Выражение функции XOR через медианы

Теорема:

$x_0 \oplus x_1 \oplus \ldots \oplus x_{2m} = \langle \neg x_0, s_1, s_2, \ldots, s_{2m} \rangle$,
$s_j = \langle x_0, x_j, x_{j+1}, \ldots, x_{j+m-1}, \neg x_{j+m}, \neg x_{j+m+1}, \ldots, \neg x_{j+2m-1} \rangle$, где x_{2m+k} обозначает то же, что и x_k, при $k \geqslant 1$.

Разберемся с условием. Мы хотим доказать, что побитовый XOR с $2m + 1$ аргументами выражается с помощью медианы с $2m + 1$ аргументом. Аргументами медианы является набор $\{s_i\}$, получаемый следующим образом:

- Выпишем последовательность $x_1, x_2, \ldots, x_{2m}$
- Первую половину аргументов (а их ровно m) возьмем с отрицанием ($\neg x_1, \neg x_2, \ldots, \neg x_m, x_{m+1}, x_{m+2}, \ldots, x_{2m}$)
- Слева к этой последовательности припишем x_0 и подадим в качестве аргументов медиане: $\langle x_0, \neg x_1, \neg x_2, \ldots, \neg x_m, x_{m+1}, x_{m+2}, \ldots, x_{2m} \rangle$ — так мы получили s_{m+1}
- Остальные s_i получаются "циклическим сдвигом" отрицания (без учета x_0), например, вправо (так мы получим все "циклические сдвиги" отрицаний):
  - $s_1 = \langle x_0, x_1, x_2, x_3, \ldots, x_{m-1}, x_m, \neg x_{m+1}, \neg x_{m+2}, \neg x_{m+3}, \ldots, \neg x_{2m-1}, \neg x_{2m} \rangle$
  - $s_m = \langle x_0, \neg x_1, \neg x_2, \neg x_3, \ldots, \neg x_{m-1}, x_m, x_{m+1}, x_{m+2}, x_{m+3} \ldots, x_{2m-1}, \neg x_{2m} \rangle$
  - $s_{m+2} = \langle x_0, x_1, \neg x_2, \neg x_3, \ldots, \neg x_{m-1}, \neg x_m, \neg x_{m+1}, x_{m+2}, x_{m+3} \ldots, x_{2m-1}, x_{2m} \rangle$,
  - $s_{m+3} = \langle x_0, x_1, x_2, \neg x_3, \ldots, \neg x_{m-1}, \neg x_m, \neg x_{m+1}, \neg x_{m+2}, x_{m+3}, \ldots, x_{2m-1}, x_{2m} \rangle$,

И нужно проверить, что $\langle \neg x_0, s_1, s_2, \ldots, s_{2m} \rangle = x_0 \oplus x_1 \oplus \ldots \oplus x_{2m}$.

Содержание

Вспомогательные утверждения

Лемма:

Каждой s_i можно однозначно сопоставить в пару такую s_j, что все переменные (кроме x_0) с отрицанием из s_i в s_j будут без отрицания и наоборот. Аргументы x_0 у всех s_i одинаковые, поэтому будем разбивать на пары без учета x_0.

Доказательство:

Мы строим набор s_i, циклически сдвигая отрезок отрицания переменных, пока не получим все возможные. Совершив ровно m таких шагов, мы сдвинем начало отрезка отрицания на следующую позицию после его конца. Таким образом, там, где был отрезок отрицания, будет отрезок без отрицания, и наоборот.

Назовем такую пару (s_i, s_j) **двойственной**, и будем обозначать через $\neg s_i$ двойственную s_i пару.

Пусть на j-ом месте у s_i стоит единица ($j > 0$). Назовем этот аргумент **самостоятельной единицей**.

Утверждение:

> Если в s_i ровно n самостоятельных единиц, то в $\neg s_i$ их будет $(2m - n)$.

У двойственного элемента все самостоятельные единицы станут нулями, а все нули — единицами. А всего позиций $2m$.

Утверждение:

> Среди x_i четное число единиц $\Leftrightarrow$ найдется двойственная пара, элементы которой имеют одинаковое количество самостоятельных единиц.

Пусть A_i — множество аргументов (за исключением x_0) s_i с отрицанием, B_i — без отрицания (тоже за исключением x_0). Оба множества по условию мощности m. Пусть среди A_i ровно a_i переменных равны единице, тогда оставшиеся $(m - a_i)$ из них — нули. Аналогично среди B_i ровно b_i единиц и $(m - b_i)$ нулей. Самостоятельные единицы s_i получаются из нулей среди A_i и единиц среди B_i. Тогда в s_i будет $(m - a_i) + b_i$ самостоятельных единиц. В $\neg s_i$ переменные заменятся на их отрицания, поэтому самостоятельные единицы в ней получаются из единиц среди A_i и нулей среди B_i. Поэтому количество самостоятельных единиц в $\neg s_i$ будет $a_i + (m - b_i)$.

$\Leftarrow$

Приравняем количества самостоятельных единиц в паре: $(m - a_i) + b_i = a_i + (m - b_i) \Leftrightarrow a_i = b_i$

А a_i и b_i — количества единиц в A_i и в B_i соответственно, и, так как множество всех аргументов s_i это $A_i \cup B_i$, то $(a_i + b_i)$ и есть количество единиц среди ее аргументов. Но $a_i = b_i$, значит $a_i + b_i$ четное.

Вообще, утверждения "нашлась двойственная пара, элементы которой имеют одинаковое количество самостоятельных единиц" (1) и "нашлась s_i с количеством самостоятельных единиц, равным m" равносильны.

И правда, выше мы поняли, что (1) $\Leftrightarrow a_i = b_i$. Посчитаем количество самостоятельных единиц в s_i. $((m - a_i) + b_i) = m \Leftrightarrow a_i = b_i$.

$\Rightarrow$

Пусть среди $x_i (i > 0)$ будет $2t$ единиц. Давайте найдем s_j, в которой среди A_j единиц столько же, сколько и среди B_j. Тогда в ней будет $a_j = b_j$, из чего и будет следовать требуемое. Рассмотрим любую s_k. Будем считать, что в A_k меньше половины единиц ($a_k < t$), иначе рассмотрим двойственную ей, в ней будет меньше половины, или, если равенство, то мы уже нашли такую. Будем последовательно сдвигать

отрицания вправо на одну позицию, переходя от s_l к s_{l+1}. За каждый сдвиг количество единиц в A_l может измениться только на 1. Действительно, если в A_l добавились и ушли разные числа, то количество единиц изменилось на 1 (увеличилось или уменьшилось), а если одинаковые — то не поменялось. Таким образом, сделав m шагов, мы дойдем от s_k до $\neg s_k$, причем количество единиц в A_l будет изменяться не более, чем на 1. Изначально оно было a_l, а станет — $2t - a_l$. Тогда выполняются неравенства: $a_k \leqslant t \leqslant 2t - a_k$. Левый знак верен просто потому, что мы так выбрали s_k, а правый, очевидно, равносилен первому. Таким образом, мы, изменяя a_l не больше, чем на единицу, пришли из a_k в $2t - a_k$, причем число t было между ними. Поэтому мы обязательно на каком-то шаге оказались с $a_{l'} = t$, то есть ровно половина единиц попала в $A_{l'}$, чего мы и хотели.

Заметим также, что мы доказали наличие **одной пары**, но на самом деле таких может быть больше. Давайте такие пары назовем **особенными**, а остальные — обычными.

Доказательство теоремы

Теорема:

$$x_0 \oplus x_1 \oplus \ldots \oplus x_{2m} = \langle \neg x_0, s_1, s_2, \ldots, s_{2m} \rangle,$$
$$s_j = \langle x_0, x_j, x_{j+1}, \ldots, x_{j+m-1}, \neg x_{j+m}, \neg x_{j+m+1}, \ldots, \neg x_{j+2m-1} \rangle$$

Доказательство:

Пусть k_i — количество самостоятельных единиц у s_i.

Рассмотрим два случая.

1. $x_0 = 0$.
   - Тогда в каждой s_i будет стоять вместо него 0, то есть количество аргументов-единиц в точности равно количеству самостоятельных единиц.
   - Пусть $k_i \geqslant m + 1 \Rightarrow k_{i+m} \leqslant m - 1$ (и аналогично с противоположным знаком) $\Rightarrow$ в обычных парах одна s_i будет равна 1, а вторая 0.
   - При нечетном количестве единиц особенных пар не будет, будет только ровно m обычных пар, из каждой ровно одна s_i даст единицу. Тогда среди всех s_i будет ровно m единиц, и, подставив их в конечную медиану, вместе с $\neg x_0 = 1$, получим ровно $m + 1$ аргумент, равный 1. Тогда медиана вернет 1, что и должен вернуть XOR нечетного числа единиц.
   - При четном количестве у нас найдется особенная пара, а в этих s_i и $\neg s_i$ ровно по m самостоятельных единиц, а значит, они обе будут равны 0. Тогда всего среди s будет не более $(m - 1)s_i$ равных одному, значит, конечная медиана вернет 0, что и нужно при XOR-е четного числа единиц.
2. $x_0 = 1$
   - Тогда в каждой s_i будет стоять вместо него 1, то есть количество аргументов-единиц для s_i на один больше количества самостоятельных единиц.
   - Пусть $k_i \geqslant m + 1 \Rightarrow k_{i+m} \leqslant m - 1$ (и аналогично с противоположным знаком) $\Rightarrow$ по-прежнему (тут с учетом $x_0 = 1$) в обычных парах одна s_i будет равна 1, а вторая 0.
   - При нечетном количестве единиц особенных пар нет, будет снова только ровно m обычных пар, из каждой ровно одна s_i даст единицу. Тогда среди всех s_i будет ровно m единиц, и,

подставив их в конечную медиану, вместе с $\neg x_0 = 0$, получим ровно m аргументов, равных 1 . Тогда медиана вернет 0, что и должен вернуть XOR четного числа единиц.

- При четном количестве у нас найдется особенная пара, а в этих s_i и $\neg s_i$ ровно по m самостоятельных единиц, а значит, они обе будут равны 1, ведь вместе с $x_0 = 1$ среди аргументов медиан будет по $m + 1$ единиц. Тогда всего среди s_i будет не менее $m + 1$ $s_i = 1$, значит, конечная медиана вернет 1, что и нужно при XOR-е нечетного числа единиц.

См. также

- Представление функции формулой, полные системы функций
- Представление функции класса DM с помощью медианы
- Определение булевой функции

Источники информации

- Notes on Majority Boolean Algebra (https://si2.epfl.ch/~demichel/publications/archive/2016/2016_ismvl_1.pdf)
- Multi-input XOR Gate Using Multi-input Majority Function (https://www.researchgate.net/profile/Esam_Alkaldy/publication/277518459_A_Novel_Design_Approach_for_Multi-input_XOR_Gate_Using_Multi-input_Majority_Function/links/568b60df08ae051f9afa9b56/A-Novel-Design-Approach-for-Multi-input-XOR-Gate-Using-Multi-input-Majority-Function.pdf)
- Upper bounds on formula size for specific functions (http://sites.math.rutgers.edu/~sk1233/courses/topics-S13/lec1.pdf)

- Эта страница последний раз была отредактирована 4 сентября 2022 в 19:36.