<u>שאלה 1:</u>

סעיף 1.1:

$$HXH=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}*\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}*\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}=\frac{1}{2}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}*\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}=\sigma_z$$

בנוסף H אוניטרית והרמיטית ולכן מתקיים כי:

$$HXH=Z\Longrightarrow X=H^{-1}ZH^{-1}=H^{*}ZH^{*}=HZH$$

סעיף 1.2:

אסמן $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$, לכן מתקיים כי ההסתברות למדוד את $|0\rangle$

בבסיס החישוב היא $|\alpha|^2$. בנוסף מתקיים כי $H|\psi\rangle=\alpha|+\rangle+\beta|-\rangle$.

לכן ההסתברות למדוד את $|+\rangle$ בבסיס הדמר היא גם $|\alpha|^2$.

כלומר המדידות שקולות ובפרט 0 מתאים ל- +.

סעיף 1.3:

$$SXS^{*}=\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}*\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}*\begin{pmatrix}1 & 0\\ 0 & -i\end{pmatrix}=\begin{pmatrix}0 & 1\\ i & 0\end{pmatrix}*\begin{pmatrix}1 & 0\\ 0 & -i\end{pmatrix}=\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}=\sigma_y$$

$$S^{*}YS=\begin{pmatrix}1 & 0\\ 0 & -i\end{pmatrix}*\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix}*\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}=\begin{pmatrix}0 & -i\\ 1 & 0\end{pmatrix}*\begin{pmatrix}1 & 0\\ 0 & i\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}=\sigma_x$$

סעיף 1.4:

אסמן $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. מתקיים כי:

$$S^*|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

$$S^*|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ -i \end{pmatrix} = -i * |1\rangle$$

לכן יתקיים כי:

$$HS^*|\psi\rangle = HS^*(\alpha|0\rangle + \beta|1\rangle) = H(\alpha|0\rangle - \beta i|1\rangle) = (\alpha|+\rangle - \beta i|-\rangle) =$$

$$= \frac{\alpha - \beta i}{\sqrt{2}} |0\rangle + \frac{\alpha + \beta i}{\sqrt{2}} |1\rangle$$

לכן ההסתברות למדוד את $|0\rangle$ בבסיס החישוב היא $\frac{|\alpha-\beta i|^2}{2}$.

בנוסף, ההסתברות למדוד את $|+_i\rangle$ בבסיס העצמי של Y נתונה ע"י:

$$|\langle +_i|\psi\rangle|^2 = \left|\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix}\right|^2 = \left|\frac{\alpha - \beta i}{\sqrt{2}}\right|^2 = \frac{|\alpha - \beta i|^2}{2}$$

לכן ההסתברות למדוד את $|+_i\rangle$ בבסיס העצמי של Y היא גם $\frac{|\alpha-\beta i|^2}{2}$.

כלומר המדידות שקולות ובפרט $|0\rangle$ מתאים ל- $|+_i\rangle$.

שאלה 2:

סעיפים 2.1+2.2:

תחילה, מתקיים כי $U = CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

כלומר יתקיים כי:

$$U * |++\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} * \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = |++\rangle$$

$$U * |+-\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} * \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} = |--\rangle$$

$$U * |-+\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} * \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix} = |-+\rangle$$

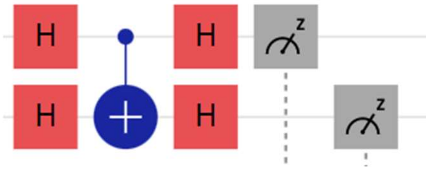
$$U * |--\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} * \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} = |+-\rangle$$

כעת נוכיח את הטענה בטבלה, בהתבסס על פעולת U בבסיס הדמר:

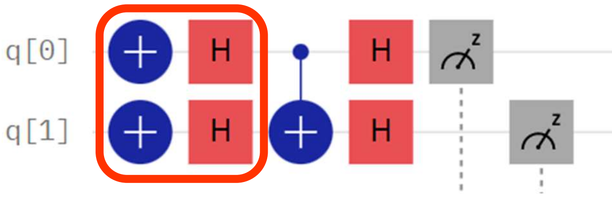
q_0q_1	HxH	(HxH)U	HxH
$\|00\rangle$	$\|++\rangle$	$\|++\rangle$	$\|00\rangle$
$\|01\rangle$	$\|+-\rangle$	$\|--\rangle$	$\|11\rangle$
$\|10\rangle$	$\|-+\rangle$	$\|-+\rangle$	$\|10\rangle$
$\|11\rangle$	$\|--\rangle$	$\|+-\rangle$	$\|01\rangle$

מהטבלה רואים שהשער שמומש הוא בדיוק שער CNOT שבו הביט השני הוא ביט הקונטרול.

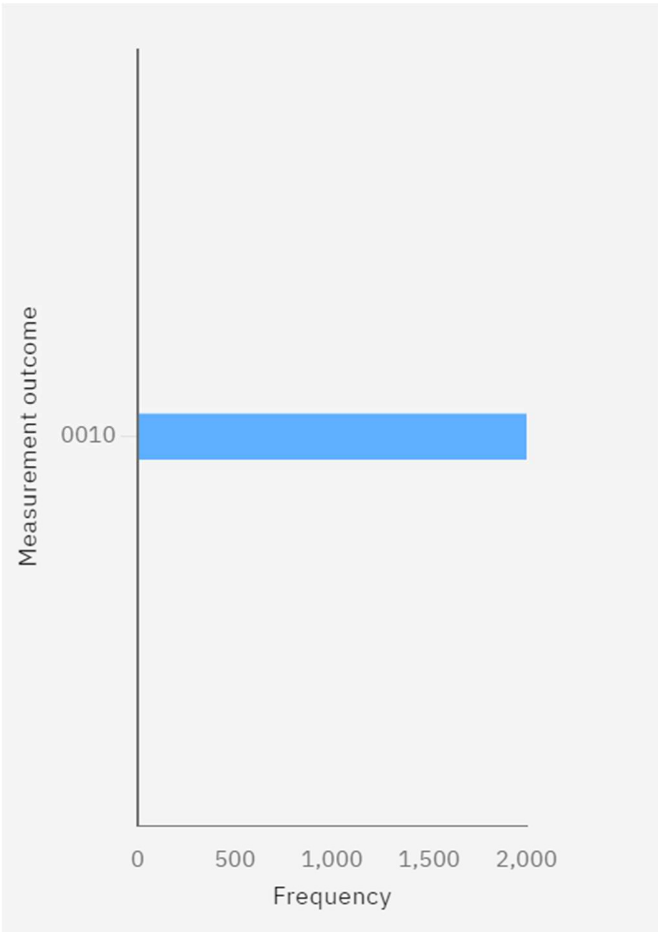
תוצאות ה Quantum composer:



זהו שרטוט המעגל ללא שערי המצב ההתחלתי.



זהו שרטוט המעגל יחד עם השערים הנחוצים להכנת המצב $|--\rangle$.



זוהי ההיסטוגרמה עבור ההרצה של המעגל שתיארנו עם המצב ההתחלתי $|--\rangle$.

כפי שניתן לראות תוצאת הניסוי לפי המחשב הקוונטי היא 0010 ולכן לאחר שנהפוך את המספרים נקבל את המצב הקוונטי $|0100\rangle$.

בפרט אנו עובדים רק עם 2 הקיוביטים הראשונים ולכן המצב שנקבל יהיה $|01\rangle$. מצב זה תואם את התאוריה מפני שלפי שאלה 1, מדידה זו למדידה של $|+-\rangle$ בבסיס הדמר, שזה בדיוק הפלט שהיינו מצפים מהשער עבור הקלט $|--\rangle$.

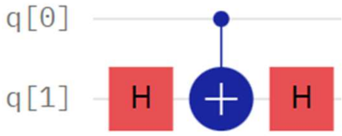
שאלה 3:

סעיף 3.1:

השער CZ הוא מקרה פרטי של שער C-V ולכן ייצוגו כמטריצה בבסיס

החישוב יהיה $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

סעיף 3.2:



אראה כי מתקיים ש- $CZ = (IxH)CNOT(IxH)$:

$$IxH = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

$$\Longrightarrow (IxH)CNOT = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & -1 & 1 \end{pmatrix}$$

$$\Longrightarrow (IxH)CNOT(IxH) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = CZ$$

סעיף 3.3:

הסיבה לכך שהיינו מקבלים תוצאות זהות לפעולת הזהות היא ש-CZ מותיר את המצב פריק ורק מוסיף פאזה למצב הקיוביט השני ולכן כאשר נמדוד את המערכת ההסתברות לכל מצב בסיס תישאר זהה.

שאלה 4:

סעיף 4.1:

ניתן לראות כי $U\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, U\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}$

כלומר בתת המערכת של $|00\rangle, |11\rangle$ יתקיים כי

U מעבירה את $|0\rangle$ ל- $|+\rangle$ ואת $|1\rangle$ ל- $|-\rangle$.

כלומר U היא מטריצת הדמר והיא נתונה על ידי $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$

סעיף 4.2:

קוד הגריי המתאים הוא 11->10->00 ולכן מטריצת הפרמוטציה

המתאימה תהיה $A=\begin{pmatrix}0&0&1&0\\0&1&0&0\\1&0&0&0\\0&0&0&1\end{pmatrix}$

כמו כן שער ה C-V המתאים יהיה C-H כאשר H זו מטריצת הדמר

והוא יהיה נתון על ידי $C-H=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&\frac{1}{\sqrt{2}}&\frac{1}{\sqrt{2}}\\0&0&-\frac{1}{\sqrt{2}}&\frac{1}{\sqrt{2}}\end{pmatrix}$

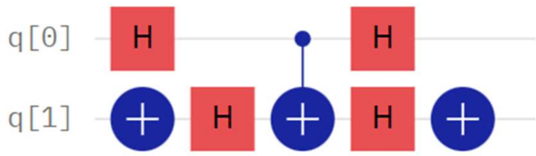
סעיף 4.3:

אראה כי $U = A * C - H * A$:

$$A * C - H * A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} * \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} * \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 & -\frac{1}{\sqrt{2}} \end{pmatrix} = U$$

סעיף 4.4:



תחילה, על ידי חישוב פשוט ניתן לקבל את פעולת A על שני קיוביטים.

נסכמה בטבלה הבאה:

q_0q_1	A
$\|00\rangle$	$\|10\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|00\rangle$
$\|11\rangle$	$\|11\rangle$

כלומר A היא שער הדומה ל CNOT שבו ביט הקונטרול הוא הקיוביט השני, אך פעולת ה NOT תתבצע אם ורק אם ערכו 0.

בפרט ראינו בשאלה 2 מימוש לשער דומה, שבו ביט הקונטרול הוא הקיוביט

השני אך הפעולה מתבצעת כאשר ערכו 1.

לכן ניתן להעביר את ערכו של הקיוביט השני ב NOT ואז בשער משאלה 2

ולבסוף שוב שער NOT כדי לשחזר את ערכו.

חישוב ישיר:

$$(IxNOT) * (HxH) * CNOT * (HxH) * (IxNOT) =$$

$$= \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} * \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} * CNOT * (HxH) * (IxNOT) =$$

$$= \frac{1}{2} * \begin{pmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \end{pmatrix} * \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} * (HxH) * (IxNOT) =$$

$$= \frac{1}{2} * \begin{pmatrix} 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \end{pmatrix} * \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} * (IxNOT) =$$

$$= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} * \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = A$$

לכן חישוב זה אכן יוצר את A.

When Not on this biases is variation of ,Hadamard transform:

$$\binom{b}{a} = \frac{1}{\sqrt{2}}\left(\binom{a}{b} + \binom{c}{d}\right) \qquad V_1 = \binom{a}{b}$$

$$\longrightarrow$$

$$\binom{d}{c} = \frac{1}{\sqrt{2}}\left(\binom{a}{b} - \binom{c}{d}\right) \qquad V_2 = \binom{c}{d}$$

$$\longrightarrow \binom{b}{a} = \frac{1}{\sqrt{2}}\binom{a+c}{b+d} \to \begin{cases} b = \dfrac{a+c}{\sqrt{2}} \\ a = \dfrac{b+a}{\sqrt{2}} \end{cases}$$

$$\longrightarrow \left(d + \frac{a+c}{\sqrt{2}}\right) \cdot \frac{1}{\sqrt{2}} = a \to c + \sqrt{2}d = a$$

Same process

$$\binom{d}{c} = \frac{1}{\sqrt{2}}\left(\binom{a}{b} - \binom{c}{d}\right) \to c = \sqrt{2}b - a$$

$$1 = a^2 + b^2 = b^2 + \left(c + \sqrt{2}d\right)^2 = c^2 + 2\left(\sqrt{2}cd + d^2\right) + b^2$$

Normelaize $\quad \to 2\sqrt{2}cd + d^2 + b^2 = 0$

Same process $\longrightarrow \quad 2\sqrt{2}ba = 2\sqrt{2}cd - ab = cd$

$$-\frac{cd}{b}c' = -bd' \to c^2 d = d'b^2 \to c^2 = d^2$$

$$(\sigma c)^2 + (bd)^2 + 2abdC = a^2c^2 + b^2d^2 - 2cdc'd' = 0$$

$$\to a^2 = d^2 \qquad a = \frac{1}{\sqrt{2}} = \frac{c}{i}$$

$$a^2 = c^2 = d^2 = b^2 = \frac{1}{2}$$

$$\frac{i}{\sqrt{2}} = \sqrt{2}b - \frac{1}{\sqrt{2}} \rightarrow b = \frac{1}{2} + \frac{i}{2}$$

$$bd' + ac' = 0 \rightarrow -\frac{i}{2} + \left(\frac{1}{2} + \frac{i}{2}\right)^2 = 0$$

For the base of v1 and v2 we getting the transformation U:

$$U = \begin{bmatrix} \boxed{V_2} & \boxed{V_1} \end{bmatrix} \longrightarrow U^t \sigma_x U = \qquad \boxed{t = \frac{1}{\sqrt{2}}}$$

$$\begin{pmatrix} t & t^2 - t^2 i \\ -ti & t^2 + t^2 i \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} t & ti \\ t^2 + t^2 i & t^2 - t^2 i \end{pmatrix}$$

$$= \begin{pmatrix} t^3 - t^3 i + t^3 + t^3 i & t^3 i + t^3 + t^3 - t^3 i \\ t^3 i + t^3 + t^3 - t^3 i & t^3 - t^3 - t^3 i - t^3 \end{pmatrix}$$

$$= \begin{pmatrix} t & t \\ t & -t \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H$$

Now the implementation of the gate c-V is:
With the transformation U deger transform the second qubit then activate CNOT on the both qubits and finally transform again the second qubit with U.

$$C - V = \left(I_2 \otimes U^{\dagger}\right) \subset NOT\left(I_2 \otimes U\right)$$

$$= \begin{pmatrix} U^{\dagger} & 0 \\ 0 & U^{\dagger} \end{pmatrix} \cdot \begin{pmatrix} I2 & 0 \\ 0 & \sigma_x \end{pmatrix} \cdot \begin{pmatrix} U & 0 \\ 0 & U \end{pmatrix}$$

$$= \begin{pmatrix} U^{+}U & 0 \\ 0 & V^{\sigma} \times U^{+} \end{pmatrix} = c - V$$

$$\downarrow$$

$$\begin{pmatrix} I_2 & 0 \\ 0 & H \end{pmatrix}$$

QUESTION 5.A

JANUARY 2023

for this question we will define the sign **r_(i)** when i is the index of r, the mathematics parts will be under **bold** marks**.**

Perhaps **r_(i) = r_(i-2) mod(r_(i-1))** .
Under **N** we can find **q,r** in **N** when **r < r_(i-1)** such that:
r_(i-2) = q • r_(i) + r -> r_(i) = (q • r_(i-1) + r) mod(r_(i-1)) = r

<=
Perhaps **a |r_(i-1) , a| r_(i)** there for two fixed numbers we will define them as q_(1) and **q_(2)** for them we will get: **r_(i-1) = a•q_(1) , r_(i) = a•q_(2)**
-> r_(i-2) = r_(i-1)•q + r = r_(i) + q•a q_(1) = a•(q_(2) + q•q_(1))
according the definition **a | r_(i)**

=>
for a in **N** (natural numbers) , **a |r_(i-2) , a| r_(i-1)** <-> **a |r_(i-2) , a| r_(i)** :
If **a |r_(i-2) , a| r_(i-1)** there are two fixed numbers in N we will define them as **q_(1)** and **q_(2)** such that **r_(i-1) = a • q_(2)** and **r_(i-2) = a • q_(1)** :
Now, lets note what we got:
first **r_(i-2) = q • r_(i-1) + r = q • a • q_(2) + r -> a•(q_(1) - q•q_(2))**
-> a | r_(i)

So let's organize all of what we got :
we prove **{a such as a|r_(i-1) , a|r_(i)} = {a such as a|r_(i-2) , a|r_(i-1)}**
-> gcd(r_(i-2)) = max {a such as a|r_(i-1) , a|r_(i)}=
= max {a such as a|r_(i-2) , a|r_(i-1)} = gcd(r_(i-1) , r_(i))

QUESTION 5.B

JANUARY 2023

Let **x** fixed number in **N** and **x>0**.
defined **gcd(x, 0) = m**
0 = 0•x so **x|0** therefore **x** dividing **0** , additionally,**gcd(x, 0) ⩽ max{a:a|x} =x** regarding the fact the **gcd(x, 0)** dividing **x**, we got all of we wanted (for this clause at list) **gcd(x,0) = x**.

QUESTION 5.C

JANUARY 2023

Let's analyze each iteration of this algorithm:
The algorithm gets two numbers, like we saw in clause 1 the algorithm is updating the two numbers, such as in each iteration is the same gcd value.
Then the algorithm updates the two numbers for smaller numbers with the same gcd as the previous numbers, in this routine one of the two numbers will update to be zero in some iteration.
Then the algorithms return the number x which is the gcd of the two numbers
like we saw in clause 2.
 therefore the algorithm finds the gcd of the two numbers.

JANUARY 2023

QUESTION 5.D

let **i** in **N** when we assume **$i \geqslant 2$** and **$(r_{(i-1)}) \bmod (r_{(i-2)}) = r$**
There are **q,r** in **N** when **$r < r_{(i-1)}$** and **$r_{(i-2)} = q \bullet r_{(i-2)}$**
and **$r_{(i)} < r_{(i-1)}$** according that **$r_{(i)} = q \bullet r_{(i-1)} + (r) \bmod (r_{(i-1)}) = r$**.

Now lats prove that **$r_{(i)} < r_{(i-1)} < r_{(i-2)}$** when **$a>b$** , **$r_{(1)}$** is **b** and **$r_{(0)}$** is a.
Induction:
Base:
$i=2 \to b = r_{(1)} = r_{(i-1)} < r_{(i-2)} = r_{(0)} = a$
$r_{(i)} < r_{(i-1)} \to r_{(i)} < r_{(i-1)} < r_{(i-2)}$

Step:
For **$i>2$** under the induction emphasis assuming **$r_{(i)} < r_{(i-1)} < r_{(i-2)}$**
$\to r_{(i)} < r_{(i-1)}$ and like we prove above therefore **$r_{(i+1)} < r_{(i)}$**
$\to r_{(i+1)} < r_{(i)} < r_{(i-1)}$

$\Rightarrow r_{(i+1)} < r_{(i)} < r_{(i-1)} = r_{(i-1)} \bullet q = r_{(i)} + r_{(i-1)} \bullet q$
$\to r_{(i)} < r_{(i-1)} < r_{(i)} + r_{(i-1)} \bullet q \to 0 < r_{(i-1)} - r_{(i)} < r_{(i-1)} \bullet q$
$\to r_{(i-2)} = q \bullet r_{(i-1)} + \geqslant r_{(i-1)} + r_{(i)} > 2 \bullet r_{(i)}$ for $q \geqslant 1$.
$\to r_{(i)} < r_{(i-2)} / 2$

Let's organize all of the steps under what we proved above.
First, let's note in each iteration we reduce the bits using at least in one bit because the algorithm cuts the information of one of the numbers in a half according that the algorithm updating in each iteration one of the numbers for a smaller number, smaller at least as half of one of the two numbers.
So how many iterations does the algorithm?
the depth is **$\log(a+b)$** so at most as the number of bits of the input
what is **$\log(a+b)$**.
The polynomial iteration of the algorithm **is $r (\bmod r)$** , so the algorithm is polynomial in the input length (**i-1** , **i-2**).