# Нижние оценки

- Доказать, что данную задачу нельзя решить быстрее, чем указано
- Нижние оценки: чем больше, тем точнее. (Для верхних оценок – наоборот)
- Обычно более сложная задача, чем нахождение верхних оценок
- Рассмотрим на примере одной задачи: умножения матрицы на вектор.

# Определения

- *Поле*: (A,+,*,0,1)
  - Кольцо с 1
  - * - коммутативно
  - $\forall\ a \in A \setminus \{0\}\ \exists\ a^{-1}: aa^{-1} = 1$
- *Формальные переменные*: $x \notin A$
- *Расширение поля формальными переменными*: $F[x_1,\ldots,x_n]$ – наименьшее коммутативное кольцо (B,+,*,0,1), такое что $B \supseteq A \cup \{x_1,\ldots,x_n\}$

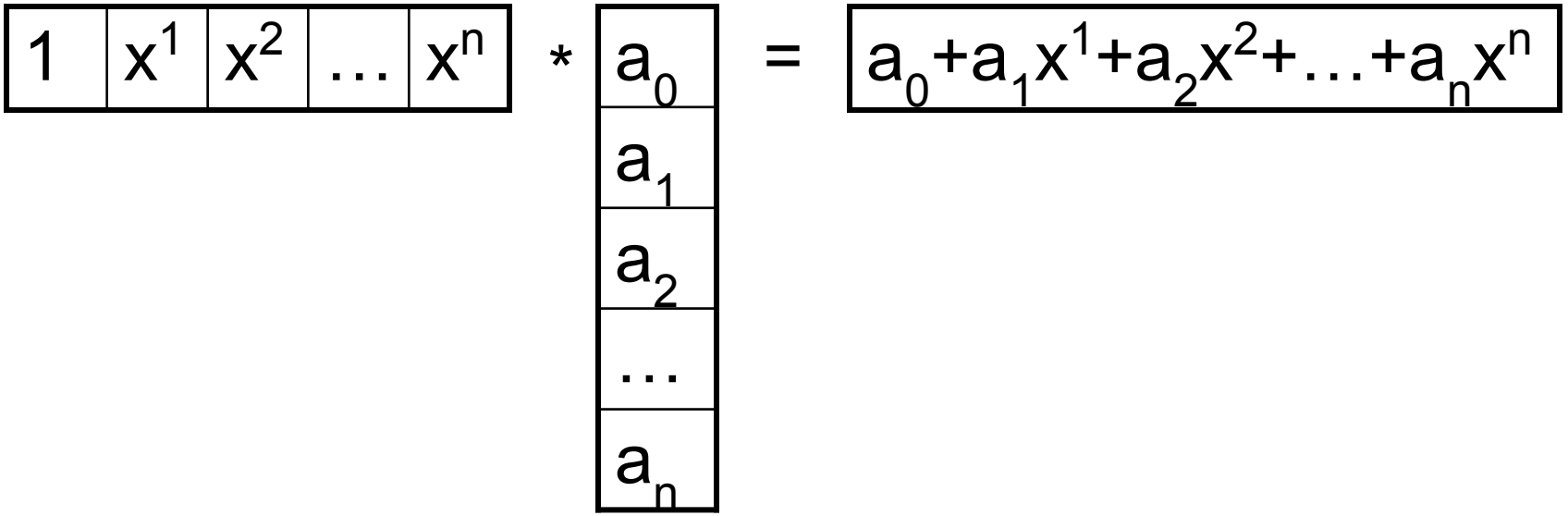
# Матричные формулировки

- Умножение комплексных чисел: (a+ib)(c+id)

| | | | | | | |
|---|---|---|---|---|---|---|
| a | -b | * | c | = | ac – bd |
| b | a | | d | | bc + ad |

# Матричные формулировки

- Вычисление полинома



# Модель вычислений

- $X = \{x_1,\ldots,x_n\}$ – формальные переменные (параметры программы)
- $Y = \{y_1,\ldots,y_n\}$ – вспомогательные переменные (вычисляются на основе $x_i$)
- *Неветвящаяся программа* $\pi$ над F – конечная последовательность команд вида

  $a := b \oplus c$

  где
  - $a \in Y$
  - $b,c \in X \cup F \cup Y$
  - $\oplus \in \{+,-,*\}$

# Термальное значение

- $v : X \cup Y \rightarrow F[x_1,\ldots,x_n]$ – значения переменных «в терминах» $x_1,\ldots,x_n$.
  - $v(c) = c$, если $c \in F$
  - $v(x) = x$, если $x \in X$
  - $v(y) = v(b) \oplus v(c)$, если $y \in Y$ и в программе есть команда $y := b \oplus c$.
- *Программа* $\pi$ *вычисляет* множество полиномов $\{ v(a) \mid a \in X \cup Y\}$

# Пример: ac-bd, ad+bc

X = {a,b,c,d}, Y = {y1, y2, … }

- $y_1 := ac$
- $y_2 := bd$
- $y_3 := y_1+y_2$ ⟸
- $y_4 := ad$
- $y_5 := bc$
- $y_6 := y_1+y_2$ ⟸

4 умножения

- $y_1 := a+b$
- $y_2 := y_1c$
- $y_3 := d-c$
- $y_4 := ay_3$
- $y_5 := y_4+y_2$ ⟸
- $y_6 := d+c$
- $y_7 := by_6$
- $y_8 := y_2-y_7$ ⟸

3 умножения

# Определения

- Вектора $v_1,\ldots,v_k$ $\in F^m[a_1,\ldots,a_n]$ *линейно-независимы по модулю* $F^m$, если

  $\forall u_1,\ldots u_k \in F : (\Sigma u_i v_i \in F^m \Rightarrow \forall i : u_i=0)$
- *Ранг матрицы* M над $F[a_1,\ldots,a_n]$
  - *по строкам* – количество л.-н. строк
  - *по столбцам* – количество л.-н. столбцов

- **Пример**: M= | $a_1$ | $a_2$ | $a_3$ |
  - ранг по строкам = 1
  - ранг по столбцам = 3

# Теорема о нижней оценке (1)

- **Теорема**. Пусть M – (r×p)-матрица над $F[a_1,\ldots,a_n]$, $x=[x_1,\ldots,x_p]^T$ - столбец. Тогда, если ранг M по строкам равен r, то любое вычисление Mx требует *не менее r умножений*.

- $X=\{a_1,\ldots,a_n, x_1,\ldots,x_p\}$ – формальные переменные.

# Доказательство

- Пусть требуется s умножений
- $e_1,\ldots,e_s$ - вычисляются на шагах с умножением
- Тогда Mx = Ne + f, где
  - N – (r×s)-матрица над F
  - e = $[e_1,\ldots,e_s]$
  - f – вектор линейных комбинаций над $x_i$

# Доказательство

- Пусть r>s (противное)
- Тогда строки N линейно-зависимы (в обычном смысле матриц над полем)
- То есть $\exists y=[y_1,\ldots,y_r] \in F^r$, $y \neq \underline{0}$ : $yN = \underline{0}$
  ($\underline{0}$ - нулевой вектор)
- Домножая слева на y, получаем:
  $(yM)x = (yN)e + yf = yf$
- Поскольку в yf нет $x_i x_j$, то в yM нет xi
- Т.е. $yM \in F^m$ и строки M линейно зависимы.
- Противоречие. Конец доказательства.

# Теорема о нижней оценке (2)

- **Теорема**. Пусть M – (r×p)-матрица над $F[a_1,\ldots,a_n]$, $x=[x_1,\ldots,x_p]^T$ – столбец, $y \mathrm{O} F^p[a_1,\ldots,a_n]$. Тогда, если ранг M по столбцам равен q, то любое вычисление Mx+y требует *не менее q активных умножений*.
- *Активное умножение* y*z, если v(y) содержит $x_i$, а $v(z) \notin F$ или наоборот

# Активное умножение - примеры

| v(y) | v(z) | |
|---|---|---|
| $3+a_2$ | $x_1+2x_3$ | Активно |
| 3 | $x_1+2x_3$ | Неактивно |
| $3+a_2$ | $a_1+2a_3$ | Неактивно |

# Доказательство (индукция)

- q = 1)
  - Существует $m_{ij} \in F[a_1,\ldots,a_n] \setminus F$
  - Mx (a значит, и MX+y) содержит произведение $m_{ij}x_j$
  - Без активных умножений можно вычислить только $P(a_1,\ldots,a_n) + L(x_1,\ldots,x_p)$, где
    - P – полином
    - L – линейная комбинация
  - Следовательно, есть хотя бы одно активное умножение.

# Доказательство (индукция)

- Шаг индукции: q>1
  - Пусть $\pi$ – вычисление для Mx+y.
  - По предположению индукции $\pi$ содержит q-1 активное умножение
  - Пусть f := gh – первое активное умножение, где (без потери общности)

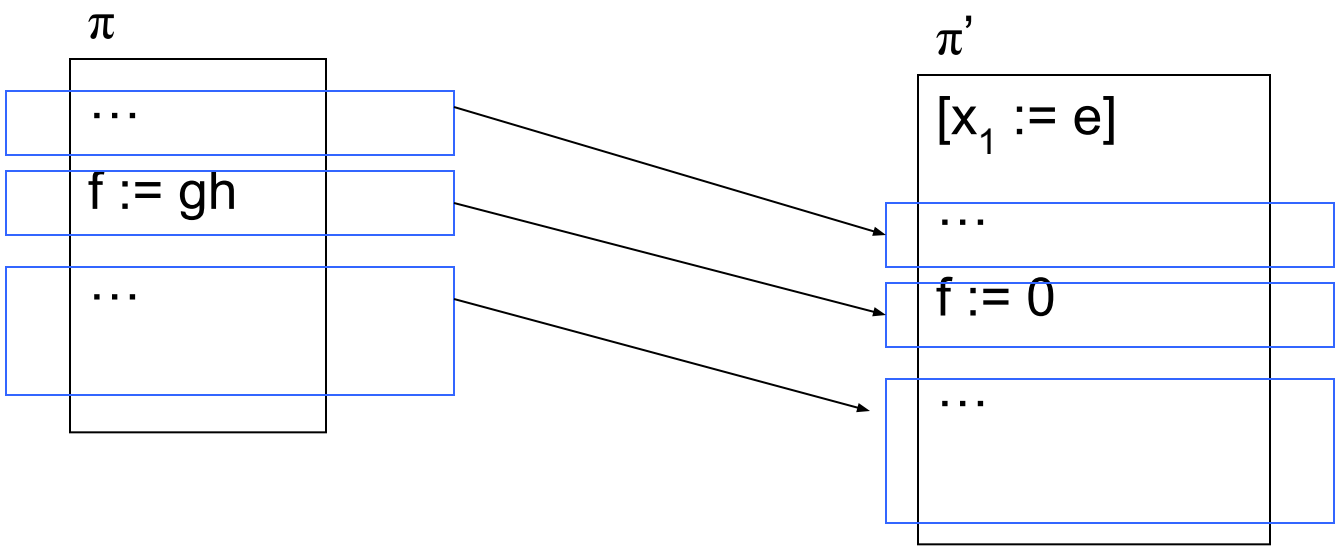
    $v(g) = P(a_1,\ldots,a_n) + (c_1x_1+\ldots+c_px_p)$, $c_1 \neq 0$
  - Заметим, что значение $x_1$ равное

    $e = - c_1^{-1} (P(a_1,\ldots,a_n) + (c_2x_2+\ldots+c_px_p))$

    обращает v(g) в 0.

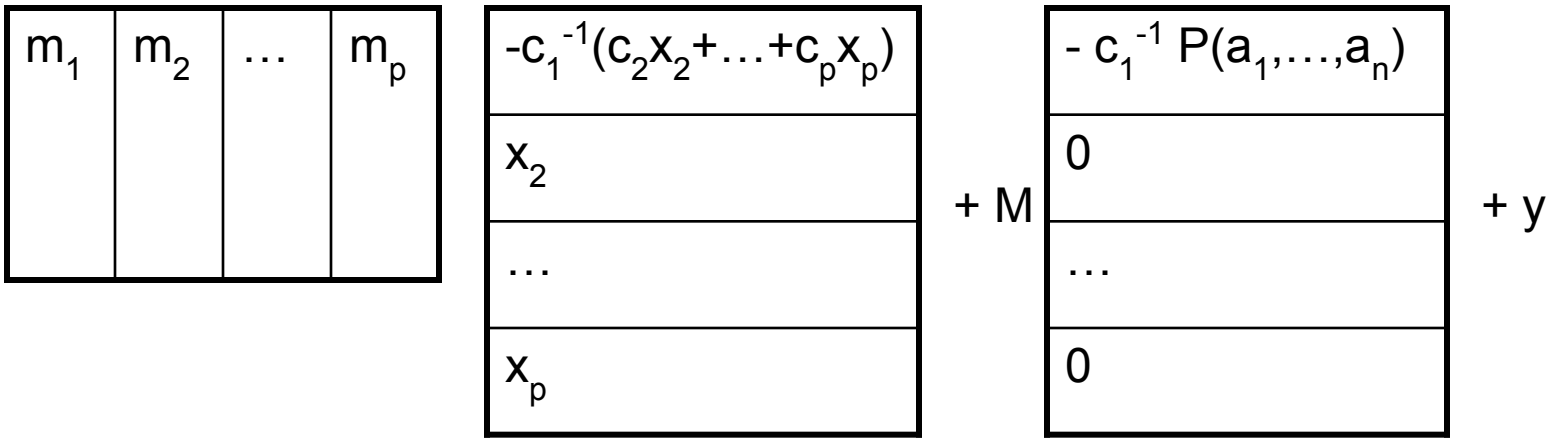
# Доказательство

- Построим $\pi'$ – вычисление для Mx+y при $x_1$=e
  - имеет на одно активное умножение меньше, чем $\pi$
  - $x_1$ – «рабочая» переменная



# Доказательство

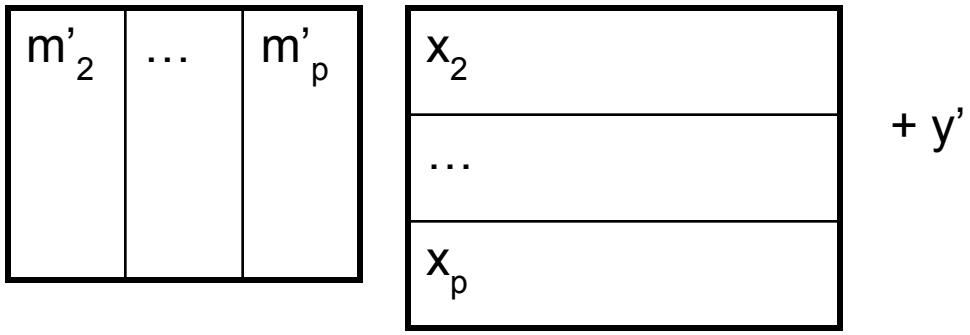
- $\pi$’ вычисляет M’x’ + y’, причём ранг M’ по столбцам равен q-1




- Положим
  - $m'_i = m_i + c_1^{-1} c_i m_1$, i=2..p
  - $y' = M \times [- c_1^{-1} P(a_1,\ldots,a_n),0,\ldots] + y$

# Доказательство

- $\pi'$ вычисляет M'x' + y', причём ранг M' по столбцам равен q-1(докажем позже)



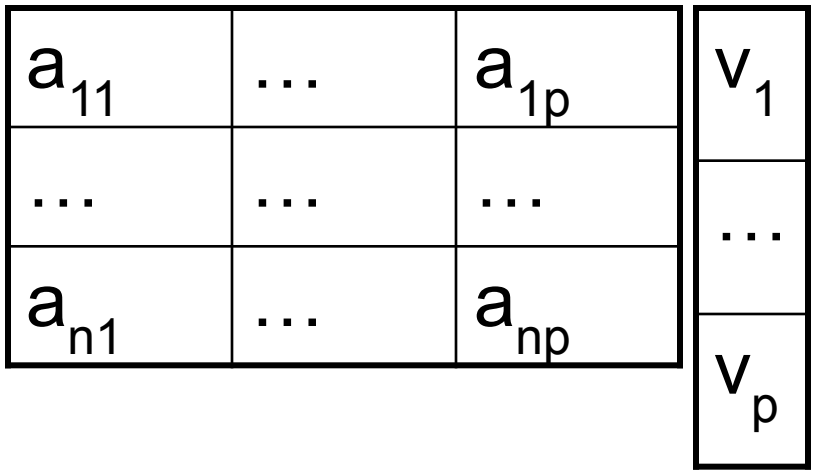

- По предположению индукции в $\pi'$ по крайней мере q-1 активное умножение, а значит в M – по крайней мере q.
- Конец доказательства.

# Использованная лемма

- **Лемма**. Пусть задан набор векторов $v_1,\ldots,v_k \mathrm{OF}^m[a_1,\ldots,a_m]$. Если среди них есть q линейно-независимых, то для любых $b_2,\ldots b_k \mathrm{OF}$ в наборе $v_2+b_2v_1,,\ldots,v_k+b_2v_k$ есть q-1 линейно-независимый вектор.
- **Доказательство**. Аналогично доказательству из линейной алгебры.

# Пример

- Вычисление умножения матрицы на вектор




- требует по крайней мере max(n,p) умножений

# Пример

- Вычисление умножения матрицы на вектор

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $v_1$ | … | $v_p$ | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | $v_1$ | … | $v_p$ | 0 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | … | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | $v_1$ | … | $v_p$ |

| |
|---|
| $a_{11}$ |
| … |
| $a_{1p}$ |
| … |
| $a_{n1}$ |
| … |
| $a_{np}$ |

- требует по крайней мере $n \times p$ умножений – *лучшая оценка*

# Пример

- Вычисление полинома требует по крайней мере n умножений.