3.4 АЛГЕБРА ЖЕГАЛКІНА

3.4.1. Алгебра Жегалкіна

Алгебра $<B, \{\wedge, \oplus, 0, 1\}>$, що утворена множиною $B=\{0, 1\}$ разом з операціями $\wedge$ (кон'юнкції), $\oplus$ (додавання за модулем 2) і константами 0, 1, називається ***алгеброю Жегалкіна***.

Приклад. Формула $(x \oplus y \oplus z) \wedge (x \oplus z \oplus 1) \oplus x \wedge y \oplus 1$, де x, y, z — булеві змінні, є прикладом формули алгебри Жегалкіна, тому що вона містить операції кон'юнкції і суми за модулем 2.

Тотожності алгебри Жегалкіна

Властивості кон'юнкції:

1) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ — асоціативність
2) $x \wedge y = y \wedge x$ — комутативність
3) $x \wedge x = x$ — ідемпотентність
4) $x \wedge 0 = 0, x \wedge 1 = x$ — дії з константами

Властивості операції додавання за модулем 2:

5) $x \oplus (y \oplus z) = (x \oplus y) \oplus z$ — асоціативність
6) $x \oplus y = y \oplus x$ — комутативність
7) $x \oplus x = 0$ — закон зведення подібних доданків
8) $x \oplus 0 = x$ — операція з константою 0
9) $x(y \oplus z) = xy \oplus xz$ — дистрибутивність $\wedge$ відносно $\oplus$

Операція сума за модулем 2 (або XOR) відіграє важливу роль у програмуванні, при обробці та кодуванні інформації. Вона має важливу властивість — наявність оберненого елемента x' для кожного $x \in \{0, 1\}$ (операції диз'юнкції і кон'юнкції такої властивості не мають). У цій алгебрі кожний елемент є оберненим до самого себе: $x' = x$. Це дозволяє розв'язувати рівняння шляхом додавання до обох частин однакових елементів. Наприклад, рівняння виду $x \oplus a = b$ розв'язується так:

$$x \oplus a \oplus a = b \oplus a;$$
$$x \oplus 0 = b \oplus a;$$
$$x = b \oplus a.$$

Можливість розв'язку подібних рівнянь, що відсутня у булевій алгебрі, обумовила широке застосування операції XOR, зокрема, при кодуванні інформації.

Будь-яка булева функція може бути зображена через операції кон'юнкції, диз'юнкції, заперечення.

Для доведення зображення будь-якої булевої функції формулою алгебри Жегалкіна достатньо виразити диз'юнкцію і заперечення через кон'юнкцію і додавання за модулем 2 — операції алгебри Жегалкіна.

Зображення заперечення в алгебрі Жегалкіна формулою $\underline{\overline{x} = x \oplus 1}$ виходить з таблиці істинності:

x	$\overline{x}$	$x \oplus 1$
0	1	1
1	0	0

Зображення диз'юнкції в алгебрі Жегалкіна реалізується формулою

$$\underline{x \vee y = xy \oplus x \oplus y}.$$

Доведемо цю формулу аналітично:

$$x \vee y = \overline{\overline{x \vee y}} = \overline{\overline{x} \wedge \overline{y}} = \overline{(x \oplus 1) \wedge (y \oplus 1)} = (x \oplus 1) \wedge (y \oplus 1) \oplus 1 =$$
$$= (x \wedge y) \oplus x \oplus y \oplus 1 \oplus 1 = xy \oplus x \oplus y\,.$$

Будь-яка логічна функція може бути зображена формулою в алгебрі Жегалкіна.

3.4.2 Поліном Жегалкіна

Серед всіх еквівалентних зображень функції в алгебрі Жегалкіна виділяється особливий вид формул, що називаються поліном Жегалкіна.

Поліномом Жегалкіна називається довільна формула алгебри Жегалкіна, яка має вигляд суми за модулем 2 кон'юнкцій булевих змінних.

Якщо у кожний член поліному Жегалкіна кожна змінна входить один раз та поліном не містить однакових членів, то такий поліном Жегалкіна називається ***канонічним***.

Приклад: $xy \oplus x \oplus 1$.

Кількість змінних, що входять до елементарної кон'юнкції, називається ***рангом елементарної кон'юнкції***.

Кількість попарно різних елементарних кон'юнкцій у поліномі називається ***довжиною полінома***.

Зображення у вигляді поліному існує та єдине для кожної булевої функції.

В поліном Жегалкіна не входять фіктивні змінні.

3.4.2.1 Побудова поліному Жегалкіна аналітичним способом

Для побудови поліному Жегалкіна функції, що задана деякою формулою алгебри Жегалкіна, необхідно розкрити всі дужки в даній формулі за законом дистрибутивності і виконати всі можливі спрощення з використанням законів дій з константами, ідемпотентності і зведення подібних доданків.

Приклад. Зобразити поліномами Жегалкіна логічні функції імплікацію ($\rightarrow$) і еквівалентність (~).

Розв'язок. Спочатку запишемо ДДНФ даних функцій, потім виразимо операції диз'юнкції та заперечення через операції кон'юнкції та додавання за модулем 2. Одержавши формулу алгебри Жегалкіна, користуючись описаним вище правилом, одержимо поліном Жегалкіна для кожної з даних функцій:

$$x \rightarrow y = \bar{x} \vee y = (x \oplus 1) \vee y = (x \oplus 1)\, y \oplus (x \oplus 1) \oplus y =$$
$$= xy \oplus y \oplus x \oplus 1 \oplus y = xy \oplus x \oplus 1;$$
$$x \sim y = xy \vee \bar{x}\,\bar{y} = x\,y\;\bar{x}\,\bar{y} \oplus xy \oplus \bar{x}\,\bar{y} = xy \oplus \bar{x}\,\bar{y} =$$
$$= xy \oplus (x \oplus 1)(y \oplus 1) = xy \oplus xy \oplus x \oplus y \oplus 1 = x \oplus y \oplus 1.$$

За видом полінома Жегалкіна визначається така важлива властивість булевих функцій, як лінійність.

Булева функція називається ***лінійною***, якщо її поліном Жегалкіна не містить кон'юнкцій змінних.

Чи є лінійними операції булевої алгебри? Заперечення — лінійна функція, оскільки її поліном Жегалкіна $x \oplus 1$ не містить кон'юнкцій змінних. Диз'юнкція — нелінійна функція, оскільки її поліном Жегалкіна $x \oplus y \oplus xy$ містить кон'юнкцію змінних x і y.

Приклад. Визначити, чи лінійні функції імплікації ($\rightarrow$) та еквівалентності (~).

Розв'язок. Проаналізуємо структуру формул, що виведені у попередньому прикладі. З нього видно, що імплікація ($\rightarrow$) є нелінійною функцією, а еквівалентність (~) — функція лінійна.

Приклад. Дослідити на лінійність функцію $f(x, y, z) = (x \vee y) \rightarrow \bar{z}$.

Розв'язок. Побудуємо поліном Жегалкіна функції $f(x, y, z)$, використовуючи наступні тотожності:

$$x \rightarrow y = \bar{x} \vee y, \quad x \vee y = xy \oplus x \oplus y, \quad \bar{x} = x \oplus 1:$$

$$f(x, y, z) = (x \vee y) \rightarrow \bar{z} = \overline{(x \vee y)} \vee \bar{z} = \overline{(x \vee y)}\,\bar{z} \oplus \overline{(x \vee y)} \oplus \bar{z} =$$

$$= \big((x \vee y) \oplus 1\big)(z \oplus 1) \oplus \big((x \vee y) \oplus 1\big) \oplus (z \oplus 1) =$$
$$= \big(xy \oplus x \oplus y \oplus 1\big)(z \oplus 1) \oplus \big(xy \oplus x \oplus y \oplus 1\big) \oplus z \oplus 1 =$$
$$= xyz \oplus xy \wedge 1 \oplus xz \oplus x \wedge 1 \oplus yz \oplus y \wedge 1 \oplus 1 \wedge z \oplus 1 \wedge 1 \oplus xy \oplus x \oplus y \oplus 1 \oplus z \oplus 1 =$$
$$= xyz \oplus xy \oplus xz \oplus x \oplus yz \oplus y \oplus z \oplus 1 \oplus xy \oplus x \oplus y \oplus 1 \oplus z \oplus 1 =$$
$$= xyz \oplus xz \oplus yz \oplus 1.$$

Функція $f(x, y, z) = (x \vee y) \to \bar{z}$ не є лінійною, оскільки її поліном Жегалкіна містить кон'юнкції змінних.

3.4.2.2 Побудова поліному Жегалкіна методом невизначених коефіцієнтів

Метод невизначених коефіцієнтів засновано на тому, що для будь-якої булевої функції існує єдиний поліном Жегалкіна.

Приклад. Побудувати поліном Жегалкіна для функції $f_{13}(x, y)$ – імплікації, використовуючи метод невизначених коефіцієнтів.

Розв'язок. Запишемо поліном для даної функції у вигляді суми за модулем 2 всіх можливих елементарних кон'юнкцій для x, y з невизначеними коефіцієнтами:

$$f(x, y) = x \to y = a_{11}xy \oplus a_{10}x \oplus a_{01}y \oplus a_{00},$$

де коефіцієнти a_i приймають значення з множини {0, 1} і визначають присутність або відсутність елементарної кон'юнкції в поліномі.

Шукаємо послідовно значення коефіцієнтів, підставляючи значення змінних і функції на різних інтерпретаціях:

$f(0, 0) = 0 \to 0 = 1,$

$1 = a_{11} \wedge 0 \wedge 0 \oplus a_{10} \wedge 0 \oplus a_{01} \wedge 0 \oplus a_{00} \quad \Rightarrow \quad a_{00} = 1;$

$f(0, 1) = 0 \to 1 = 1,$

$1 = a_{11} \wedge 0 \wedge 1 \oplus a_{10} \wedge 0 \oplus a_{01} \wedge 1 \oplus 1 = 0 \oplus 0 \oplus a_{01} \oplus 1 = a_{01} \oplus 1 \quad \Rightarrow \quad a_{01} = 0;$

$f(1, 0) = 1 \to 0 = 0,$

$0 = a_{11} \wedge 1 \wedge 0 \oplus a_{10} \wedge 1 \oplus 0 \wedge 0 \oplus 1 = 0 \oplus a_{10} \oplus 0 \oplus 1 = a_{10} \oplus 1 \quad \Rightarrow \quad a_{10} = 1;$

$f(1, 1) = 1 \to 1 = 1,$

$1 = a_{11} \wedge 1 \wedge 1 \oplus 1 \wedge 1 \oplus 0 \wedge 1 \oplus 1 = a_{11} \oplus 1 \oplus 1 = a_{11} \quad \Rightarrow \quad a_{11} = 1;$

Підставивши одержані значення коефіцієнтів одержуємо поліном Жегалкіна для функції *f*:

$$f(x, y) = x \to y = a_{11}xy \oplus a_{10}x \oplus a_{01}y \oplus a_{00} = 1 \wedge xy \oplus 1 \wedge x \oplus 0 \wedge y \oplus 1 = xy \oplus x \oplus 1.$$

3.4.2.3 Побудова поліному Жегалкіна за ДДНФ

1. замінити операції $\vee$ на $\oplus$;
2. замінити $\bar{x} = x \oplus 1$;

3. розкрити дужки і звести подібні.

Приклад. Побудувати поліном Жегалкіна для функції

$$f(x, y, z) = \bar{x}\, y\, z \vee x\, \bar{y}\, z \vee x\, y\, \bar{z} \vee x\, y\, z = \bar{x}\, y\, z \oplus x\, \bar{y}\, z \oplus x\, y\, \bar{z} \oplus x\, y\, z =$$

$$= (x \oplus 1)\, y\, z \oplus x(y \oplus 1)\, z \oplus x\, y\, (z \oplus 1) \oplus x\, y\, z =$$

$$= x\, y\, z \oplus y\, z \oplus x\, y\, z \oplus x\, z \oplus x\, y\, z \oplus x\, y \oplus x\, y\, z = y\, z \oplus x\, z \oplus x\, y.$$

3.4.2.4 Побудова поліному Жегалкіна методом трикутника

За **методом трикутника**:

- будується таблиця істинності, в якій рядки йдуть в порядку зростання двійкових кодів від 000 ... 00 до 111 ... 11;
- будується допоміжна трикутна таблиця, в якій перший стовпець збігається зі стовпцем значень функції в таблиці істинності;
- комірка в кожному наступному стовпці виходить шляхом сумування за модулем два двох комірок попереднього стовпчика, що стоять в тому ж рядку і рядком нижче;
- стовпці допоміжної таблиці нумеруються двійковими кодами в тому ж порядку, що і рядки таблиці істинності;
- кожному двійковому коду ставиться у відповідність один з членів полінома Жегалкіна в залежності від позицій коду, в яких стоять одиниці.

Якщо у верхньому рядку будь-якого стовпчика стоїть одиниця ($c_i = 1$), то відповідний член присутній в поліномі Жегалкіна:

$$f(x, y, z) = c_0 \oplus c_1 z \oplus c_2 y \oplus c_3 yz \oplus c_4 x \oplus c_5 xz \oplus c_6 xy \oplus c_7 xyz\,.$$

Приклад. Побудувати поліном Жегалкіна для функції $f(x, y, z)$, що задана таблицею істинності:

	x	y	z	$f(x, y, z)$
0	0	0	0	0
1	0	0	1	1
2	0	1	0	1
3	0	1	1	0
4	1	0	0	1
5	1	0	1	1
6	1	1	0	1
7	1	1	1	0

Розв'язок. Будуємо допоміжну трикутну таблицю:

				1	*z*	*y*	*yz*	*x*	*xz*	*xy*	*xyz*
	x	*y*	*z*	000	001	010	011	100	101	110	111
0	0	0	0	0	1	1	0	1	1	1	1
1	0	0	1	1	0	1	1	0	0	0	
2	0	1	0	1	1	0	1	0	0		
3	0	1	1	0	1	1	1	0			
4	1	0	0	1	0	0	1				
5	1	0	1	1	0	1					
6	1	1	0	1	1						
7	1	1	1	0							

Отже, $c_0 = 0,\ \ c_1 = 1,\ c_2 = 1,\ c_3 = 0,\ c_4 = 1,\ c_5 = 1,\ c_6 = 1,\ c_7 = 1.$

Таким чином, поліном Жегалкіна має наступний вигляд:

$$f\left(x, y, z\right) = c_0 \oplus c_1 z \oplus c_2 y \oplus c_3 yz \oplus c_4 x \oplus c_5 xz \oplus c_6 xy \oplus c_7 xyz =$$

$$= z \oplus y \oplus x \oplus xz \oplus xy \oplus xyz\ .$$