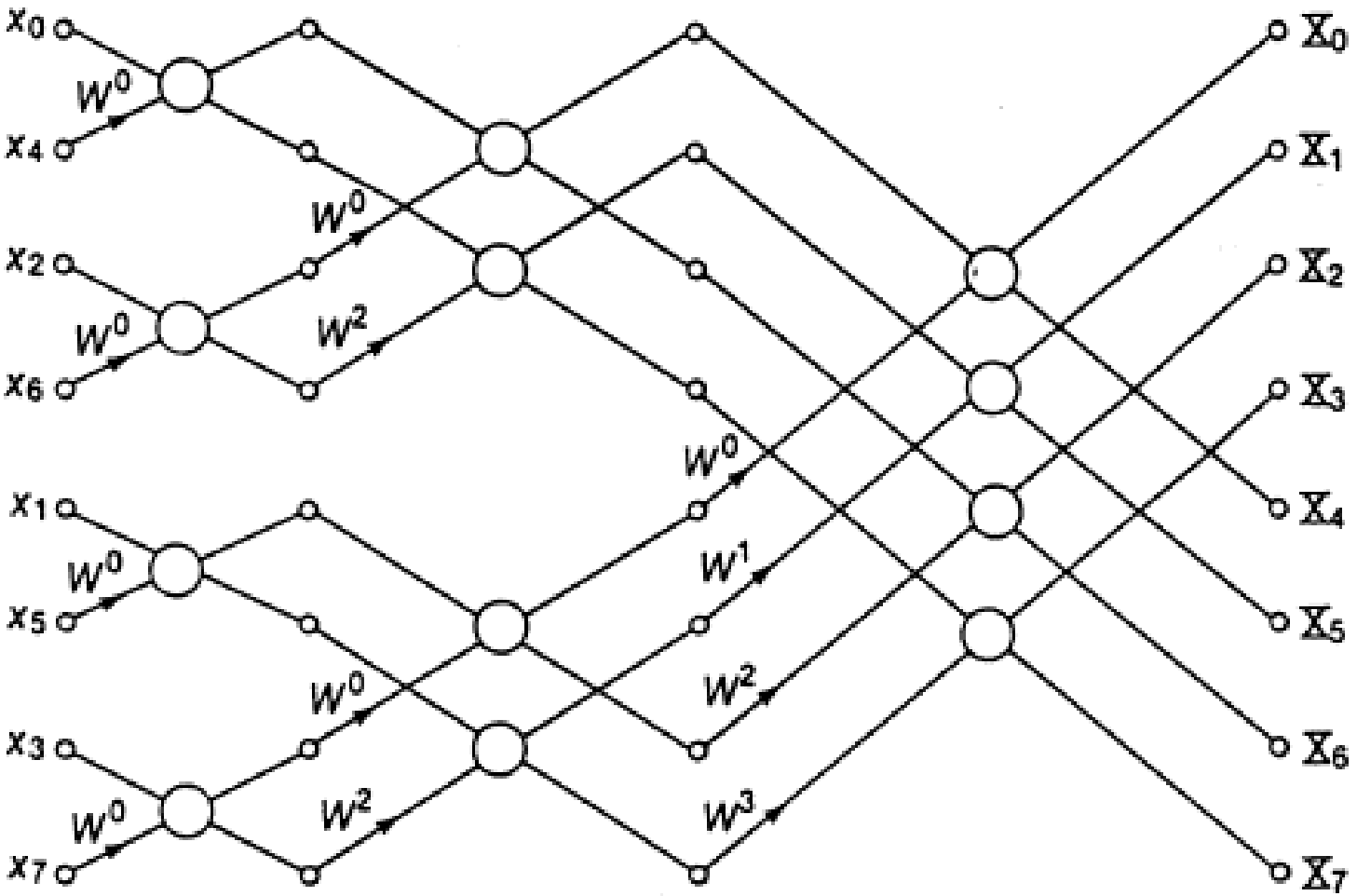
FFT i CRT

Andrzej Chmielowiec

Instytut Podstawowych Problemów Techniki
Polskiej Akademii Nauk

24 marca 2010

Iloczyny wyznaczane podczas wykonywania FFT



Faktoryzacja $X^8 - 1$

$$
\begin{array}{lllll}
(X^8-1) & & & & \\
 & (X^4-1) & & & \\
 & & (X^2-1) & (X-1) & = (X-\omega_8^0) \\
 & & & (X+1) & = (X-\omega_8^4) \\
 & & (X^2+1) & (X-\omega_8^2) & = (X-\omega_8^2) \\
 & & & (X+\omega_8^2) & = (X-\omega_8^6) \\
 & (X^4+1) & & & \\
 & & (X^2-\omega_8^2) & (X-\omega_8) & = (X-\omega_8^1) \\
 & & & (X+\omega_8) & = (X-\omega_8^5) \\
 & & (X^2+\omega_8^2) & (X-\omega_8^3) & = (X-\omega_8^3) \\
 & & & (X+\omega_8^3) & = (X-\omega_8^7)
\end{array}
$$

Dyskretna transformata Fouriera

$$
\begin{array}{llllll}
 & & & A & \bmod (X-1) & = A(\omega_8^0) \\
 & & A \bmod (X^2-1) & A & \bmod (X+1) & = A(\omega_8^4) \\
 & A \bmod (X^4-1) & & & & \\
 & & A \bmod (X^2+1) & A & \bmod (X-\omega_8^2) & = A(\omega_8^2) \\
 & & & A & \bmod (X+\omega_8^2) & = A(\omega_8^6) \\
A & & & & & \\
 & & & A & \bmod (X-\omega_8) & = A(\omega_8^1) \\
 & & A \bmod (X^2-\omega_8^2) & A & \bmod (X+\omega_8) & = A(\omega_8^5) \\
 & A \bmod (X^4+1) & & & & \\
 & & A \bmod (X^2+\omega_8^2) & A & \bmod (X-\omega_8^3) & = A(\omega_8^3) \\
 & & & A & \bmod (X+\omega_8^3) & = A(\omega_8^7)
\end{array}
$$

Chińskie twierdzenie o resztach

Jeśli $m = m_1 \cdots m_k$ i dla $i \neq j$ mamy $NWD(m_i, m_j) = 1$, to układ kongruencji

$$\begin{cases} x & \equiv & x_1 \bmod m_1 \\ & \vdots & \\ x & \equiv & x_k \bmod m_k \end{cases}$$

ma dokładnie jedno rozwiązanie modulo m.

Jeśli przyjąć, że $M_i = \frac{m}{m_i}$ oraz $B_i M_i \equiv 1 \bmod m_i$, to liczba

$$x = x_1 B_1 M_1 + \cdots + x_k B_k M_k$$

jest rozwiązaniem tego układu kongruencji.