Міністерство освіти і науки, молоді та спорту України
Національний технічний університет України
“Київський політехнічний інститут”
Фізико-Технічний інститут

Лабораторна робота №1
з Симетричної криптографії

Студент групи ФІ-93
Карловський Володимир Олександрович

Задачі

1. Написати програми для підрахунку частот букв і частот біграм в тексті, а також підрахунку 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.
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.

№1

Для отримання детального результату треба запустити програму (інструкція в README.md) не розміщую результат тут бо в російському алфавіті 33 літери => 33*33 = 1089 біграм

Короткі результати ентропій:

```
statByLettersWithSpaces has entropy: 4.462151364016589
statByLettersWithoutSpaces has entropy: 4.462151364016587
statByBigramsWithIntersAndWithoutSpaces has entropy: 4.1453958533961
statByBigtamsWithIntersAndWithSpaces has entropy: 3.963214806411822
statByBigramsWithoutIntersAndWithoutSpaces has entropy: 4.145212314083568
statByBigtamsWithoutIntersAndWithSpaces has entropy: 3.90831788858674
```

Тобто

$H_1 = 4,46$ – ентропія літер з пробілами і без, очевидно, збігаються

$H_2 = 4,14$ – ентропія біграм з перетином і без пробілів

$H_2 = 3,96$ – ентропія біграм з перетином і з пробілами

$H_2 = 4,14$ – ентропія біграм без перетину і без пробілів

$H_2 = 3,90$ – ентропія біграм без перетину і з пробілами

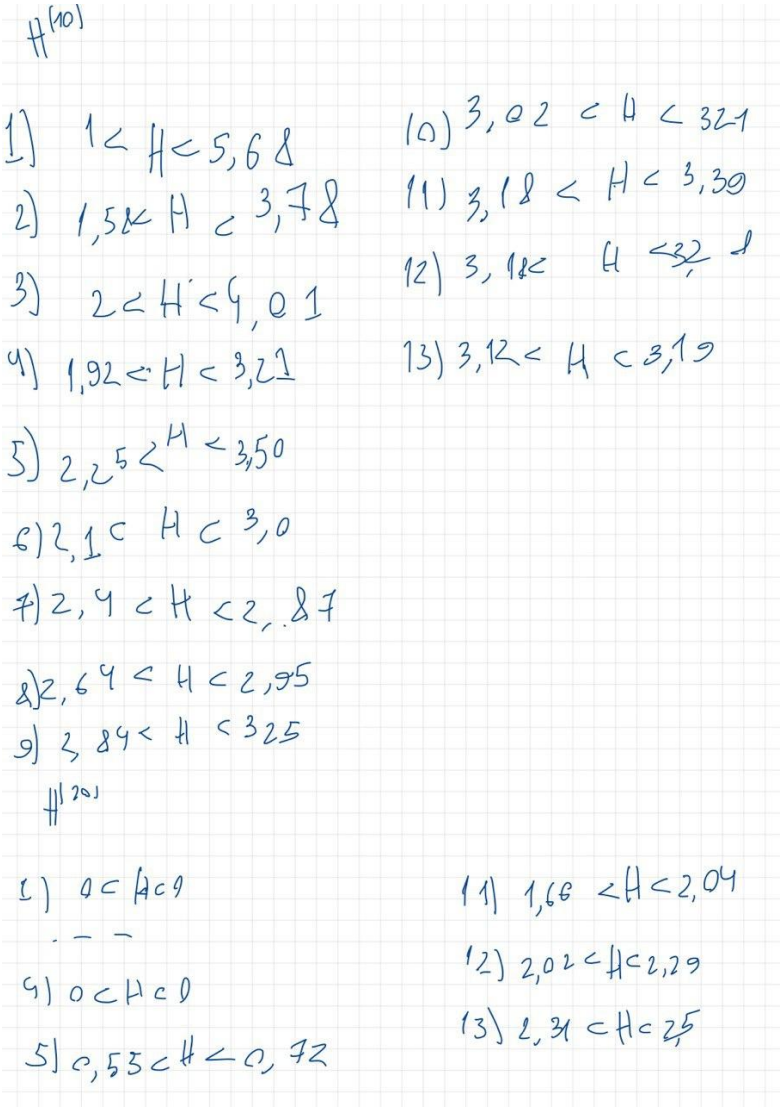
№2

Результати:

$H^{(10)} = 3,15$

$H^{(20)} = 2,53$

$H^{(30)} = 2,3$



6) $0,45 < H < 0,65$

7) $1,2 < H < 1,14$

8) $1,95 < H < 1,54$

9) $1,29 < H < 1,44$

10) $1,63 < H < 1,71$

14) $2,29 < H < 2,55$

15) $2,14 < H < 2,45$

16) $2,4 < H < 2,64$

17) $2,59 < H < 2,81$

18) $2,64 < H < 2,85$

19) $2,99 < H < 2,7$

20) $2,37 < H < 2,69$

$H^{(30)}$

1) $0 < H < 0$

3) $0,91 < H < 1,08$

4) $0,11 < H < 0,81$

5) $0,69 < H < 0,12$

6) $0,91 < H < 1,01$

7) $1,21 < H < 1,37$

8) $1,06 < H < 1,29$

9) $0,94 < H < 1,22$

10) $1,3 < H < 1,51$

11) $1,12 < H < 1,49$

12) $1,51 < H < 1,78$

13) $1,60 < H < 1,88$

22) $2,2 < H < 2,4$

6

2,3

№3

$H_{inf} \approx H^{(30)}$

$$H_0 = log_2 32 = 5$$
$$R = 1 - 2.3 / 5 = 0.5$$