Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Защита информации и надёжность информационных систем

Студент: Лопатнюк П.В.

ФИТ 3 курс 1 группа

Преподаватель: Нистюк О.А.

Минск 2025

# Лабораторная работа № 8

# СЖАТИЕ/РАСПАКОВКА ДАННЫХ МЕТОДОМ БАРРОУЗА − УИЛЕРА

**Цель**: приобретение практических навыков использования метода Барроуза − Уилера для сжатия/распаковки данных.

**Задачи**:

1. Закрепить теоретические знания по алгебраическому описанию и использованию методов сжатия/распаковки (архивации/ разархивации) данных на основе метода Барроуза − Уилера (Burrows Wheeler transform, BWT).
2. Разработать приложение для реализации метода Барроуза − Уилера.
3. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# Теоретические сведения

Данная лабораторная работа открывает второй раздел практикума, относящийся к методам сжатия данных (англ. data compression), которые играют важную роль в решении проблемы защиты информации, ведь архивация данных необходима не только для экономии места на локальном дисковом носителе, но и для переноса информации, резервирования, резервного копирования и т. п. Исходя из этого, далее дадим краткую характеристику данному классу методов преобразования информации. Сжатие информации является одним из способов ее кодирования.

Развитие методов сжатия данных имеют длинную историю, которая началась задолго до появления компьютеров и компьютерных сетей.

Основная цель сжатия – обеспечить более компактное представление данных, вырабатываемых источником, т. е. уменьшить физический объем сообщений, генерируемых источником, и сократить время его передачи (читай – стоимость) по каналам связи. Фундаментальная теорема К. Шеннона о кодировании информации утверждает, что «стоимость кодирования всегда не меньше энтропии источника, хотя может быть сколь угодно близка к ней». Поэтому для любого алгоритма сжатия всегда имеется некоторый предел степени (или эффективности) сжатия, определяемый энтропией входного потока (или сжимаемого сообщения).

Все алгоритмы сжатия преобразуют входной поток данных, минимальной единицей которых является бит, а максимальной – байт или несколько байт. Основными техническими характеристиками процессов сжатия и результатов их работы являются:

* Степень сжатия (англ. compress rating), или отношение R (англ. ratio) объемов исходного (до сжатия, Vдс) и результирующего (после сжатия, Vпс) потоков данных (сообщений).
* Скорость сжатия − время, затрачиваемое на сжатие некоторого объема информации входного потока до получения из него эквивалентного выходного потока.
* Качество сжатия − величина, показывающая, насколько сильно сжат выходной поток при помощи применения к нему повторного сжатия по этому же или иному алгоритму.

Первое отношение показывает, какую часть объема сообщения (файла) до сжатия занимает сообщение (файл) после сжатия; второе отношение выражает основной физический смысл сжатия и показывает степень сжатия.

Что касается третьей из приведенных технических характеристик (качества сжатия), то она показывает, по существу, совместимость данного метода с другими. Это важно, если принять во внимание то обстоятельство, что практически все современные архиваторы основаны на использовании нескольких разных методов сжатия (кодирования).

Существуют различные подходы к реализации сжатия информации. Они отличаются математической базой, уровнем сложности (простоты) практической реализации, форматом кодируемого потока данных, степенью соответствия сжимаемых и распакованных данных.

По критерию, связанному с характером или форматом данных или степенью соответствия сжимаемых данных распакованным, все методы сжатия разделяют на два класса: обратимое и необратимое сжатие, или иначе: сжатие без потерь и сжатие с частичной потерей информации (англ. lossy compression).

Понятно, что недопустимы никакие потери при упаковке текстовых документов, кодов компьютерных программ, файлов баз данных.

Сжатие с потерей информации реализуется на основе таких известные форматов данных и алгоритмов сжатия, как JPEG и MPEG. Алгоритм JPEG используется при сжатии фотоизображений. Алгоритмы MPEG используют при сжатии видео и музыки.

Методы и алгоритмы сжатия с потерей информации применяют обычно для решения так называемых потребительских задач. Это значит, например, что если фотография передается для просмотра, а музыка для воспроизведения, то подобные алгоритмы применять можно. Если же они передаются для дальнейшей обработки, например для редактирования, то никакая потеря информации в исходном файле недопустима. Считают, что на фотографических иллюстрациях, предназначенных для воспроизведения на экране, потеря 5% информации не критична, а в некоторых случаях можно допустить и 20−25% уровень потерь.

В настоящее время можно встретить достаточно большое число архивирующих и сжимающих утилит, большинство из которых доступны для некоммерческого использования. Поддержка популярных форматов файловых архивов начинает включаться в разные утилиты и программы. Часто используемые форматы становятся стандартными форматами архивов (zip, arj, rar, ha, pak, cab и др.).

BWT-преобразование (англ. Burrows-Wheeler Transform) – техника сжатия информации (в особенности текстов), основанная на преобразовании, открытом в 1983 г. BWT не сжимает данные в классическом понимании процесса, но преобразует блок данных в формат, исключительно подходящий для сжатия. BWT оперирует сразу целым блоком данных, который выделяется из входного потока (сообщения).

Прямое преобразование (формально – сжатие) выполняется в 4 этапа:

1. выделяется блок данных (строка длиной k символов некоторого алфавита мощностью N), который обозначим символом М;
2. составляется таблица W1 размером k×k всех циклических сдвигов входной строки M: W1 = (M);
3. производится лексикографическая (в алфавитном порядке) сортировка строк таблицы W1, в результате чего получается таблица W2 того же размера;
4. в качестве выходной строки (обозначим ее BWT(М), z) выбирается последний столбец (Мk) таблицы W2 преобразования и номер строки z, совпадающей с исходной строкой М. Как видим, выходная строка (сжатое сообщение) всегда по объему превышает входную.

Обратимость преобразования, т. е. возможность извлечения М из BWT(М), i основана на рекурсивности преобразования. Вспомним, что общим для рекурсивных функций, рекурсивных алгоритмов и рекуррентных последовательностей является то, что для вычисления очередного значения функции, получения очередной реализации алгоритма, определения очередного члена последовательности необходимо обращаться к предшествующим их значениям, вычисленным раньше.

Итак, входной для обратного преобразования является информация вида BWT(М), i. Это преобразование заключается в выполнении k одинаковых шагов, каждый из которых состоит из 2 операций, с целью воссоздания матрицы W2:

1. в крайний справа пустой столбец матрицы записывается последовательность символов Мk;
2. производится лексикографическая сортировка столбцов заполненной части воссоздаваемой матрицы. После k шагов матрица W2 будет получена. Зная значение числа z, получаем входной блок М сообщения. Как видим, последующий вид матрицы определяется предыдущим ее состоянием.

# Практическое задание

1. Разработать авторское приложение в соответствии с целью лабораторной работы. Входной блок данных может иметь произвольную длину.

|  |
| --- |
| public static BWTResult Encode(string text)  {  Console.WriteLine($"--- Запуск ПРЯМОГО преобразования BWT для строки: '{text}' (сдвиги ВПРАВО) ---");  if (string.IsNullOrEmpty(text))  {  Console.WriteLine("[ПРЕДУПРЕЖДЕНИЕ] Входная строка пуста или null. Возвращаем пустой результат.");  return new BWTResult { TransformedText = "", OriginalIndex = -1 };  }  int n = text.Length;  List<string> rotations = new List<string>(n);  string currentRotation = text;  Console.WriteLine("\n[ШАГ 1] Генерация циклических сдвигов (ротаций) ВПРАВО:");  for (int i = 0; i < n; i++)  {  rotations.Add(currentRotation);  Console.WriteLine($" Сдвиг {i + 1,2}: {currentRotation}"); // i+1 для 1-based нумерации сдвигов  if (n > 0) // Эта проверка избыточна, т.к. n = text.Length и мы уже проверили string.IsNullOrEmpty  {  char lastChar = currentRotation[n - 1];  string restOfString = currentRotation.Substring(0, n - 1);  currentRotation = lastChar + restOfString;  }  }  Console.WriteLine("\n[ШАГ 2] Лексикографическая сортировка сдвигов:");  rotations.Sort(StringComparer.Ordinal); // Используем Ordinal для консистентности с поиском  Console.WriteLine(" Отсортированная матрица (M):");  for (int i = 0; i < n; i++)  {  Console.WriteLine($" [{i.ToString().PadLeft(2)}] {rotations[i]} {(rotations[i].Equals(text, StringComparison.Ordinal) ? "<- Исходная строка" : "")}");  }  Console.WriteLine("\n[ШАГ 3] Извлечение последнего столбца (L):");  StringBuilder transformedTextBuilder = new StringBuilder(n);  for (int i = 0; i < n; i++)  {  transformedTextBuilder.Append(rotations[i][n - 1]);  }  string transformedText = transformedTextBuilder.ToString();  Console.WriteLine($" => Последний столбец (L): '{transformedText}'");  Console.WriteLine("\n[ШАГ 4] Поиск 0-based индекса исходной строки (I) в отсортированной матрице:");  int originalIndex = -1;  for (int i = 0; i < n; i++)  {  if (rotations[i].Equals(text, StringComparison.Ordinal))  {  originalIndex = i;  break;  }  }  if (originalIndex != -1)  {  Console.WriteLine($" => Исходная строка '{text}' найдена. Индекс (I): {originalIndex} (это {originalIndex + 1}-я строка в M)");  }  else  {  // Этого не должно произойти, если текст не пустой, т.к. исходная строка всегда будет одним из сдвигов  Console.WriteLine($" [ОШИБКА!] Исходная строка '{text}' НЕ найдена в отсортированной матрице! Это неожиданно.");  }  Console.WriteLine("--- Прямое преобразование BWT завершено. ---\n");  return new BWTResult { TransformedText = transformedText, OriginalIndex = originalIndex };  } |

Листинг 1.1 – Метод прямого преобразования

1. С помощью приложения выполнить прямое и обратное преобразования 3 отдельных блоков данных, состоящих:

а) из собственного имени (можно краткий вариант записи);

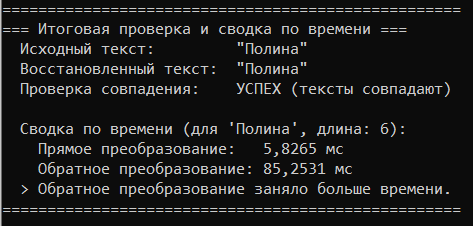


Рисунок 2.1 – Анализ длительности преобразований для задания а

б) собственной фамилии;

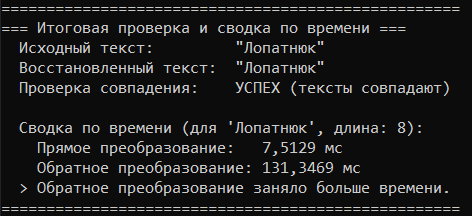


Рисунок 2.2 – Анализ длительности преобразований для задания б

в) варианта в соответствии с таблицей ниже.

Таблица 2.1

|  |  |
| --- | --- |
| Вариант | Входной блок данных |
| 8 | самообороноспособность |

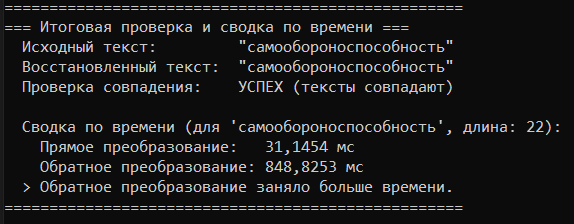


Рисунок 2.3 – Анализ длительности преобразований для задания в

Прямое преобразование BWT для входного блока данных (строки) S длины n выполняется в несколько шагов:

Шаг 1. Формирование матрицы циклических сдвигов  
 Формируется матрица, состоящая из n строк, где каждая строка является циклическим сдвигом исходной строки S. В данном примере используется циклический сдвиг, где на каждом шаге последний символ строки перемещается в ее начало.  
 Исходная строка: S = «лодка» (n=5)

Сдвиг 0: лодка

Сдвиг 1: алодк (последний символ 'а' из «лодка» перемещен в начало)

Сдвиг 2: калод (последний символ 'к' из «алодк» перемещен в начало)

Сдвиг 3: дкало (последний символ 'д' из «калод» перемещен в начало)

Сдвиг 4: одкал (последний символ 'о' из «дкало» перемещен в начало)

Шаг 2. Лексикографическая сортировка матрицы  
 Полученная матрица циклических сдвигов сортируется лексикографически (по алфавиту, как в словаре). Сравнение строк обычно происходит по кодам символов. Получаем отсортированную матрицу M'.

Исходные сдвиги:  
 лодка  
 алодк  
 калод  
 дкало  
 одкал

Отсортированная матрица M':  
 [0]: алодк  
 [1]: дкало  
 [2]: калод  
 [3]: лодка <- Исходная строка  
 [4]: одкал

Шаг 3. Формирование строки L и определение индекса I  
Результатом прямого преобразования BWT является строка L, которая формируется путем конкатенации символов, находящихся в последнем столбце отсортированной матрицы M'.

Последний столбец матрицы M':  
 алодк  
 дкало  
 калод  
 лодка  
 одкал

Таким образом, строка L = «кодал».

Помимо строки L, для обратного преобразования необходимо сохранить индекс I строки в отсортированной матрице M', которая совпадает с исходной строкой S.  
 Исходная строка «лодка» находится в отсортированной матрице M' на 4-й позиции (индекс 3, так как нумерация с 0). Следовательно, I = 3 (или I = 4, если считать с 1-й строки).

Результат прямого преобразования: Пара (L, I). В нашем примере: («кодал», 3) (или 4-я строка).

Обратное преобразование позволяет восстановить исходную строку S, имея только результат прямого преобразования – строку L и индекс I. Метод основан на итеративном восстановлении отсортированной матрицы M'.

Входные данные: L = «кодал», I = 3 (0-индексированный, соответствует 4-й строке), n = 5.

Начальное состояние: Создается n пустых строк.  
 [0]: ' '  
 [1]: ' '  
 [2]: ' '  
 [3]: ' '  
 [4]: ' '

Итеративное построение и сортировка (n итераций): Процесс повторяется n раз. На каждой итерации j (от 1 до n):

Добавление столбца L: Текущие строки матрицы расширяются путем добавления в начало каждой строки i соответствующего символа L[i].

Сортировка строк: Полученные после добавления столбца строки снова сортируются лексикографически.

Итерация 1 (Построение последнего столбца будущей M')

Добавляем L = «к о д а л» к пустым строкам:  
 'к' + '' = 'к'  
 'о' + '' = 'о'  
 'д' + '' = 'д'  
 'а' + '' = 'а'  
 'л' + '' = 'л'

Сортируем полученные строки ('к', 'о', 'д', 'а', 'л'):  
 [0]: а  
 [1]: д  
 [2]: к  
 [3]: л  
 [4]: о

Итерация 2 (Построение предпоследнего столбца будущей M')

Добавляем L = «к о д а л» к строкам из предыдущей итерации ('а', 'д', 'к', 'л', 'о'):  
 'к' + 'а' = 'ка'  
 'о' + 'д' = 'од'  
 'д' + 'к' = 'дк'  
 'а' + 'л' = 'ал'  
 'л' + 'о' = 'ло'

Сортируем полученные строки ('ка', 'од', 'дк', 'ал', 'ло'):  
 [0]: ал  
 [1]: дк  
 [2]: ка  
 [3]: ло  
 [4]: од

Итерация 3

Добавляем L = «к о д а л» к строкам ('ал', 'дк', 'ка', 'ло', 'од'):  
 'к' + 'ал' = 'кал'  
 'о' + 'дк' = 'одк'  
 'д' + 'ка' = 'дка'  
 'а' + 'ло' = 'ало'  
 'л' + 'од' = 'лод'

Сортируем ('кал', 'одк', 'дка', 'ало', 'лод'):  
 [0]: ало  
 [1]: дка  
 [2]: кал  
 [3]: лод  
 [4]: одк

Итерация 4

Добавляем L = «к о д а л» к строкам ('ало', 'дка', 'кал', 'лод', 'одк'):  
 'к' + 'ало' = 'кало'  
 'о' + 'дка' = 'одка'  
 'д' + 'кал' = 'дкал'  
 'а' + 'лод' = 'алод'  
 'л' + 'одк' = 'лодк'

Сортируем ('кало', 'одка', 'дкал', 'алод', 'лодк'):  
 [0]: алод  
 [1]: дкал  
 [2]: кало  
 [3]: лодк  
 [4]: одка

Итерация 5 (Построение первого столбца будущей M')

Добавляем L = «к о д а л» к строкам ('алод', 'дкал', 'кало', 'лодк', 'одка'):  
 'к' + 'алод' = 'калод'  
 'о' + 'дкал' = 'одкал'  
 'д' + 'кало' = 'дкало'  
 'а' + 'лодк' = 'алодк'  
 'л' + 'одка' = 'лодка'

Сортируем ('калод', 'одкал', 'дкало', 'алодк', 'лодка'):  
 [0]: алодк  
 [1]: дкало  
 [2]: калод  
 [3]: лодка <- Строка с индексом I=3  
 [4]: одкал

После n=5 итераций получена полная отсортированная матрица циклических сдвигов M'. Исходная строка S находится в этой матрице по индексу I, сохраненному во время прямого преобразования.

Извлекаем строку с индексом I = 3 (4-я строка) из финальной матрицы: «лодка».

Результат обратного преобразования: Исходная строка S: «лодка».

1. Перевести первые 3 символа из блока данных, указанного в варианте таблицы, в бинарную последовательность в соответствии с кодами ASCII. Выполнить прямое и обратное преобразование.

с:

* Unicode код: U+0441
* Представление в UTF-8 (Hex): D1 81
* Представление в UTF-8 (Двоичный): 11010001 10000001

а:

* Unicode код: U+0430
* Представление в UTF-8 (Hex): D0 B0
* Представление в UTF-8 (Двоичный): 11010000 10110000

м:

* Unicode код: U+043C
* Представление в UTF-8 (Hex): D0 BC
* Представление в UTF-8 (Двоичный): 11010000 10111100

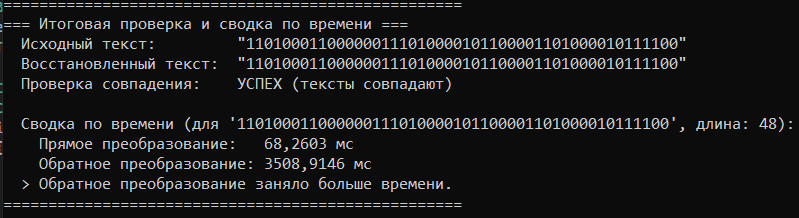


Рисунок 3.1 – Анализ длительности преобразований для бинарной последовательности

# Вывод

В рамках настоящей лабораторной работы было проведено исследование принципов и выполнена практическая реализация Преобразования Барроуза-Уилера (BWT). Данное преобразование является обратимым блочным алгоритмом, который группирует схожие символы во входной последовательности, что служит эффективным этапом предварительной обработки данных перед их сжатием.