# Полином Жегалкина

**Определение.** *Положительной конъюнкцией* называется элементарная конъюнкция, не содержащая инверсий переменных. Договоримся обозначать положительную конъюнкцию через K+.

**Примеры.** K1+=x1x2 x3, K2+= x4, K3+=1. •

**Определение.** *Полиномом Жегалкина*, или *алгебраической нормальной формой (АНФ)*, булевой функции f(x1, …, xn) называется дизъюнкция с исключением различных положительных конъюнкций переменных из множества X={x1, …, xn}, то есть формула вида

P= K1+ https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif… https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifKp+,

задающая функцию f(x1, …, xn.

**Пример.** P=x1x3https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif x1x2 x4https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif x2 https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif1 – полином Жегалкина. •

**Определение.** *Длиной полинома Жегалкина назовем* количество конъюнкций в полиноме, а его *степенью* – наибольший из рангов конъюнкций, входящих в полином.

**Пример.** Длина полинома Жегалкина из предыдущего примера равна 4, а степень – 3.

Условимся считать константу 0 полиномом длины и степени 0.

**Определение.** Полином Жегалкина называется *линейным*, если его степень не превышает единицы.

**Примеры.** P1=1, P2=x https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gify https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif1 – линейные полиномы. •

Напомним основные равносильности для дизъюнкции с исключением (подраздел 4.3), необходимые для дальнейших рассуждений.

*Свойства 0 и 1:* x https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif0 = x, x https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif1 = x .

*Закон коммутативности:* x https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gify = y https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifx.

*Закон ассоциативности:* x https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif(y https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifz) = (x https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gify) https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifz = x https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gify https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifz.

*Закон дистрибутивности:* x(y https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifz) = xy https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifxz.

Добавим к ним еще две равносильности (первая очевидна, доказательство второй предоставляется читателю):

x https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifx = 0,

x https://ido.tsu.ru/iop_res/bulevfunc/text/img/img4.gify = x https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gify https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifxy.

Если в последней равносильности переменные заменить конюнкциями, то получим:

K1https://ido.tsu.ru/iop_res/bulevfunc/text/img/img4.gif K2= K1https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif K2https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif K1K2.

Для ортогональных конъюнкций равносильность примет вид:

K1https://ido.tsu.ru/iop_res/bulevfunc/text/img/img4.gif K2= K1https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif K2.

В частности, совершенная ДНФ булевой функции f(x1, …, xn) состоит из попарно ортогональных конъюнкций, значит

https://ido.tsu.ru/iop_res/bulevfunc/text/img/g15_3_1_1.gif

# Теорема о существовании полинома Жегалкина.

Любая булева функция представима полиномом Жегалкина.

## Доказательство.

Константа 0 – это полином Жегалкина по договоренности. Любая другая булева функция f(x1, …, xn) представима совершенной ДНФ (подраздел 7.3.), а значит, как только что было показано, и формулой вида:

https://ido.tsu.ru/iop_res/bulevfunc/text/img/g15_3_1_2.gif

Эта формула не является полиномом Жегалкина, если содержит переменные с инверсиями. От инверсий можно избавиться, используя равносильность x =x https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif1. Раскрыв в полученной формуле скобки на основе закона дистрибутивности, получим сумму положительных конъюнкций, которая не является полиномом Жегалкина, если в ней конъюнкции повторяются. Используя равносильности x https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifx = 0 и x https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif0 = x, удалим пары одинаковых конъюнкций. В результате получим полином Жегалкина.

# Теорема о единственности полинома Жегалкина.

Каждая булева функция имеет единственный полином Жегалкина.

## Доказательство.

Как только что было замечено, число различных полиномов Жегалкина булевых функций *n* аргументов равно числу булевых векторов длины 2*n*, то есть равно 22*n*. Но количество различных булевых функций n аргументов тоже равно 22*n* (по теореме о числе булевых функций), и каждая булева функция представима полиномом Жегалкина (по теореме о существовании полинома), следовательно, на каждую булеву функцию приходится ровно по одному полиному Жегалкина. •

Таким образом, наряду с совершенной ДНФ, совершенной КНФ и сокращенной ДНФ, полином Жегалкина является еще одной канонической формой представления булевых функций.

# Лемма о числе положительных конъюнкций.

Число различных положительных конъюнкций переменных из множества

X={x1 …, xn} равно 2*n*.

## Доказательство.

Каждая положительная конъюнкция состоит из подмножества переменных из X, то есть представляется булевым вектором длины *n*, и наоборот, каждый вектор длины *n* задает положительную конъюнкцию подмножества переменных X. Значит, число различных положительных конъюнкций равно числу векторов длины *n*, то есть равно 2*n*.

# Определения и примеры

**Определение.** Форму представления полинома Жегалкина

P = c0 K0+ https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifc1K1+ https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif… https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifc2*n* –1 K2*n* –1+

булевой функции f(x1, …, xn), где ci – булевы константы, назовем *формой с коэффициентами.*

Число 2*n* положительных конъюнкций Ki+ определяется леммой. Договоримся однозначно связывать с номером конъюнкции Ki+ ее вид по следующему правилу: число i представлять булевым вектором a1 … an, который, в свою очередь, задаст подмножество переменных, составляющих конъюнкцию Ki+.

**Пример.** При n=3 конъюнкция K5+=x1x3, так как число 5 представляется булевым вектором 101, который задает подмножество переменных {x1,x3} множества {x1, x2, x3}. •

Таким образом, полином Жегалкина булевой функции *n* аргументов однозначно определяется вектором своих коэффициентов π=c0 c1… c2*n* –1, и наоборот, любой булев вектор длины 2*n* однозначно определяет полином Жегалкина функции *n* аргументов.

**Пример.** Полином Жегалкина

P=1 https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifx https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifxz https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifyzhttps://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif xyz = K0+ https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifK4+https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif K5+ https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifK3+ https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gifK7+ =

= 1 K0+ https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif0 K1+ https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif0 K2+ https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif1 K3+ https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif1 K4+ https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif1 K5+ https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif0 K6+ https://ido.tsu.ru/iop_res/bulevfunc/text/img/img7.gif1 K7+

представляется вектором коэффициентов π=10011101. •

Из последних рассуждений следует, что число различных полиномов Жегалкина булевых функций *n* аргументов равно числу различных булевых векторов длины 2*n*.

# Любая булева функция однозначно задается совершенной ДНФ, причем однозначно.

Совершенная дизъюнктивная нормальная форма (СДНФ) — это такая [ДНФ](https://ru.wikipedia.org/wiki/%D0%94%D0%9D%D0%A4), которая удовлетворяет трём условиям:

* в ней нет одинаковых элементарных конъюнкций
* в каждой конъюнкции нет одинаковых пропозициональных букв
* каждая элементарная конъюнкция содержит каждую пропозициональную букву из входящих в данную [ДНФ](https://ru.wikipedia.org/wiki/%D0%94%D0%9D%D0%A4) пропозициональных букв, причём в одинаковом порядке.

Любая [булева формула](https://ru.wikipedia.org/wiki/%D0%91%D1%83%D0%BB%D0%B5%D0%B2%D0%B0_%D1%84%D0%BE%D1%80%D0%BC%D1%83%D0%BB%D0%B0), не являющаяся тождественно ложной, может быть приведена к СДНФ, причем единственным образом, то есть для любой выполнимой функции алгебры логики существует своя СДНФ, причём единственная.