Разработка модуля вычисления синдромов и восстановления утраченных дисков в RAID-массиве с использованием арифметики поля $GF(2^{256})$

Быкова Юлия, Веселков Иван

студенты кафедры системного программирования СПбГУ

Почему именно $GF(2^{256})$?

- Используем векторное вычисление
- Размер страйпа 4 Кбайт (2^{12} байт)
- Размер регистра SSE 16 байт (2^4 байт)
- $2^{12} / 2^4 = 2^8 = 256$ переменных
- 256 буферов обрабатывается одновременно

Инструменты

- Язык программирования C
  - Компиляторные оптимизации
  - Распределение регистров
  - Переносимость кода
- Генератор кода
  - Минимизация ручного труда

Цели

- Реализация функции вычисления синдромов и восстановления утраченных дисков с элементами в поле $GF(2^{256})$
- Сравнение производительности с полями размера 2^8 и 2^{16}

Расчет синдромов

Формула расчета:

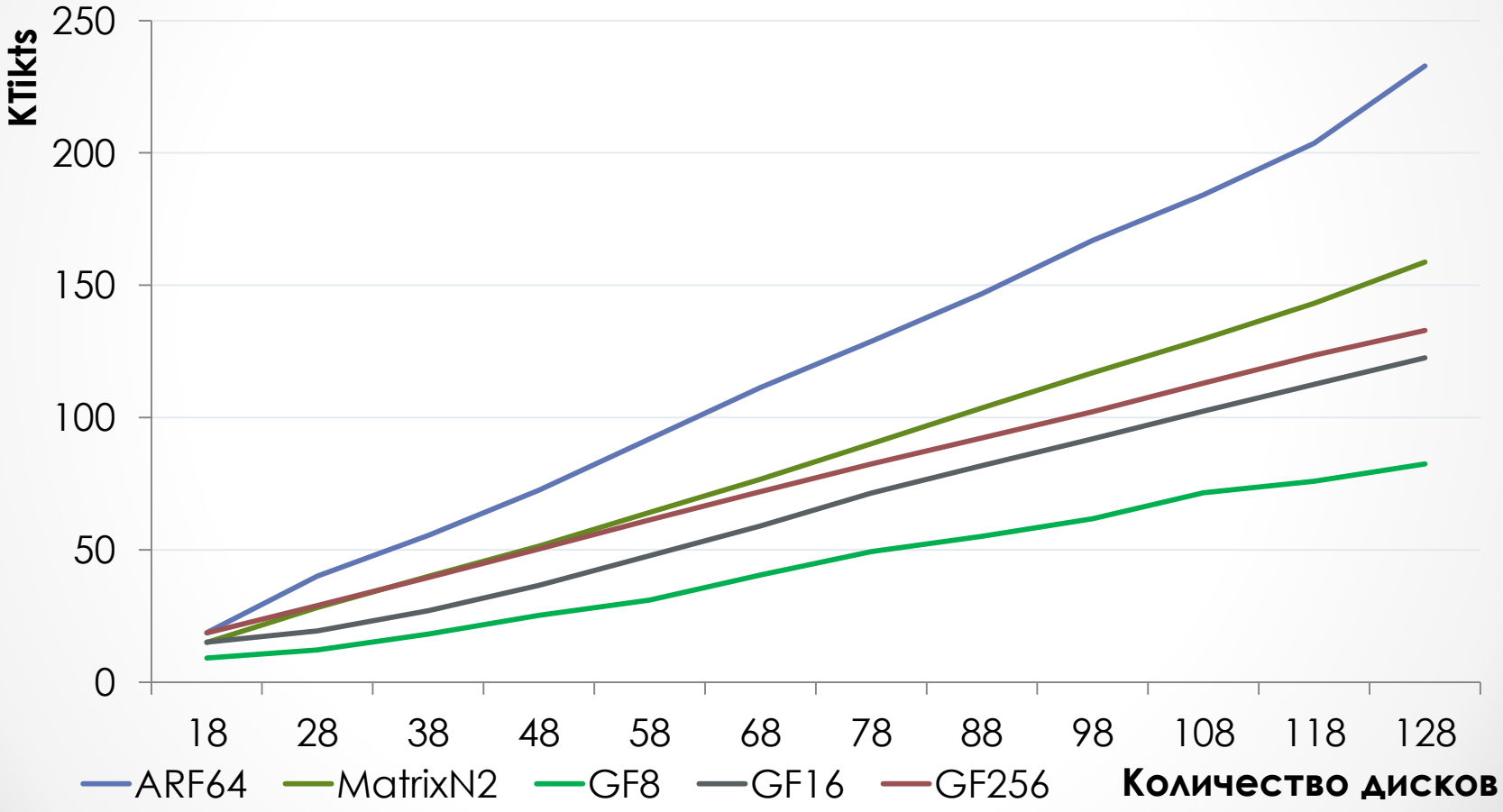
$$P = D_0 + D_1 + \cdots + D_n$$

$$Q = D_0 x^n + D_1 x^{n-1} + \cdots + D_{n-1} x + D_n$$

Факторизация:

$$Q = \Big(\big((D_0 x + D_1) x + D_2 \big) x + \cdots \Big) x + D_n$$

Расчет синдромов



Восстановление дисков

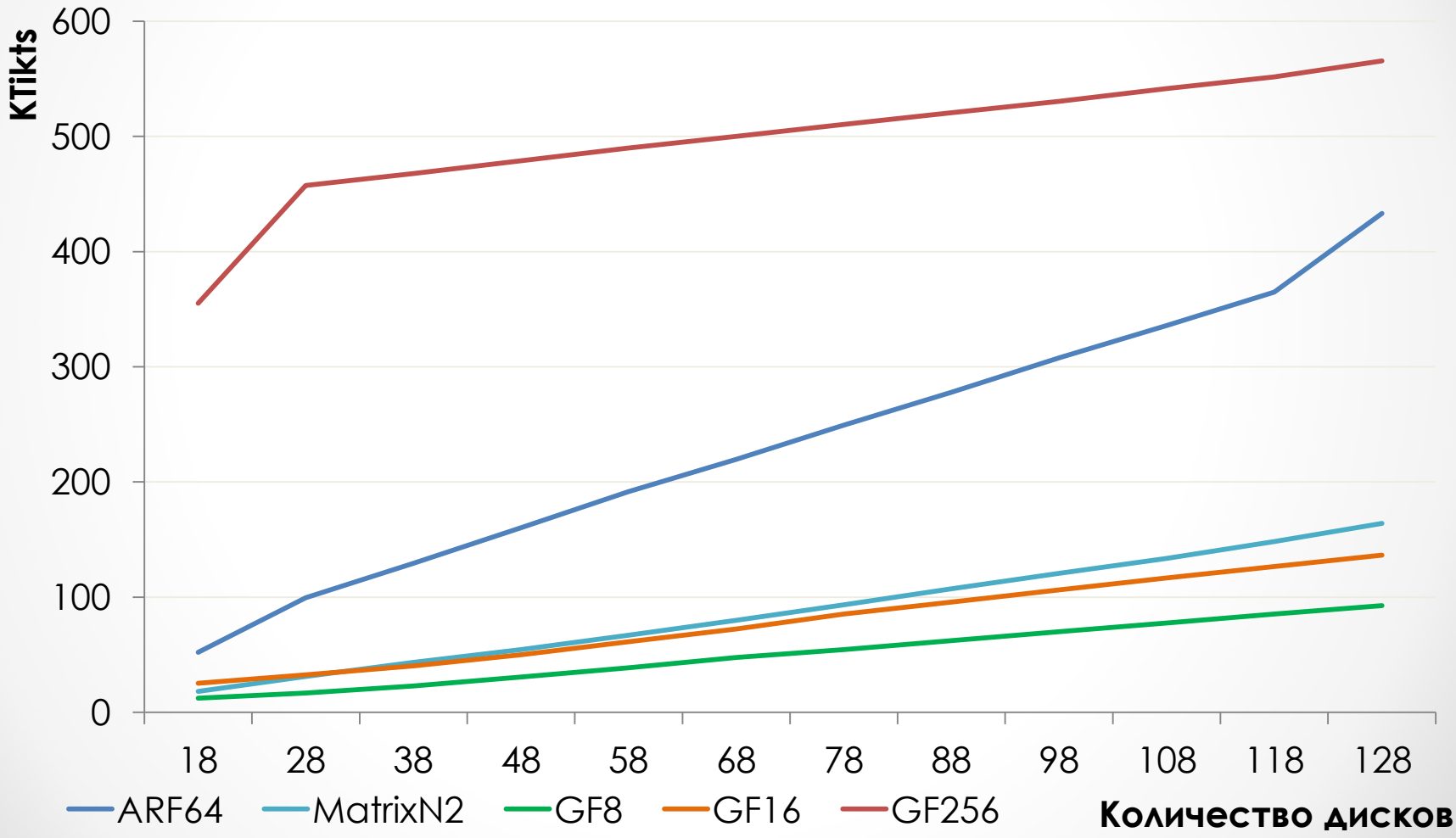
Формула восстановления:

$$D_j = \frac{(Q + \bar{Q}) * x^{-(n-k-1)} + P + \bar{P}}{x^{k-j} + 1}$$

$$D_k = D_j + P + \bar{P}$$

Предподсчет значений

Восстановление дисков



Результаты

- Разработаны код-генераторы для генерации кода функций расчета двух синдромов и восстановления двух отказавших дисков
- Подготовлена среда испытаний, программа тестов производительности
- Осуществлена проверка корректности получившихся функций и протестирована их производительность