Parallel ODEF Operations

Anna Johnsto

Overviev

0 10.11.0

Iools

Useful Rings: CRT

DFT & Parallel Multiplication

Reduction i

Other DFT

Conjugates Traces

Summary

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

Anna Johnston

Washington State University

14 July 2009

Parallel ODEF Operations

> Anna Johnstor

Overview

.

Tools

Useful Rings: CRT

DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages

Conjugates & Traces

Parallel ODEF Operations

Anna Johnsto

0 7 0 . 7 . 0

1001

Useful Rings: CRT DFT & Parallel Multiplication

Reduction i DFT Form

Other DFT Advantages Conjugates & Traces

- Overview
- 2 Tools
 - Trivial Reduction
 - Useful Rings: CRT
 - DFT & Parallel Multiplication

Parallel ODEF Operations

Anna Johnsto

Overvie

Useful Rings: CRT DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces Inverses

- Overview
- 2 Tools
 - Trivial Reduction
 - Useful Rings: CRT
 - DFT & Parallel Multiplication
- 3 Reduction in DFT Form

Parallel ODEF Operations

Anna Johnsto

Overvie

Tools

Useful Rings: CRT DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces Inverses

- Overview
- 2 Tools
 - Trivial Reduction
 - Useful Rings: CRT
 - DFT & Parallel Multiplication
- Reduction in DFT Form
- 4 Other DFT Advantages
 - Conjugates & Traces
 - Inverses

Parallel ODEF Operations

Anna Johnsto

Overvie

Trivial Reduction
Useful Rings:
CRT
DFT & Parallel
Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces Inverses

- Overview
- 2 Tools
 - Trivial Reduction
 - Useful Rings: CRT
 - DFT & Parallel Multiplication
- 3 Reduction in DFT Form
- 4 Other DFT Advantages
 - Conjugates & Traces
 - Inverses
- Summary

Parallel ODEF Operations

Anna Johnsto

Overview

Tools

Useful Rings: CRT DFT & Parallel

Reduction i DFT Form

Other DFT Advantages Conjugates &

Conjugates Traces Inverses

Summary

An Order Dividing Extension Field is:

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

Parallel ODEF Operations

Anna Johnsto

Overview

Tools

Useful Rings: CRT DFT & Parallel

Reduction in

Other DFT Advantages Conjugates &

Summary

An Order Dividing Extension Field is:

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

Parallel ODEF Operations

Anna Johnsto

Overview

Table

Useful Rings: CRT DFT & Parallel

Reduction in

Other DFT Advantages Conjugates &

Summary

An Order Dividing Extension Field is:

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

Parallel ODEF Operations

Anna Johnsto

Overview

Tools

Useful Rings: CRT DFT & Parallel Multiplication

Reduction in

Other DFT Advantages

Conjugates & Traces Inverses

Summar

An Order Dividing Extension Field is:

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

- $GF(P^2)$, where P is odd
- $GF(19^3)$
- $GF((2^4)^5)$

- $GF(101^5)$
- $GF(29^7)$
- $GF((5^2)^3)$

Parallel ODEF Operations

Anna Johnsto

Overview

Tools

Useful Rings: CRT DFT & Parallel

Reduction i

Other DFT Advantages Conjugates & Traces

Summary

Why Do We Care?

Parallel ODEF Operations

Anna Johnsto

Overview

Tools

Useful Rings: CRT DFT & Parallel

Reduction i

Other DFT Advantages Conjugates & Traces

Summar

Why Do We Care?

 Optimal Extension Fields for Elliptic Curve Cryptosystems

Parallel ODEF Operations

Anna Johnsto

Overview

Tools

Useful Rings: CRT DFT & Parallel Multiplication

Reduction i DFT Form

Other DFT Advantages Conjugates & Traces

Summary

Why Do We Care?

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

Parallel ODEF Operations

Anna Johnsto

Overview

Tools

Useful Rings: CRT DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces Inverses

Summar

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

Parallel ODEF Operations

Anna Johnsto

Overview

Tools

Trivial Reduction
Useful Rings:
CRT
DFT & Parallel
Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces Inverses

Summary

Why Do We Care?

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

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

Parallel ODEF Operations

Anna Johnsto

Vervieu

Tools

Trivial Reducti Useful Rings:

Useful Rings: CRT DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces Inverses

- Overview
- 2 Tools
 - Trivial Reduction
 - Useful Rings: CRT
 - DFT & Parallel Multiplication
- Reduction in DFT Form
- 4 Other DFT Advantages
 - Conjugates & Traces
 - Inverses
- 5 Summary

Parallel ODEF Operations

Anna Johnsto

S

Iools

Trivial Reduction
Useful Rings:

DFT & Parall

Reduction i

Other DFT Advantages

Traces

Summary

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

Parallel ODEF Operations

Anna Johnsto

Overvie

- .

Trivial Reduction

Useful Rings: CRT DFT & Parallel

Reduction i

Other DFT

Conjugates Traces

Summary

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

•
$$\Rightarrow \sqrt[q]{u} \notin \mathbb{F}$$

•
$$r(x) = x^q - u$$
 is irreducible over \mathbb{F}

Parallel ODEF Operations

Anna Johnsto

Overvie

Tool

Trivial Reduction
Useful Rings:
CRT
DFT & Parallel

Reduction i

Other DFT Advantages

Conjugates Traces

Summary

- $u \in \mathbb{F}$, $u^{\frac{P-1}{q}} \neq 1$
- $GF(P^q) \cong \mathbb{F}[x]/r(x)\mathbb{F}[x]$
- $\bullet \ \Rightarrow \ \sqrt[q]{u} \not \in \mathbb{F}$
- $r(x) = x^q u$ is irreducible over \mathbb{F}

Parallel ODEF Operations

Anna Johnsto

Overvie

Tools

Trivial Reduction
Useful Rings:
CRT
DFT & Parallel
Multiplication

Reduction i

Other DFT Advantages

Conjugates Traces Inverses

Summary

- $u \in \mathbb{F}$, $u^{\frac{P-1}{q}} \neq 1$
- $GF(P^q) \cong \mathbb{F}[x]/r(x)\mathbb{F}[x]$

- $\bullet \ \Rightarrow \ \sqrt[q]{u} \not \in \mathbb{F}$
- $r(x) = x^q u$ is irreducible over \mathbb{F}

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Table

Trivial Reduction Useful Rings: CRT

DFT & Parallel Multiplication

Reduction i DFT Form

Other DFT Advantages

Conjugates Traces Inverses

Summary

- $u \in \mathbb{F}$, $u^{\frac{P-1}{q}} \neq 1$
- $GF(P^q) \cong \mathbb{F}[x]/r(x)\mathbb{F}[x]$

- $\bullet \ \Rightarrow \ \sqrt[q]{u} \not \in \mathbb{F}$
- $r(x) = x^q u$ is irreducible over \mathbb{F}

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



$$\sum_{k=0}^{q-1} (v_k + uv_{q+k}) x^k \bmod r(x)$$

Parallel ODEF Operations

Anna Johnsto

Overvie

Trivial Reducti
Useful Rings:

CRT DFT & Paralle

Reduction in

Other DFT Advantages

Conjugates & Traces

Summary

What does it do on Polynomials

Parallel ODEF Operations

Anna Johnsto

Overviev

Overviev

Tools

Trivial Reduction
Useful Rings:
CRT

CRT
DFT & Parallel
Multiplication

Reduction i

Other DFT Advantages Conjugates &

Summary

What does it do on Polynomials

 Gives the discrete Fourier Transform

Parallel ODEF Operations

Anna Johnsto

. .

OVEIVIEV

Trivial Reduction
Useful Rings:
CRT

DFT & Parallel Multiplication

Reduction i DFT Form

Other DFT Advantages Conjugates & Traces

Summary

What does it do on Polynomials

• Gives the discrete Fourier Transform

Enables field reduction within the DFT ring

Parallel ODEF Operations

Anna Johnsto

Overview

Tools

Useful Rings: CRT

DFT & Parallel Multiplication

Reduction i DFT Form

Other DFT Advantages Conjugates & Traces

Summary

What does it do on Polynomials

• Gives the discrete Fourier Transform

Enables field reduction within the DFT ring

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

Parallel ODEF Operations

Anna Johnsto

Overviev

OVEIVIE

Tools

Useful Rings: CRT DFT & Parallel

Reduction i

Other DFT Advantages

Conjugates Traces

Summary

What does it do on Polynomials

• Gives the discrete Fourier Transform

 Enables field reduction within the DFT ring

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

$$\bigoplus$$

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

Parallel ODEF Operations

Anna

Overviev

Trivial Reduction
Useful Rings:

CRT
DFT & Parallel

Reduction i

Other DFT Advantages Conjugates & Traces

Summan

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

Parallel ODEF Operations

Anna Johnsto

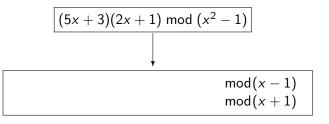
Overviev

Trivial Reduction
Useful Rings:
CRT

DFT & Parallel

Reduction i DFT Form

Other DFT Advantages Conjugates & Traces



Parallel ODEF Operations

> Anna Johnsto

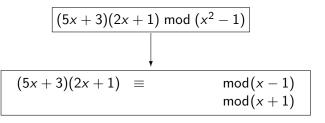
Overviev

Trivial Reduction
Useful Rings:
CRT

Reduction i

DFT Form

Advantages Conjugates & Traces



Parallel ODEF Operations

> Anna Johnsto

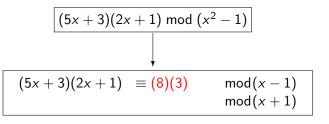
Overvie

Trivial Reduction Useful Rings: CRT

DFT & Parallel Multiplication

Reduction i DFT Form

Other DFT Advantages Conjugates & Traces



Parallel ODEF Operations

> Anna Johnsto

Overviev

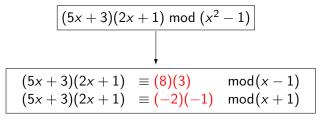
Trivial Reduction Useful Rings: CRT

DFT & Parallel

Reduction i

Other DFT Advantages Conjugates &

Summan



Parallel ODEF Operations

> Anna Johnsto

Overvie

- .

Trivial Reduction
Useful Rings:

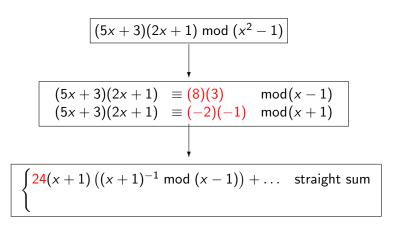
DFT & Paralle

Reduction in

DFT Form

Other DFT Advantages

Conjugates & Traces Inverses



Parallel ODEF Operations

Anna

Overviev

Trivial Reductio
Useful Rings:

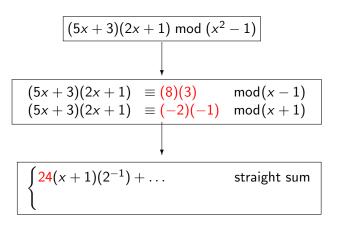
DFT & Paralle

Reduction i

Other DFT Advantages

Conjugates of Traces

Summarv



Parallel ODEF Operations

> Anna Johnsto

Overviev

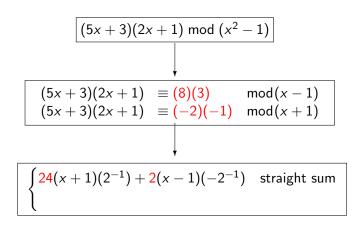
Trivial Reduction
Useful Rings:
CRT

DFT & Paralle

Reduction i

Other DFT Advantages

Conjugates Traces



Parallel ODEF Operations

> Anna Johnsto

Overviev

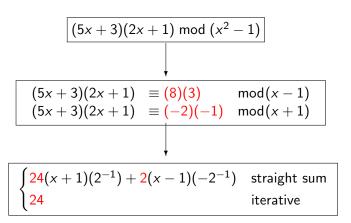
Trivial Reduction Useful Rings: CRT

DFT & Paralle Multiplication

Reduction i

Other DFT

Conjugates Traces Inverses



Parallel ODEF Operations

Anna Johnsto

Overviev

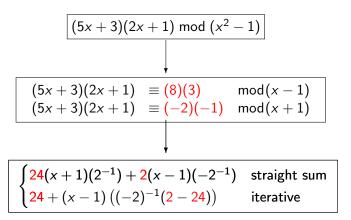
Trivial Reduction Useful Rings: CRT

DFT & Paralle Multiplication

Reduction in

Other DFT

Conjugates of Traces



The CRT in Action: Multiplication

Parallel ODEF Operations

Anna

Overvie

0 10.11.0

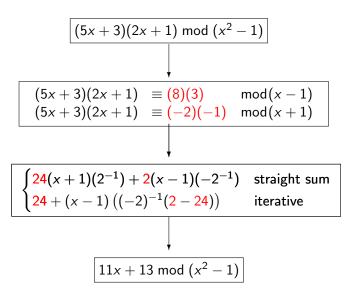
Trivial Reduction
Useful Rings:
CRT

DFT & Paralle Multiplication

Reduction in DFT Form

Other DFT

Conjugates & Traces



Parallel ODEF Operations

Useful Rings: CRT

Over
$$GF(7)$$

 $(x^3 + 2)$

 $\mod (x^2 - 3)$

Parallel ODEF Operations

Useful Rings: CRT

Over GF(7)

 $0 \mod (x^2 - 1), (x^3 + 2)$

 $\mod (x^2 - 3)$

Parallel ODEF Operations

> Anna Johnsto

Overview

OVEIVIE

Trivial Reduction
Useful Rings:
CRT

CRT DFT & Parallel Multiplication

Reduction i DFT Form

Other DFT Advantages Conjugates & Traces

Over
$$GF(7)$$

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

Parallel ODEF Operations

Anna Johnsto

Overviev

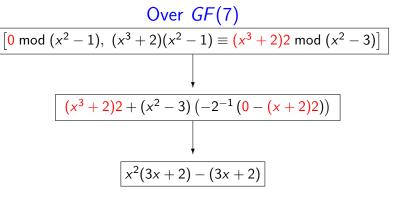
Trivial Reduction
Useful Rings:
CRT

DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages

Conjugates Traces Inverses



Parallel ODEF Operations

Anna Johnsto

Overview

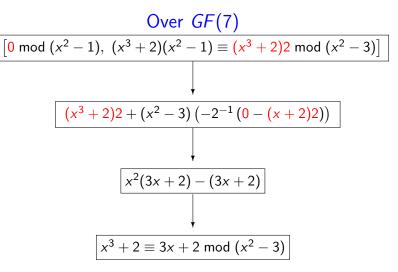
Trivial Reduction
Useful Rings:
CRT

CRT DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages

Conjugates Traces Inverses



Parallel ODEF Operations

Anna Johnsto

)verview

0 10.11.0.

Trivial Reduction

DFT & Parallel Multiplication

Reduction i

Other DFT Advantages Conjugates &

Summary

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

Parallel ODEF Operations

Anna Johnsto

Overview

0 10.11.0

Trivial Reduct

Useful Rings: CRT

DFT & Parallel Multiplication

Reduction i

Other DFT Advantages

Conjugates & Traces

Summary

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

$$\bigvee$$

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

Parallel ODEF Operations

Anna

. .

Overviev

Tools

Trivial Reduction
Useful Rings:

DFT & Parallel Multiplication

Reduction in

Other DET

Advantages Conjugates & Traces

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

Parallel ODEF Operations

Anna Johnsto

)vervie

Trivial Re

OSETUL Rings: CRT DFT & Parallel

DFT & Parallel Multiplication

Reduction i DFT Form

Other DFT Advantages

Conjugates Traces Inverses

Summar

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

Discrete Fourier Transform Multiplication

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Trivial Reduction
Useful Rings:
CRT

DFT & Parallel Multiplication

Reduction i DFT Form

Other DFT Advantages Conjugates & Traces

Summar

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

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Useful Rings: CRT DFT & Paralle

DFT & Parallel Multiplication

Reduction i DFT Form

Other DFT Advantages Conjugates & Traces

Summary

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

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Useful Rings: CRT DFT & Paralle

DFT & Parallel Multiplication

Reduction i DFT Form

Other DFT Advantages Conjugates & Traces

Summary

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

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 ODEF Operations

Anna Johnsto

Overvie

Useful Rings: CRT DFT & Parallel Multiplication

Reduction in

Other DFT Advantages Conjugates & Traces

Summar

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

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?? __

Parallel ODEF Operations

Anna Johnsto

Overviev

0 10.11.0

Trivial Reduction
Useful Rings:
CRT
DFT & Parallel

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces Inverses

- Overview
- 2 Tools
 - Trivial Reduction
 - Useful Rings: CRT
 - DFT & Parallel Multiplication
- 3 Reduction in DFT Form
- 4 Other DFT Advantages
 - Conjugates & Traces
 - Inverses
 - 5 Summary

Parallel ODEF Operations

Anna Johnsto

Overvie

Tools

Useful Rings: CRT DFT & Parallel

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summarv

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Tools

Useful Rings: CRT DFT & Parallel

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summarv

- 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 $[0 \mod (x^{2q} 1), \alpha(x^{2q} 1) \mod r(x)];$

Parallel ODEF Operations

Anna Johnsto

Overvie

Tools

Useful Rings: CRT DFT & Parallel

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summary

- 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 $[0 \mod (x^{2q}-1), \alpha(x^{2q}-1) \mod r(x)];$
- Divide by $(x^{2q} 1)$.

Parallel ODEF Operations

Anna Johnsto

Overvie

Tools

Useful Rings: CRT DFT & Parallel

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summary

- 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 $[0 \mod (x^{2q} 1), \alpha(u^2 1) \mod r(x)];$
- Divide by $(x^{2q} 1)$.

Parallel ODEF Operations

Anna Johnsto

Overvie

Tool

Useful Rings: CRT DFT & Paralle

Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summarv

- 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 $\left[0 \mod (x^{2q}-1), \alpha(u^2-1) \mod r(x)\right]$;
- Divide by $(x^{2q} 1)$.

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Tools

Useful Rings: CRT DFT & Parallel

Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates &

Summary

- 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 $[0 \mod (x^{2q}-1), \alpha(u^2-1) \mod r(x)];$
- Divide by $(x^{2q} 1)$.

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Useful Reduction
Useful Rings:
CRT
DFT & Parallel
Multiplication

Reduction in DFT Form

Other DFT Advantages

Conjugates & Traces Inverses

Summary

- 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 $[0 \mod (x^{2q} 1), \alpha(u^2 1) \mod r(x)];$
- Divide by $(x^{2q} 1)$.

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Useful Rings: CRT

DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages

Conjugates & Traces Inverses

Summar

- 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 $[0 \mod (x^{2q} 1), \alpha(u^2 1) \mod r(x)];$
- Divide by $(x^{2q} 1)$.

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

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Useful Rings: CRT DFT & Parallel

Multiplication
Reduction in

DFT Form

Other DFT Advantages Conjugates & Traces Inverses

Summar

- 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 $[0 \mod (x^{2q} 1), \alpha(u^2 1) \mod r(x)];$
- Divide by $(x^{2q} 1)$.

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

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

Parallel ODEF Operations

Anna

Overviev

Trivial Reduction

DFT & Parall

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summan

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

Parallel ODEF Operations

Anna Johnsto

. .

OVEIVIC

Trivial Reduction Useful Rings: CRT DFT & Parallel

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

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

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

Parallel ODEF Operations

Anna

Overview

Trivial Reduction Useful Rings: CRT DFT & Parallel

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

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

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

Parallel ODEF Operations

Anna

Overvie

0 10.11.0

Trivial Reduction
Useful Rings:
CRT
DFT & Parallel

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summar

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

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

Notice

• $Deg(\alpha(u^2-1)) < 2q$

Deg (Γ) < 2q

Parallel ODEF Operations

Anna

Overvie

Trivial Reductio
Useful Rings:
CRT
DFT & Parallel

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summan

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

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

Notice

•
$$Deg(\alpha(u^2-1)) < 2q$$

Parallel ODEF Operations

Anna

Overvie

Trivial Reduction
Useful Rings:
CRT

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summar

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

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

Notice

•
$$Deg(\alpha(u^2-1)) < 2q$$

•
$$Deg(\Gamma) < 2q$$

$$\Gamma = x^q \sum_{i=0}^{q-1} c_i x^j + \dots$$

Parallel ODEF Operations

Anna Johnsto

Overvie

Trivial Reduction Useful Rings: CRT DFT & Parallel

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summary

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

Parallel ODEF Operations

Anna Johnsto

Overvie

_ .

Trivial Reductio Useful Rings: CRT

DFT & Paralle

Reduction in DFT Form

Other DFT Advantages

Conjugates of Traces

Summary

$\Gamma = x^{q} \sum_{j=0}^{q-1} c_{j} x^{j} + \sum_{j=0}^{q-1} d_{j} x^{j}$

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

Parallel ODEF Operations

Anna

Overvie

Trivial Reduction
Useful Rings:
CRT

Reduction in DFT Form

Other DFT Advantages

Conjugates & Traces

Summar

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

- Compute $\Gamma = (x^q + u)\alpha \mod (x^{2q} 1)$
- Subtract off $\sum_{i=0}^{q-1} d_i x^i$

Parallel ODEF Operations

Anna Johnston

Overvie

Tools

Trivial Reductio
Useful Rings:
CRT
DFT & Parallel
Multiplication

Reduction in DFT Form

Other DFT Advantages

Conjugates & Traces Inverses

Summary

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

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

Parallel ODEF Operations

Anna

Overvie

Trivial Reduction
Useful Rings:
CRT
DFT & Parallel
Multiplication

Reduction in DFT Form

Other DFT Advantages

Conjugates & Traces Inverses

Summary

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

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

Most Significant q terms of Γ – in Parallel

Parallel ODEF Operations

Anna Johnsto

Overvie

Trivial Reductio
Useful Rings:
CRT
DFT & Parallel
Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summary

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

Computational Reduction - In Parallel

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Table

Useful Rings: CRT DFT & Parallel

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summary

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

Computational Reduction - In Parallel

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Trivial Reduction
Useful Rings:
CRT
DFT & Parallel

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summar

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

Computational Reduction - In Parallel

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

Parallel ODEF Operations

Anna Johnstor

Overvie

Tools

Useful Rings: CRT DFT & Parallel

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summary

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

Computational Reduction – In Parallel

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Trivial Reduction
Useful Rings:
CRT
DFT & Parallel

DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates &

Summar

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

Computational Reduction - In Parallel

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

CO

Parallel ODEF Operations

Anna Johnsto

Overvie

Trivial Reduction
Useful Rings:
CRT

DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates &

Summarv

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

Computational Reduction - In Parallel

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

CC

Parallel ODEF Operations

Anna Johnsto

Overvie

Trivial Reductio
Useful Rings:
CRT

DFT & Paralle Multiplication

Reduction in DFT Form

Other DFT Advantages

Conjugates & Traces Inverses

Summary

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

Computational Reduction – In Parallel

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

CO

Parallel ODEF Operations

Anna Johnsto

Overvie

Trivial Reduction
Useful Rings:
CRT

DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Summary

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

Computational Reduction - In Parallel

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

СС

Parallel ODEF Operations

Anna Johnsto

Overvie

Trivial Reduction Useful Rings: CRT

DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages

Conjugates & Traces Inverses

Summary

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

Computational Reduction - In Parallel

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

CC

Parallel ODEF Operations

Reduction in DFT Form

Other DFT

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

Computational Reduction – In Parallel

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

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

Parallel ODEF Operations

Anna Johnsto

Marview

OVCIVIC

Trivial Reduct Useful Rings:

Useful Rings: CRT DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages

Conjugates & Traces Inverses

- Overview
- 2 Tools
 - Trivial Reduction
 - Useful Rings: CRT
 - DFT & Parallel Multiplication
- Reduction in DFT Form
- 4 Other DFT Advantages
 - Conjugates & Traces
 - Inverses
- 5 Summary

Conjugates are Cyclic Shifts

Parallel ODEF Operations

Anna

Overviev

Tools

Trivial Reduction
Useful Rings:
CRT

DFT & Paralle Multiplication

Reduction i

Other DFT

Advantages Conjugates & Traces

Inverses

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

Conjugates are Cyclic Shifts

Parallel ODEF Operations

Anna

Overview

0 10.11.0.

Trivial Reduction

DFT & Paralle

Multiplication

DFT Form

Other DFT Advantages

Conjugates & Traces

Conjugates are Cyclic Shifts

Parallel ODEF Operations

Anna Johnsto

Overvie

Trivial Reduction
Useful Rings:
CRT

DFT & Paralle Multiplication

Reduction i DFT Form

Other DFT Advantages Conjugates & Traces

Summar

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

$$\downarrow \downarrow$$

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

$$\downarrow \downarrow$$

 $\alpha^{P^j} = \begin{bmatrix} d_{(2q-1)+2j} & d_{(2q-2)+2j} & \dots & d_{2j+2} & d_{2j+1} & d_{2j} \end{bmatrix}$

Parallel ODEF Operations

Anna

Overvie

Trivial Reductio
Useful Rings:
CRT

Reduction i

Other DFT Advantages Conjugates & Traces

Inverses

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

Parallel ODEF Operations

Anna

Overvie

Trivial Reduction
Useful Rings:
CRT

DFT & Paralle

Reduction i

Other DFT

Conjugates & Traces

Inverses

Parallel ODEF Operations

Anna Johnsto

Overvie

Tools

Trivial Reduction Useful Rings: CRT DFT & Parallel Multiplication

DFT Form

Other DFI
Advantages
Conjugates &
Traces

Inverses

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

$$W$$

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

Parallel ODEF Operations

Anna

Overvie

Trivial Reduction
Useful Rings:
CRT
DET & Parallel

DFT & Paralle Multiplication

Reduction in

Other DFT Advantages

Conjugates & Traces

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

$$\downarrow \qquad \qquad \downarrow$$

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

Parallel ODEF Operations

Anna Johnsto

Overviev

Tools

Useful Rings: CRT

DFT & Paralle Multiplication

Reduction i

Other DFT

Conjugates & Traces

ITACCS

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

Parallel ODEF Operations

Anna Johnsto

Overviev

Trivial Reduction
Useful Rings:
CRT

DFT & Paral Multiplication

Reduction i

Other DFT Advantages Conjugates & Traces

Inverse

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Trivial Reduct

CRT DFT & Parallel Multiplication

Reduction in

DFT Form

Other DFT Advantages Conjugates & Traces

Inverses

Summar

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

A few definitions

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

Parallel ODEF Operations

Anna Johnsto

Overvie

Tools

Trivial Reduction
Useful Rings:
CRT

DFT & Paralle Multiplication

Reduction in DFT Form

Other DFT Advantages

Conjugates & Traces

Summar

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

A few definitions

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

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

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

Parallel ODEF Operations

> Anna Johnsto

Overvie

1 0015

Useful Rings: CRT DFT & Paralle

Multiplication Reduction in

DFT Form

Other DF I Advantages Conjugates &

Traces Inverses

Summar

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

Conjugates

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

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

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

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

Parallel ODEF Operations

> Anna Johnsto

Verview

Tools

Useful Rings: CRT

DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages

Conjugates & Traces Inverses

Summar

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

Conjugates

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

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

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

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

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

Parallel ODEF Operations

> Anna Johnsto

Overvie

Tools

Useful Rings: CRT

DFT & Parallel Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates &

Traces Inverses

Summary

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

Conjugates

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

$$= \left[d_k \mod (x - h^k) \right]_{k=0}^{2q-1} \qquad \qquad \equiv \sum_{j=0}^{q-1} a_j h^{j(2+k)} \mod (x - h^k)$$

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

Parallel ODEF Operations

> Anna Johnsto

Overvie

10015

Useful Rings: CRT DFT & Paralle

Multiplication

DFT Form

Other DFT Advantages Conjugates &

Traces Inverses

Summary

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

Conjugates

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

$$= \left[d_k \mod (x - h^k) \right]_{k=0}^{2q-1} \qquad \equiv \sum_{j=0}^{q-1} a_j h^{j(2+k)} \mod (x - h^k)$$

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

Parallel ODEF Operations

Anna Johnsto

Overview

Table

Trivial Reduction Useful Rings: CRT DFT & Parallel

Reduction in

Other DFT Advantages Conjugates &

Inverses

Summary

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

Parallel ODEF Operations

Anna Johnsto

Overviev

Trivial Reduction
Useful Rings:
CRT
DFT & Parallel
Multiplication

Reduction in

Other DFT Advantages Conjugates &

Inverses Summary

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

Parallel ODEF Operations

Anna

Overvie

Trivial Red

CRT
DFT & Parallel

Multiplication

Reduction in DFT Form

Other DFT Advantages

Inverses

Summary

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



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

Parallel ODEF Operations

Anna

Overvie

Trivial Reduction
Useful Rings:
CRT
DFT & Parallel
Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces

Inverses Summar

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



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

Summary

Parallel ODEF Operations

Anna Johnsto

Overvi

T. ...

Trivial Reductio
Useful Rings:
CRT
DFT & Parallel
Multiplication

Reduction in DFT Form

Other DFT Advantages Conjugates & Traces Inverses

- ullet 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