Летняя суперкомпьютерная академия – 2012

Лукция 2. Методы решения систем линейных уравнений над $\mathbb{F}_2$

Замарашкин Николай Леонидович

Институт вычислительной математики РАН

Практикум

1. Монтгомери
   - 1.1 построить случайные матрицы размера $5 \cdot 10^6$, с 50 и 500 ненулевых элементов в строке
   - 1.2 написать эквивалент умеренно масштабируемой реализации метода Монтгомери
   - 1.3 написать эквивалент хорошо масштабируемой реализации метода Монтгомери
   - 1.4 сравнить эффективность реализаций для числа процессоров 100, 500 и 5000
2. BP алгоритм
   - 2.1 написать параллельную версию BP алгоритма
   - 2.2 построить кривую производительности для кода длины 18000

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Задана матрица $H \in \mathbb{F}_2^{m \times n}$, с $m < n$.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Задана матрица $H \in \mathbb{F}_2^{m \times n}$, с $m < n$. Найти нетривиальный вектор $c \in \mathbb{F}_2^n$:

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Задана матрица $H \in \mathbb{F}_2^{m \times n}$, с $m < n$. Найти нетривиальный вектор $c \in \mathbb{F}_2^n$:

$$Hc = 0. \tag{1}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Задана матрица $H \in \mathbb{F}_2^{m \times n}$, с $m < n$. Найти нетривиальный вектор $c \in \mathbb{F}_2^n$:

$$Hc = 0. \tag{1}$$

Считается, что матрица H является большой разреженной матрицей.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Задана матрица $A \in \mathbb{F}_2^{n \times n}$,

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Задана матрица $A \in \mathbb{F}_2^{n \times n}$, такая, что $A = A^T$,

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Задана матрица $A \in \mathbb{F}_2^{n \times n}$, такая, что $A = A^T$, и вектор $b \in \mathbb{F}_2^n$.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Задана матрица $A \in \mathbb{F}_2^{n \times n}$, такая, что $A = A^T$, и вектор $b \in \mathbb{F}_2^n$. Найти вектор $x \in \mathbb{F}_2^n$:

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Задана матрица $A \in \mathbb{F}_2^{n \times n}$, такая, что $A = A^T$, и вектор $b \in \mathbb{F}_2^n$. Найти вектор $x \in \mathbb{F}_2^n$:

$$Ax = b.$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Задана матрица $A \in \mathbb{F}_2^{n \times n}$, такая, что $A = A^T$, и вектор $b \in \mathbb{F}_2^n$. Найти вектор $x \in \mathbb{F}_2^n$:

$$Ax = b.$$

Считается, что матрица A является большой разреженной матрицей.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Что нам может предложить вычислительная математика?

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Что нам может предложить вычислительная математика?

Будем искать метод среди тех, которые решают следующую задачу.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Что нам может предложить вычислительная математика?

Будем искать метод среди тех, которые решают следующую задачу.

Задана матрица $A \in \mathbb{R}^{n \times n}$,

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Что нам может предложить вычислительная математика?

Будем искать метод среди тех, которые решают следующую задачу.

Задана матрица $A \in \mathbb{R}^{n \times n}$, такая, что $A = A^{\mathsf{T}} > 0$,

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Что нам может предложить вычислительная математика?

Будем искать метод среди тех, которые решают следующую задачу.

Задана матрица $A \in \mathbb{R}^{n \times n}$, такая, что $A = A^T > 0$, и вектор $b \in \mathbb{R}^n$.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Что нам может предложить вычислительная математика?

Будем искать метод среди тех, которые решают следующую задачу.

Задана матрица $A \in \mathbb{R}^{n \times n}$, такая, что $A = A^T > 0$, и вектор $b \in \mathbb{R}^n$. Найти вектор $x \in \mathbb{R}^n$:

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Что нам может предложить вычислительная математика?

Будем искать метод среди тех, которые решают следующую задачу.

Задана матрица $A \in \mathbb{R}^{n \times n}$, такая, что $A = A^T > 0$, и вектор $b \in \mathbb{R}^n$. Найти вектор $x \in \mathbb{R}^n$:

$$Ax = b.$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Что нам может предложить вычислительная математика?

Будем искать метод среди тех, которые решают следующую задачу.

Задана матрица $A \in \mathbb{R}^{n \times n}$, такая, что $A = A^T > 0$, и вектор $b \in \mathbb{R}^n$. Найти вектор $x \in \mathbb{R}^n$:

$$Ax = b.$$

Считается, что матрица A является большой разреженной матрицей.

Таким методом, например, является метод Ланцоша.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$Ax = b, \quad A = A^T > 0$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$Ax = b, \quad A = A^T > 0$$

Определим пространство Крылова размера l как линейную оболочку векторов

$$\mathcal{K}_l = \mathcal{K}_l(A, b) = \text{Span}\left(b, Ab, \cdots, A^{l-1}\right).$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$Ax = b, \quad A = A^T > 0$$

Определим пространство Крылова размера l как линейную оболочку векторов

$$\mathcal{K}_l = \mathcal{K}_l(A, b) = \text{Span}\left(b, Ab, \cdots, A^{l-1}\right).$$

Вообще говоря,

$$\dim(\mathcal{K}_l(A, b)) \leq l.$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Рассмотрим последовательность пространств Крылова, увеличивающейся размерности, $\mathcal{K}_1, \mathcal{K}_2, \cdots, \mathcal{K}_l$.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Рассмотрим последовательность пространств Крылова, увеличивающейся размерности, $\mathcal{K}_1, \mathcal{K}_2, \cdots, \mathcal{K}_l$.
Будем последовательно (до тех пор пока это возможно) строить A-ортогональный базис $w_k,\ k = 1, \cdots, l$:

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Рассмотрим последовательность пространств Крылова, увеличивающейся размерности, $\mathcal{K}_1, \mathcal{K}_2, \cdots, \mathcal{K}_l$.
Будем последовательно (до тех пор пока это возможно) строить A-ортогональный базис $w_k,\ k = 1, \cdots, l$:

- $w_i \neq 0$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Рассмотрим последовательность пространств Крылова, увеличивающейся размерности, $\mathcal{K}_1, \mathcal{K}_2, \cdots, \mathcal{K}_l$.
Будем последовательно (до тех пор пока это возможно) строить A-ортогональный базис $w_k,\ k = 1, \cdots, l$:

- $w_i \neq 0$
- $\mathrm{Span}(w_1, \cdots, w_k) = \mathcal{K}_k$ для всех $k = 1, \cdots$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Рассмотрим последовательность пространств Крылова, увеличивающейся размерности, $\mathcal{K}_1, \mathcal{K}_2, \cdots, \mathcal{K}_l$.
Будем последовательно (до тех пор пока это возможно) строить A-ортогональный базис $w_k,\ k = 1, \cdots, l$:

- $w_i \neq 0$
- $\mathrm{Span}(w_1, \cdots, w_k) = \mathcal{K}_k$ для всех $k = 1, \cdots$
- $w_i^T A w_j = 0$ для любых $i \neq j$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Рассмотрим последовательность пространств Крылова, увеличивающейся размерности, $\mathcal{K}_1, \mathcal{K}_2, \cdots, \mathcal{K}_l$.
Будем последовательно (до тех пор пока это возможно) строить A-ортогональный базис $w_k,\ k = 1, \cdots, l$:

- $w_i \neq 0$
- $\mathrm{Span}(w_1, \cdots, w_k) = \mathcal{K}_k$ для всех $k = 1, \cdots$
- $w_i^T A w_j = 0$ для любых $i \neq j$
- $w_i^T A w_i \neq 0$, для всех $i = 1, \cdots$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$A = A^T > 0$$

Как строить A-ортогональный базис?

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$A = A^T > 0$$

Как строить A-ортогональный базис?

Запишем

$$w_{k+1} = Aw_k - \sum_{i=1}^{k} w_i c_i \tag{2}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$A = A^T > 0$$

Как строить A-ортогональный базис?

Запишем

$$w_{k+1} = Aw_k - \sum_{i=1}^{k} w_i c_i \qquad (2)$$

Для $j < k+1$ получим

$$0 = w_j^T A w_{k+1}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$A = A^T > 0$$

Как строить A-ортогональный базис?

Запишем

$$w_{k+1} = Aw_k - \sum_{i=1}^{k} w_i c_i \tag{2}$$

Для $j < k+1$ получим

$$\begin{aligned} 0 &= w_j^T A w_{k+1} \\ &= w_j^T A^2 w_k - w_j^T \left(\sum_{i=1}^{k} A w_i c_i \right) \end{aligned}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$A = A^T > 0$$

Как строить A-ортогональный базис?

Запишем

$$w_{k+1} = Aw_k - \sum_{i=1}^{k} w_i c_i \tag{2}$$

Для $j < k+1$ получим

$$\begin{aligned} 0 &= w_j^T A w_{k+1} \\ &= w_j^T A^2 w_k - w_j^T \left(\sum_{i=1}^{k} A w_i c_i \right) \\ &= w_j^T A^2 w_i - w_j^T A w_j \cdot c_j \end{aligned}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$
\begin{aligned}
w_{k+1} &= Aw_k - \sum_{i=1}^{k} w_i c_i \\
c_j &= \frac{w_j^T A^2 w_i}{w_j^T A w_j}
\end{aligned}
$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$A = A^T > 0$$

Короткие соотношения:

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$A = A^T > 0$$

Короткие соотношения:

1. $A = A^T \quad \Rightarrow \quad w_j^T A^2 w_i = w_i^T A^2 w_j$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$A = A^T > 0$$

Короткие соотношения:

1. $A = A^T \quad \Rightarrow \quad w_j^T A^2 w_i = w_i^T A^2 w_j$
2. $w_j \in \mathcal{K}_j \quad \Rightarrow \quad Aw_j \in \mathcal{K}_{j+1} \quad \Rightarrow$, если $j + 1 < i$, то $w_j^T A^2 w_i = 0$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$A = A^T > 0$$

Короткие соотношения:

1. $A = A^T \Rightarrow w_j^T A^2 w_i = w_i^T A^2 w_j$
2. $w_j \in \mathcal{K}_j \Rightarrow Aw_j \in \mathcal{K}_{j+1} \Rightarrow$, если $j+1 < i$, то $w_j^T A^2 w_i = 0$

Следовательно, справедливо:

$$\begin{aligned} w_{k+1} &= Aw_k - w_k c_k - w_{k-1} c_{k-1} \\ c_j &= \frac{w_j^T A^2 w_i}{w_j^T A w_j} \end{aligned}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Для некоторого наименьшего l (почему?)

$$A\mathcal{K}_l \subset \mathcal{K}_l$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Для некоторого наименьшего l (почему?)

$$A\mathcal{K}_l \subset \mathcal{K}_l$$

Пусть $w_1, \cdots, w_l$, соответствующий ортогональный базис.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Для некоторого наименьшего l (почему?)

$$A\mathcal{K}_l \subset \mathcal{K}_l$$

Пусть $w_1, \cdots, w_l$, соответствующий ортогональный базис.
Составим невырожденную (почему?) матрицу
$W = [w_1, \cdots, w_l]$.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Для некоторого наименьшего l (почему?)

$$A\mathcal{K}_l \subset \mathcal{K}_l$$

Пусть $w_1, \cdots, w_l$, соответствующий ортогональный базис.
Составим невырожденную (почему?) матрицу
$W = [w_1, \cdots, w_l]$.
Решение системы $Ax = b$ будем искать в виде

$$x = W\alpha.$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$AW\alpha = b \Rightarrow$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$\begin{aligned} AW\alpha &= b \Rightarrow \\ W^T AW\alpha &= W^T b \Rightarrow \end{aligned}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$\begin{aligned} AW\alpha &= b \Rightarrow \\ W^T AW\alpha &= W^T b \Rightarrow \end{aligned}$$

$$\begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d_l \end{bmatrix} \alpha = \begin{bmatrix} w_1^T b \\ w_2^T b \\ \cdots \\ w_l^T b \end{bmatrix},$$

где $d_i = w_i^T A w_i$.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Запишем решение в виде

$$x = WD^{-1}W^{T}b = \sum_{i=1}^{l} \frac{w_i^{T}b}{w_i^{T}Aw_i} w_i$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Запишем решение в виде

$$x = WD^{-1}W^{T}b = \sum_{i=1}^{l} \frac{w_i^{T}b}{w_i^{T}Aw_i} w_i$$

Важно, что

$$x_{k+1} = x_k + \frac{w_{k+1}^{T}b}{w_{k+1}^{T}Aw_{k+1}} w_{k+1}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$w_k^T A w_k \neq 0$$

Что мешает перенести Ланцоша на $\mathbb{F}_2$ напрямую?

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$w_k^T A w_k \neq 0$$

Что мешает перенести Ланцоша на $\mathbb{F}_2$ напрямую?

Считая w_k случайными, с вероятностью $\frac{1}{2}$ число $w_k^T A w_k = 0$.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$w_k^T A w_k \neq 0$$

Что мешает перенести Ланцоша на $\mathbb{F}_2$ напрямую?

Считая w_k случайными, с вероятностью $\frac{1}{2}$ число $w_k^T A w_k = 0$.

Поправить ситуацию может построение блочного метода!

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$Ax = b, \quad A = A^T > 0$$

Блочный вариант метода Ланцоша:

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$Ax = b, \quad A = A^T > 0$$

Блочный вариант метода Ланцоша:

1. $W_{k+1} = AW_k - W_k \cdot C_k - W_{k-1} \cdot C_{k-1}$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$Ax = b, \quad A = A^T > 0$$

Блочный вариант метода Ланцоша:

1. $W_{k+1} = AW_k - W_k \cdot C_k - W_{k-1} \cdot C_{k-1}$

$$C_j = \left(W_j^T A W_j\right)^{-1} W_j^T A^2 W_i, \quad C_j \in \mathbb{R}^{n_b \times n_b}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$Ax = b, \quad A = A^T > 0$$

Блочный вариант метода Ланцоша:

1. $W_{k+1} = AW_k - W_k \cdot C_k - W_{k-1} \cdot C_{k-1}$

$$C_j = \left(W_j^T A W_j\right)^{-1} W_j^T A^2 W_i, \quad C_j \in \mathbb{R}^{n_b \times n_b}$$

с невырожденной (почему?) $W_j^T A W_j \in \mathbb{R}^{n_b \times n_b}$

2. $x_k = \sum_{i=1}^{k} W_i \left(W_{k+1}^T A W_{k+1}\right)^{-1} W_{k+1}^T b$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Блочный метод Ланцоша $A = A^* > 0$

$$W_{i+1} = AW_i - W_iC_{i+1,i} - W_{i-1}C_{i+1,i-1}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Блочный метод Ланцоша $A = A^* > 0$

$$W_{i+1} = AW_i - W_iC_{i+1,i} - W_{i-1}C_{i+1,i-1}$$

Метод Монтгомери $A = A^T$

$$V_{i+1} = AV_iS_iS_i^T - V_iD_{i+1} - V_{i-1}E_{i+1} - V_{i-2}F_{i+1}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Блочный метод Ланцоша $A = A^* > 0$

$$W_{i+1} = AW_i - W_iC_{i+1,i} - W_{i-1}C_{i+1,i-1}$$

Метод Монтгомери $A = A^T$

$$V_{i+1} = AV_iS_iS_i^T - V_iD_{i+1} - V_{i-1}E_{i+1} - V_{i-2}F_{i+1}$$

$$W_{i+1} = V_{i+1}S_{i+1}$$

так, чтобы $W_{i+1}^TAW_{i+1}$ была обратима!

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Метод Монтгомери $A = A^T \in \mathbb{F}_2^n$

$$V_{i+1} = AV_iS_iS_i^T - V_iD_{i+1} - V_{i-1}E_{i+1} - V_{i-2}F_{i+1}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Метод Монтгомери $A = A^T \in \mathbb{F}_2^n$

$$V_{i+1} = AV_iS_iS_i^T - V_iD_{i+1} - V_{i-1}E_{i+1} - V_{i-2}F_{i+1}$$

Для матриц D_{i+1}, E_{i+1} и F_{i+1}:

$$D_{i+1} = I_{n_b} - W_i^{inv}\left(V_i^TA^2V_iS_iS_i^T + V_i^TAV_i\right)$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Метод Монтгомери $A = A^T \in \mathbb{F}_2^n$

$$V_{i+1} = AV_iS_iS_i^T - V_iD_{i+1} - V_{i-1}E_{i+1} - V_{i-2}F_{i+1}$$

Для матриц D_{i+1}, E_{i+1} и F_{i+1}:

$$\begin{aligned} D_{i+1} &= I_{n_b} - W_i^{inv}\left(V_i^TA^2V_iS_iS_i^T + V_i^TAV_i\right) \\ E_{i+1} &= -W_{i-1}^{inv}(V_i^TAV_i)S_iS_i^T \end{aligned}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Метод Монтгомери $A = A^T \in \mathbb{F}_2^n$

$$V_{i+1} = AV_iS_iS_i^T - V_iD_{i+1} - V_{i-1}E_{i+1} - V_{i-2}F_{i+1}$$

Для матриц D_{i+1}, E_{i+1} и F_{i+1}:

$$\begin{aligned} D_{i+1} &= I_{n_b} - W_i^{inv}\left(V_i^TA^2V_iS_iS_i^T + V_i^TAV_i\right) \\ E_{i+1} &= -W_{i-1}^{inv}(V_i^TAV_i)S_iS_i^T \\ F_{i+1} &= \cdots \end{aligned}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Метод Монтгомери $A = A^T \in \mathbb{F}_2^n$

$$V_{i+1} = AV_iS_iS_i^T - V_iD_{i+1} - V_{i-1}E_{i+1} - V_{i-2}F_{i+1}$$

Для матриц D_{i+1}, E_{i+1} и F_{i+1}:

$$\begin{aligned} D_{i+1} &= I_{n_b} - W_i^{inv}\left(V_i^TA^2V_iS_iS_i^T + V_i^TAV_i\right) \\ E_{i+1} &= -W_{i-1}^{inv}(V_i^TAV_i)S_iS_i^T \\ F_{i+1} &= \cdots \\ W_i^{inv} &= S_i(W_i^TAW_i)^{-1}S_i^T, \quad W_i^{inv} \in \mathbb{F}_2^{n_b \times n_b} \end{aligned}$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Метод Монтгомери $A = A^T \in \mathbb{F}_2^n$

$$V_{i+1} = AV_iS_iS_i^T - V_iD_{i+1} - V_{i-1}E_{i+1} - V_{i-2}F_{i+1}$$

Для матриц D_{i+1}, E_{i+1} и F_{i+1}:

$$\begin{aligned} D_{i+1} &= I_{n_b} - W_i^{inv}\left(V_i^TA^2V_iS_iS_i^T + V_i^TAV_i\right) \\ E_{i+1} &= -W_{i-1}^{inv}(V_i^TAV_i)S_iS_i^T \\ F_{i+1} &= \cdots \\ W_i^{inv} &= S_i(W_i^TAW_i)^{-1}S_i^T, \quad W_i^{inv} \in \mathbb{F}_2^{n_b \times n_b} \end{aligned}$$

Решение

$$x_k = \sum_{i=1}^{k} W_i \left(W_{k+1}^TAW_{k+1}\right)^{-1} W_{k+1}^Tb$$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Каким выбрать размер n_b блока?

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Каким выбрать размер n_b блока?

Ответ:

- на 32 - разрядной машине кратным 32
- на 64 - разрядной машине кратным 64

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Вот как, например, может выглядеть операция умножения разреженной матрицы на вектор.

```
for(i = 1; i <= n + 1; i++) {
    for (j = ia(i); j < ia(i+1); j++) {
        y[i]  ^= x[ja[j]];
    }
}
```

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

А вот "axpy".

```
for (i = 1; i < n + 1; i++) {
    y[i] ^= a[i];
}
```

Отличный пример параллельных вычислений в алгоритме! Ускорение в 32 или 64 раза.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

$$\text{сложность} \approx \alpha n^2/64 = 2.0 \cdot 10^{17} \text{операций}$$

Вывод: необходимо дополнительно ускорять вычисления.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Пока все с трека не разбежались, самое время приступить к паралельным вычислениям! :)

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Пока все с трека не разбежались, самое время приступить к параллельным вычислениям! :)

Какие операции имеются в алгоритме?

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Пока все с трека не разбежались, самое время приступить к параллельным вычислениям! :)

Какие операции имеются в алгоритме?

1. $A \cdot V$, где $A \in \mathbb{F}_2^{n \times n}$, $V \in \mathbb{F}_2^{n \times n_b}$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Пока все с трека не разбежались, самое время приступить к параллельным вычислениям! :)

Какие операции имеются в алгоритме?

1. $A \cdot V$, где $A \in \mathbb{F}_2^{n \times n}$, $V \in \mathbb{F}_2^{n \times n_b}$
2. $V \cdot W$, где $V \in \mathbb{F}_2^{n \times n_b}$, $W \in \mathbb{F}_2^{n_b \times n_b}$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Пока все с трека не разбежались, самое время приступить к параллельным вычислениям! :)

Какие операции имеются в алгоритме?

1. $A \cdot V$, где $A \in \mathbb{F}_2^{n \times n}$, $V \in \mathbb{F}_2^{n \times n_b}$
2. $V \cdot W$, где $V \in \mathbb{F}_2^{n \times n_b}$, $W \in \mathbb{F}_2^{n_b \times n_b}$
3. $V^T \cdot V$, где $V \in \mathbb{F}_2^{n \times n_b}$

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Инструменты

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Инструменты

1. "разбиение"матрицы (графа) (балансировка вычислений!)

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Инструменты

1. "разбиение"матрицы (графа) (балансировка вычислений!)
2. изменение размера блока (блок может быть кратен 32 или 64!) (сложность!)

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Инструменты

1. "разбиение"матрицы (графа) (балансировка вычислений!)
2. изменение размера блока (блок может быть кратен 32 или 64!) (сложность!)
3. алгоритм циклических пересылок (не учитывает топологию!)

Будут рассмотрены две реализации

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Инструменты

1. "разбиение"матрицы (графа) (балансировка вычислений!)
2. изменение размера блока (блок может быть кратен 32 или 64!) (сложность!)
3. алгоритм циклических пересылок (не учитывает топологию!)

Будут рассмотрены две реализации

1. умеренно масштабируемая

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Инструменты

1. "разбиение"матрицы (графа) (балансировка вычислений!)
2. изменение размера блока (блок может быть кратен 32 или 64!) (сложность!)
3. алгоритм циклических пересылок (не учитывает топологию!)

Будут рассмотрены две реализации

1. умеренно масштабируемая
2. хорошо масштабируемая

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Несколько слов о технологии Graph Partitioning.

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Достоинства метода Монтгомери:

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Достоинства метода Монтгомери:

1. простота описания и предсказуемость поведения

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Достоинства метода Монтгомери:

1. простота описания и предсказуемость поведения
2. наличие хорошо масштабируемой реализации

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Достоинства метода Монтгомери:

1. простота описания и предсказуемость поведения
2. наличие хорошо масштабируемой реализации
3. возможность для предобусловливания

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Достоинства метода Монтгомери:

1. простота описания и предсказуемость поведения
2. наличие хорошо масштабируемой реализации
3. возможность для предобусловливания

Недостатки метода Монтгомери:

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Достоинства метода Монтгомери:

1. простота описания и предсказуемость поведения
2. наличие хорошо масштабируемой реализации
3. возможность для предобусловливания

Недостатки метода Монтгомери:

1. необходимость высокоскоростной сети обмена для систем с большим числом ядер

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Достоинства метода Монтгомери:

1. простота описания и предсказуемость поведения
2. наличие хорошо масштабируемой реализации
3. возможность для предобусловливания

Недостатки метода Монтгомери:

1. необходимость высокоскоростной сети обмена для систем с большим числом ядер
2. существенное увеличение общей сложности вычислений при росте размера блока

Методы для систем над $\mathbb{F}_2$

1. Метод Монтгомери

Достоинства метода Монтгомери:

1. простота описания и предсказуемость поведения
2. наличие хорошо масштабируемой реализации
3. возможность для предобусловливания

Недостатки метода Монтгомери:

1. необходимость высокоскоростной сети обмена для систем с большим числом ядер
2. существенное увеличение общей сложности вычислений при росте размера блока
3. быстрое насыщение для умеренно масштабируемой реализации