q [28] = 0
q [29] = 0
q [30] = 0
q [31] = 0
q [32] = 0
Строка состояния:


Лабороторная работа №1
Произольная часть текста:
лядит_смешно_иногда_просто_не
Использованные буквы:
Порядок n-граммы:
5 символов
10 символов
15 символов
20 символов
25 символов
30 символов
35 символов
40 символов
45 символов
50 символов
Введенный символ:
Символ по счету:
Номер эксперимента: 51
Поле ввода символов:
Продолжить
Другой
Неравенство для энтропии:
1,7653849859274< H < 2,49112946255746
Двоичная таблица угаданных символов:
Вероятности:
q [1] = 0,58
q [2] = 0,08
q [3] = 0,06
q [4] = 0,02
q [5] = 0,04
q [6] = 0
q [7] = 0,02
q [8] = 0
q [9] = 0
q [10] = 0,02
q [11] = 0,02
q [12] = 0,02
q [13] = 0
q [14] = 0
q [15] = 0
q [16] = 0
q [17] = 0
q [18] = 0
q [19] = 0
q [20] = 0
q [21] = 0
q [22] = 0,02
q [23] = 0
q [24] = 0,02
q [25] = 0,02
q [26] = 0
q [27] = 0,04
q [28] = 0,02
q [29] = 0
q [30] = 0
q [31] = 0
q [32] = 0,02
Строка состояния:

Висновки: При виконанні лабораторної роботи ми засвоїли поняття ентропії на символ джерела та надлишковості та навчилися їх вимірювати, набули навичок щодо їх оцінки. Також, враховуючи отримані дані, можна зробити висновок: при визначенні надлишковості, чим більше n, тим більше R прямує до теоретичного значення, 0,74.