УДК 517.518

31. ПОЛИНОМ ЖЕГАЛКИНА И ЕГО ПРИЛОЖЕНИЯ

Угликов С.А., студент гр.373901, Максимчик Е.В., студент гр.373901, Русина Н.В., аспирант

Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь

Ефремов А.А. – канд. экон. наук, доцент каф. ЭИ

Аннотация. В данной работе представлено исследование полинома Жегалкина, который является ключевым элементом в области булевой алгебры и цифровой логики.

Ключевые слова. Полином Жегалкина, булева функция, метод треугольника, теорему Жегалкина.

В современной дискретной математике и теории булевых функций особое место занимает полином Жегалкина. Этот полином представляет собой многочлен над полем Z_2, то есть полином с коэффициентами 0 и 1, где произведение реализуется как конъюнкция, а сложение — как исключающее “или”. Предложенный Иваном Ивановичем Жегалкиным в 1927 году, полином Жегалкина стал удобным инструментом для представления функций булевой логики и нашёл широкое применение в различных областях, от криптографии до теории сложности алгоритмов.

Целью данной работы является исследование свойств полинома Жегалкина, методов его построения и применения в различных областях математики и информатики. В работе будут рассмотрены различные подходы к построению полинома Жегалкина, включая метод треугольника и метод быстрого преобразования Фурье, а также их практическое применение

Методы представления полинома:

Эти методы позволяют представить булевую функцию в виде полинома Жегалкина, что удобно для анализа и оптимизации цифровых схем.

Представление полинома Жегалкина с помощью эквивалентных преобразований ДНФ:

Функция записывается в виде дизъюнктивной нормальной формы (ДНФ), то есть как суммы произведений литералов и их отрицаний. Применяются эквивалентные преобразования, чтобы преобразовать ДНФ в полином Жегалкина [1]. Например, используются законы де Моргана, законы ассоциативности и коммутативности для перехода к нужному виду.

$$XY \vee \overline{X}\,\overline{Y} = XY \oplus \overline{X}\,\overline{Y} \oplus XY\overline{X}\,\overline{Y} = XY \oplus \overline{X}\,\overline{Y} = XY \oplus (X \oplus 1)(Y \oplus 1) =$$
$$= XY \oplus XY \oplus X \oplus Y \oplus 1 = X \oplus Y \oplus 1.$$

Рисунок 1 – Пример преобразования ДНФ в полином Жегалкина

Представление полинома Жегалкина с помощью эквивалентных преобразований СДНФ:

Аналогично предыдущему методу, только функция записывается в виде совершенной дизъюнктивной нормальной формы (СДНФ), то есть как произведения сумм литералов и их отрицаний. Применяются эквивалентные преобразования, чтобы преобразовать СДНФ в полином Жегалкина.

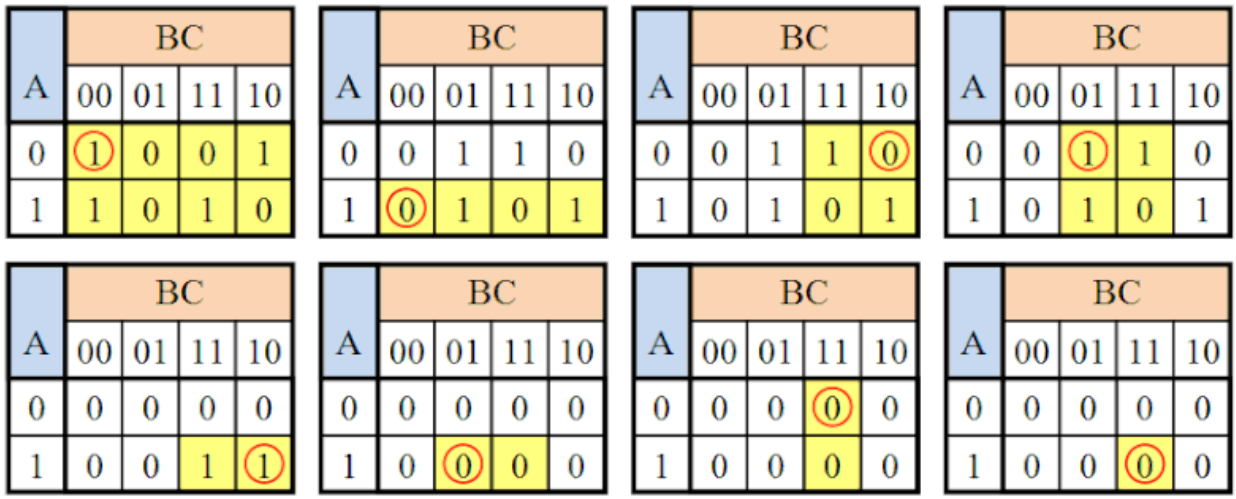
Представление полинома Жегалкина с помощью карты Карно:

Логическая функция трёх переменных P(A, B, C), представленная в виде карты Карно, преобразуется в полином Жегалкина следующими шагами:

1. Рассматриваем все ячейки карты Карно в порядке возрастания количества единиц в их кодах. Для функции трёх переменных последовательность ячеек будет 000—100 — 010—001 — 110—101 — 011—111. Каждой ячейке карты Карно сопоставляем член полинома Жегалкина в зависимости от позиций кода, в которых стоят единицы. Например, ячейке 111 соответствует член *ABC*, ячейке 101 — член *AC*, ячейке 010 — член *B*, ячейке 000 — член 1.
2. Если в рассматриваемой ячейке находится 0, переходим к следующей ячейке.
3. Если в рассматриваемой ячейке находится 1, добавляем в полином Жегалкина соответствующий член, инвертируем в карте Карно все ячейки, где этот член равен 1, и переходим к следующей ячейке. Например, если при рассмотрении ячейки 110 в ней оказывается единица, то в полином Жегалкина добавляется член *AB* и инвертируются все ячейки карты Карно, где *A* = 1 и *B* = 1.

Если единице равна ячейка 000, то в полином Жегалкина добавляется член 1 и инвертируется вся карта Карно.

4. Процесс преобразования можно считать законченным [2], когда после очередной инверсии все ячейки карты Карно становятся нулевыми.



$$P = 1 \oplus C \oplus AB$$

Рисунок 2 – Преобразование карты Карно в полином Жегалкина

Метод треугольника:

1. Метод треугольника (часто называемый методом треугольника Паскаля) позволяет преобразовать таблицу истинности в полином Жегалкина путём построения вспомогательной треугольной таблицы в соответствии со следующими правилами:

2. Строится полная таблица истинности, в которой строки идут в порядке возрастания двоичных кодов от 000…00 до 111…11.

3. Строится вспомогательная треугольная таблица, в которой первый столбец совпадает со столбцом значений функции в таблице истинности.

4. Ячейка в каждом последующем столбце получается путём суммирования по модулю 2 двух ячеек предыдущего столбца — стоящей в той же строке и строкой ниже.

5. Столбцы вспомогательной таблицы нумеруются двоичными кодами в том же порядке, что и строки таблицы истинности.

6. Каждому двоичному коду ставится в соответствие один из членов полинома Жегалкина в зависимости от позиций кода, в которых стоят единицы. Например, ячейке 111 соответствует член *ABC*, ячейке 101 — член *AC*, ячейке 010 — член *B*, ячейке 000 — член 1 и т. д.

7. Если в верхней строке какого-либо столбца стоит единица, то соответствующий член присутствует в полиноме Жегалкина [3].

A	*B*	*C*	*P*
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	0
1	1	1	1

000	001	010	011	100	101	110	111
1	*C*	*B*	*BC*	*A*	*AC*	*AB*	*ABC*
1	1	0	0	0	0	1	0
0	1	0	0	0	1	1	
1	1	0	0	1	0		
0	1	0	1	1			
1	1	1	0				
0	0	1					
0	1						
1							

$$P = 1 \oplus C \oplus AB$$

Рисунок 3 – Преобразования таблицы истинности в полином Жегалкина

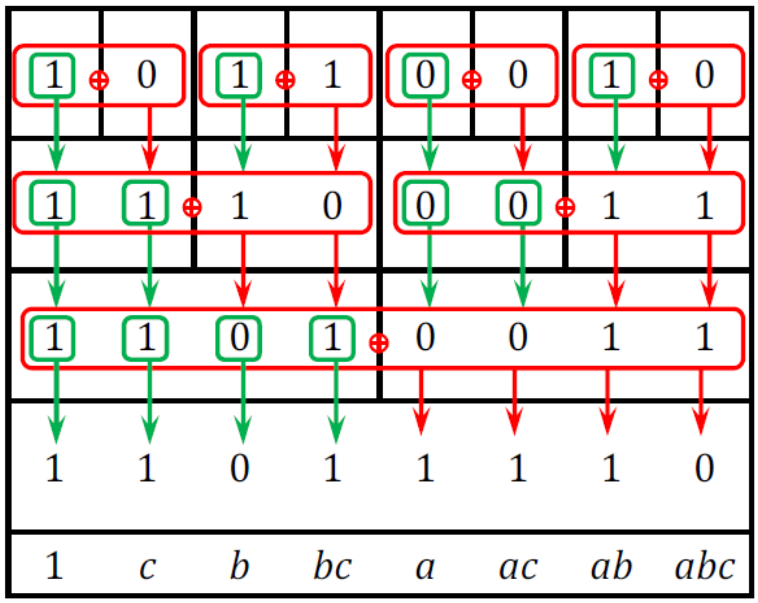
Метод БПФ (быстрого преобразования Фурье)

Наиболее экономным с точки зрения объёма вычислений и целесообразным для построения полинома Жегалкина вручную является метод быстрого преобразования Фурье (БПФ).

Строим таблицу, состоящую из 2^N столбцов и $N + 1$ строк, где N — количество переменных в функции. В верхней строке таблицы размещаем вектор значений функции, то есть последний столбец таблицы истинности.

Каждую строку полученной таблицы разбиваем на блоки (чёрные линии на рисунке). В первой строке блок занимает одну клетку, во второй строке — две, в третьей — четыре, в четвёртой — восемь и т. д. Каждому блоку в некоторой строке, который мы будем называть «нижний блок», всегда соответствует ровно два блока в предыдущей строке. Будем называть их «левый верхний блок» и «правый верхний блок».

Построение начинается со второй строки. Содержимое левых верхних блоков без изменения переносится в соответствующие клетки нижнего блока (зелёные стрелки на рисунке). Затем над правым верхним и левым верхним блоками побитно производится операция «сложение по модулю два», и полученный результат переносится в соответствующие клетки правой части нижнего блока (красные стрелки на рисунке). Эта операция проводится со всеми строками сверху вниз и со всеми блоками в каждой строке. После окончания построения [4] в нижней строке оказывается строка чисел, которая является коэффициентами полинома Жегалкина, записанными в той же последовательности, что и в описанном выше методе треугольника.



$$f(a,b,c) = 1 \oplus a \oplus c \oplus ab \oplus ac \oplus bc$$

Рисунок 4 – Построение полинома Жегалкина методом Паскаля

Метод суммирования:

Этот метод основан на суммировании мономов полинома Жегалкина по модулю 2. Последовательно складываются мономы, используя правила сложения булевых переменных (XOR), чтобы получить полином Жегалкина.

Существование и единственность представления (теорема Жегалкина):

По теореме Жегалкина каждая булева функция единственным образом представляется в виде полинома Жегалкина.

Доказательство: Теорема доказывается следующим образом. Заметим, что различных булевых функций от n переменных 2^{2^n} штук. При этом конъюнкций от n переменных существует ровно 2^n, так как из n возможных сомножителей каждый или входит в конъюнкцию, или нет. В полиноме у каждой такой конъюнкции стоит 0 или 1, то есть существует 2^{2^n} различных полиномов Жегалкина от n переменных. Теперь достаточно лишь доказать, что различные полиномы реализуют различные функции. Предположим противное. Тогда приравняв два различных полинома и перенеся один из них в другую часть равенства, получим полином, тождественно равный нулю и имеющий ненулевые коэффициенты. Тогда рассмотрим слагаемое с единичным коэффициентом наименьшей

длины, то есть с наименьшим числом переменных, входящих в него (любой один, если таких несколько). Подставив единицы на места этих переменных и нули на места остальных, получим, что на этом наборе только одно это слагаемое принимает единичное значение, то есть нулевая функция на одном из наборов принимает значение 1. Противоречие. Значит, каждая булева функция реализуется полиномом Жегалкина единственным образом.

Сферы применения:

1. Теория кодирования: Полиномы Жегалкина используются для создания и анализа линейных блочных кодов, которые играют важную роль в обеспечении надежности передачи данных.

2. Компьютерная наука: В области алгоритмов и структур данных полиномы Жегалкина могут быть полезны для представления и манипулирования булевыми функциями.

3. Цифровая электроника: Полиномы Жегалкина используются для минимизации логических схем и создания оптимальных цифровых схем.

4. Математическая логика и теория доказательств: Полиномы Жегалкина используются для формализации и анализа булевой логики.

5. Криптография: Полиномы Жегалкина могут быть использованы в криптографических алгоритмах для обеспечения безопасности данных.

В ходе данной работы были рассмотрены основные свойства и методы построения полинома Жегалкина, а также его применение в различных областях. Мы установили, что полином Жегалкина является мощным инструментом в теории булевых функций, позволяющим уникальным образом представлять булевы функции в алгебраической форме. Это представление не только облегчает анализ сложности функций, но и способствует более эффективному синтезу логических схем.

Методы построения полинома Жегалкина, такие как метод треугольника и быстрое преобразование Фурье, демонстрируют гибкость и адаптивность этого подхода к различным задачам. В частности, было показано, что эти методы могут быть использованы для оптимизации вычислительных процессов и уменьшения сложности алгоритмов.

Таким образом, полином Жегалкина остаётся актуальным и перспективным направлением в современной математике и информатике. Его применение в криптографии, теории кодирования и разработке программного обеспечения открывает новые горизонты для исследований и разработок. В заключение, мы можем утверждать, что полином Жегалкина будет продолжать играть ключевую роль в развитии дискретной математики и её приложений в будущем.

Список использованных источников:

1. *https://ru.wikipedia.org/wiki/Полином_Жегалкина – Дата доступа: 12.04.2024*
2. *Дайняк А.Б, Щуплецов М.С. Булевы функции и полиномы. — МГУ имени М.В. Ломоносова, 2006.*