О корреляционно-иммунных функциях с максимальной алгебраической иммунностью

Хильчук И.С., Зюбина Д.А.
Научный руководитель: Токарева Н.Н.

Конференция "Женщины в математике" в Институте математики им. С. Л. Соболева
Новосибирск, 6 июня 2022

Основными компонентами симметричных шифров являются булевы функции, от криптографических свойств которых зависит способность шифра противостоять различным видам криптоанализа.

Рассматриваются два свойства: алгебраическая иммунность и корреляционная иммунность функций от малого числа переменных.

Обозначим через $\mathbb{Z}_2$ множество $\{0,1\}$, тогда $\mathbb{Z}_2^n$ — векторное пространство двоичных векторов длины n. Пусть $\oplus$ обозначает сложение по модулю 2. Определим *скалярное произведение* $\langle x, y\rangle$ двух векторов из $\mathbb{Z}_2^n$ как число $x_1y_1 \oplus \ldots \oplus x_ny_n$. *Булева функция* f — это произвольное отображение из $\mathbb{Z}_2^n$ в $\mathbb{Z}_2$. Любую булеву функцию можно единственным образом записать в *алгебраической нормальной форме (АНФ, полином Жегалкина)* :

$$f(x_1,\ldots,x_n) = \left(\bigoplus_{k=1}^{n}\bigoplus_{i_1,\ldots,i_k} a_{i_1,\ldots,i_k}\, x_{i_1}\cdot\ldots\cdot x_{i_k}\right)\oplus a_0,$$

где при каждом k все индексы $i_1,\ldots,i_k$ различны и параметры $a_0, a_{i_1},\ldots,a_{i_k}$ принимают значения 0 или 1.

Носитель булевой функции — множество всех векторов, на которых функция принимает значение 1:

$$supp(f) = \{x \in \mathbb{Z}_2^n : f(x) = 1\}.$$

Весом Хэмминга $wt(f)$ булевой функции f от n переменных называется число ненулевых координат ее вектора значений. *Расстояние Хэмминга* $dist(f, g)$ между двумя булевыми функциями f и g от n переменных — число векторов $x \in \mathbb{Z}_2^n$, на которых функции принимают различные значения, или, что эквивалентно, $dist(f, g) = wt(f \oplus g)$.

Булев куб — граф $\mathbb{E}^n$, вершинами которого являются все двоичные векторы длины n, т. е. $V = \{(x_1, \ldots, x_n) : x_i \in \mathbb{Z}_2\}$, а ребрами соединяются только те векторы, расстояние Хэмминга между которыми равно единице. Число n называется размерностью булева куба.

Гранью размерности k в булевом кубе $\mathbb{E}^n$ называется множество

$$\Gamma^{a_1,\ldots,a_{n-k}}_{i_1,\ldots,i_{n-k}} = \{x_{i_1} = a_1, \ldots, x_{i_{n-k}} = a_{n-k}\}.$$

Множество $\{i_1, \ldots, i_{n-k}\}$ называется направлением грани.

Пусть f — булева функция от n переменных. *Геометрическим представлением* булевой функции f назовём подграф булева куба $\mathbb{E}^n$, индуцированный носителем функции f.
Два подграфа булева куба $\mathbb{E}^n$, индуцированные соответственно носителями функций f_1 и f_2, назовём *изоморфными по метрическому вложению*, если найдётся автоморфизм $\phi : \mathbb{E}^n \to \mathbb{E}^n$ булева куба $\mathbb{E}^n$, под действием которого подграф, индуцированный носителем функции f_1 переходит в подграф, индуцированный носителем f_2.

Булева функция f от n переменных называется *корреляционно-иммунной порядка* r, $1 \leq r \leq n$, если для любой её подфункции $f^{a_1,\ldots,a_r}_{i_1,\ldots,i_r}$, полученной фиксацией r переменных, выполняется равенство

$$wt(f^{a_1,\ldots,a_r}_{i_1,\ldots,i_r}) = \frac{wt(f)}{2^r}.$$

Имеет место эквивалентное определение. Булева функция f от n переменных является корреляционно-иммунной порядка $n-k$, $1 \leq k \leq n$, если любой грани $\Gamma^{a_1,\ldots,a_{n-k}}_{i_1,\ldots,i_{n-k}}$ булева куба $\mathbb{E}^n$ размерности k принадлежит одинаковое число точек носителя функции f, а именно $wt(\Gamma^{a_1,\ldots,a_{n-k}}_{i_1,\ldots,i_{n-k}}) = wt(f) \cdot 2^{-(n-k)}$.

Функция g называется *аннулятором* функции f, если g не равен тождественно нулю и $f * g \equiv 0$.
Алгебраическая иммунность $AI(f)$ функции f — минимальная из степеней аннуляторов функций f и $f \oplus 1$.

Для $n = 3$ была получена полная классификация булевых функций с корреляционной иммунностью порядка 3, 2, 1. Всего существует

- 2 функции порядка 3 — функции-константы;
- 4 функции порядка 2 — функции-константы и функции-счётчики чётности;
- 18 функций порядка 1.

Из всех 18 булевых функций от трёх переменных ни одна не имеет максимально возможное значение алгебраической иммунности (т.е. $AI(f) < 2$).

Для $n = 4$ также была получена полная классификация булевых функций с корреляционной иммунностью порядка 4, 3, 2, 1. Всего существует

- 2 функции порядка 4 — функции-константы;
- 4 функции порядка 3 — функции-константы и функции-счётчики чётности (аналогично ситуации для функции от 3 переменных);
- 12 функций порядка 2;
- 648 функций порядка 1.

Существует 392 функции с максимальной алгебраической иммунностью ($AI(f) = 2$) и корреляционной иммунностью порядка 1 ($CI(f) = 1$). Существуют такие функции веса 6 (96 функций), 8 (200 функций), 10 (96 функций).

Рассмотрим функции веса 6 с $AI(f) = 2$, $CI(f) = 1$, принимающие значение 1 на нулевом векторе (их 36), и индуцированные их носителями подграфы булева куба $\mathbb{E}^4$. Здесь и далее в работе тонкими линиями обозначены расстояния между несмежными вершинами графа. Подграфы данного вида симметричны относительно вертикальной оси, мы не различаем симметричные вершины.

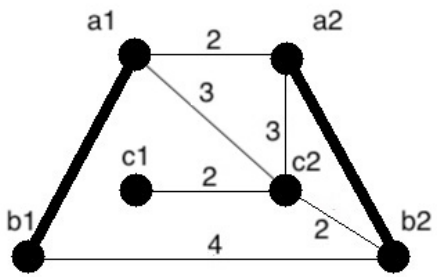


Рис.: Подграф из G_6

Утверждение

Не существует других подграфов булева куба $\mathbb{E}^4$, изоморфных по вложению подграфам из G_6 и содержащих нулевой вектор булева куба. От того, какой вершиной индуцированного носителем подграфа является нулевой вектор булева куба, зависит вид алгебраической нормальной формы функции f.

- нулевой вектор – изолированная вершина (12 функций), пример АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_4 \oplus x_3 \oplus x_2 \oplus x_1 \oplus 1$$

- нулевой вектор – вершина $a_i, i = 1, 2$ (12 функций), пример АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_3x_4 \oplus x_2x_4 \oplus x_4 \oplus x_3 \oplus x_2 \oplus 1,$$

- нулевой вектор – вершина $b_i, i = 1, 2$ (12 функций), пример АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_3x_4 \oplus x_4 \oplus x_3 \oplus x_2 \oplus 1.$$

Индуцированные носителями функций веса десять (60 функций) подграфы булева куба также изоморфны по вложению между собой.

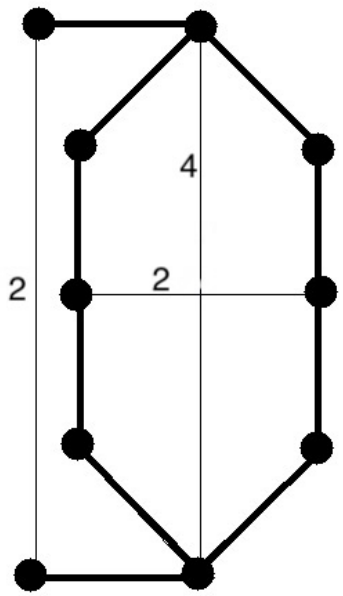


Рис.: Подграф из G_{10}

АНФ таких функций зависит от того, какой вершиной подграфа является нулевой вектор булева куба:

Пример для n = 4, $wt(f) = 10$

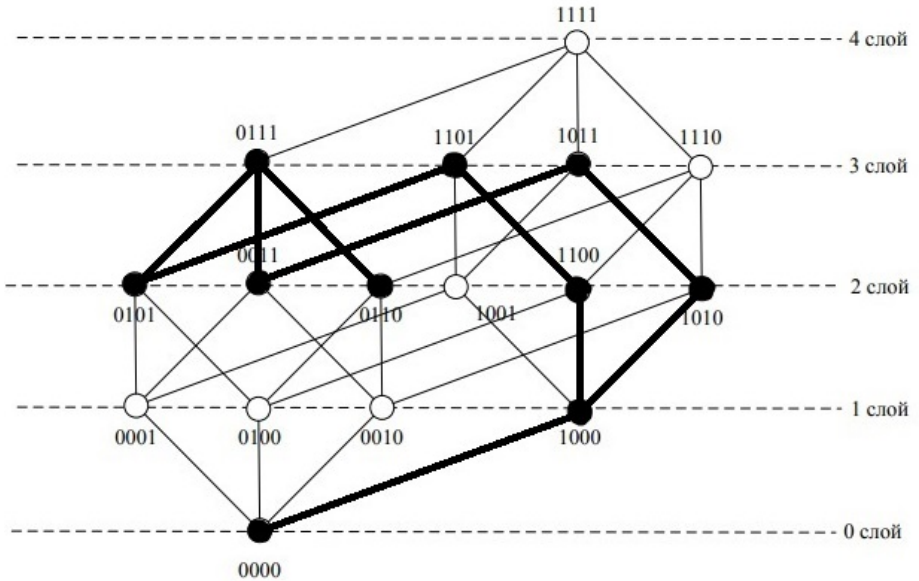


Рис.: Нулевой вектор — вершина степени один (12 функций)

АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1$$

Пример для n = 4, $wt(f) = 10$

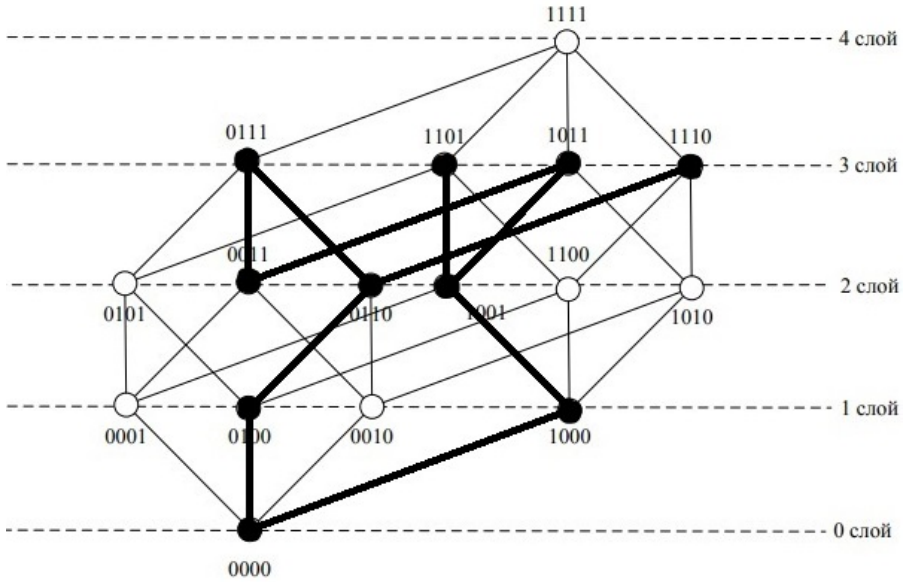


Рис.: Нулевой вектор — вершина степени два, равноудаленная от вершин степени три (12 функций)

АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_4 \oplus x_2x_3 \oplus x_3 \oplus x_4 \oplus 1$$

Пример для n = 4, $wt(f) = 10$

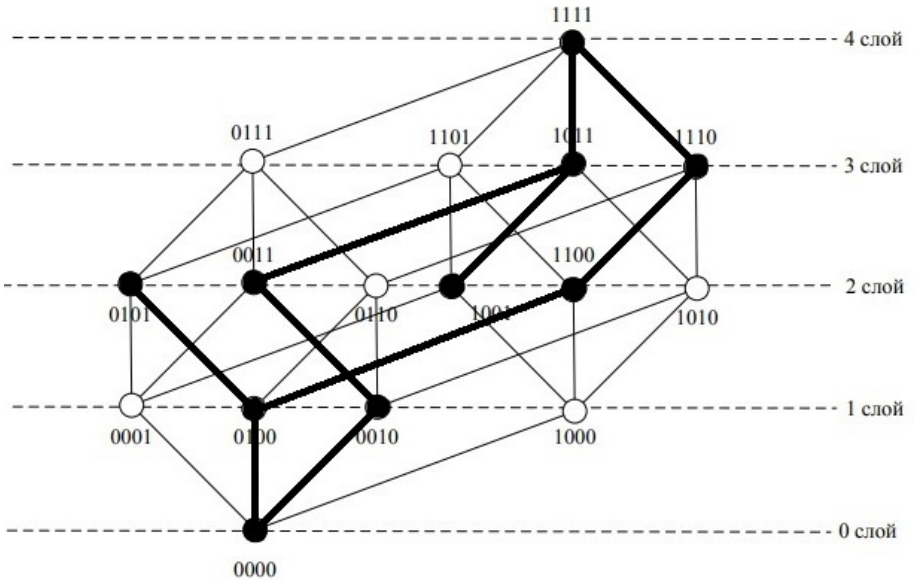


Рис.: Нулевой вектор — вершина степени два (24 функции)

АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus$$

$$\oplus x_1 \oplus x_4 \oplus 1$$

Пример для n = 4, $wt(f) = 10$

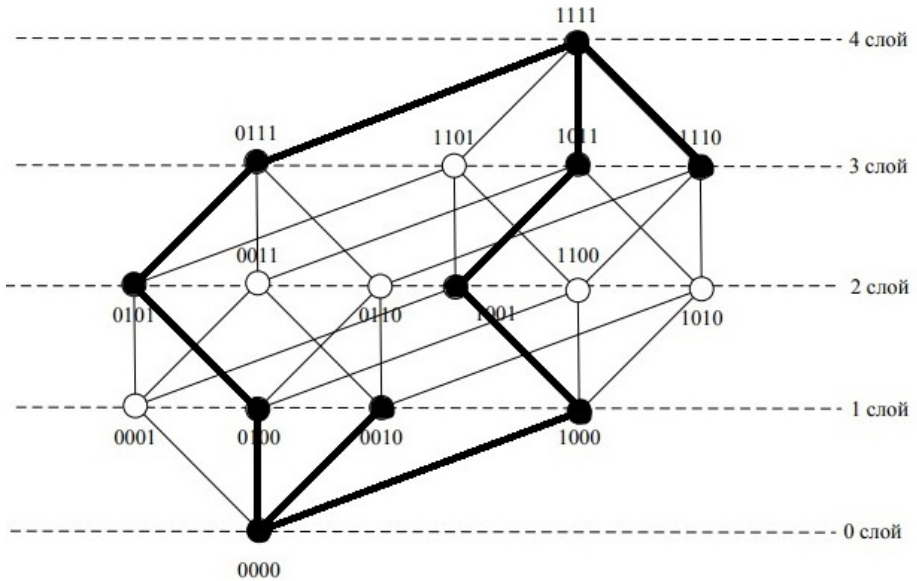


Рис.: Нулевой вектор — вершина степени три (12 функций)

АНФ:

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_3x_4 \oplus x_2x_3x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_4 \oplus 1$$

Функций веса 8 — 200, индуцированные носителями функций подграфы имеют четыре возможных вида.

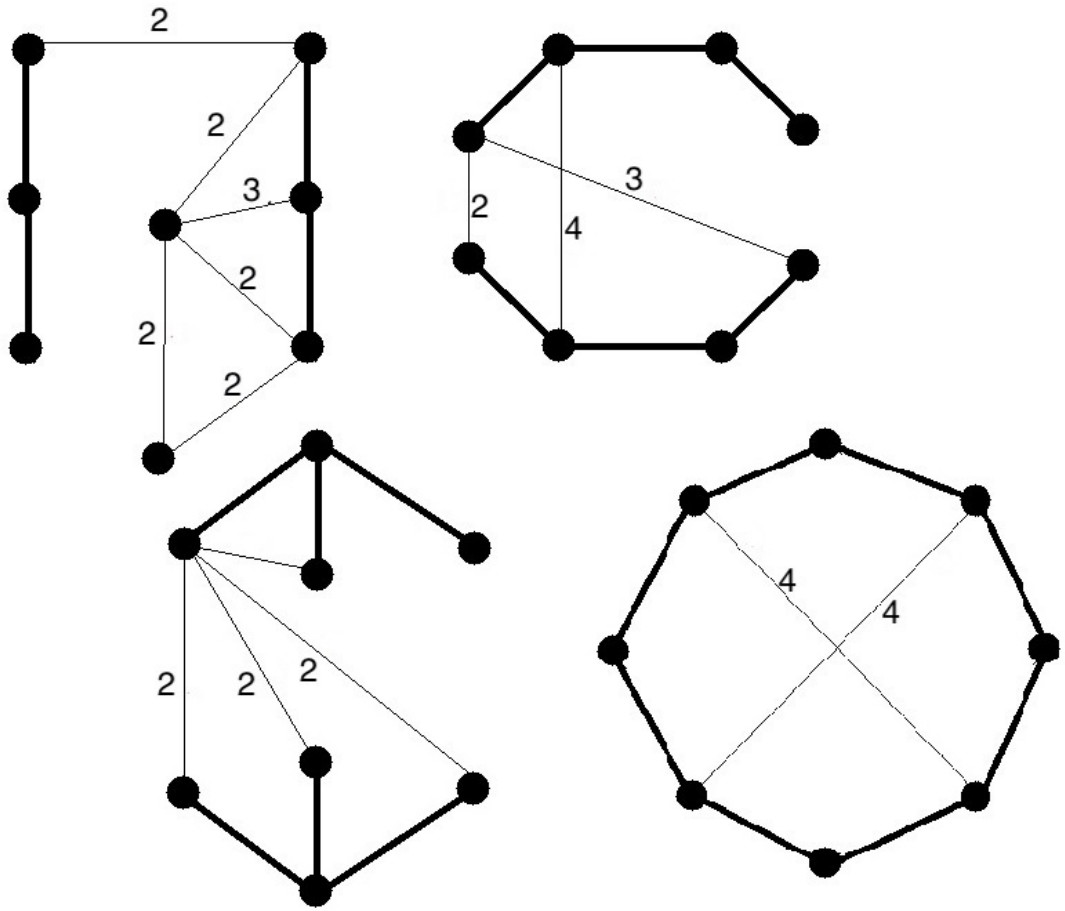


Рис.: Подграфы из G_8

1. Два 2-пути и две изолированные вершины.
   - нулевой вектор – вершина степени два (6 функций), пример АНФ:
   $$x_1x_2 \oplus x_3 \oplus x_4 \oplus 1$$
   - нулевой вектор – вершина степени один(12 функций), пример АНФ:
   $$x_1x_2 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1$$
   - нулевой вектор – изолированная вершина (6 функций), пример АНФ:
   $$x_3x_4 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1$$

2. Два 3-пути.
   - нулевой вектор – вершина степени два (24 функции), пример АНФ:

$$x_1x_2 \oplus x_2x_3 \oplus x_3 \oplus x_4 \oplus 1$$

   - нулевой вектор – вершина степени один (24 функции), пример АНФ:

$$x_1x_2 \oplus x_3x_4 \oplus x_2 \oplus x_3 \oplus x_4 \oplus 1$$

3. Две вершины степени три.
   - нулевой вектор – вершина степени три (4 функции), пример АНФ:

$$x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_4 \oplus 1$$

   - нулевой вектор – вершина степени один (12 функций), пример АНФ:

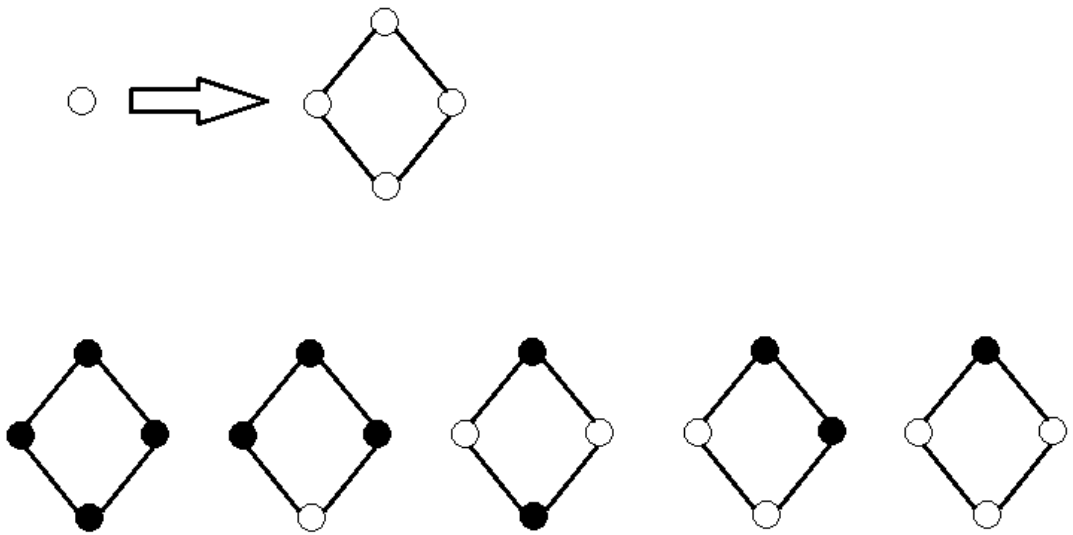
$$x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1$$

4. "Змея в коробке"(12 функций), пример АНФ:

$$x_1x_2 \oplus x_1x_4 \oplus x_2x_3 \oplus x_3x_4 \oplus x_3 \oplus x_4 \oplus 1$$

Построение б.ф. от шести переменных

Построение булевых функций от шести переменных:



Построение б.ф. от шести переменных

Все функции от 4 переменных подходят для построения функций от шести переменных с сохранением параметров алгебраической и корреляционной иммунности, однако пока не найден способ повысить алгебраическую иммунность до максимальной для функций от шести переменных ($AI(f) = 3$).

При $n = 5$ был взят полный список булевых функций с максимальной алгебраической иммунностью ($AI(f) = 3$) - всего их 197 765 122. Из них 48 384 функций имеют корреляционную иммунность порядка 1 ($CI(f) = 1$). Функций с более высоким порядком корреляционной иммунности среди функций с максимальной алгебраической иммунностью не существует.

В результате была получена полная классификация булевых функций от 3, 4 и 5 переменных с максимальной алгебраической иммунностью и обладающих корреляционной иммунностью.
В дальнейшем планируется разработать переход для функций от 4 переменных в функции от 6 переменных с повышением алгебраической иммунности и исследовать связь алгебраической иммунности и корреляционной.