НТУУ «Київський політехнічний інститут ім. Ігоря Сікорського»

Навчально-науковий Фізико-технічний інститут

**Криптографія**

Комп’ютерний практикум №1

*Експериментальна оцінка ентропії на символ джерела відкритого тексту*

Варіант №6

Виконали:

Студенти 3 курсу НН ФТІ

групи ФБ-31

Гаврилюк Володимир

Гек Роман

Було проаналізовано текст розміром >1MB, текст був попередньо відфільтрований як і було вказано у методичних вказівках

Був написаний скрипт мовою Python, який обчислює:

- частоти появи кожного символу в тексті;

- ентропію H1 на основі частот символів;

- частоти появи біграм двома методами: з перетином (крок 1 символ) та - без перетину (крок 2 символи)

- ентропію H2 для обох методів підрахунку біграм

- усі розрахунки були проведені для двох варіантів тексту: з пробілами та з видаленими пробілами

Результати програмного аналізу:  
Таблиця частот символів (з пробілами)

Зображення, що містить текст, знімок екрана, меню, дизайн

Вміст на основі ШІ може бути неправильним.

Таблиця частот символів (без пробілів)

Зображення, що містить текст, знімок екрана, меню, дизайн

Вміст на основі ШІ може бути неправильним.

Підсумкові значення ентропій:  
Зображення, що містить текст, Шрифт, знімок екрана

Вміст на основі ШІ може бути неправильним.

Надлишковість:  
Зображення, що містить текст, Шрифт, знімок екрана

Вміст на основі ШІ може бути неправильним.

Далі було проведено експерименти з CoolPinkProgram.exe, для кожної n-грами по 50 експериментів. Під час експериментів навмисно підроблювати результати не намагалися, як виходило так і вгадували символи.

Експерименти із CoolPinkProgram

H10

Зображення, що містить текст, електроніка, знімок екрана, програмне забезпечення

Вміст на основі ШІ може бути неправильним.

H20

Зображення, що містить текст, електроніка, знімок екрана, програмне забезпечення

Вміст на основі ШІ може бути неправильним.

H30

Зображення, що містить текст, знімок екрана, Веб-сайт, Веб-сторінка

Вміст на основі ШІ може бути неправильним.

**Підсумок та висновки**

В ході виконання роботи було експериментально досліджено статистичні властивості російської мови. Також ми провели оцінку ентропії та надлишковості за допомогою різних моделей. Отримані результати дозволяють зробити декілька висновків

1. Підтверджено теоретичну залежність ентропій від моделі джерела. Чітко видно ієрархію H0 > H1 > H2 > Hn. Врахування зв’язків між сусідніми символами (модель біграм, або n-грам) значно зменшує невизначеність у порівнянні з моделлю, що враховує тільки частоти окремо одного символу.
2. Доведено вплив довжини контексту на точність оцінки ентропій. Оцінка умовної ентропії в експериментах показала, що зі збільшенням кількості символів (n) ентропія значно зменшується. Так середнє значення H10 складає близько ~2.35 біт, тоді як H30 складає ~1.81 біт. Це свідчить, що російська мова має залежності, які дозволяють людині ефективно передбачити наступні символи.
3. Встановлено значну надлишковість російської мови. Найбільш точні оцінки, які були отримані, показують, що надлишковість російської мови може сягати 60-70%. Це означає, що більше половини символів у тексті є передбачуваними і визначаються структурними закономірностями мови. Простіші статистичні моделі (H1, H2) недооцінюють реальну надлишковість, показуючи значення в діапазоні 10-20%.
4. Також проаналізовано вплив алфавіту на ентропію. Видалення пробілів з тексту призвело до незначного зростання ентропії (H1 з та без – 4.43 біт, 4.49 біт). Це пояснюється тим, що пробіл є дуже частим символом, структурно передбачуваним. Його видалення усуває частину передбачуваності з тексту, роблячи його в середньому трішки більш хаотичним для аналізу.