Dhirubhai Ambani Institute of Information and
Communication Technology
Gandhinagar, Gujarat 382007

PC433 BTP-I
PC434 BTP-II

Under the guidance of
Prof. Arpita Mal

by

Nikita Shah

Student ID: 202101209

1 Proof:

Given: Let $n \in \mathbb{N}, n > 2$

$$\boldsymbol{X} = \begin{bmatrix} x_{00} & x_{01} & \cdots & x_{0(n-1)} \\ x_{10} & x_{11} & \cdots & x_{1(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ x_{(2^n-1)0} & x_{(2^n-1)1} & \cdots & x_{(2^n-1)(n-1)} \end{bmatrix}, \quad \text{Dimensions of } \boldsymbol{X} = 2^n \times n.$$

The (i, j)-th entry of matrix $\boldsymbol{X}$ is defined as follows:

$$x_{ij} = \begin{cases} -1 & \text{if } i < 2^{n-1} \text{ and } j = 0, \\ (-1)^{\left(\lfloor \frac{i}{2^{n-1-j}} \rfloor \mod 2\right)+1} & \text{if } i < 2^{n-1} \text{ and } j \neq 0, \\ 1 & \text{if } X_i \geq 2^{n-1} \text{ and } j = 0, \\ (-1)^{\left(\lfloor \frac{i}{2^{n-1-j}} \rfloor \mod 2\right)} & \text{if } i < 2^{n-1} \text{ and } j \neq 0, \end{cases}$$

$$\boldsymbol{Y} = \begin{bmatrix} y_{00} & y_{01} & \cdots & y_{0(n-2)} & 1 \\ y_{10} & y_{11} & \cdots & y_{1(n-2)} & 1 \\ \vdots & \vdots & \ddots & \vdots & \\ y_{(2^{(n-1)}-1)0} & y_{(2^{(n-1)}-1)1} & \cdots & y_{(2^{(n-1)}-1)(n-2)} & 1 \end{bmatrix}, \quad \text{Dimensions of } \boldsymbol{Y} = 2^{n-1} \times n.$$

The (i, j)-th entry of matrix $\boldsymbol{Y}$ is defined as follows:

$$y_{ij} = \begin{cases} (-1)^{\left(\lfloor \frac{i}{2^{n-2-j}} \rfloor \mod 2\right)+1} & \text{if } j \neq 0, \\ 1 & \text{if } j = n-1, \end{cases}$$

$$\boldsymbol{B} = \begin{bmatrix} b_{00} & b_{01} & \cdots & b_{0(n^2-1)} \\ b_{10} & b_{11} & \cdots & b_{1(n^2-1)} \\ \vdots & \vdots & \ddots & \vdots \\ b_{(2^{2n-1}-1)0} & b_{(2^{2n-1}-1)1} & \cdots & b_{(2^{2n-1}-1)(n^2-1)} \end{bmatrix}, \quad \text{Dimensions of } \boldsymbol{B} = 2^{2n-1} \times n^2.$$

The (i, j)-th entry of matrix $\boldsymbol{B}$ is defined as follows:

$$b_{ij} = x_{pk} * y_{ql}$$

$$b_{ij} = \text{(p, k)-th entry of } \boldsymbol{X} * \text{(q, l)-th entry of } \boldsymbol{Y}$$

$$p = \left\lfloor \frac{i}{2^{n-1}} \right\rfloor, \quad q = i \mod 2^{n-1}, \quad k = j \mod n, \quad l = \left\lfloor \frac{j}{n} \right\rfloor$$

To Prove: Prove that $R_i - R_{i+1} = R_{i+2} - R_{i+3} \quad \forall i \in \mathbb{W}$, $i \mod 4 = 0$, where R_i is the i^{th} row of $\boldsymbol{B}$.

Proof.

$$p^{\text{th}} \text{ row of } \boldsymbol{X} \ \mapsto \ x_p := (x_{p0}, x_{p1}, \cdots, x_{p(n-1)})$$
$$q^{\text{th}} \text{ row of } \boldsymbol{Y} \ \mapsto \ y_q := (y_{q0}, y_{q1}, \cdots, y_{q(n-2)}, 1)$$
$$x_p = -x_{p+2^{n-1}}$$

$$i^{\text{th}} \text{ row of } \boldsymbol{B} \ \mapsto \ R_i := y_q \cdot x_p$$
$$p = \left\lfloor \frac{i}{2^{n-1}} \right\rfloor, \quad q = i \mod 2^{n-1}$$

$$(i+1)^{\text{th}} \text{ row of } \boldsymbol{B} \ \mapsto \ R_{i+1} := y_{q_1} \cdot x_{p_1}$$
$$p_1 = \left\lfloor \frac{i+1}{2^{n-1}} \right\rfloor = \left\lfloor \frac{i}{2^{n-1}} \right\rfloor = p \qquad (\because i \mod 4 = 0)$$
$$q_1 = (i+1) \mod 2^{n-1} = 1 + (i \mod 2^{n-1}) = 1 + q \qquad (n > 2)$$

$$\therefore R_i - R_{i+1} := y_q \cdot x_p - y_{q_1} \cdot x_{p_1}$$

$$\therefore R_i - R_{i+1} := (y_q - y_{q_1}) \cdot x_p \tag{1}$$

$$(i+2)^{\text{th}} \text{ row of } \boldsymbol{B} \ \mapsto \ R_{i+2} := y_{q_2} \cdot x_{p_2}$$
$$p_2 = \left\lfloor \frac{i+2}{2^{n-1}} \right\rfloor = \left\lfloor \frac{i}{2^{n-1}} \right\rfloor = p$$
$$q_2 = (i+2) \mod 2^{n-1} = 2 + (i \mod 2^{n-1}) = 2 + q$$

$$(i+3)^{\text{th}} \text{ row of } \boldsymbol{B} \ \mapsto \ R_{i+3} := y_{q_3} \cdot x_{p_3}$$
$$p_3 = \left\lfloor \frac{i+3}{2^{n-1}} \right\rfloor = \left\lfloor \frac{i}{2^{n-1}} \right\rfloor = p$$
$$q_3 = (i+3) \mod 2^{n-1} = 3 + (i \mod 2^{n-1}) = 3 + q$$

$$\therefore R_{i+2} - R_{i+3} := (y_{q_2} - y_{q_3}) \cdot x_p \tag{2}$$

We need to prove that

$$R_i - R_{i+1} = R_{i+2} - R_{i+3}$$
$$\therefore (y_q - y_{q_1}) \cdot x_p = (y_{q_2} - y_{q_3}) \cdot x_p$$
$$\therefore y_q - y_{q_1} = y_{q_2} - y_{q_3}$$
$$\therefore y_q - y_{q+1} = y_{q+2} - y_{q+3} \quad \forall 0 \le q < 2^{n-1}$$

$$\therefore (-1)^{\left(\lfloor \frac{q}{2^{n-2-l}} \rfloor \mod 2\right)+1} - (-1)^{\left(\lfloor \frac{q+1}{2^{n-2-l}} \rfloor \mod 2\right)+1}$$
$$= (-1)^{\left(\lfloor \frac{q+2}{2^{n-2-l}} \rfloor \mod 2\right)+1} - (-1)^{\left(\lfloor \frac{q+3}{2^{n-2-l}} \rfloor \mod 2\right)+1} \quad \forall 0 \le l < n, n > 2 \quad (3)$$

For $l = n-1, \quad y_{ql} = 1 \quad \forall 0 \le q < 2^{n-1}$.

$$\therefore L.H.S.\ (3) = 0 \text{ and } R.H.S.\ (3) = 0$$
$$\therefore L.H.S.\ (3) = R.H.S.\ (3)$$

Now, $i \mod 4 = 0$. Since $q = i \mod 2^{n-1}, n > 2$, let $i = 2^{n-1}c_1 + q = 4c_2 + q$.
$\therefore i \mod 4 = (4c_2 + q) \mod 4 = q \mod 4 = 0$.
For $0 \le l < n-1$, $(q+1) \mod 2^{n-2-l} \ne 0$ and $(q+3) \mod 2^{n-2-l} \ne 0$.
$\therefore \left(\lfloor \frac{q}{2^{n-2-l}} \rfloor \mod 2\right) = \left(\lfloor \frac{q+1}{2^{n-2-l}} \rfloor \mod 2\right)$ and $\left(\lfloor \frac{q+2}{2^{n-2-l}} \rfloor \mod 2\right) = \left(\lfloor \frac{q+3}{2^{n-2-l}} \rfloor \mod 2\right)$.

$$\therefore L.H.S.\ (3) = 0 \text{ and } R.H.S.\ (3) = 0$$
$$\therefore L.H.S.\ (3) = R.H.S.\ (3)$$

Thus, (3) holds for $\forall 0 \le l < n$, $n > 2$.
Hence, proved.

□

Conclusion: We have shown linear dependencies amongst rows R_i, R_{i+1}, R_{i+2} and R_{i+3} of $\boldsymbol{B}$ for given constraints.

Example: Let $n = 3$

$$\boldsymbol{X} = \begin{bmatrix} -1 & -1 & -1 \\ -1 & -1 & 1 \\ -1 & 1 & -1 \\ -1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \\ 1 & -1 & -1 \end{bmatrix} \quad \text{Dimensions of } \boldsymbol{X} = 8 \times 3.$$

$$\boldsymbol{Y} = \begin{bmatrix} -1 & -1 & 1 \\ -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{Dimensions of } \boldsymbol{Y} = 4 \times 3.$$

Dimensions of $\boldsymbol{B} = 8 \times 4$.

Here, $2^{n-1} = 4$ and $R_i = -R_{i+16}$
$\therefore R_0 - R_1 = R_2 - R_3 \implies R_{16} - R_{17} = R_{18} - R_{19}$,
$R_4 - R_5 = R_6 - R_7$,
$R_8 - R_9 = R_{10} - R_{11}$,
$R_{12} - R_{13} = R_{14} - R_{15}$
and similarly the rest of the row dependencies can be shown.