# Parallel Multiplication, Trivial Traces and Conjugates in Order Dividing Extension Fields

Anna Johnston

Washington State University

14 July 2009

# Outline





1. Overview

# Outline

# Outline

# Outline

# Outline

# Order Dividing Extension Fields



**An Order Dividing Extension Field is:**

- Extension field with degree $q$ over a finite base field $\mathbb{F}$ . . .

Examples

# Order Dividing Extension Fields



**An Order Dividing Extension Field is:**

- Extension field with degree $q$ over a finite base field $\mathbb{F}$ ...
- where the degree $q$ divides $|\mathbb{F}^*| = (P - 1)$ ...

Examples

# Order Dividing Extension Fields

**An Order Dividing Extension Field is:**

- Extension field with degree $q$ over a finite base field $\mathbb{F}$ . . .
- where the degree $q$ divides $|\mathbb{F}^*| = (P - 1)$ . . .
- and $q$ is prime.

Examples

# Order Dividing Extension Fields



**An Order Dividing Extension Field is:**

- Extension field with degree $q$ over a finite base field $\mathbb{F}$ . . .
- where the degree $q$ divides $|\mathbb{F}^*| = (P - 1)$ . . .
- and $q$ is prime.

Examples

- $GF(P^2)$, where $P$ is odd
- $GF(19^3)$
- $GF\left(\left(2^4\right)^5\right)$
- $GF(101^5)$
- $GF(29^7)$
- $GF\left(\left(5^2\right)^3\right)$

# Why and What



Why Do We Care?

What We Will Show

# Why and What



## Why Do We Care?

- Optimal Extension Fields for Elliptic Curve Cryptosystems

## What We Will Show

# Why and What





## Why Do We Care?

- Optimal Extension Fields for Elliptic Curve Cryptosystems
- Root computation ($\sqrt[q]{\alpha}$) using Cipolla's algorithm

## What We Will Show

# Why and What



Why Do We Care?

- Optimal Extension Fields for Elliptic Curve Cryptosystems
- Root computation ($\sqrt[q]{\alpha}$) using Cipolla's algorithm

What We Will Show

- Parallel multiplication and reduction using discrete Fourier transforms

# Why and What

## Why Do We Care?

- Optimal Extension Fields for Elliptic Curve Cryptosystems
- Root computation ($\sqrt[q]{\alpha}$) using Cipolla's algorithm

## What We Will Show

- Parallel multiplication and reduction using discrete Fourier transforms
- Added benefits to DFT form: conjugates, traces, inverses

# Two Term Representation



## Trivial Field Reduction

- $u \in \mathbb{F}$, $u^{\frac{P-1}{q}} \neq 1$

# Two Term Representation



## Trivial Field Reduction

- $u \in \mathbb{F}$, $u^{\frac{P-1}{q}} \neq 1$

- $\Rightarrow \sqrt[q]{u} \notin \mathbb{F}$
- $r(x) = x^q - u$ is irreducible over $\mathbb{F}$

# Two Term Representation



## Trivial Field Reduction

- $u \in \mathbb{F}$, $u^{\frac{P-1}{q}} \neq 1$
- $GF(P^q) \cong \mathbb{F}[x]/r(x)\mathbb{F}[x]$
- $\Rightarrow \sqrt[q]{u} \notin \mathbb{F}$
- $r(x) = x^q - u$ is irreducible over $\mathbb{F}$

# Two Term Representation

## Trivial Field Reduction

- $u \in \mathbb{F}$, $u^{\frac{P-1}{q}} \neq 1$
- $GF(P^q) \cong \mathbb{F}[x]/r(x)\mathbb{F}[x]$
- $\Rightarrow \sqrt[q]{u} \notin \mathbb{F}$
- $r(x) = x^q - u$ is irreducible over $\mathbb{F}$

$$\sum_{k=0}^{2q-1} v_k x^k \in \mathbb{F}[x]$$

# Two Term Representation





## Trivial Field Reduction

- $u \in \mathbb{F}$, $u^{\frac{P-1}{q}} \neq 1$
- $GF(P^q) \cong \mathbb{F}[x]/r(x)\mathbb{F}[x]$
- $\Rightarrow \quad \sqrt[q]{u} \notin \mathbb{F}$
- $r(x) = x^q - u$ is irreducible over $\mathbb{F}$

$$\sum_{k=0}^{2q-1} v_k x^k \in \mathbb{F}[x]$$

$$\Downarrow$$

$$\sum_{k=0}^{q-1} \left(v_k + u v_{q+k}\right) x^k \bmod r(x)$$

# The Chinese Remainder Theorem

## What does it do on Polynomials

# The Chinese Remainder Theorem



## What does it do on Polynomials

- Gives the discrete Fourier Transform

# The Chinese Remainder Theorem

## What does it do on Polynomials

- Gives the discrete Fourier Transform
- Enables field reduction within the DFT ring

# The Chinese Remainder Theorem



## What does it do on Polynomials

- Gives the discrete Fourier Transform
- Enables field reduction within the DFT ring

$$\sum_{k=0}^{n-1} v_k x^k \bmod \left( \prod_j h_j(x) \right)$$

# The Chinese Remainder Theorem



## What does it do on Polynomials

- Gives the discrete Fourier Transform
- Enables field reduction within the DFT ring

$$\sum_{k=0}^{n-1} v_k x^k \bmod \left(\prod_j h_j(x)\right)$$

$$\Updownarrow$$

$$\left[\sum_{k=0}^{n-1} v_k x^k \bmod h_j(x)\right]_j$$

# The CRT in Action: Multiplication



$$\boxed{(5x + 3)(2x + 1) \bmod (x^2 - 1)}$$

# The CRT in Action: Multiplication



$$(5x+3)(2x+1) \bmod (x^2-1)$$

↓

$$\bmod (x-1)$$
$$\bmod (x+1)$$

# The CRT in Action: Multiplication



$$(5x + 3)(2x + 1) \bmod (x^2 - 1)$$

↓

$$(5x+3)(2x+1) \equiv \quad \bmod (x-1)$$
$$\bmod (x+1)$$

# The CRT in Action: Multiplication

$$(5x + 3)(2x + 1) \bmod (x^2 - 1)$$

↓

$$(5x + 3)(2x + 1) \equiv (8)(3) \quad \bmod (x - 1)$$
$$\bmod (x + 1)$$

# The CRT in Action: Multiplication



$$(5x+3)(2x+1) \bmod (x^2-1)$$

$$\begin{aligned}(5x+3)(2x+1) &\equiv (8)(3) && \bmod (x-1)\\ (5x+3)(2x+1) &\equiv (-2)(-1) && \bmod (x+1)\end{aligned}$$

# The CRT in Action: Multiplication

$$(5x+3)(2x+1) \bmod (x^2-1)$$

↓

$$\begin{aligned}(5x+3)(2x+1) &\equiv (8)(3) && \bmod (x-1)\\ (5x+3)(2x+1) &\equiv (-2)(-1) && \bmod (x+1)\end{aligned}$$

↓

$$\begin{cases} 24(x+1)\left((x+1)^{-1} \bmod (x-1)\right) + \ldots & \text{straight sum} \\ \end{cases}$$

# The CRT in Action: Multiplication

$$(5x+3)(2x+1) \bmod (x^2-1)$$

↓

$$\begin{aligned}(5x+3)(2x+1) &\equiv (8)(3) && \bmod(x-1)\\ (5x+3)(2x+1) &\equiv (-2)(-1) && \bmod(x+1)\end{aligned}$$

↓

$$\begin{cases} 24(x+1)(2^{-1}) + \dots & \text{straight sum} \\ \end{cases}$$

# The CRT in Action: Multiplication



$$(5x+3)(2x+1) \bmod (x^2-1)$$

$$\downarrow$$

$$\begin{aligned} (5x+3)(2x+1) &\equiv (8)(3) & \bmod (x-1) \\ (5x+3)(2x+1) &\equiv (-2)(-1) & \bmod (x+1) \end{aligned}$$

$$\downarrow$$

$$\left\{ 24(x+1)(2^{-1}) + 2(x-1)(-2^{-1}) \quad \text{straight sum} \right.$$

# The CRT in Action: Multiplication



$$(5x+3)(2x+1) \bmod (x^2-1)$$

↓

$$\begin{aligned}(5x+3)(2x+1) &\equiv (8)(3) && \bmod (x-1)\\ (5x+3)(2x+1) &\equiv (-2)(-1) && \bmod (x+1)\end{aligned}$$

↓

$$\begin{cases} 24(x+1)(2^{-1}) + 2(x-1)(-2^{-1}) & \text{straight sum} \\ 24 & \text{iterative} \end{cases}$$

# The CRT in Action: Multiplication





$$(5x+3)(2x+1) \bmod (x^2-1)$$

↓

$$\begin{aligned} (5x+3)(2x+1) &\equiv (8)(3) && \bmod (x-1) \\ (5x+3)(2x+1) &\equiv (-2)(-1) && \bmod (x+1) \end{aligned}$$

↓

$$\begin{cases} 24(x+1)(2^{-1}) + 2(x-1)(-2^{-1}) & \text{straight sum} \\ 24 + (x-1)\left((-2)^{-1}(2-24)\right) & \text{iterative} \end{cases}$$

# The CRT in Action: Multiplication



$$(5x+3)(2x+1) \bmod (x^2-1)$$

$$\downarrow$$

$$\begin{aligned}(5x+3)(2x+1) &\equiv (8)(3) && \bmod (x-1)\\ (5x+3)(2x+1) &\equiv (-2)(-1) && \bmod (x+1)\end{aligned}$$

$$\downarrow$$

$$\begin{cases} 24(x+1)(2^{-1}) + 2(x-1)(-2^{-1}) & \text{straight sum} \\ 24 + (x-1)\left((-2)^{-1}(2-24)\right) & \text{iterative} \end{cases}$$

$$\downarrow$$

$$11x + 13 \bmod (x^2-1)$$

# The CRT in Action: Reduction





## Over $GF(7)$

$$\left[ (x^3 + 2) \qquad \bmod (x^2 - 3) \right]$$

# The CRT in Action: Reduction



## Over $GF(7)$

$$\left[0 \bmod (x^2-1),\ (x^3+2) \qquad \bmod (x^2-3)\right]$$

# The CRT in Action: Reduction



## Over $GF(7)$

$$\left[0 \bmod (x^2-1),\ (x^3+2)(x^2-1) \equiv (x^3+2)2 \bmod (x^2-3)\right]$$

# The CRT in Action: Reduction



## Over $GF(7)$

$$\left[0 \bmod (x^2-1),\ (x^3+2)(x^2-1) \equiv (x^3+2)2 \bmod (x^2-3)\right]$$

$\downarrow$

$$(x^3+2)2 + (x^2-3)\left(-2^{-1}\left(0-(x+2)2\right)\right)$$

$\downarrow$

$$x^2(3x+2)-(3x+2)$$

# The CRT in Action: Reduction



## Over $GF(7)$

$$\left[0 \bmod (x^2-1),\ (x^3+2)(x^2-1) \equiv (x^3+2)2 \bmod (x^2-3)\right]$$

$$\downarrow$$

$$(x^3+2)2 + (x^2-3)\left(-2^{-1}\left(0-(x+2)2\right)\right)$$

$$\downarrow$$

$$x^2(3x+2) - (3x+2)$$

$$\downarrow$$

$$x^3+2 \equiv 3x+2 \bmod (x^2-3)$$

# Parallel Multiplication



If $h \in \mathbb{F}$ is a $2q$-th primitive root of unity

# Parallel Multiplication



If $h \in \mathbb{F}$ is a $2q$-th primitive root of unity

$$\Downarrow$$

$$\boxed{(x^{2q} - 1) = \prod_{k=0}^{2q-1} (x - h^k)}$$

# Parallel Multiplication



DFT Modulus: $\boxed{(x^{2q}-1) = \prod_{k=0}^{2q-1}\left(x - h^k\right)}$

# Parallel Multiplication



DFT Modulus: $\boxed{(x^{2q} - 1) = \prod_{k=0}^{2q-1} (x - h^k)}$

## Discrete Fourier Transform Multiplication

- $f(x), g(x) \in \mathbb{F}[x]/(x^q - u)\mathbb{F}[x]$ have degree less than $q$.

# Parallel Multiplication



DFT Modulus: $\boxed{(x^{2q} - 1) = \prod_{k=0}^{2q-1} \left(x - h^k\right)}$

## Discrete Fourier Transform Multiplication

- $f(x), g(x) \in \mathbb{F}[x]/(x^q - u)\mathbb{F}[x]$ have degree less than $q$.
- $f(x)g(x)$ has degree less than $2q$

# Parallel Multiplication

DFT Modulus: $\boxed{(x^{2q}-1)=\prod_{k=0}^{2q-1}\left(x-h^k\right)}$

## Discrete Fourier Transform Multiplication

- $f(x), g(x) \in \mathbb{F}[x]/(x^q-u)\mathbb{F}[x]$ have degree less than $q$.
- $f(x)g(x)$ has degree less than $2q$
- Multiplication in $2q$ DFT loses no information

# Parallel Multiplication



DFT Modulus: $\boxed{(x^{2q} - 1) = \prod_{k=0}^{2q-1} (x - h^k)}$

## Discrete Fourier Transform Multiplication

- $f(x), g(x) \in \mathbb{F}[x]/(x^q - u)\mathbb{F}[x]$ have degree less than $q$.
- $f(x)g(x)$ has degree less than $2q$
- Multiplication in $2q$ DFT loses no information

$$f(x)g(x) \bmod (x^{2q} - 1) \equiv f(x)g(x) \bmod (x^q - u)$$

# Parallel Multiplication

DFT Modulus: $\boxed{(x^{2q}-1)=\prod_{k=0}^{2q-1}(x-h^k)}$

## Discrete Fourier Transform Multiplication

- $f(x), g(x) \in \mathbb{F}[x]/(x^q-u)\mathbb{F}[x]$ have degree less than $q$.
- $f(x)g(x)$ has degree less than $2q$
- Multiplication in $2q$ DFT loses no information

$$f(x)g(x) \bmod (x^{2q}-1) \equiv f(x)g(x) \bmod (x^q-u)$$

Reduction??

# Field Reduction Within the Ring



## Theoretical Reduction

- Reduction modulo $r(x) = (x^q - u)$
- $\alpha \in \mathbb{F}[x]$, $deg(\alpha) < 2q$;

# Field Reduction Within the Ring



## Theoretical Reduction

- Reduction modulo $r(x) = (x^q - u)$
- $\alpha \in \mathbb{F}[x]$, $deg(\alpha) < 2q$;
- Use the CRT with moduli $r(x)$ and $(x^{2q} - 1)$;
- Compute $\left[0 \bmod (x^{2q} - 1),\ \alpha(x^{2q} - 1) \bmod r(x)\right]$;

# Field Reduction Within the Ring



## Theoretical Reduction

- Reduction modulo $r(x) = (x^q - u)$
- $\alpha \in \mathbb{F}[x]$, $deg(\alpha) < 2q$;
- Use the CRT with moduli $r(x)$ and $(x^{2q} - 1)$;
- Compute $\left[0 \bmod (x^{2q} - 1),\ \alpha(x^{2q} - 1) \bmod r(x)\right]$;
- Divide by $(x^{2q} - 1)$.

# Field Reduction Within the Ring

## Theoretical Reduction

- Reduction modulo $r(x) = (x^q - u)$
- $\alpha \in \mathbb{F}[x]$, $deg(\alpha) < 2q$;
- Use the CRT with moduli $r(x)$ and $(x^{2q} - 1)$;
- Compute $\left[0 \bmod (x^{2q} - 1),\ \alpha(u^2 - 1) \bmod r(x)\right]$;
- Divide by $(x^{2q} - 1)$.

# Field Reduction Within the Ring



## Theoretical Reduction

- Reduction modulo $r(x) = (x^q - u)$
- $\alpha \in \mathbb{F}[x]$, $deg(\alpha) < 2q$;
- Use the CRT with moduli $r(x)$ and $(x^{2q} - 1)$;
- Compute $\left[0 \bmod (x^{2q} - 1),\ \alpha(u^2 - 1) \bmod r(x)\right]$;
- Divide by $(x^{2q} - 1)$.

$$\mathcal{C}(\alpha) = \alpha(u^2 - 1) +$$

# Field Reduction Within the Ring





## Theoretical Reduction

- Reduction modulo $r(x) = (x^q - u)$
- $\alpha \in \mathbb{F}[x]$, $deg(\alpha) < 2q$;
- Use the CRT with moduli $r(x)$ and $(x^{2q} - 1)$;
- Compute $\left[0 \bmod (x^{2q} - 1),\ \alpha(u^2 - 1) \bmod r(x)\right]$;
- Divide by $(x^{2q} - 1)$.

$$\mathcal{C}(\alpha) = \alpha(u^2 - 1) + (x^q - u)$$

# Field Reduction Within the Ring

## Theoretical Reduction

- Reduction modulo $r(x) = (x^q - u)$
- $\alpha \in \mathbb{F}[x]$, $deg(\alpha) < 2q$;
- Use the CRT with moduli $r(x)$ and $(x^{2q} - 1)$;
- Compute $\left[0 \bmod (x^{2q} - 1),\ \alpha(u^2 - 1) \bmod r(x)\right]$;
- Divide by $(x^{2q} - 1)$.

$$\mathcal{C}(\alpha) = \alpha(u^2 - 1) + (x^q - u)\left((x^q - u)^{-1}(-(u^2 - 1))\alpha \bmod (x^{2q} - 1)\right)$$

# Field Reduction Within the Ring



## Theoretical Reduction

- Reduction modulo $r(x) = (x^q - u)$
- $\alpha \in \mathbb{F}[x]$, $deg(\alpha) < 2q$;
- Use the CRT with moduli $r(x)$ and $(x^{2q} - 1)$;
- Compute $\left[0 \bmod (x^{2q} - 1),\ \alpha(u^2 - 1) \bmod r(x)\right]$;
- Divide by $(x^{2q} - 1)$.

$$\mathcal{C}(\alpha) = \alpha(u^2 - 1) + (x^q - u)\left((x^q - u)^{-1}(-(u^2 - 1))\alpha \bmod (x^{2q} - 1)\right)$$

---

$$\begin{aligned} -(u^2 - 1) &\equiv x^{2q} - u^2 \bmod (x^{2q} - 1) \\ &\equiv (x^q - u)(x^q + u) \end{aligned}$$

# Field Reduction Within the Ring



## Theoretical Reduction

- Reduction modulo $r(x) = (x^q - u)$
- $\alpha \in \mathbb{F}[x]$, $deg(\alpha) < 2q$;
- Use the CRT with moduli $r(x)$ and $(x^{2q} - 1)$;
- Compute $\left[0 \bmod (x^{2q} - 1),\ \alpha(u^2 - 1) \bmod r(x)\right]$;
- Divide by $(x^{2q} - 1)$.

$$\mathcal{C}(\alpha) = \alpha(u^2 - 1) + (x^q - u)\left((x^q + u)\alpha \bmod (x^{2q} - 1)\right)$$

---

$$-(u^2 - 1)(x^q - u)^{-1} \equiv (x^q + u) \bmod (x^{2q} - 1)$$

# Field Reduction Within the Ring: II



$$\mathcal{C}(\alpha) = \alpha(u^2 - 1) + (x^q - u)\left((x^q + u)\alpha \bmod (x^{2q} - 1)\right)$$

# Field Reduction Within the Ring: II

$$\mathcal{C}(\alpha) = \alpha(u^2 - 1) + (x^q - u)\left((x^q + u)\alpha \bmod (x^{2q} - 1)\right)$$

$$\boxed{\Gamma = (x^q + u)\alpha \bmod (x^{2q} - 1)}$$

# Field Reduction Within the Ring: II



$$\mathcal{C}(\alpha) = \alpha(u^2 - 1) + (x^q - u)\Gamma$$

$$\boxed{\Gamma = (x^q + u)\alpha \bmod (x^{2q} - 1)}$$

# Field Reduction Within the Ring: II



$$\mathcal{C}(\alpha) = \alpha(u^2 - 1) + (x^q - u)\Gamma$$

$$\boxed{\Gamma = (x^q + u)\alpha \bmod (x^{2q} - 1)}$$

## Notice

- $Deg\left(\alpha(u^2 - 1)\right) < 2q$
- $Deg\left(\Gamma\right) < 2q$

# Field Reduction Within the Ring: II



$$\begin{aligned}\mathcal{C}(\alpha) &= \alpha(u^2 - 1) + (x^q - u)\Gamma \\ &= x^{2q}\left(\sum_{j=0}^{q-1} c_j x^j\right) - \left(\sum_{j=0}^{q-1} c_j x^j\right)\end{aligned}$$

$$\boxed{\Gamma = (x^q + u)\alpha \bmod (x^{2q} - 1)}$$

## Notice

- $Deg\left(\alpha(u^2 - 1)\right) < 2q$
- $Deg\left(\Gamma\right) < 2q$

# Field Reduction Within the Ring: II



$$\begin{aligned}\mathcal{C}(\alpha) &= \alpha(u^2 - 1) + (x^q - u)\Gamma \\ &= x^{2q}\left(\sum_{j=0}^{q-1} c_j x^j\right) - \left(\sum_{j=0}^{q-1} c_j x^j\right)\end{aligned}$$

$$\boxed{\Gamma = (x^q + u)\alpha \bmod (x^{2q} - 1)}$$

## Notice

- $Deg\left(\alpha(u^2 - 1)\right) < 2q$
- $Deg\left(\Gamma\right) < 2q$

$$\Gamma = x^q \sum_{j=0}^{q-1} c_j x^j + \ldots$$

# Most Significant $q$ terms of $\Gamma$



$$\Gamma = (x^q + u)\alpha \bmod (x^{2q} - 1)$$

**Computational Reduction**

# Most Significant $q$ terms of $\Gamma$



$$\Gamma = x^q \sum_{j=0}^{q-1} c_j x^j + \sum_{j=0}^{q-1} d_j x^j$$

## Computational Reduction

- Compute $\Gamma = (x^q + u)\alpha \bmod (x^{2q} - 1)$

# Most Significant $q$ terms of $\Gamma$



$$\Gamma - \sum_{j=0}^{q-1} d_j x^j = x^q \sum_{j=0}^{q-1} c_j x^j$$

## Computational Reduction

- Compute $\Gamma = (x^q + u)\alpha \bmod (x^{2q} - 1)$
- Subtract off $\sum_{j=0}^{q-1} d_j x^j$

# Most Significant $q$ terms of $\Gamma$



$$\frac{\Gamma - \sum_{j=0}^{q-1} d_j x^j}{x^q} = \sum_{j=0}^{q-1} c_j x^j$$

## Computational Reduction

- Compute $\Gamma = (x^q + u)\alpha \bmod (x^{2q} - 1)$
- Subtract off $\sum_{j=0}^{q-1} d_j x^j$
- Divide by $x^q \bmod (x^{2q} - 1)$

# Most Significant $q$ terms of $\Gamma$



$$\frac{\Gamma - \sum_{j=0}^{q-1} d_j x^j}{x^q} = \sum_{j=0}^{q-1} c_j x^j$$
$$\equiv \alpha \bmod r(x)$$

## Computational Reduction

- Compute $\Gamma = (x^q + u)\alpha \bmod (x^{2q} - 1)$
- Subtract off $\sum_{j=0}^{q-1} d_j x^j$
- Divide by $x^q \bmod (x^{2q} - 1)$

# Most Significant $q$ terms of $\Gamma$ – in Parallel



$$\alpha \equiv \left[a_j \bmod (x - h^j)\right]_{j=0}^{2q-1}$$

## Computational Reduction – In Parallel

- Compute $\Gamma = (x^q + u)\alpha \bmod (x^{2q} - 1)$ cc

# Most Significant $q$ terms of $\Gamma$ – in Parallel



$$\alpha \equiv \left[a_j \bmod \left(x - h^j\right)\right]_{j=0}^{2q-1}$$

## Computational Reduction – In Parallel

- Compute $\Gamma = \Gamma_0 = [g_{0,j}]_{j=0}^{2q-1}$

# Most Significant $q$ terms of $\Gamma$ – in Parallel



$$\alpha \equiv \left[a_j \bmod (x - h^j)\right]_{j=0}^{2q-1}$$

## Computational Reduction – In Parallel

- Compute $\Gamma = \Gamma_0 = [g_{0,j}]_{j=0}^{2q-1}$ where $g_{0,j} = \left((-1)^j + u\right) a_j$

# Most Significant $q$ terms of $\Gamma$ – in Parallel



$$\alpha \equiv \left[a_j \bmod (x - h^j)\right]_{j=0}^{2q-1}$$

## Computational Reduction – In Parallel

- Compute $\Gamma = \Gamma_0 = [g_{0,j}]_{j=0}^{2q-1}$ where $g_{0,j} = \left((-1)^j + u\right) a_j$ CC
- Subtract off $\sum_{j=0}^{q-1} d_j x^j$ CC

# Most Significant $q$ terms of $\Gamma$ – in Parallel



$$\alpha \equiv \left[a_j \bmod \left(x - h^j\right)\right]_{j=0}^{2q-1}$$

## Computational Reduction – In Parallel

- Compute $\Gamma = \Gamma_0 = [g_{0,j}]_{j=0}^{2q-1}$ where $g_{0,j} = \left((-1)^j + u\right) a_j$ CC
- For $i = 0$ to $q - 1$:
  - Compute $d_i = (2q)^{-1} \sum_{j=0}^{2q-1} g_{i,j}$

CC

# Most Significant $q$ terms of $\Gamma$ – in Parallel



$$\alpha \equiv \left[a_j \bmod (x - h^j)\right]_{j=0}^{2q-1}$$

## Computational Reduction – In Parallel

- Compute $\Gamma = \Gamma_0 = [g_{0,j}]_{j=0}^{2q-1}$ where $g_{0,j} = \left((-1)^j + u\right) a_j$ CC
- For $i = 0$ to $q - 1$:
  - Compute $d_i = (2q)^{-1} \sum_{j=0}^{2q-1} g_{i,j}$
  - $x\Gamma_{i+1} = [g_{i,j} - d_i]_{j=0}^{2q-1}$

CC

# Most Significant $q$ terms of $\Gamma$ – in Parallel

$$\alpha \equiv \left[a_j \bmod (x - h^j)\right]_{j=0}^{2q-1}$$

## Computational Reduction – In Parallel

- Compute $\Gamma = \Gamma_0 = [g_{0,j}]_{j=0}^{2q-1}$ where $g_{0,j} = \left((-1)^j + u\right) a_j$ cc
- For $i = 0$ to $q - 1$:
  - Compute $d_i = (2q)^{-1} \sum_{j=0}^{2q-1} g_{i,j}$
  - $x\Gamma_{i+1} = [g_{i,j} - d_i]_{j=0}^{2q-1}$
  - Divide by $x^q \bmod (x^{2q} - 1)$

cc

# Most Significant $q$ terms of $\Gamma$ – in Parallel



$$\alpha \equiv \left[a_j \bmod (x - h^j)\right]_{j=0}^{2q-1}$$

## Computational Reduction – In Parallel

- Compute $\Gamma = \Gamma_0 = [g_{0,j}]_{j=0}^{2q-1}$ where $g_{0,j} = \left((-1)^j + u\right) a_j$ CC
- For $i = 0$ to $q-1$:
  - Compute $d_i = (2q)^{-1} \sum_{j=0}^{2q-1} g_{i,j}$
  - $x\Gamma_{i+1} = [g_{i,j} - d_i]_{j=0}^{2q-1}$
  - Multiply by $x^{-1} = \left[h^{2q-j}\right]_{j=0}^{2q-1}$

CC

# Most Significant $q$ terms of $\Gamma$ – in Parallel



$$\alpha \equiv \left[a_j \bmod (x - h^j)\right]_{j=0}^{2q-1}$$

## Computational Reduction – In Parallel

- Compute $\Gamma = \Gamma_0 = [g_{0,j}]_{j=0}^{2q-1}$ where $g_{0,j} = \left((-1)^j + u\right) a_j$
- For $i = 0$ to $q - 1$:
  - Compute $d_i = (2q)^{-1} \sum_{j=0}^{2q-1} g_{i,j}$
  - $x\Gamma_{i+1} = [g_{i,j} - d_i]_{j=0}^{2q-1}$
  - Multiply by $x^{-1} = \left[h^{2q-j}\right]_{j=0}^{2q-1}$
  - $\Gamma_{i+1} = [g_{i+1,j}]_{j=0}^{2q-1} = \left[h^{2q-j}\left(g_{i,j} - d_i\right)\right]_{j=0}^{2q-1}$

# Most Significant $q$ terms of $\Gamma$ – in Parallel

$$\alpha \equiv \left[a_j \bmod (x - h^j)\right]_{j=0}^{2q-1}$$

## Computational Reduction – In Parallel

- Compute $\Gamma = \Gamma_0 = [g_{0,j}]_{j=0}^{2q-1}$ where $g_{0,j} = \left((-1)^j + u\right) a_j$
- For $i = 0$ to $q-1$:
  - Compute $d_i = (2q)^{-1} \sum_{j=0}^{2q-1} g_{i,j}$
  - $x\Gamma_{i+1} = [g_{i,j} - d_i]_{j=0}^{2q-1}$
  - Multiply by $x^{-1} = \left[h^{2q-j}\right]_{j=0}^{2q-1}$
  - $\Gamma_{i+1} = [g_{i+1,j}]_{j=0}^{2q-1} = \left[h^{2q-j}(g_{i,j} - d_i)\right]_{j=0}^{2q-1}$

$$\Gamma_q \equiv \alpha \bmod r(x)$$

# Conjugates are Cyclic Shifts



$$\alpha = [d_{2q-1}\ d_{2q-2}\ d_{2q-3}\ \ldots\ d_2\ d_1\ d_0]$$

# Conjugates are Cyclic Shifts



$$\alpha = [d_{2q-1}\ d_{2q-2}\ d_{2q-3}\ \ldots\ d_2\ d_1\ d_0]$$

$$\Downarrow$$

$$\alpha^P = [d_1\ d_0\ \ldots\ d_4\ d_3\ d_2]$$

# Conjugates are Cyclic Shifts



$$\alpha = [d_{2q-1}\ d_{2q-2}\ d_{2q-3}\ \ldots\ d_2\ d_1\ d_0]$$

$$\Downarrow$$

$$\alpha^P = [d_1\ d_0\ \ldots\ d_4\ d_3\ d_2]$$

$$\Downarrow$$

$$\alpha^{P^j} = \left[d_{(2q-1)+2j}\ d_{(2q-2)+2j}\ \ldots\ d_{2j+2}\ d_{2j+1}\ d_{2j}\right]$$

# Trace Computation in DFT Form



$$\alpha^{P^j} = [d_{k+2j}]_{k=0}^{2q-1}$$

# Trace Computation in DFT Form



$$\alpha^{P^j} = [d_{k+2j}]_{k=0}^{2q-1}$$

$$\Downarrow$$

$$Tr(\alpha) = \sum_{j=0}^{q-1} \alpha^{P^j} =$$

# Trace Computation in DFT Form



$$\alpha^{P^j} = [d_{k+2j}]_{k=0}^{2q-1}$$

$$\Downarrow$$

$$Tr(\alpha) = \sum_{j=0}^{q-1} \alpha^{P^j} = \left[ \sum_{j=0}^{q-1} d_{k+2j} \right]_{k=0}^{2q+1}$$

# Trace Computation in DFT Form



$$\alpha^{P^j} = [d_{k+2j}]_{k=0}^{2q-1}$$

$$\Downarrow$$

$$Tr(\alpha) = \sum_{j=0}^{q-1} \alpha^{P^j} = \sum_{j=0}^{q-1} d_{2j} = \sum_{j=0}^{q-1} d_{2j+1}$$

# Trivial Conjugates





$$h = u^{\frac{P-1}{2q}}$$

# Trivial Conjugates





$$h = u^{\frac{P-1}{2q}} \Rightarrow x^{P-1} \equiv u^{\frac{P-1}{q}} \equiv h^2 \bmod r(x)$$

# Trivial Conjugates



$$h = u^{\frac{P-1}{2q}} \;\Rightarrow\; x^{P-1} \equiv u^{\frac{P-1}{q}} \equiv h^2 \bmod r(x)$$

## A few definitions

Let:

$$\alpha \equiv \sum_{j=0}^{q-1} a_j x^j \bmod r(x)$$

# Trivial Conjugates



$$h = u^{\frac{P-1}{2q}} \Rightarrow x^{P-1} \equiv u^{\frac{P-1}{q}} \equiv h^2 \bmod r(x)$$

## A few definitions

Let:

$$\alpha \equiv \sum_{j=0}^{q-1} a_j x^j \bmod r(x)$$

$$= \left[ d_k \bmod (x - h^k) \right]_{k=0}^{2q-1}$$

$$d_k = \sum_{j=0}^{q-1} a_j h^{jk}$$

# Trivial Conjugates



$$h = u^{\frac{P-1}{2q}} \Rightarrow x^{P-1} \equiv u^{\frac{P-1}{q}} \equiv h^2 \bmod r(x)$$

## Conjugates

Let:

$$\alpha \equiv \sum_{j=0}^{q-1} a_j x^j \bmod r(x)$$

$$= \left[ d_k \bmod (x - h^k) \right]_{k=0}^{2q-1}$$

$$d_k = \sum_{j=0}^{q-1} a_j h^{jk}$$

$$\alpha^P \equiv \sum_{j=0}^{q-1} a_j x^{Pj} \bmod r(x)$$

# Trivial Conjugates



$$h = u^{\frac{P-1}{2q}} \Rightarrow x^{P-1} \equiv u^{\frac{P-1}{q}} \equiv h^2 \bmod r(x)$$

**Conjugates**

Let:

$$\alpha \equiv \sum_{j=0}^{q-1} a_j x^j \bmod r(x)$$

$$= \left[d_k \bmod (x - h^k)\right]_{k=0}^{2q-1}$$

$$d_k = \sum_{j=0}^{q-1} a_j h^{jk}$$

$$\alpha^P \equiv \sum_{j=0}^{q-1} a_j x^{Pj} \bmod r(x)$$

$$\equiv \sum_{j=0}^{q-1} a_j h^{2j} x^j \bmod r(x)$$

# Trivial Conjugates



$$h = u^{\frac{P-1}{2q}} \Rightarrow x^{P-1} \equiv u^{\frac{P-1}{q}} \equiv h^2 \bmod r(x)$$

**Conjugates**

Let:

$$\alpha \equiv \sum_{j=0}^{q-1} a_j x^j \bmod r(x)$$
$$= \left[ d_k \bmod (x - h^k) \right]_{k=0}^{2q-1}$$
$$d_k = \sum_{j=0}^{q-1} a_j h^{jk}$$

$$\alpha^P \equiv \sum_{j=0}^{q-1} a_j x^{Pj} \bmod r(x)$$
$$\equiv \sum_{j=0}^{q-1} a_j h^{j(2+k)} \bmod (x - h^k)$$

# Trivial Conjugates





$$h = u^{\frac{P-1}{2q}} \Rightarrow x^{P-1} \equiv u^{\frac{P-1}{q}} \equiv h^2 \bmod r(x)$$

**Conjugates**

Let:

$$\alpha \equiv \sum_{j=0}^{q-1} a_j x^j \bmod r(x)$$

$$= \left[d_k \bmod (x - h^k)\right]_{k=0}^{2q-1}$$

$$d_k = \sum_{j=0}^{q-1} a_j h^{jk}$$

$$\alpha^P \equiv \sum_{j=0}^{q-1} a_j x^{Pj} \bmod r(x)$$

$$\equiv \sum_{j=0}^{q-1} a_j h^{j(2+k)} \bmod (x - h^k)$$

$$= \left[d_{k+2 \bmod 2q}\right]_{k=0}^{2q-1}$$

# Simple Inverse Computation



## Using the norm

$$N(\alpha) = \prod_{k=0}^{q-1} \alpha^{P^k}$$

# Simple Inverse Computation



## Using the norm

$$N(\alpha) = \alpha \prod_{k=1}^{q-1} \alpha^{P^k}$$

# Simple Inverse Computation



## Using the norm

$$N(\alpha) = \alpha \prod_{k=1}^{q-1} \alpha^{P^k}$$

$$\Downarrow$$

$$\alpha^{-1} = N(\alpha)^{-1} \prod_{k=1}^{q-1} \alpha^{P^k}$$

## Using the norm

$$N(\alpha) = \alpha \prod_{k=1}^{q-1} \alpha^{P^k}$$

$$\Downarrow$$

$$[d_k]^{-1} = N(\alpha)^{-1} \prod_{k=1}^{q-1} [d_{2k+j}]_{j=0}^{2q-1}$$

# Summary

- Order dividing extension fields: $GF(P^q)$ where $q \,|\, P-1$
- Reviewed techniques for parallel extension field multiplication (DFT)
- Described new field reduction technique within the DFT form
- Described field traits exposed in DFT form