1 Polynomial calculus proofs

Опр: Дано поле K и множество переменных. **Polynomial calculus refutation** множества аксиом P, это последовательность полиномов такие что последняя строчка это 1 и каждая строчка это либо аксиома, либо получается из предедущих строчек использованием правил вывода: $\frac{f \quad g}{\alpha f+\beta g}$ и $\frac{f}{x\cdot f}$. Где α, β из K это скаляры а x любая переменная.

Опр: Степень опровержения равна d если степени все полиномов в опровержении степени не больше d.

Мы считаем, что полиномы x^2-x входят в аксиомы для всех переменных x. Это означает, что аксиомы $f_1, ..., f_k$ опровержимы тогда и только тогда когда $f_1 = f_2 = ... = f_k = 0$ не имеет $0-1$ решений.

Обозн: Для полинома f пусть $\bar{f}$ это единственный полилинейный полином равный f по модулю идеала порожденного всеми полиномами $x^2 - x$.

Обозн: Множество из чисел от 1 до i будем обозначать как $[i]$

Обозн: $x_{ij} = 1$ означает, что голубь i стоит в клетке j.

Пусть $Q_i = 1 - \sum_{j\in[n]} x_{ij}$. Тогда $\neg PHP_n^m$

это следующие полиномы:

1) Q_i для $i \in [m]$ 2) $x_{ij}x_{ij'}$ для $i \in [m], j, j' \in [n], j \neq j'$ 3) $x_{ij}x_{i'j}$ для $i, i' \in [m], j \in [n], i \neq i'$

Опр: Пусть T это множество всех мономов $x_{i_1j_1}...x_{i_kj_k}$ таких что все i_l различны и все j_l различны и пусть T_d будет множество всех мономов степени не более d.

Утв: Любой полином это линейная комбинация термов из T без увеличения степени.

Мы хотим построить базис B_d от векторного пространтсва порожденного T_d так чтобы элементами базиса были произведения неких переменных и неких аксиом Q, например $x_{3,1}x_{5,3}Q_2Q_4$. Если мы справимся все строчки доказательства выписать в этом базисе то 1 нельзя будет вывести из аксиом. Определение B_d использует понятие "pigeon dance"которое мы сейчас определим

Опр: Пусть $A = \{a|a$ функция из $[m]$ в

$$\{0, 1, ..., n\}$$

такая что

$$\forall i, a(i) = a(i')$$

означает что $i = i'\}$

Опр:A_d= $\{a \in A||a| \leq d\}$

Для $a = \{(i_1, j_1), ..., (i_k, j_k), (i'_1, 0), ..., (i'_l, 0)$ где j_m ненулевые, определяем $x_a = x_{i_1,j_1}...x_{i_k,j_k}Q_{i'_1}..Q_{i'_l}$ и

$$\hat{a} = \{(i_1, j_1), ..., (i_k, j_k)\}$$

Опр: Интуитивно, pigeon dance это когда у нас есть расстановка голубей по клеткам (те которые не в какой то клетке считаем в клетке 0), и мы передвигаем первого голубя до какой то незабитой клетки большей по номеру чем в той который он сидит. И так с каждем голубем.

Опр: Минимальный pigeon dance это когда передвигаем голубей до **минимальной** незабитой клетки большей по номеру.

Теорема 1. *Если существует pigeon dance то существует минимальный pigeon dance.*

Опр *$B_d = \{x_a | a \in A_d$ и существует pigeon dance на тех голубях которые не в клетке 0$\}$*

Утв *Если $d \leq \lceil n/2 \rceil$ и $a \in A_d$ то существует pigeon dance на a тогда и только тогда когда существует на $\hat{a}$*

Утв *Минимальный pigeon dance это биекция*

Утв *B_d это базис*

Теорема 2. *PHP^n_m не имеет polynomial calculus refutation степени $\leq \lceil n/2 \rceil$*