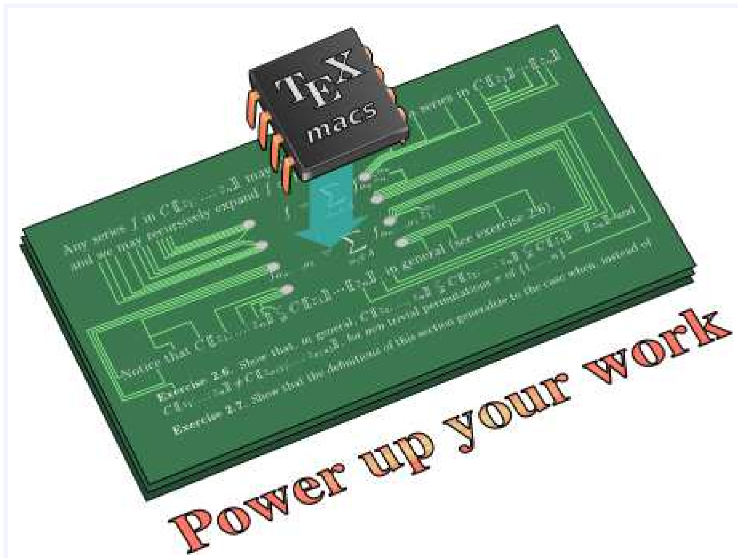
The Frobenius FFT

Joris van der Hoeven, Robin Larrieu

CNRS, École polytechnique



Kaiserslautern, July 26, 2017

http://www.TeXmacs.org

Theorem. (Harvey–vdH–Lecerf 2014) *Two n-bit integers can be multiplied in time*

$$\mathsf{I}(n) \;=\; O(n \log n \, 8^{\log^* n}).$$

Theorem. (Harvey–vdH–Lecerf 2014) *Let q be a prime power. Then two polynomials of degree $<n$ in $\mathbb{F}_q[x]$ can be multiplied in time*

$$\mathsf{M}_q(n) \;=\; O(n \log q \log (n \log q) \, 8^{\log^* (n \log q)}).$$

This bound is uniform in q.

Integer multiplication

- Pollard's number theoretic FFTs (1971): $\mathbb{Z} \rightsquigarrow (\mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \mathbb{F}_{p_3})[x]$

Integer multiplication

- Pollard's number theoretic FFTs (1971): $\mathbb{Z} \rightsquigarrow (\mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \mathbb{F}_{p_3})[x]$
- Smoothing jumps in the complexity: mixed radix FFTs or TFTs

Integer multiplication

- Pollard's number theoretic FFTs (1971): $\mathbb{Z} \rightsquigarrow (\mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \mathbb{F}_{p_3})[x]$
- Smoothing jumps in the complexity: mixed radix FFTs or TFTs

Polynomial multiplication in $\mathbb{F}_q[x]$

- Schönhage–Strassen multiplication (1971) and Schönhage's triadic version (1975)

Integer multiplication

- Pollard's number theoretic FFTs (1971): $\mathbb{Z} \rightsquigarrow (\mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \mathbb{F}_{p_3})[x]$
- Smoothing jumps in the complexity: mixed radix FFTs or TFTs

Polynomial multiplication in $\mathbb{F}_q[x]$

- Schönhage–Strassen multiplication (1971) and Schönhage's triadic version (1975)
- Harvey–vdH–Lecerf (ISSAC 2016): better practical algorithms in characteristic 2

Integer multiplication

- Pollard's number theoretic FFTs (1971): $\mathbb{Z} \rightsquigarrow (\mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \mathbb{F}_{p_3})[x]$
- Smoothing jumps in the complexity: mixed radix FFTs or TFTs

Polynomial multiplication in $\mathbb{F}_q[x]$

- Schönhage–Strassen multiplication (1971) and Schönhage's triadic version (1975)
- Harvey–vdH–Lecerf (ISSAC 2016): better practical algorithms in characteristic 2
- Larrieu (ISSAC 2017): generalization of TFTs to mixed radix setting

Integer multiplication

- Pollard's number theoretic FFTs (1971): $\mathbb{Z} \rightsquigarrow (\mathbb{F}_{p_1} \times \mathbb{F}_{p_2} \times \mathbb{F}_{p_3})[x]$
- Smoothing jumps in the complexity: mixed radix FFTs or TFTs

Polynomial multiplication in $\mathbb{F}_q[x]$

- Schönhage–Strassen multiplication (1971) and Schönhage's triadic version (1975)
- Harvey–vdH–Lecerf (ISSAC 2016): better practical algorithms in characteristic 2
- Larrieu (ISSAC 2017): generalization of TFTs to mixed radix setting

Main lesson

- Privilege methods that use few FFT evaluation points $\rightsquigarrow$
  use finite fields $\mathbb{F}_q$ with multiplicative groups of smooth order
  - Pollard's method $>$ Schönhage–Strassen
  - Harvey–vdH–Lecerf $>$ Schönhage's triadic FFT
  - Mixed radii and/or TFT whenever possible

Rely on the “Babylonian field” $\mathbb{F}_{2^{60}}$, whose multiplicative group has order

```
Pari] factor (2^60 - 1)
```

Rely on the "Babylonian field" $\mathbb{F}_{2^{60}}$, whose multiplicative group has order

```
Pari] factor (2^60 - 1)
```

$$\%1 = \begin{pmatrix} 3 & 2 \\ 5 & 2 \\ 7 & 1 \\ 11 & 1 \\ 13 & 1 \\ 31 & 1 \\ 41 & 1 \\ 61 & 1 \\ 151 & 1 \\ 331 & 1 \\ 1321 & 1 \end{pmatrix}$$

Rely on the "Babylonian field" $\mathbb{F}_{2^{60}}$, whose multiplicative group has order

```
Pari] factor (2^60 - 1)
```

$$\%1 = \begin{pmatrix} 3 & 2 \\ 5 & 2 \\ 7 & 1 \\ 11 & 1 \\ 13 & 1 \\ 31 & 1 \\ 41 & 1 \\ 61 & 1 \\ 151 & 1 \\ 331 & 1 \\ 1321 & 1 \end{pmatrix}$$

Multiplication in $\mathbb{F}_{2^{60}}[x]$

Fast native mixed radix FFT-multiplication

Rely on the "Babylonian field" $\mathbb{F}_{2^{60}}$, whose multiplicative group has order

```
Pari] factor (2^60 - 1)
```

$$\%1 = \begin{pmatrix} 3 & 2 \\ 5 & 2 \\ 7 & 1 \\ 11 & 1 \\ 13 & 1 \\ 31 & 1 \\ 41 & 1 \\ 61 & 1 \\ 151 & 1 \\ 331 & 1 \\ 1321 & 1 \end{pmatrix}$$

Multiplication in $\mathbb{F}_{2^{60}}[x]$

Fast native mixed radix FFT-multiplication

Multiplication in $\mathbb{F}_2[x]$

Kronecker segmentation $\mathbb{F}_2[x] \rightsquigarrow \mathbb{F}_2[x]_{<30}[y] \rightsquigarrow \mathbb{F}_{2^{60}}[y]$, $y = x^{30}$

Rely on the "Babylonian field" $\mathbb{F}_{2^{60}}$, whose multiplicative group has order

```
Pari] factor (2^60 - 1)
```

$$\%1 = \begin{pmatrix} 3 & 2 \\ 5 & 2 \\ 7 & 1 \\ 11 & 1 \\ 13 & 1 \\ 31 & 1 \\ 41 & 1 \\ 61 & 1 \\ 151 & 1 \\ 331 & 1 \\ 1321 & 1 \end{pmatrix}$$

Multiplication in $\mathbb{F}_{2^{60}}[x]$

Fast native mixed radix FFT-multiplication

Multiplication in $\mathbb{F}_2[x]$

Kronecker segmentation $\mathbb{F}_2[x] \rightsquigarrow \mathbb{F}_2[x]_{<30}[y] \rightsquigarrow \mathbb{F}_{2^{60}}[y]$, $y = x^{30}$

Multiplication in $\mathbb{F}_{2^k}[x]$

Various strategies to reduce to multiplication in $\mathbb{F}_{2^{60}}[x]$

Question

What if we directly compute products of polynomials in $\mathbb{F}_2[x]$ inside $\mathbb{F}_{2^{60}}[x]$?

Question

What if we directly compute products of polynomials in $\mathbb{F}_2[x]$ inside $\mathbb{F}_{2^{60}}[x]$?

A priori

This is 60 times more expensive

Question

What if we directly compute products of polynomials in $\mathbb{F}_2[x]$ inside $\mathbb{F}_{2^{60}}[x]$?

A priori

This is 60 times more expensive

But

If $P \in \mathbb{F}_2[x]$ and $\omega \in \mathbb{F}_{2^{60}}$ primitive root of unity and $\phi\colon \mathbb{F}_{2^{60}} \to \mathbb{F}_{2^{60}}; x \mapsto x^2$, then

$$P(\phi(\omega^i)) \;=\; \phi(P(\omega^i))$$

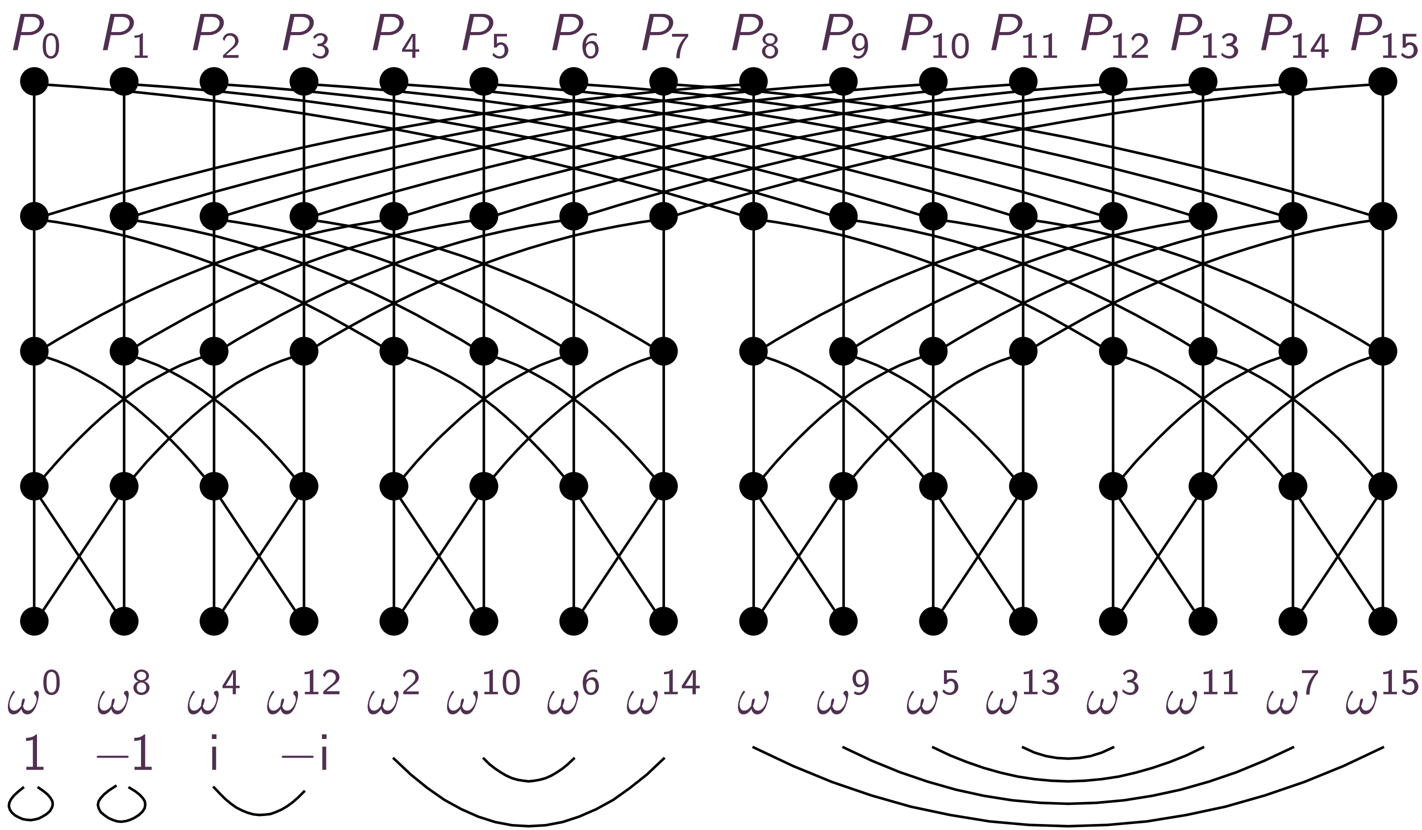
$\rightsquigarrow$ we only to compute $P(\omega^i)$ for one element in the orbit $\omega, \phi(\omega), \phi^2(\omega), \ldots$

Given $P \in \mathbb{R}[x]_{<n}$, $n \in 2^{\mathbb{N}}$, and $\omega = \exp\left(\frac{2\,\pi\,\mathrm{i}}{n}\right)$, compute

$$\begin{aligned}\mathrm{RFFT}_{\omega}(P) &:= (P(\omega^k))_{k \in \mathcal{S}}\\ \mathcal{S} &= \{k \colon \hat{k} \leqslant \widehat{n-k}\}\end{aligned}$$

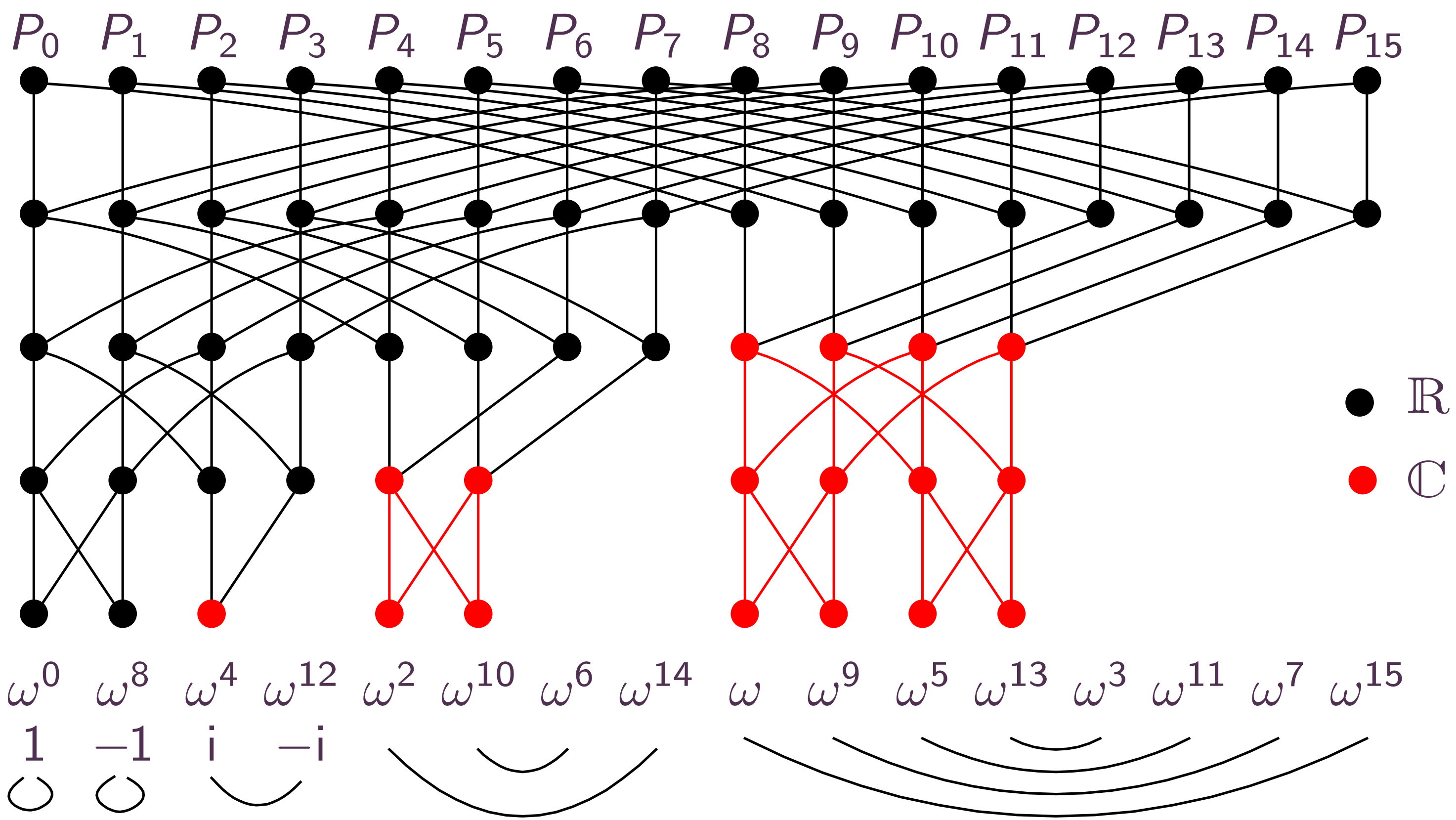
Given $P \in \mathbb{R}[x]_{<n}$, $n \in 2^{\mathbb{N}}$, and $\omega = \exp\left(\frac{2\pi i}{n}\right)$, compute

$$\begin{aligned} \mathrm{RFFT}_\omega(P) &:= (P(\omega^k))_{k \in \mathcal{S}} \\ \mathcal{S} &= \{k : \hat{k} \leqslant \widehat{n-k}\} \end{aligned}$$



Given $P \in \mathbb{R}[x]_{<n}$, $n \in 2^{\mathbb{N}}$, and $\omega = \exp\left(\frac{2\pi i}{n}\right)$, compute

$$\begin{aligned} \mathrm{RFFT}_\omega(P) &:= (P(\omega^k))_{k \in \mathcal{S}} \\ \mathcal{S} &= \{k : \hat{k} \leqslant \widehat{n-k}\} \end{aligned}$$



Given $(P, Q) \in \mathbb{R}[x]_{<n}^2$, $n \in 2^{\mathbb{N}}$, and $\omega = \exp\left(\frac{2\pi i}{n}\right)$, compute $(\mathrm{FFT}_\omega(P), \mathrm{FFT}_\omega(Q))$

Given $(P, Q) \in \mathbb{R}[x]_{<n}^2$, $n \in 2^{\mathbb{N}}$, and $\omega = \exp\left(\frac{2\pi\mathrm{i}}{n}\right)$, compute $(\mathrm{FFT}_\omega(P), \mathrm{FFT}_\omega(Q))$

Given $(P, Q) \in \mathbb{R}[x]^2_{<n}$, $n \in 2^{\mathbb{N}}$, and $\omega = \exp\left(\frac{2\,\pi\,\mathrm{i}}{n}\right)$, compute $(\mathrm{FFT}_\omega(P), \mathrm{FFT}_\omega(Q))$

$+$

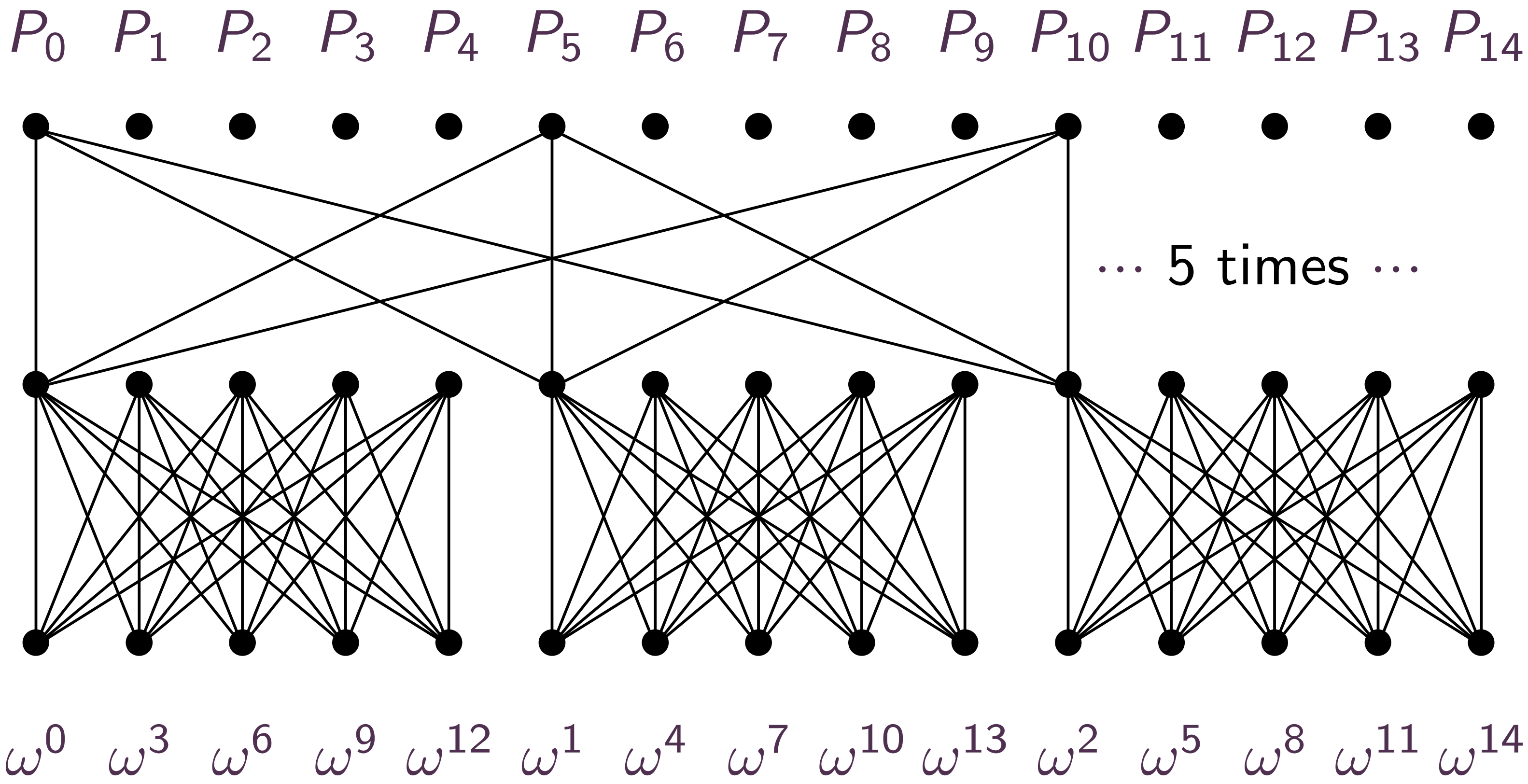
i

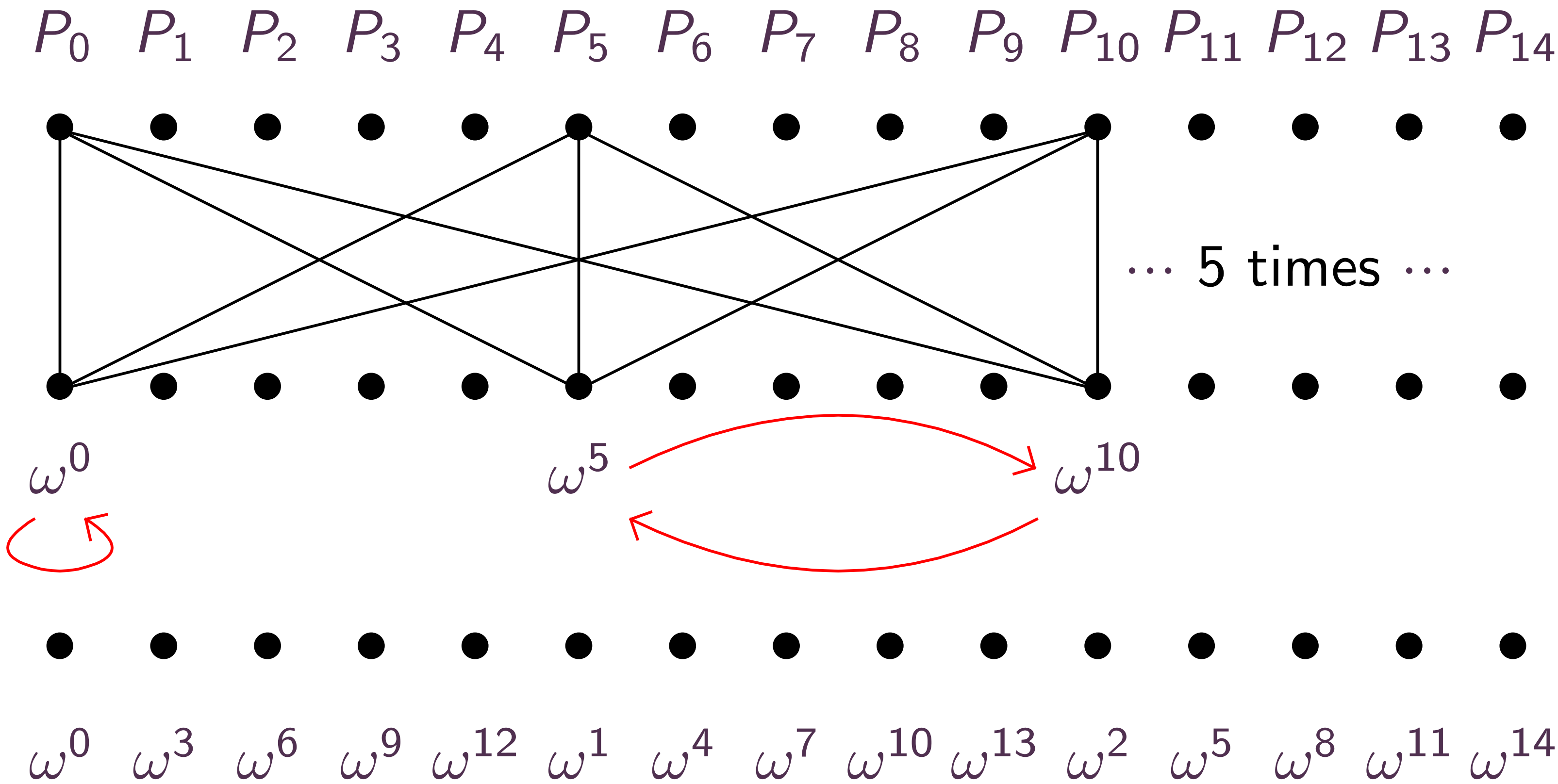
Given $(P, Q) \in \mathbb{R}[x]^2_{<n}$, $n \in 2^{\mathbb{N}}$, and $\omega = \exp\left(\frac{2\pi\mathrm{i}}{n}\right)$, compute $(\mathrm{FFT}_\omega(P), \mathrm{FFT}_\omega(Q))$

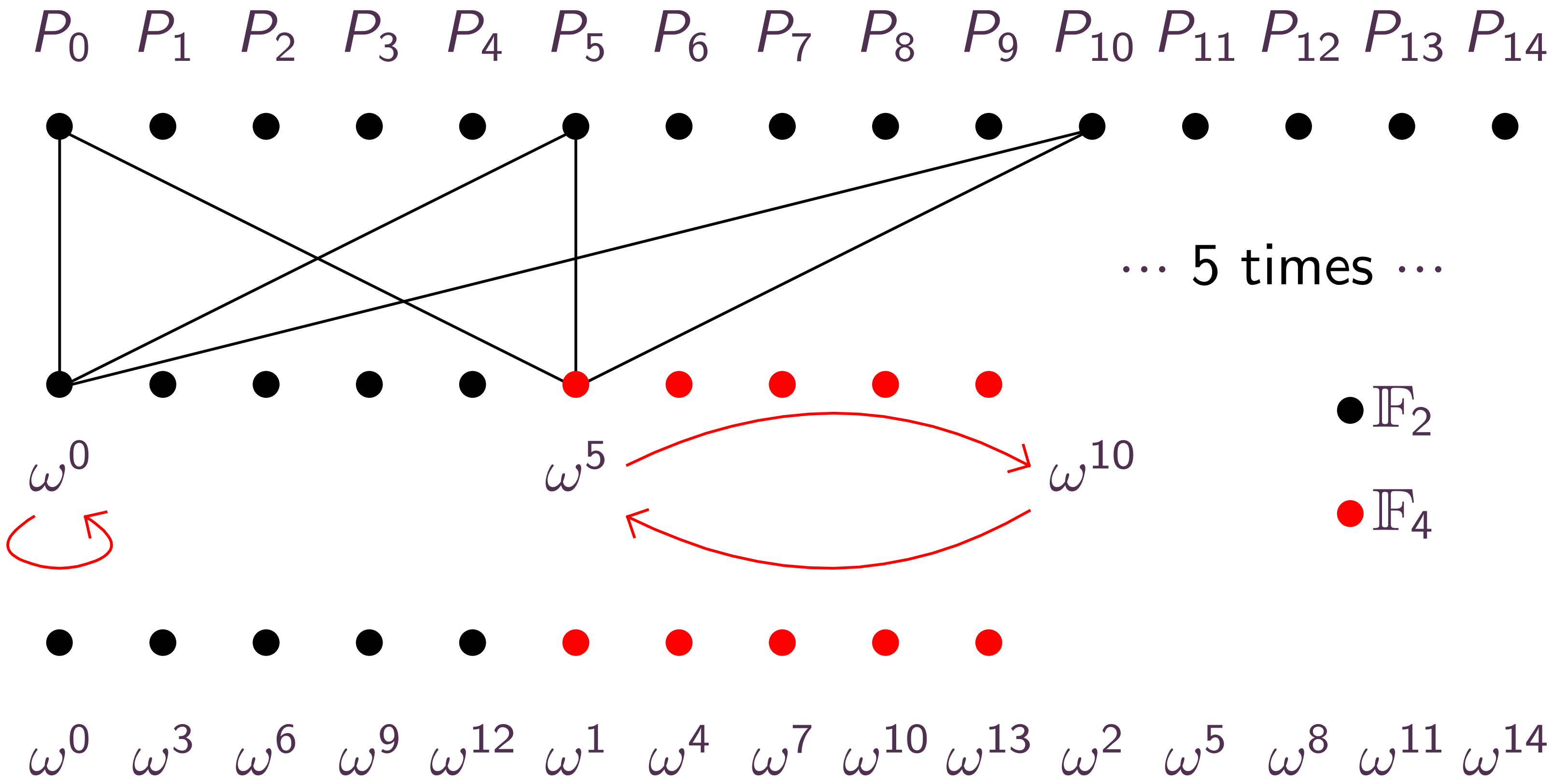
$+$

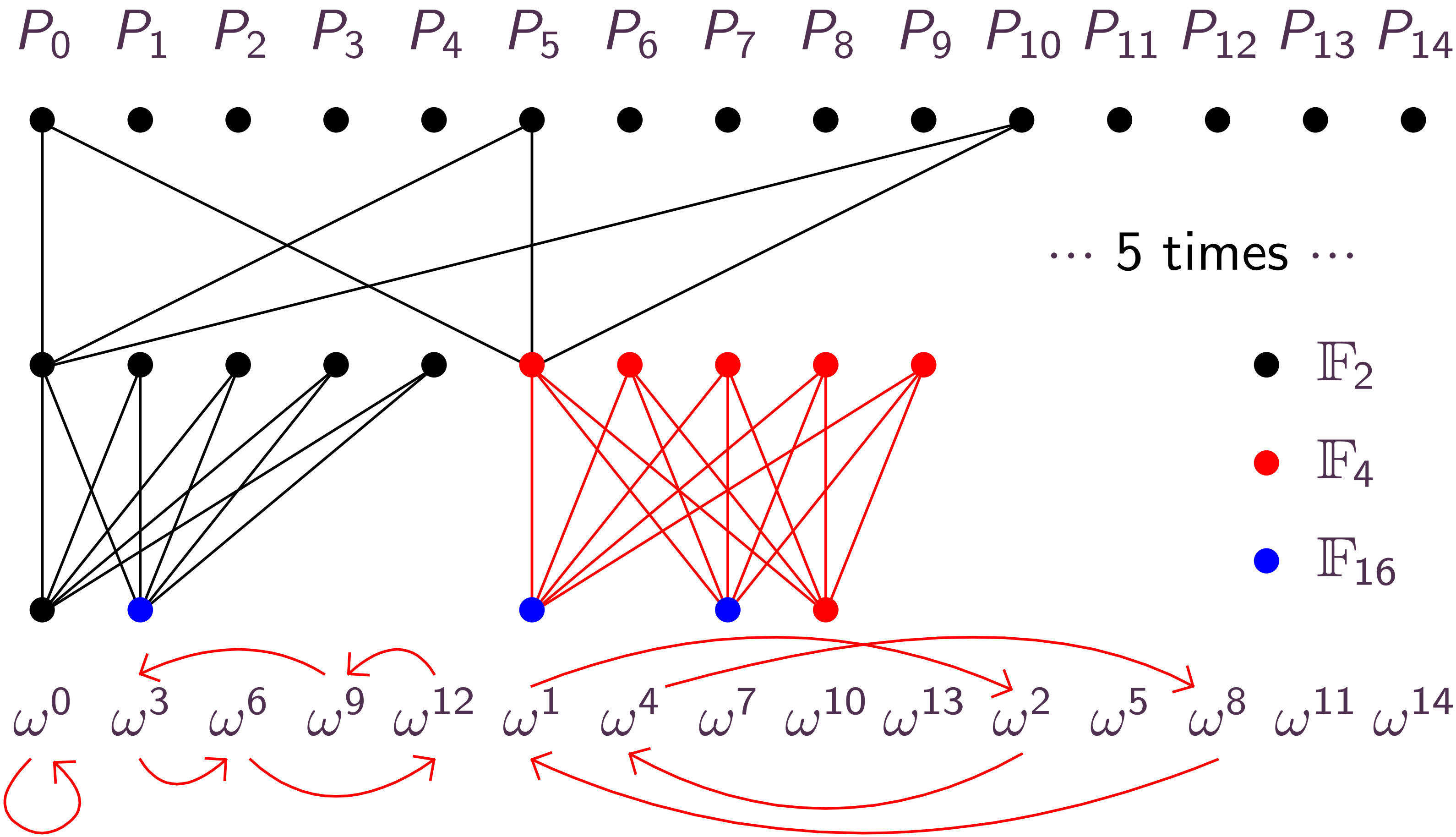
i

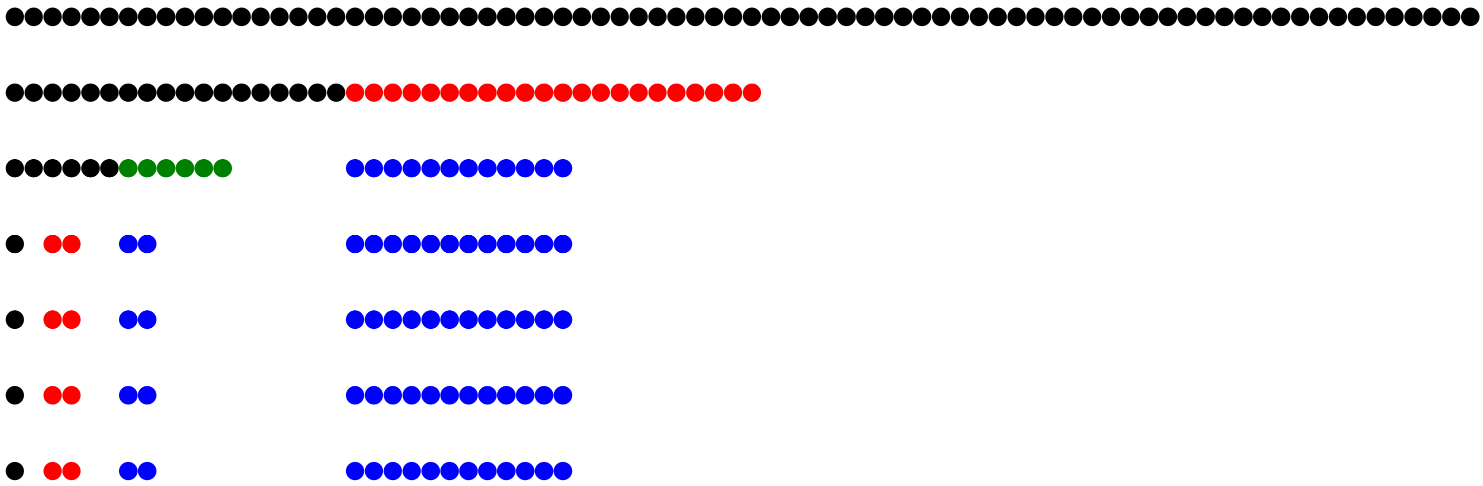
$$\begin{aligned} R &= P + Q\,\mathrm{i} \\ P(\omega^k) &= \tfrac{1}{2}\left(R(\omega^k) + \overline{R(\omega^k)}\right) \\ Q(\omega^k) &= \tfrac{1}{2\mathrm{i}}\left(R(\omega^k) - \overline{R(\omega^k)}\right) \end{aligned}$$

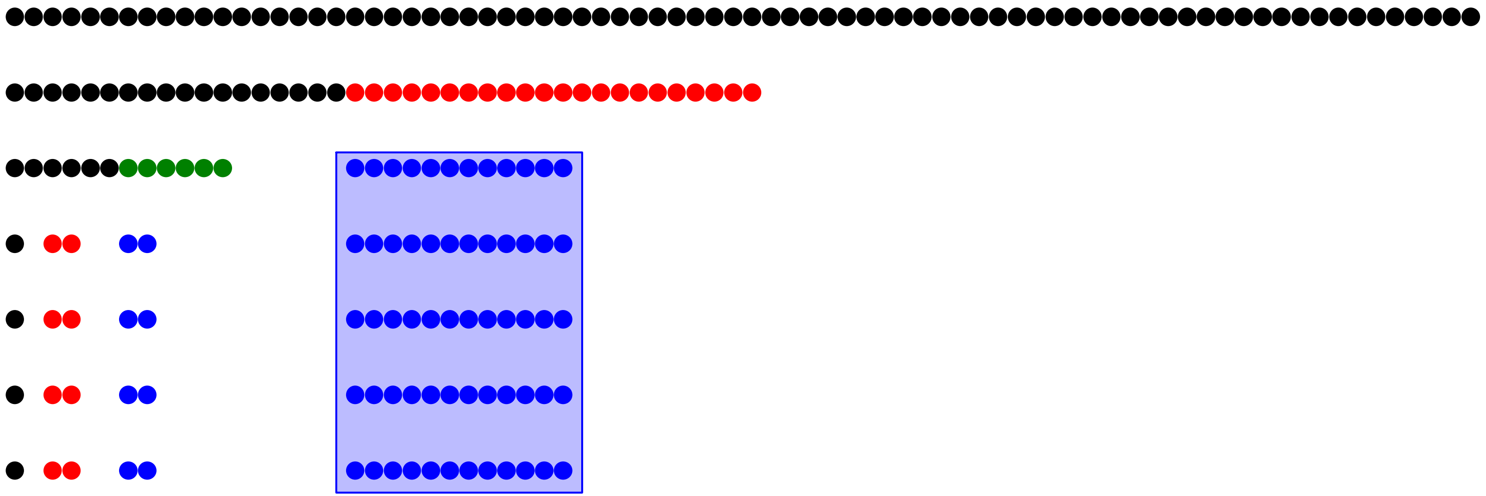

P_0 P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 P_{10} P_{11} P_{12} P_{13} P_{14}
⋯ 5 times ⋯
ω^0 ω^3 ω^6 ω^9 ω^{12} ω^1 ω^4 ω^7 ω^{10} ω^{13} ω^2 ω^5 ω^8 ω^{11} ω^{14}


P_0 P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 P_{10} P_{11} P_{12} P_{13} P_{14}
$\cdots$ 5 times $\cdots$
ω^0
ω^5
ω^{10}
ω^0 ω^3 ω^6 ω^9 ω^{12} ω^1 ω^4 ω^7 ω^{10} ω^{13} ω^2 ω^5 ω^8 ω^{11} ω^{14}


P_0 P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 P_{10} P_{11} P_{12} P_{13} P_{14}
$\cdots$ 5 times $\cdots$
$\mathbb{F}_2$
$\mathbb{F}_4$
ω^0
ω^5
ω^{10}
ω^0 ω^3 ω^6 ω^9 ω^{12} ω^1 ω^4 ω^7 ω^{10} ω^{13} ω^2 ω^5 ω^8 ω^{11} ω^{14}


P_0 P_1 P_2 P_3 P_4 P_5 P_6 P_7 P_8 P_9 P_{10} P_{11} P_{12} P_{13} P_{14}
$\cdots$ 5 times $\cdots$
$\mathbb{F}_2$
$\mathbb{F}_4$
$\mathbb{F}_{16}$
ω^0 ω^3 ω^6 ω^9 ω^{12} ω^1 ω^4 ω^7 ω^{10} ω^{13} ω^2 ω^5 ω^8 ω^{11} ω^{14}





Special case

Compute FFFT of $P \in \mathbb{F}_2[x]_{<n}$, where n is large and $61 \mid n$

Special case

Compute FFFT of $P \in \mathbb{F}_2[x]_{<n}$, where n is large and $61 \mid n$

First step with radix 61

For $0 \leqslant k < \frac{n}{61}$ and $P_k^\sharp = P_k + P_{k+n/61}\, y + \cdots + P_{k+60n/61}\, y^{60}$,

- Compute $P_k^\sharp(1) \in \mathbb{F}_2$
- Compute $P_k^\sharp(\omega^{n/61}) \in \mathbb{F}_{2^{60}}$
- Take $\omega^{n/61} = \alpha$, where $\mathbb{F}_{2^{60}} = \mathbb{F}_2[\alpha]$ and $\frac{\alpha^{61}-1}{\alpha-1} = 0$

Special case

Compute FFFT of $P \in \mathbb{F}_2[x]_{<n}$, where n is large and $61 \mid n$

First step with radix 61

For $0 \leqslant k < \frac{n}{61}$ and $P_k^\sharp = P_k + P_{k+n/61}\, y + \cdots + P_{k+60n/61}\, y^{60}$,

- Compute $P_k^\sharp(1) \in \mathbb{F}_2$
- Compute $P_k^\sharp(\omega^{n/61}) \in \mathbb{F}_{2^{60}}$
- Take $\omega^{n/61} = \alpha$, where $\mathbb{F}_{2^{60}} = \mathbb{F}_2[\alpha]$ and $\frac{\alpha^{61}-1}{\alpha - 1} = 0$

Remaining steps

- One FFFT of size $n/61$
- One full FFT of size $n/61$ over $\mathbb{F}_{2^{60}}$

Special case

Compute FFFT of $P \in \mathbb{F}_2[x]_{<n}$, where n is large and $61 \mid n$

First step with radix 61

For $0 \leqslant k < \frac{n}{61}$ and $P_k^\sharp = P_k + P_{k+n/61}\, y + \cdots + P_{k+60n/61}\, y^{60}$,

- Compute $P_k^\sharp(1) \in \mathbb{F}_2$
- Compute $P_k^\sharp(\omega^{n/61}) \in \mathbb{F}_{2^{60}}$
- Take $\omega^{n/61} = \alpha$, where $\mathbb{F}_{2^{60}} = \mathbb{F}_2[\alpha]$ and $\frac{\alpha^{61}-1}{\alpha-1} = 0$

Remaining steps

- One FFFT of size $n/61$
- One full FFT of size $n/61$ over $\mathbb{F}_{2^{60}}$

Stay tuned...