# CS621/CSL611
# Quantum Computing For Computer Scientists

## Quantum Search

Dhiman Saha

Winter 2024

IIT Bhilai

# Quantum Search

## Simon's Algorithm

## Simon's problem

- **Input:** For a positive integer $n$, input to the problem is a function of the form

$$f : \{0,1\}^n \to \{0,1\}^n$$

- **Restriction:** Access to this function is restricted to queries to the black-box transformation $U_f$
- **Property**: $f$ is promised to obey a certain property: $\exists s \in \{0,1\}^n$ such that

$$[f(x) = f(y)] \iff [x \oplus y \in \{0^n, s\}], \ \ \forall x, y \in \{0,1\}^n$$

- **Goal:** Find the string $s$

| $x$ | $f(x)$ |
|---|---|
| 000 | 101 |
| 001 | 010 |
| 010 | 000 |
| 011 | 110 |
| 100 | 000 |
| 101 | 110 |
| 110 | 101 |
| 111 | 010 |

- String $s$ is 110.
- Every output of $f$ occurs twice,
- The two input strings corresponding to any one given output have bitwise XOR equal to $s = 110$

**Note**

Note that the possibility that $s = 0^n$ is not ruled out. In this case the function $f$ is simply required to be a one-to-one function.

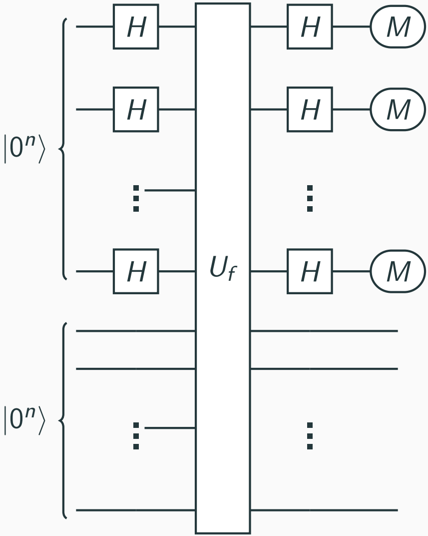
Work out the requirements on $f$ if $s = 011$.

- **Non-quantum algorithm to find** $s$:
  - Compute $f$ for many inputs
  - Hope to find collision

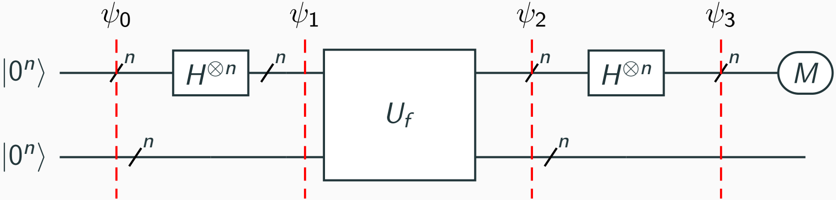
**Note** — **Classical Period Finding**

- If the function is a two-to-one function, then we will not have to evaluate more than half the inputs before we get a repeat.
- If we evaluate more than half the strings and still cannot find a match, then we know that $f$ is one to one and that $s = 0^n$.
- So, in the worst case, $2^{n-1} + 1$ function evaluations will be needed.

- **Quantum algorithm to find** $s$:
  - Simon's algorithm finds s with $\approx n$ quantum evaluations of $f$




$$U_f\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus f(x)\rangle$$




$$(H^{\otimes n} \otimes I) U_f (H^{\otimes n} \otimes I) |0^n\rangle |0^n\rangle$$

## General Expression: $H^{\otimes n}|0^n\rangle$

- $k = 1$

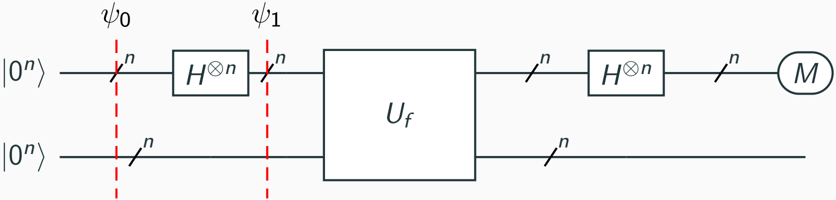
$$H|0\rangle = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{1}{\sqrt{2}} \sum_{x \in \{0,1\}} |x\rangle$$

- $k = 2$

$$\begin{aligned} H^{\otimes 2}|0\rangle|0\rangle &= \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{\sqrt{2^2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2^2}} \sum_{x \in \{0,1\}^2} |x\rangle \end{aligned}$$

- $k = n$

$$\boxed{H^{\otimes n}|0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle}$$

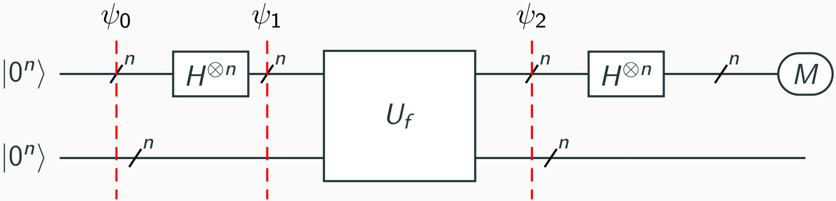



- Initial state:

$$|\psi_0\rangle = |0^n\rangle |0^n\rangle$$

- After the $H-$transforms, we have a state that is in a **superposition of all possible inputs**:

$$|\psi_1\rangle = (H^{\otimes n} \otimes I) |0^n\rangle |0^n\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0^n\rangle$$

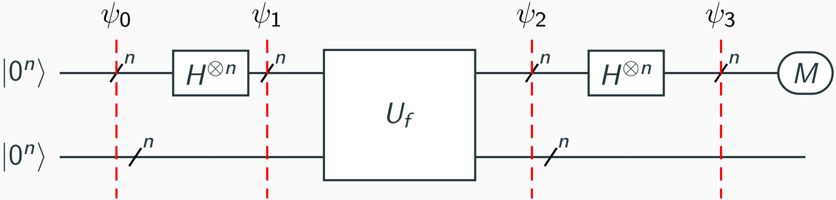



- The state after the $U_f$ transformation gives evaluation of $f$ on **all** the possibilities.

$$|\psi_2\rangle = U_f \left( \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |0^n\rangle \right) = \left( \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle \right)$$

- Recall, $U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$

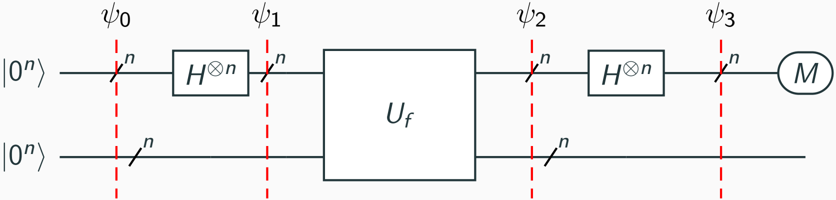
## Step-3: $\psi_3$ — Circuit Slicing




- After final $H-$transforms, we get:

$$|\psi_3\rangle = (H^{\otimes n} \otimes I) \left( \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \, |f(x)\rangle \right)$$

## Step-3: $\psi_3$ — Circuit Slicing



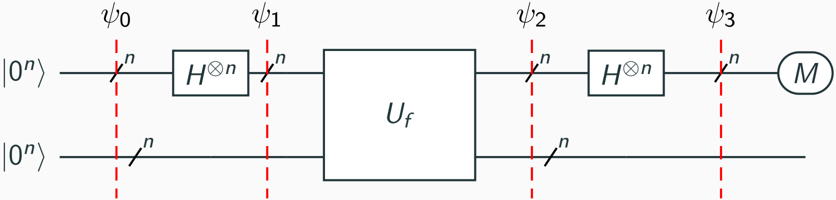

- After final $H-$transforms, we get:

$$|\psi_3\rangle = (H^{\otimes n} \otimes I)\left(\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle\, |f(x)\rangle\right)$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} \left(\frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}\, |y\rangle\right) |f(x)\rangle$$

Recall $H^{\oplus n}\,|x\rangle$

## Step-3: $\psi_3$ — Circuit Slicing




- After final $H-$transforms, we get:

$$
\begin{aligned}
|\psi_3\rangle &= (H^{\otimes n} \otimes I) \left( \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle \, |f(x)\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} \left( \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} \, |y\rangle \right) |f(x)\rangle \\
&= \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} \, |y\rangle \, |f(x)\rangle
\end{aligned}
$$

Recall $H^{\oplus n}|x\rangle$

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle |f(x)\rangle$$

**Note**

For each input $x$ and for each $y$, due to the property of $f$ it is assured that:

$$|y\rangle |f(x)\rangle = |y\rangle |f(x \oplus s)\rangle$$

- The coefficient for this ket is then:

$$\frac{(-1)^{x \cdot y} + (-1)^{(x \oplus s) \cdot y}}{2}$$

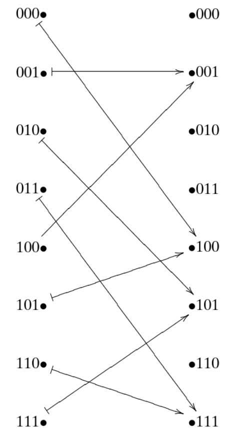
$$\frac{(-1)^{x\cdot y}+(-1)^{\boxed{(x\oplus s)\cdot y}}}{2}=\frac{(-1)^{x\cdot y}+(-1)^{\boxed{(x\cdot y)\oplus(s\cdot y)}}}{2}$$

$$=\frac{(-1)^{x\cdot y}+(-1)^{(x\cdot y)}(-1)^{(s\cdot y)}}{2}=\begin{cases}0 & \text{if } (s\cdot y)=1\\ \pm 1 & \text{if } (s\cdot y)=0\end{cases}$$

### Implication

- Measurement always results in some string $y$ that satisfies $(s\cdot y)=0 \leftarrow$ Recall orthogonal vectors.
- Distribution uniform over all of the strings that satisfy this constraint.
- Is this enough to determine $s$? Yes![1]

[1] With some classical post-processing




- $|\psi_0\rangle = |000\rangle\,|000\rangle$
- $|\psi_1\rangle = \frac{1}{\sqrt{8}} \sum_{x \in \{0,1\}^3} |x\rangle\,|000\rangle$
- $$|\psi_2\rangle = \frac{1}{\sqrt{8}} \sum_{x \in \{0,1\}^3} |x\rangle\,|f(x)\rangle$$
$$= \frac{1}{\sqrt{8}} \begin{pmatrix} |000\rangle\,|100\rangle + |001\rangle\,|001\rangle + \\ |010\rangle\,|101\rangle + |011\rangle\,|111\rangle + \\ |100\rangle\,|001\rangle + |101\rangle\,|100\rangle + \\ |110\rangle\,|111\rangle + |111\rangle\,|101\rangle \end{pmatrix}$$
- $|\psi_3\rangle = \frac{\sum_{x \in \{0,1\}^3} \sum_{y \in \{0,1\}^3} (-1)^{(x \cdot y)} |y\rangle |f(x)\rangle}{8}$

$$
\begin{aligned}
|\varphi_3\rangle = \frac{1}{8}(&(+1)|000\rangle \otimes |f(000)\rangle + (+1)|000\rangle \otimes |f(001)\rangle + (+1)|000\rangle \otimes |f(010)\rangle + (+1)|000\rangle \otimes |f(011)\rangle \\
&+ (+1)|000\rangle \otimes |f(100)\rangle + (+1)|000\rangle \otimes |f(101)\rangle + (+1)|000\rangle \otimes |f(110)\rangle + (+1)|000\rangle \otimes |f(111)\rangle \\
&+ (+1)|001\rangle \otimes |f(000)\rangle + (-1)|001\rangle \otimes |f(001)\rangle + (+1)|001\rangle \otimes |f(010)\rangle + (-1)|001\rangle \otimes |f(011)\rangle \\
&+ (+1)|001\rangle \otimes |f(100)\rangle + (-1)|001\rangle \otimes |f(101)\rangle + (+1)|001\rangle \otimes |f(110)\rangle + (-1)|001\rangle \otimes |f(111)\rangle \\
&+ (+1)|010\rangle \otimes |f(000)\rangle + (+1)|010\rangle \otimes |f(001)\rangle + (-1)|010\rangle \otimes |f(010)\rangle + (-1)|010\rangle \otimes |f(011)\rangle \\
&+ (+1)|010\rangle \otimes |f(100)\rangle + (+1)|010\rangle \otimes |f(101)\rangle + (-1)|010\rangle \otimes |f(110)\rangle + (-1)|010\rangle \otimes |f(111)\rangle \\
&+ (+1)|011\rangle \otimes |f(000)\rangle + (-1)|011\rangle \otimes |f(001)\rangle + (-1)|011\rangle \otimes |f(010)\rangle + (+1)|011\rangle \otimes |f(011)\rangle \\
&+ (+1)|011\rangle \otimes |f(100)\rangle + (-1)|011\rangle \otimes |f(101)\rangle + (-1)|011\rangle \otimes |f(110)\rangle + (+1)|011\rangle \otimes |f(111)\rangle \\
&+ (+1)|100\rangle \otimes |f(000)\rangle + (+1)|100\rangle \otimes |f(001)\rangle + (+1)|100\rangle \otimes |f(010)\rangle + (+1)|100\rangle \otimes |f(011)\rangle \\
&+ (-1)|100\rangle \otimes |f(100)\rangle + (-1)|100\rangle \otimes |f(101)\rangle + (-1)|100\rangle \otimes |f(110)\rangle + (-1)|100\rangle \otimes |f(111)\rangle \\
&+ (+1)|101\rangle \otimes |f(000)\rangle + (-1)|101\rangle \otimes |f(001)\rangle + (+1)|101\rangle \otimes |f(010)\rangle + (-1)|101\rangle \otimes |f(011)\rangle \\
&+ (-1)|101\rangle \otimes |f(100)\rangle + (+1)|101\rangle \otimes |f(101)\rangle + (-1)|101\rangle \otimes |f(110)\rangle + (+1)|101\rangle \otimes |f(111)\rangle \\
&+ (+1)|110\rangle \otimes |f(000)\rangle + (+1)|110\rangle \otimes |f(001)\rangle + (-1)|110\rangle \otimes |f(010)\rangle + (-1)|110\rangle \otimes |f(011)\rangle \\
&+ (-1)|110\rangle \otimes |f(100)\rangle + (-1)|110\rangle \otimes |f(101)\rangle + (+1)|110\rangle \otimes |f(110)\rangle + (+1)|110\rangle \otimes |f(111)\rangle \\
&+ (+1)|111\rangle \otimes |f(000)\rangle + (-1)|111\rangle \otimes |f(001)\rangle + (-1)|111\rangle \otimes |f(010)\rangle + (+1)|111\rangle \otimes |f(011)\rangle \\
&+ (-1)|111\rangle \otimes |f(100)\rangle + (+1)|111\rangle \otimes |f(101)\rangle + (+1)|111\rangle \otimes |f(110)\rangle + (-1)|111\rangle \otimes |f(111)\rangle).
\end{aligned}
$$

# Evaluating $f$ in $|\psi_3\rangle$ Expansion

$$
\begin{aligned}
|\varphi_3\rangle = \frac{1}{8}(&(+1)|000\rangle \otimes |100\rangle + (+1)|000\rangle \otimes |001\rangle + (+1)|000\rangle \otimes |101\rangle + (+1)|000\rangle \otimes |111\rangle \\
&+ (+1)|000\rangle \otimes |001\rangle + (+1)|000\rangle \otimes |100\rangle + (+1)|000\rangle \otimes |111\rangle + (+1)|000\rangle \otimes |101\rangle \\
&+ (+1)|001\rangle \otimes |100\rangle + (-1)|001\rangle \otimes |001\rangle + (+1)|001\rangle \otimes |101\rangle + (-1)|001\rangle \otimes |111\rangle \\
&+ (+1)|001\rangle \otimes |001\rangle + (-1)|001\rangle \otimes |100\rangle + (+1)|001\rangle \otimes |111\rangle + (-1)|001\rangle \otimes |101\rangle \\
&+ (+1)|010\rangle \otimes |100\rangle + (+1)|010\rangle \otimes |001\rangle + (-1)|010\rangle \otimes |101\rangle + (-1)|010\rangle \otimes |111\rangle \\
&+ (+1)|010\rangle \otimes |001\rangle + (+1)|010\rangle \otimes |100\rangle + (-1)|010\rangle \otimes |111\rangle + (-1)|010\rangle \otimes |101\rangle \\
&+ (+1)|011\rangle \otimes |100\rangle + (-1)|011\rangle \otimes |001\rangle + (-1)|011\rangle \otimes |101\rangle + (+1)|011\rangle \otimes |111\rangle \\
&+ (+1)|011\rangle \otimes |001\rangle + (-1)|011\rangle \otimes |100\rangle + (-1)|011\rangle \otimes |111\rangle + (+1)|011\rangle \otimes |101\rangle \\
&+ (+1)|100\rangle \otimes |100\rangle + (+1)|100\rangle \otimes |001\rangle + (+1)|100\rangle \otimes |101\rangle + (+1)|100\rangle \otimes |111\rangle \\
&+ (-1)|100\rangle \otimes |001\rangle + (-1)|100\rangle \otimes |100\rangle + (-1)|100\rangle \otimes |111\rangle + (-1)|100\rangle \otimes |101\rangle \\
&+ (+1)|101\rangle \otimes |100\rangle + (-1)|101\rangle \otimes |001\rangle + (+1)|101\rangle \otimes |101\rangle + (-1)|101\rangle \otimes |111\rangle \\
&+ (-1)|101\rangle \otimes |001\rangle + (+1)|101\rangle \otimes |100\rangle + (-1)|101\rangle \otimes |111\rangle + (+1)|101\rangle \otimes |101\rangle \\
&+ (+1)|110\rangle \otimes |100\rangle + (+1)|110\rangle \otimes |001\rangle + (-1)|110\rangle \otimes |101\rangle + (-1)|110\rangle \otimes |111\rangle \\
&+ (-1)|110\rangle \otimes |001\rangle + (-1)|110\rangle \otimes |100\rangle + (+1)|110\rangle \otimes |111\rangle + (+1)|110\rangle \otimes |101\rangle \\
&+ (+1)|111\rangle \otimes |100\rangle + (-1)|111\rangle \otimes |001\rangle + (-1)|111\rangle \otimes |101\rangle + (+1)|111\rangle \otimes |111\rangle \\
&+ (-1)|111\rangle \otimes |001\rangle + (+1)|111\rangle \otimes |100\rangle + (+1)|111\rangle \otimes |111\rangle + (-1)|111\rangle \otimes |101\rangle).
\end{aligned}
$$

# Simplifying $|\psi_3\rangle$

$$
\begin{aligned}
|\varphi_3\rangle = \frac{1}{8}(&(+2)|000\rangle \otimes |100\rangle + (+2)|000\rangle \otimes |001\rangle + (+2)|000\rangle \otimes |101\rangle + (+2)|000\rangle \otimes |111\rangle \\
&+ (+2)|010\rangle \otimes |100\rangle + (+2)|010\rangle \otimes |001\rangle + (-2)|010\rangle \otimes |101\rangle + (-2)|010\rangle \otimes |111\rangle \\
&+ (+2)|101\rangle \otimes |100\rangle + (-2)|101\rangle \otimes |001\rangle + (+2)|101\rangle \otimes |101\rangle + (-2)|101\rangle \otimes |111\rangle \\
&+ (+2)|111\rangle \otimes |100\rangle + (-2)|111\rangle \otimes |001\rangle + (-2)|111\rangle \otimes |101\rangle + (+2)|111\rangle \otimes |111\rangle)
\end{aligned}
$$

or

$$
\begin{aligned}
|\varphi_3\rangle = \frac{1}{8}(&(+2)|000\rangle \otimes (|100\rangle + |001\rangle + |101\rangle + |111\rangle) \\
&+ (+2)|010\rangle \otimes (|100\rangle + |001\rangle - |101\rangle - |111\rangle) \\
&+ (+2)|101\rangle \otimes (|100\rangle - |001\rangle + |101\rangle - |111\rangle) \\
&+ (+2)|111\rangle \otimes (|100\rangle - |001\rangle - |101\rangle + |111\rangle)).
\end{aligned}
$$

- Measuring the top output gives with **equal probability**:

$$000, 010, 101, \text{ or } 111$$

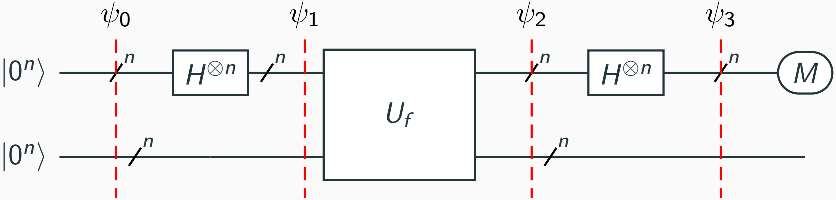
- For all these, the inner product with the missing $s$ is 0.

## Classical Post-Processing

- Measurement leads to the following system of linear equations:

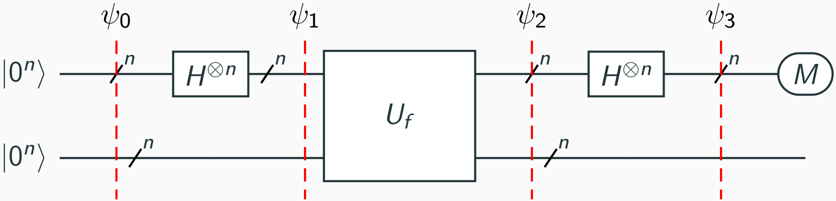
$$
\begin{aligned}
&(000 \cdot s_1 s_2 s_3 = 0) && \\
&(010 \cdot s_1 s_2 s_3 = 0) \implies && s_2 = 0 \\
&(101 \cdot s_1 s_2 s_3 = 0) \implies && s_1 \oplus s_3 = 0 \\
&(111 \cdot s_1 s_2 s_3 = 0) \implies && s_1 \oplus s_2 \oplus s_3 = 0
\end{aligned}
$$

- Since $s \neq 000$, the above system gives $s = 101$




$$(H^{\otimes n} \otimes I)U_f(H^{\otimes n} \otimes I)\,|0^n\rangle\,|0^n\rangle$$

- After running Simon's algorithm several times, we will get $n$ different $y_i$ such that $y_i \cdot c = 0$.
- This is fed into an classical linear equation solver
- Note the solver works over $GF(2)$
- The solution from the solver gives the period $s$ of function $f$




$$(H^{\otimes n} \otimes I)U_f(H^{\otimes n} \otimes I)\,|0^n\rangle\,|0^n\rangle$$

- For a given periodic $f$, we can find the period $s$ in $n$ function evaluations.
- Compare this to $2^{n-1} + 1$ needed with the classical algorithm
- *Simon's algorithm plays central roles in many cryptanalytic results*