# 1 Построение в виде таблицы истинности

## 1.1 (псевдо)случайной булевой функции от заданного числа переменных;

Просто генерируем вектор длины $2^n$ с помощью генертора случайных чисел

## 1.2 (псевдо)случайной булевой функции заданного веса от заданного числа переменных

Генерируем вектор из нулей длины $2^n$ и с помощью генератора случайных чисел генерируем индекс и ставим на его место 1 пока не получим $w$ единиц

## 1.3 (псевдо)случайной линейнойбулевой функции от заданного числа переменных

Как и выше, генерируем случайный вектор длины $n$ соответствующий присутствию(отсутсвию) переменной $x_i$ в полиноме Жегалкина и дальше считаем его таблицу истинности.

Для пункта с линейными приближениями была также создана функция GetLinearBF[f_, n_], которая по вектору $(a_1, ..., a_n)$ возвращает таблицу истинности.

Проверка того, что функция и правда получается линейной будет в пункте 2.2.

# 2 Разработка способов и реализация средствами САВ “Mathematica” преобразований представлений булевых функций

## 2.1 из многочлена Жегалкина в АНФ

Я так и не осознал как мне в принципе задавать функцию через многочлен. Максимум что мне пришло в голову это сделать что-то вроде

```
BooleanFunction[f_, n_] := Function[u, f[[FromDigits[Reverse[u], 2] + 1]]];
```

Где $f$ - Таблица истинности. Однако с этим неудобно работать/либо я просто не придумал как с этим работать.

## 2.2 из таблицы истинности в многочлен Жегалкина и АНФ

Реализуем преобразование из таблицы истинности в АНФ с помощью рекурсивного алгоритма Так как

$$f(\vec{x}) = a0 + a1 * x1 + a2 * x2 + a3 * x1x2 + ... = \sum_{\vec{\alpha} \in \{0,1\}^n} a_f(\vec{\alpha}) * \zeta(\vec{\alpha}, \vec{x})$$

Получаем матрицу преобразования из АНФ в таблицу истинности:

$$Z_n = \begin{pmatrix} Z_{n-1}, & 0 \\ Z_{n-1}, & Z_{n-1} \end{pmatrix}, Z_1 = \begin{pmatrix} 1, 0 \\ 1, 1 \end{pmatrix}$$

Получаем рекурсивный алгоритм для вычисления произведения $Z_n * \vec{a_f}$

Пусть $a_f^{(1)}$ - первые $2^{n-1}$ бит $a_f$, а $a_f^{(2)}$ - вторые. Тогда $Z_n * \vec{a_f} = (a_f^{(1)}, a_f^{(1)} \bigoplus a_f^{(2)})$.

А так как в поле по модулю 2

$Z_n = Z_n^{-1}$, то то же преобразование работает и в обратную сторону.

Многочлен Жегалкина же я получаю из АНФ просто составляя строки из бинароного представления $i$ для коэффициента АНФ $a_f[i]$;

## 2.3 из многочлена Жегалкина в таблицу истинности;

Так как многочлен Жегалкина в моём коде - строка, я не смог придумать как его преобразовывать в АНФ нормальным способом.

Поэтому представлена только функция АНФ -> таблица истинности

## 2.4 из таблицы истинности в действительный многочлен

Аналогично пункту 2.2, только теперь мы работаем не в поле по модулю 2 а в действительных числах

$$B_n = \begin{pmatrix} Z_{n-1}, & 0 \\ -Z_{n-1}, & Z_{n-1} \end{pmatrix}, B_1 = \begin{pmatrix} 1, 0 \\ -1, 1 \end{pmatrix}$$

Получаем рекурсивный алгоритм для вычисления произведения $B_n * \vec{f}$

Пусть $f^{(1)}$ - первые $2^{n-1}$ бит $f$, а $f^{(2)}$ - вторые. Тогда $B_n * \vec{f} = (f^{(1)}, f^{(2)} - f^{(1)})$.

В итоге получаем коэффиценты действительного многочлена.

## 2.5 вычисление списка спектральных коэффициентов (Фурье, Адамара-Уолша) по таблице истинности

Для Адамара-Уолша мы берем вектор значений $(-1)^{\vec{f}}$ или то же самое $1 - 2 * \vec{f}$

Умножаем его на матрицу, которая задана рекурсивно:

$$H_n = \begin{pmatrix} H_{n-1}, H_{n-1} \\ H_{n-1}, -H_{n-1} \end{pmatrix}, H_1 = \begin{pmatrix} 1, 1 \\ 1, -1 \end{pmatrix}$$

и получаем $\vec{\hat{f}} = H_n * (-1)^{\vec{f}}$ - Коэффиценты Адамара-Уолша.

Коэффициенты Фурье получаем из коэффициентов Адамара-Уолша:

$\tilde{f}(\vec{0}) = |f| = \frac{(2^n - \hat{f}(\vec{0}))}{2}$

А для остальных

$\tilde{f}(\vec{\alpha}) = -\frac{\hat{f}(\vec{\alpha}))}{2}$

### 2.6 получение таблицы истинности по спектральным коэффициентам

Я принимал за спектральные коэффициенты - коэффициенты Фурье.

Таким образом обращаем получение Фурье из А-У из предыдущего пункта. Применяем преобразование А-У и делим все на $2^n$>, потому что $H_n^{-1} = 2^{-n} * H_n$

Так как мы получили $(-1)^{\vec{f}}$ или же $1 - 2\vec{f}$

Обращаем эту операцию.

## 3 Разработка способов и реализация средствами САВ “Mathematica” инструментов исследования булевых вектор-функций

### 3.1 Построение вектор-функций для заданных размерностей ходных и выходных векторов

#### 3.1.1/2 из разрядных функций/ (псевдо)случайным образом

Та же самая проблема про задание бф как многочлена из пункта 2.1

Поэтому я просто сделал через таблицу истинности вектор функции

```
VectorFunctionR[fs_, n_, m_] := Function[u, Table[fs[[i, FromDigits[u, 2] + 1]], {i, m}]];
```

### 3.2 Исследование разрядных функций вектор-функции

#### 3.2.1 Получение разрядных функций вектор-функции, заданной таблично, где входные и выходные вектора упакованы в (целые неотрицательные) числа

Просто разворачиваем таблицу

#### 3.2.2 Получение следующих характеристик разрядных функций

- Вес

Число 1 в таблице истинности

- Число мономов для многочлена Жегалкина каждой функции

  Число 1 в векторе АНФ

- Число мономов во всех многочленах Жегалкина разрядных функциях

  Число 1 в Побитовом Или векоторов АНФ всех разрядных функций

- Список линейных аналогов и соответствующих вероятностей совпадения разрядной функции с линейной (аффинной)

  Считаем коэффициенты А-У. Из них получаем вероятности(не обязательный шаг для сортировки)

  $P(f(\vec{x}) = \vec{\alpha} * \vec{x}) = \frac{1}{2} + \frac{\hat{f}(\vec{\alpha})}{2^{n+1}}$

  Итерируемся по всем полученным вероятностям и ищем максимальную(минимальную). Возвращаем все линейные(афинные) аналоги с данной вероятностью.

- Действительный многочлен, его степень и число мономов, а также частные производные в точке (0.5,…,0.5) по каждой переменной
  - Действительный многочлен мы уже считали в пункте 2.4
  - Вероятность равенству 1 - вычисляем многочлен в точке по его коэффицентам
  - Степень - в векторе коэффициентов ищем индекс, вес бинарного представления которого максимален
  - Число мономов - считаем ненулевые элементы в векторе коэффициентов
  - Частные производные - то же что и вероятность но только убираем те коэффиценты в которых на $i$-й позиции бинарного представления - $0$

## 3.3 Получение коэффициентов Адамара-Уолша вектор-функции и соответственно списка линейных комбинаций входных и выходных переменных, вероятность равенства нулю которых максимальна (минимальна).

Анализируем уже Тетта функцию:

$$\Theta_F(\vec{x}, \vec{y}) = \begin{cases} 1 & \text{Если } \vec{F}(\vec{x}) = \vec{y} \\ 0 & \text{Иначе} \end{cases}$$

Так как

$P(\vec{a} * \vec{x} = \vec{b} * \vec{F}(\vec{x})) = 1/2 + \widetilde{\Theta}_F(\vec{a}, \vec{b})/2^{n+1}$

С помощью коэффицентов Фурье ищем наиболее вероятную комбинацию.

Минимальная из таких вероятностей позволяет найти комбинации вида

$\vec{a} * \vec{x} = \vec{b} * \vec{F}(\vec{x}) + 1$