ӘОЖ 512.563

БУЛЬДІК ФУНКЦИЯЛАР ЖӘНЕ ЖЕГАЛКИН КӨПМҮШЕЛІГІ: ТЕОРИЯСЫ, ӘДІСТЕРІ ЖӘНЕ ҚОЛДАНЫЛУЫ

Бақтыгереева Нұрсипат Ришатқызы
nurkab2002@mail.ru
7М01503 - «Математика. Білім беру үдерісін басқару» білім бағларламасының
1 курс магистранты
Х.Досмұхамедов атындағы Атырау университеті, Атырау қ, Қазақстан Республикасы
Ғылыми жетекшісі, тех.ғ.қ., профессор - Мырзашева Айгуль Нармаганбетовна

Бульдік алгебра және оның негізінде жатқан Бульдік функциялар қазіргі информатика мен компьютерлік логиканың іргетасын құрайды. Цифрлық схемаларды жобалау, логикалық элементтерді талдау, алгоритмдерді формализациялау және ақпараттық қауіпсіздік жүйелерінде Бульдік функциялар негізгі құрал ретінде қолданылады. Бульдік функцияларды әртүрлі формада көрсетуге болады, олардың ішінде Жегалкин көпмүшесі ерекше орын алады. Бұл полином логикалық функцияларды көпмүшелік түрінде сипаттайды және 2 модулі бойынша орындалатын арифметикалық амалдарға сүйенеді.

Жегалкин көпмүшелегі Бульдік функцияның құрылымын тереңірек түсінуге, оның қасиеттерін тиімді түрде бағалауға және схемаларды минималдауға мүмкіндік береді. Бұл мақалада Бульдік функция ұғымы, Жегалкин көпмүшелігінің теориясы, коэффициенттерді есептеу тәртібі және көпмүшенің практикалық қолданылу салалары жан-жақты қарастырылады.

Бульдік функция ұғымы және негізгі қасиеттері

Бульдік функция – бұл аргументтері екі мәннен (0 және 1) тұратын және нәтижесі де екілік мәндер болатын математикалық құрылым. Әрбір Бульдік функция белгілі бір логикалық ережені көрсетеді.

0 және 1 элементтерден тұратын 2 элементті жиын берілсін. {0,1} жиыны мен {0,1} жиыны арасындағы функция шартын қанағаттандыратын n орынды f сәйкестігі n айнымалы буль функциясы деп аталады. Буль функцияларының анықталу облысы мен мәндер облысының {0,1} жиыны E(f) = D(f) = {0,1} болатындығы анықтамадан белгілі.

n айнымалы Буль функциясын 2^n жатық жолдардан тұратын таблица түрінде кескіндеуге болады. Ондағы әрбір жолға айнымалылар тізімінің бағаланулары жазылады, ал айнымалылар тізімінің бағаланулары Буль функциясының анықтамасы бойынша {0,1} мәндерін қабылдайды.

Әрбір бағанның ұзындығы 2^n, ал 0 және 1 цифрларынан тұратын ұзындығы 2^n болатын әр түрлі бағандардың саны 2^{2^n} болады. Олай болса n орынды немесе n айнымалы Буль функциясының саны да 2^{2^n} болады.

Бұл формула элементтері қайталанатын алмастырудың $\tilde{A}_n^m = n^m$ формуласынан шығады, 0 және 1 тұрақтылары 0 орынды Буль функциясы деп аталады.

Пікірлер логикасындағы ақиқат мәнге 1-ді, жалған мәнге 0-ді сәйкестендірсек пікірлер логикасының әрбір F формуласына f буль функциясын сәйкестікке қоюға болады.

Егер F_1 формуласына f_1, ал F_2 формулалары f_2 буль функциясы сәйкестікке қойылса және $F_1 \equiv F_2$ болса, онда $f_1 = f_2$, болады.

Пікірлер логикасының әрбір F формуласына f буль функциясын сәйкестікке қоюға болады.

Мысалы, n=3 болғанда 3 айнымалы Буль функциясын мынадай 1 кесте арқылы көрсетуге болады, *n=3*, сондықтан кесте $2^3 = 8$ жатық жолдан тұрады.

1 кесте – Үш айнымалы Буль функциясының кестемен берілуі

x	***y***	***z***	$f(x,y,z)$
1	1	1	$f(1,1,1)$
1	1	0	$f(1,1,0)$
1	0	1	$f(1,0,1)$
1	0	0	$f(1,0,0)$
0	1	1	$f(0,1,1)$
0	1	0	$f(0,1,0)$
0	0	1	$f(0,0,1)$
0	0	0	$f(0,0,0)$

Буль алгебрасында негізгі логикалық функциялары төмендегі 2 кесте орындалады:

қолданылатын операциялар бойынша

2 кесте – Буль алгебрасындағы операциялар логикалық кестесі

x	y	$\bar{x}$	$x \vee y$	$x \wedge y$	$x \Rightarrow y$	$x \Leftrightarrow y$	$x \cdot y$	$x \oplus y$	$x \downarrow y$	$x \mid y$
1	1	0	1	1	1	1	1	0	0	0
1	0	0	1	0	0	0	0	1	0	1
0	1	1	1	0	1	0	0	1	0	1
0	0	1	0	0	1	1	0	0	1	1

Пирс жебесі - $x \downarrow y = \overline{(x \vee y)}$ - антидизъюнкция;

Шеффер штрихы - $x \mid y = \overline{(x \wedge y)}$- антиконъюнкция;

Сақиналық қосынды немесе 2 модулі бойынша қосу - белгіленуі - (x + y) немесе $x \oplus y$;

Көбейтінді амалы конъюнкциямен сәйкес – $x \cdot y = x \wedge y$.

Осы логикалық амалдар үшін келесі қасиеттер орындалады:

Пирс жебесінің қасиеттері:

1. $x \downarrow y = \overline{(x \vee y)}$,
2. $x \downarrow y = \bar{x} \wedge \bar{y}$,
3. $x \downarrow x = \bar{x}$,
4. $x \wedge y = (x \downarrow x) \downarrow (y \downarrow y)$
5. $x \vee y = (x \downarrow y) \downarrow (x \downarrow y)$
6. $x \downarrow y = y \downarrow x$,
7. $\bar{x} \downarrow \bar{y} = \overline{x \mid y}$.

Шеффер штрихының қасиеттері:

1. $x \mid y = \overline{(x \wedge y)}$,
2. $x \mid y = \bar{x} \vee \bar{y}$,
3. $x \mid x = \bar{x}$,
4. $x \wedge y = (x \mid y) \mid (x \mid y)$
5. $x \vee y = (x \mid x) \mid (y \mid y)$
6. $x \mid y = y \mid x$,
7. $x \mid \bar{x} = 1$,
8. $x \mid 0 = 1$,
9. $x \mid 1 = \bar{x}$.

Сақиналық қосынды немесе 2 модулі бойынша қосынды амалының қасиеті:

1. $x \oplus y = y \oplus x$,
2. $(x \oplus y) \oplus z = x \oplus (y \oplus z)$,
3. $x \oplus x = 0$,
4. $x \cdot (y \oplus z) = x \cdot y \oplus x \cdot z$,
5. $0 \oplus x = x$,
6. $\bar{x} = x \oplus 1$,
7. $x \oplus y = \overline{(x \Leftrightarrow y)} = x \cdot \bar{y} \vee \bar{x} \cdot$.

Көбейту амалының қасиеттері:

1. $x \cdot y = y \cdot x$,
2. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
3. $x \cdot x = x$,
4. $x \cdot (y \oplus z) = x \cdot y \oplus x \cdot z$,
5. $0 \cdot x = 0$,
6. $1 \cdot x = x$.

Жегалкин көпмүшелігі және оның математикалық негізі

Жегалкин көпмүшелігі – Бульдік функцияны көпмүшелік түрде көрсету тәсілі. Көпмүшедегі барлық амалдар 2 модулі бойынша орындалады.

Анықтама: Жегалкин көпмүшесі деп 0 немесе 1 тұрақтысынан және айнымалылардың әртүрлі бірмүшелерінің қосындысынан тұратын көпмүше, мұнда барлық айнымалылар бірінші дәрежеден аспайды.

n айнымалы буль функциясы үшін Жегалкин көпмүшесі келесі (1) түрде жазылады:

$$f(x_1, x_2, ..., x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus ... \oplus a_{12} x_1 x_2 \oplus ... \oplus a_{12...n} x_1 x_2 ... x_n. \quad (1)$$

Мұндағы әр коэффициент a_i тек 0 немесе 1 мәнін қабылдайды және олар Бульдік функцияның ақиқаттық кестесі арқылы есептеледі.

Жегалкин көпмүшесін 1927 жылы кеңес математигі Иван Жегалкин ұсынған. Шетел әдебиеттерінде бұл форма алгебралық нормаль форма (АНФ) деп аталады.

Жегалкин базисінде берілген Буль функцияларының жиыны Жегалкин алгебрасы деп аталады.

Теорема: Кез келген Буль функциясын бір ғана түрде Жегалкин көпмүшесі арқылы өрнектеуге болады.

n айнымалы үшін Жегалкин көпмүшелерінің саны барлық Буль функцияларының санына тең, яғни 2^{2^n}.

Жегалкин көпмүшесінің дәрежесі - оның құрамындағы ең жоғары дәрежелі конъюнкцияның дәрежесімен анықталады.

Жегалкин көпмүшесіне келтіру әдістері

Буль функцияларын Жегалкин көпмүшесі түрінде өрнектеудің бірнеше әдісі бар. Практикада көбінесе екі әдіс қолданылады:

1. Эквивалентті түрлендірулер әдісі.

Буль функциясы $(\cdot, \oplus, \neg)$ логикалық амалдар арқылы біртіндеп көпмүше түріне келтіріледі.

Мысал 1. f(x, y, z) = (xy ∨ z) ⇒ $\bar{y}$ функциясын Жегалкин көпмүшелігі түрінде өрнектеу керек.

Шешуі. $f(x, y, z) = (xy \vee z) \Rightarrow \bar{y} = \overline{(xy \vee z)} \vee \bar{y} = (\overline{x\bar{y}} \wedge \bar{z}) \vee \bar{y} =$

$$= \overline{\overline{(\overline{x\bar{y}} \wedge \bar{z})} \vee \bar{y}} = \overline{\overline{(\overline{x\bar{y}} \wedge \bar{z})} \wedge \bar{\bar{y}}} = \big((xy \oplus 1)(z \oplus 1) \oplus 1\big)y \oplus 1 =$$

$$= (xyz \oplus xy \oplus z \oplus 1 \oplus 1)y \oplus 1 = (xyz \oplus xy \oplus z)y \oplus 1 =$$

$= xyz \oplus xy \oplus yz \oplus 1$ – сызықтық емес Жегалкин көпмүшелігі.

2. Белгісіз коэффициенттер әдісі.

Бұл әдіс айнымалылар саны аз болғанда тиімді болады ($n \le 3$). Жегалкин көпмүшелігіне келтіру есебін шешу жұмысын мынадай ретте жүргізген дұрыс:

1) Функцияның ақиқаттық кестесін құру.

2) Жегалкин көпмүшесінің жалпы түрін жазу керек, мысалы, екі және үш айнымалы бульдік функция үшін Жегалкин көпмүшелігі (2) және (3) формула түрінде болатындығы (1) формуладан шығады:

$$f(x,y,z) = a_{12}xy + a_1x + a_2y + a_0 . \qquad (2)$$

$$f(x,y,z) = a_{123}xyz + a_{12}xy + a_{13}xz + a_{23}yz + a_1x + a_2y + a_3z + a_0 . \qquad (3)$$

3) Жегалкин көпмүшесінің өрнегіне айнымалылардың мәндер жиындарын біртіндеп қойып шығамыз. Нәтижесінде сызықтық теңдеулер алынады, олардың шешімдері Жегалкин көпмүшесінің коэффициенттерінің мәндері болып табылады. Алынған теңдеулерді шешу үшін 2 модуль бойынша қосу қасиеттері қолданылады: $a \oplus \bar{a} = 1$, $a \oplus 0 = a$, $a \oplus a = 0$. Әрбір қойылым бір коэффициентті анықтауға мүмкіндік береді.

Мысал 2. Төменде берілген буль функциясын Жегалкин көпмүшелігіне келтіру керек.

$$f(x,y,z) = (y \Leftrightarrow (yz)) \mid x .$$

Шешуі. Берілген буль функциясының ақиқаттық кестесін құрастырамыз.

3 кесте – 2 мысалдағы үш айнымалы Буль функциясының ақиқаттық кестесі

x 1	y 2	z 3	yz	$y \Leftrightarrow (yz)$	x	$f(x,y,z)$	теңдеуі	шешуі
0	0	0	0	1	0	1 - f_1	$a_0=1$	$a_0=1$
0	0	1	0	1	0	1 - f_2	$a_3+a_0=1$	$a_3=0$
0	1	0	0	0	0	1 - f_3	$a_2+a_0=1$	$a_2=0$
0	1	1	1	1	0	1 - f_4	$a_2+a_3+a_{23}+a_0=1$	$a_{23}=0$
1	0	0	0	1	1	0 - f_5	$a_1+a_0=0$	$a_1=1$
1	0	1	0	1	1	0 - f_6	$a_1+a_3+a_{13}+a_0=1$	$a_{13}=0$
1	1	0	0	0	1	1 - f_7	$a_1+a_2+a_{12}+a_0=1$	$a_{12}=1$
1	1	1	1	1	1	0 - f_8	$a_0+a_1+a_2+a_3+a_{12}+a_{13}+a_{23}+a_{123}=0$	$a_{123}=1$

(3) формулаға сәйкес үш айнымалы Жегалкин көпмүшесінің жалпы түрін жазамыз:

$$f(x,y,z) = a_{123}xyz + a_{12}xy + a_{13}xz + a_{23}yz + a_1x + a_2y + a_3z + a_0 .$$

Қорытындысында келесі (4) теңдеулер жүйесі мен жауабы (5) шығады:

$$\begin{cases} a_0 = 1, (x, y, z) = (0,0,0) \\ a_3 + a_0 = 1, (x, y, z) = (0,0,1) \\ a_2 + a_0 = 1, (x, y, z) = (0,1,0) \\ a_2 + a_3 + a_{23} + a_0 = 1, (x, y, z) = (1,0,0) \\ a_1 + a_0 = 0, (x, y, z) = (1,0,0) \\ a_1 + a_3 + a_{13} + a_0 = 0, (x, y, z) = (1,0,1) \\ a_1 + a_2 + a_{12} + a_0 = 1, (x, y, z) = (1,1,0) \\ a_0 + a_1 + a_2 + a_3 + a_{12} + a_{13} + a_{23} + a_{123} = 0, (x, y, z) = (1,1,1) \end{cases} \quad (4)$$

$$\begin{cases} a_0 = 1, \\ a_3 = 0, \\ a_2 = 0, \\ a_{23} = 0, \\ a_1 = 1, \\ a_{13} = 0, \\ a_{12} = 1, \\ a_{123} = 1. \end{cases} \quad (5)$$

Осы табылған коэффициенттердің мәндерін (3) формулаға қойып, берілген функцияның Жегалкин көпмүшесі түріндегі өрнегін аламыз:

$$f(x, y, z) = (y \Leftrightarrow (yz)) \mid x = xyz + xy + x + 1$$

Жегалкин көпмүшелігінің қолданылу салалары.

Жегалкин көпмүшесі төменде келтірілген түрлі салаларда маңызды рөл атқарады:

- Логикалық схемаларды минималдау;
- Ақпараттық қауіпсіздіктегі криптографиялық функцияларды бағалау;
- Автоматты жүйелерді жобалау;
- Деректерді шифрлау алгоритмдерінде сызықтық емес функцияларды талдау;
- Кодтау теориясы.

Көпмүше функциялардың сызықтық және сызықтық емес компоненттерін бөліп көрсетуге мүмкіндік береді, бұл криптографияда аса маңызды.

Қорытынды. Жегалкин көпмүшесі – Бульдік функцияны дәл әрі бірегей түрде сипаттаудың қуатты математикалық құралы. Оның көмегімен логикалық жүйелерді тиімді талдауға, схемаларды оңтайландыруға және күрделі функцияларды құрылымдық жағынан қарастыруға болады. Бұл мақалада берілген теориялық материалдар мен мысалдар Жегалкин көпмүшесінің практикалық маңызын толық ашады.

Пайдаланылған әдебиеттер

1. Кузнецов А. П. Дискретная математика и математическая логика. — Москва, 2018.
2. Розен К. Дискретная математика и её приложения. — М., 2020.
3. Таненбаум Э. Архитектура компьютера. — М., 2016.
4. Викторова Н. Б. Дискретная математика. Булевы функции. Сборник контрольных работ. — Москва: Проспект, 2023.
5. Марченко Л. Н., Семенчук А. В. Дискретная математика: булевы функции.— 2019.
6. Спирина М. С. Дискретная математика. — Учебное издание. — М.: [б. и.], 20xx.

7. Булевы функции и полиномы / Коллектив авторов — Учебно-методический материал спецкурса. — Москва: МГУ им. М. В. Ломоносова, 2019.

8. Андерсон Джеймс А. Дискретная математика и комбинаторика. —М.: Вильямс, 2003—960 б.

9. Нефедов В.Н. Дискретная математика. —М.: Высшая школа, 2007. —256 б.