# Brief announcement: Global certification via perfect hashing

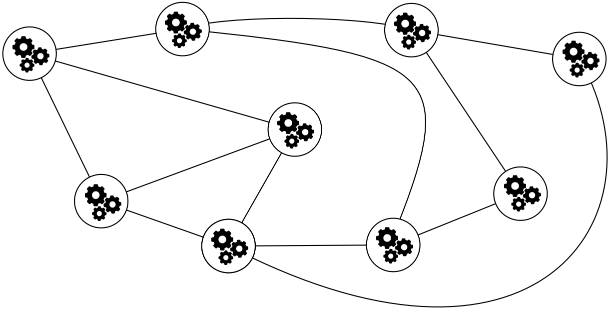
Nicolas Bousquet, Laurent Feuilloley, Sébastien Zeitoun

June 20, 2024

# Distributed certification

# Distributed certification

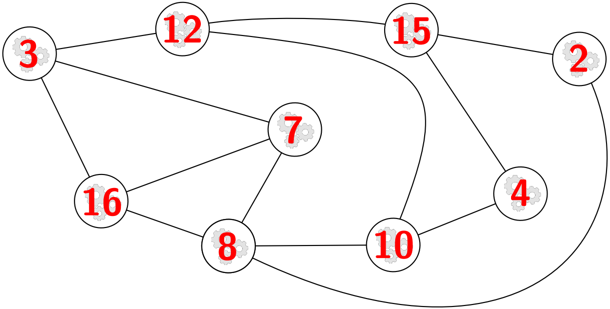
Graph $G$ on $n$ vertices



# Distributed certification

Graph $G$ on $n$ vertices

Unique identifiers in $\{1, \ldots, M(n)\}$

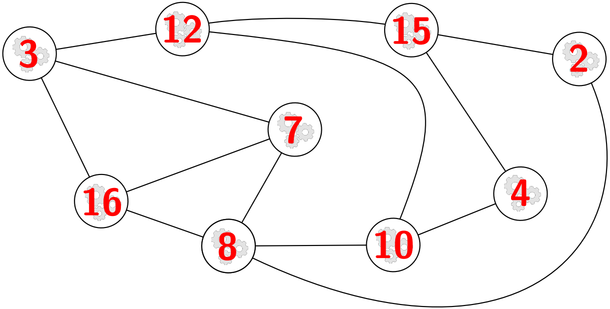


# Distributed certification

Graph $G$ on $n$ vertices

Unique identifiers in $\{1, \ldots, M(n)\}$

Goal : verify locally a graph property $\mathcal{P}$, thanks to certificates $\begin{cases} \to \text{local} \\ \to \text{global} \end{cases}$

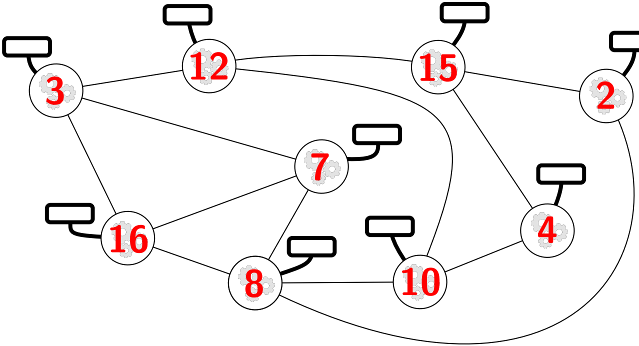


# Distributed certification

Graph $G$ on $n$ vertices

Unique identifiers in $\{1, \dots, M(n)\}$

Goal : verify locally a graph property $\mathcal{P}$, thanks to certificates → **local** / global

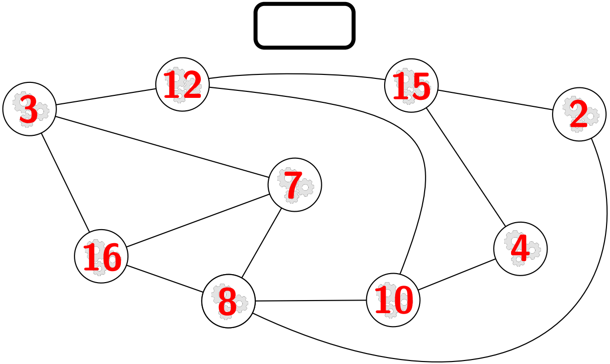


# Distributed certification

Graph $G$ on $n$ vertices

Unique identifiers in $\{1, \ldots, M(n)\}$

Goal : verify locally a graph property $\mathcal{P}$, thanks to certificates → local / **global**

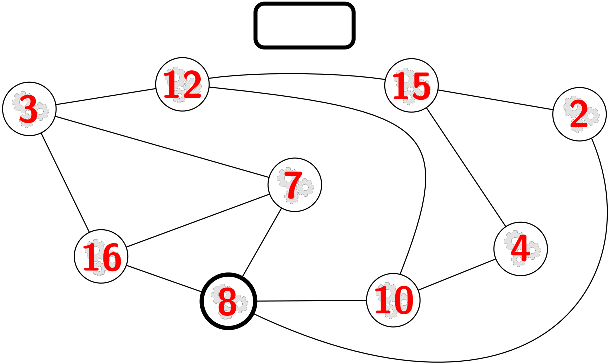


# Distributed certification

Graph $G$ on $n$ vertices

Unique identifiers in $\{1, \ldots, M(n)\}$

Goal : verify locally a graph property $\mathcal{P}$, thanks to certificates → local → **global**

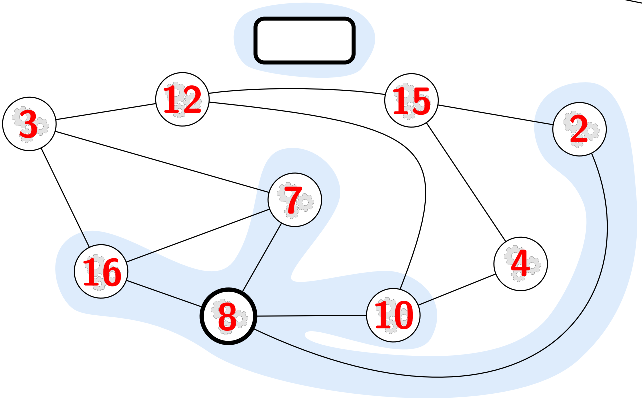


# Distributed certification

Graph $G$ on $n$ vertices

Unique identifiers in $\{1, \ldots, M(n)\}$

Goal : verify locally a graph property $\mathcal{P}$, thanks to certificates → local / **global**

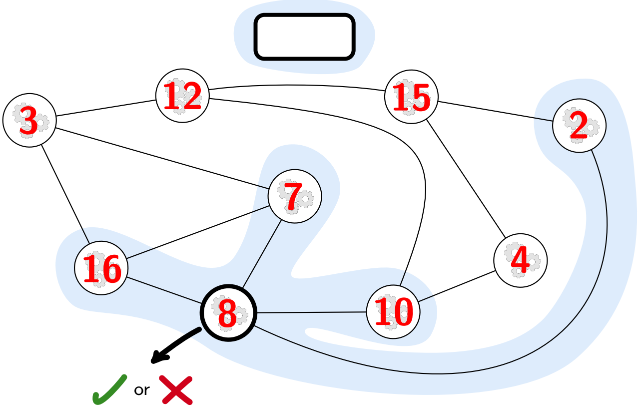


# Distributed certification

Graph $G$ on $n$ vertices

Unique identifiers in $\{1, \ldots, M(n)\}$

Goal : verify locally a graph property $\mathcal{P}$, thanks to certificates $\rightarrow$ local / **global**

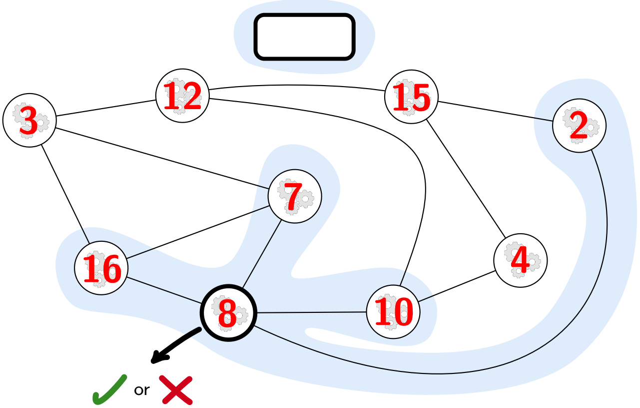


# Distributed certification

Graph $G$ on $n$ vertices

Unique identifiers in $\{1, \ldots, M(n)\}$

Goal : verify locally a graph property $\mathcal{P}$, thanks to certificates $\rightarrow$ local / **global**



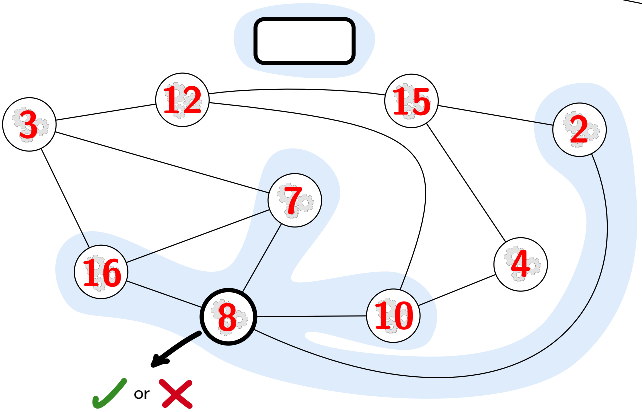

Graph (globally) accepted $\iff$ all the vertices accept (consensus)

# Distributed certification

Graph $G$ on $n$ vertices

Unique identifiers in $\{1, \ldots, M(n)\}$

Goal : verify locally a graph property $\mathcal{P}$, thanks to certificates → local / **global**



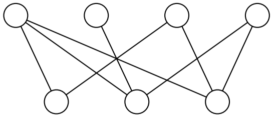

Graph (globally) accepted $\iff$ all the vertices accept (consensus)

$G$ satisfies $\mathcal{P} \iff$ there exists a certificate such that $G$ is accepted

# Certification of bipartiteness

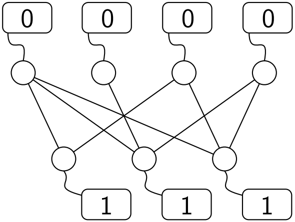
# Certification of bipartiteness

Local certification : 1 bit is sufficient



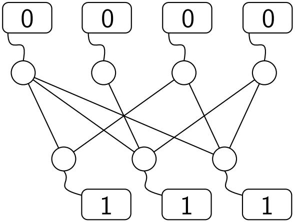
# Certification of bipartiteness

Local certification : 1 bit is sufficient

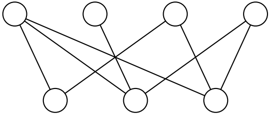


# Certification of bipartiteness

Local certification : 1 bit is sufficient

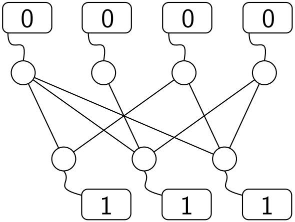



Global certification : what is the optimal size of the certificate ?

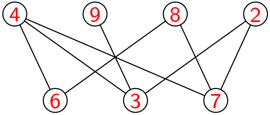


# Certification of bipartiteness

Local certification : 1 bit is sufficient

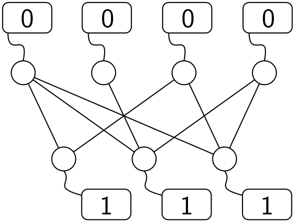



Global certification : what is the optimal size of the certificate ?

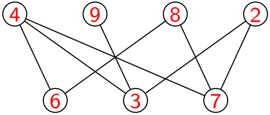


# Certification of bipartiteness

Local certification : 1 bit is sufficient



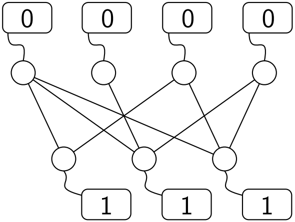

Global certification : what is the optimal size of the certificate ?



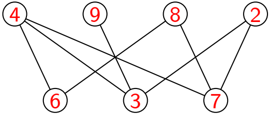

$2 \longrightarrow 0$
$3 \longrightarrow 1$
$4 \longrightarrow 0$
$6 \longrightarrow 1$
$7 \longrightarrow 1$
$8 \longrightarrow 0$
$9 \longrightarrow 0$

# Certification of bipartiteness

Local certification : 1 bit is sufficient




Global certification : what is the optimal size of the certificate ?

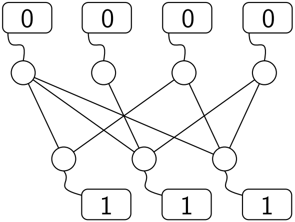



$2 \longrightarrow 0$
$3 \longrightarrow 1$
$4 \longrightarrow 0$
$6 \longrightarrow 1$
$7 \longrightarrow 1$
$8 \longrightarrow 0$
$9 \longrightarrow 0$

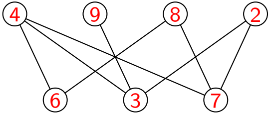
This certification : size $O(n \log M(n))$. Is it optimal ?

# Certification of bipartiteness

Local certification : 1 bit is sufficient




Global certification : what is the optimal size of the certificate ?



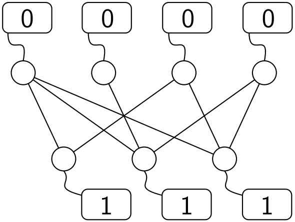

$2 \longrightarrow 0$
$3 \longrightarrow 1$
$4 \longrightarrow 0$
$6 \longrightarrow 1$
$7 \longrightarrow 1$
$8 \longrightarrow 0$
$9 \longrightarrow 0$

This certification : size $O(n \log M(n))$. Is it optimal ?

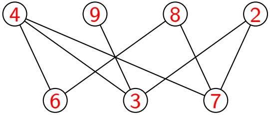
Known lower bound: $\Omega(n + \log \log M(n))$

# Certification of bipartiteness

Local certification : 1 bit is sufficient




Global certification : what is the optimal size of the certificate ?




$2 \longrightarrow 0$
$3 \longrightarrow 1$
$4 \longrightarrow 0$
$6 \longrightarrow 1$
$7 \longrightarrow 1$
$8 \longrightarrow 0$
$9 \longrightarrow 0$

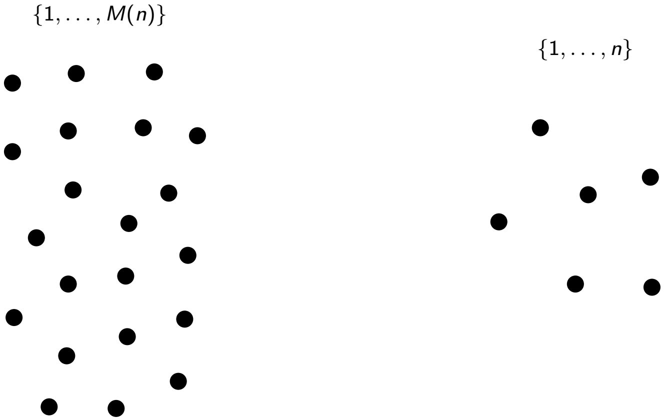
This certification : size $O(n \log M(n))$. Is it optimal ? $\longrightarrow$ **No.**

Known lower bound: $\Omega(n + \log\log M(n))$

What we proved: $O(n + \log\log M(n))$

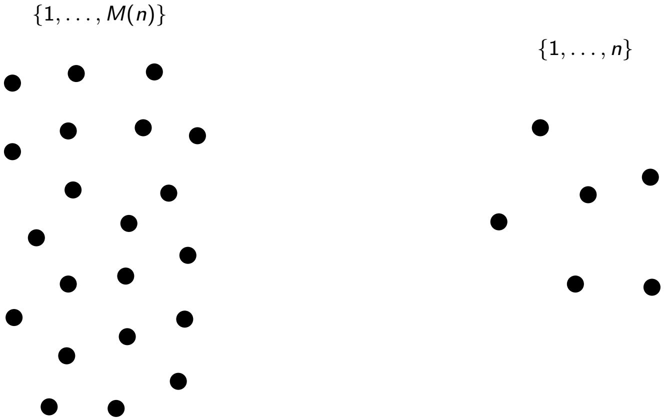
# Hash functions

# Hash functions




$H =$ family of functions $\{1, \dots, M(n)\} \to \{1, \dots, n\}$

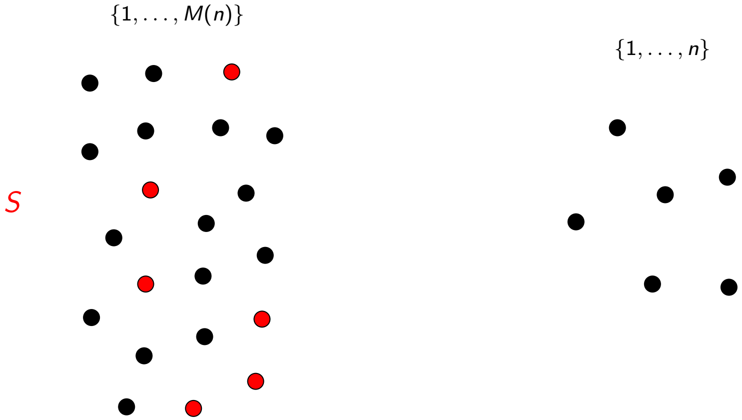
# Hash functions




$H =$ family of functions $\{1, \ldots, M(n)\} \to \{1, \ldots, n\}$

$H$ is a *perfect hash family* if: $\forall S \subseteq \{1, \ldots, M(n)\}$, $|S| = n$, $\exists h \in H$ injective on $S$

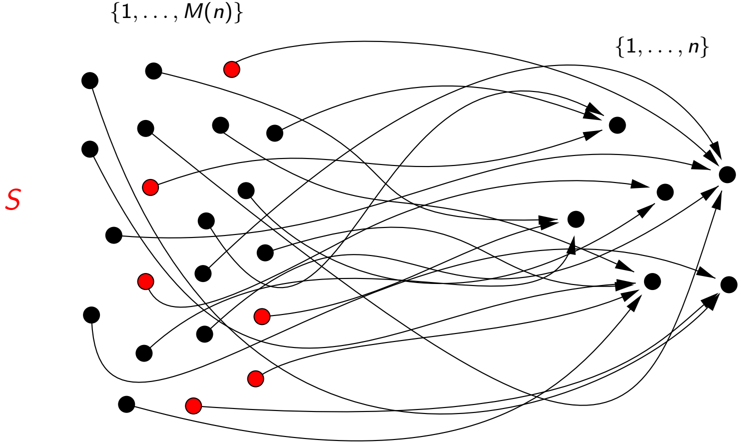
# Hash functions




$H =$ family of functions $\{1, \ldots, M(n)\} \to \{1, \ldots, n\}$

$H$ is a *perfect hash family* if: $\forall S \subseteq \{1, \ldots, M(n)\}$, $|S| = n$, $\exists h \in H$ injective on $S$

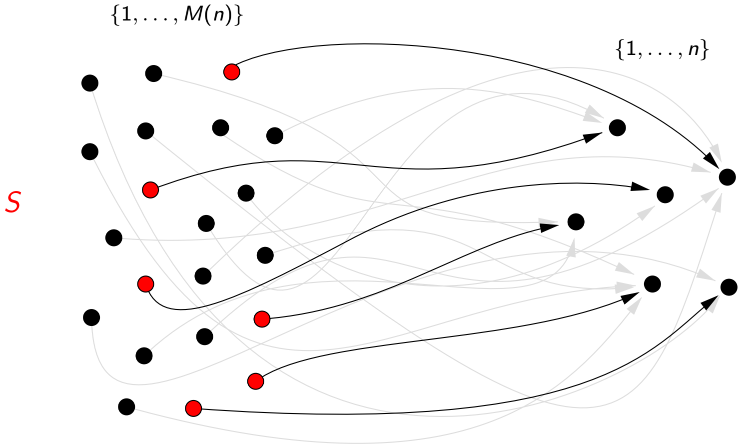
# Hash functions




$H$ = family of functions $\{1, \ldots, M(n)\} \to \{1, \ldots, n\}$

$H$ is a *perfect hash family* if: $\forall S \subseteq \{1, \ldots, M(n)\}$, $|S| = n$, $\exists h \in H$ injective on $S$

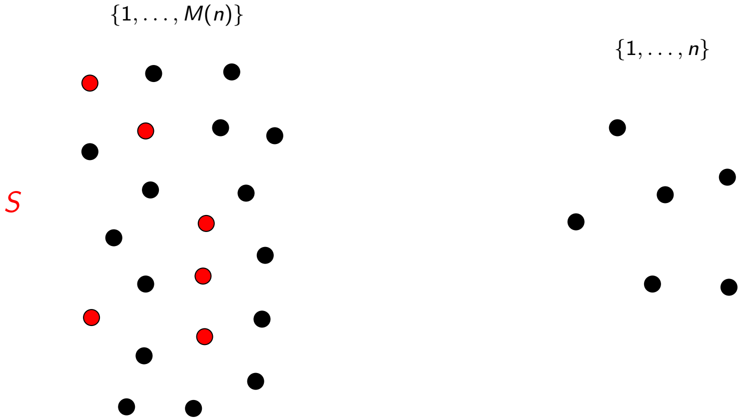
# Hash functions




$H$ = family of functions $\{1, \ldots, M(n)\} \to \{1, \ldots, n\}$

$H$ is a *perfect hash family* if: $\forall S \subseteq \{1, \ldots, M(n)\}$, $|S| = n$, $\exists h \in H$ injective on $S$

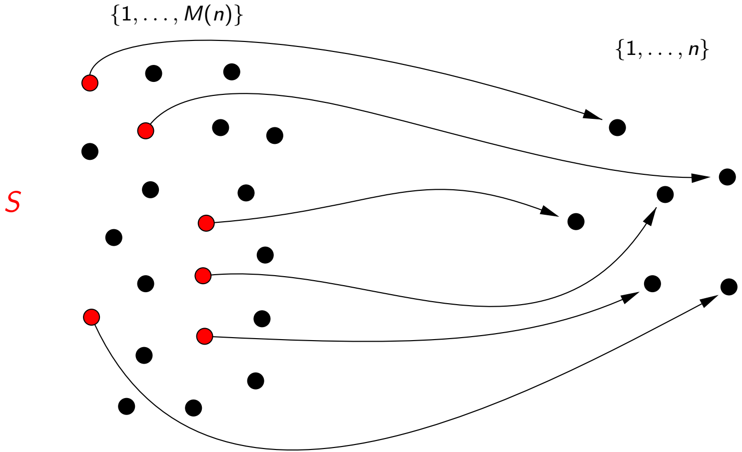
# Hash functions




$H$ = family of functions $\{1, \ldots, M(n)\} \to \{1, \ldots, n\}$

$H$ is a *perfect hash family* if: $\forall S \subseteq \{1, \ldots, M(n)\}$, $|S| = n$, $\exists h \in H$ injective on $S$

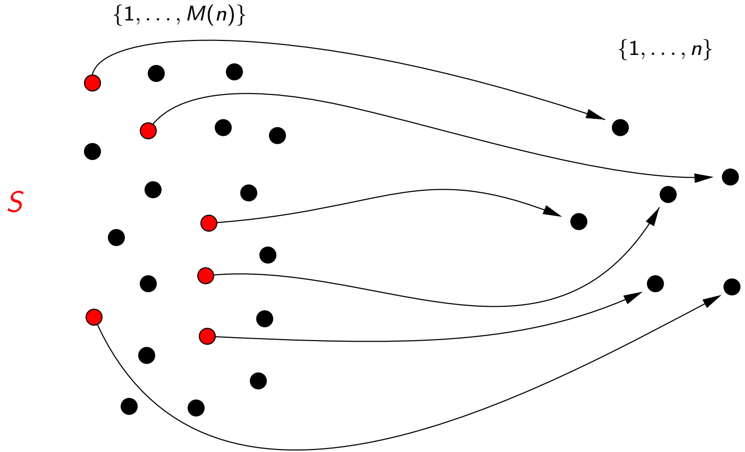
# Hash functions




$H$ = family of functions $\{1, \ldots, M(n)\} \to \{1, \ldots, n\}$

$H$ is a *perfect hash family* if: $\forall S \subseteq \{1, \ldots, M(n)\}$, $|S| = n$, $\exists h \in H$ injective on $S$

# Hash functions




$H$ = family of functions $\{1, \ldots, M(n)\} \to \{1, \ldots, n\}$

$H$ is a *perfect hash family* if: $\forall S \subseteq \{1, \ldots, M(n)\}$, $|S| = n$, $\exists h \in H$ injective on $S$

**Theorem (Mehlhorn)**

There exists a perfect hash family of size $\lceil n \log M(n) e^n \rceil$.

# Proof of the upper bound

**Theorem (Mehlhorn)**

There exists a perfect hash family of size $\lceil n \log M(n) e^n \rceil$.

# Proof of the upper bound

**Theorem (Mehlhorn)**

There exists a perfect hash family of size $\lceil n \log M(n) e^n \rceil$.

Every $h \in H$ can be represented using $O(n + \log\log M(n))$ bits.

## Proof of the upper bound

**Theorem (Mehlhorn)**

There exists a perfect hash family of size $\lceil n \log M(n) e^n \rceil$.

Every $h \in H$ can be represented using $O(n + \log\log M(n))$ bits.

Certificate:

- $h \in H$ injective on $\{Id(u) | u \in V(G)\}$

## Proof of the upper bound

**Theorem (Mehlhorn)**

There exists a perfect hash family of size $\lceil n \log M(n) e^n \rceil$.

Every $h \in H$ can be represented using $O(n + \log\log M(n))$ bits.

Certificate:

- $h \in H$ injective on $\{Id(u) | u \in V(G)\}$
- a list $L$ of $n$ bits, where $L[i]$ is the color of the vertex $u$ such that $h(Id(u)) = i$

## Proof of the upper bound

**Theorem (Mehlhorn)**

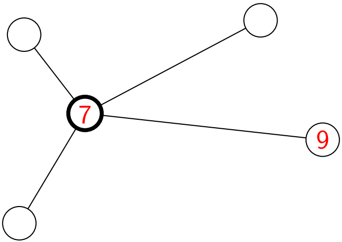
There exists a perfect hash family of size $\lceil n \log M(n) e^n \rceil$.

Every $h \in H$ can be represented using $O(n + \log\log M(n))$ bits.

Certificate:

- $h \in H$ injective on $\{Id(u) | u \in V(G)\}$
- a list $L$ of $n$ bits, where $L[i]$ is the color of the vertex $u$ such that $h(Id(u)) = i$

Verification:



## Proof of the upper bound

**Theorem (Mehlhorn)**

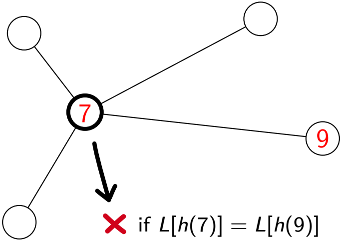
There exists a perfect hash family of size $\lceil n \log M(n) e^n \rceil$.

Every $h \in H$ can be represented using $O(n + \log\log M(n))$ bits.

Certificate:

- $h \in H$ injective on $\{Id(u) | u \in V(G)\}$
- a list $L$ of $n$ bits, where $L[i]$ is the color of the vertex $u$ such that $h(Id(u)) = i$

Verification:



# Proof of the upper bound

**Theorem (Mehlhorn)**

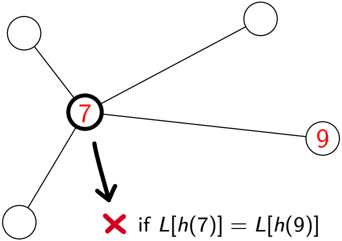
There exists a perfect hash family of size $\lceil n \log M(n) e^n \rceil$.

Every $h \in H$ can be represented using $O(n + \log\log M(n))$ bits.

Certificate:

- $h \in H$ injective on $\{Id(u) | u \in V(G)\}$
- a list $L$ of $n$ bits, where $L[i]$ is the color of the vertex $u$ such that $h(Id(u)) = i$

Verification:




✗ if $L[h(7)] = L[h(9)]$

✓ if it did not reject for any neighbor

## Proof of the upper bound

**Theorem (Mehlhorn)**

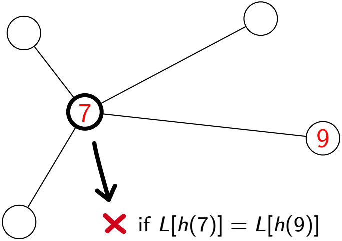
There exists a perfect hash family of size $\lceil n \log M(n) e^n \rceil$.

Every $h \in H$ can be represented using $O(n + \log\log M(n))$ bits.

Certificate:

- $h \in H$ injective on $\{Id(u) | u \in V(G)\}$
- a list $L$ of $n$ bits, where $L[i]$ is the color of the vertex $u$ such that $h(Id(u)) = i$

Verification:




✗ if $L[h(7)] = L[h(9)]$

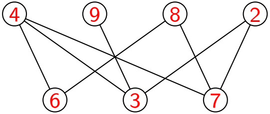
✓ if it did not reject for any neighbor

It is not necessary to check that $h$ is injective !

# Conclusion

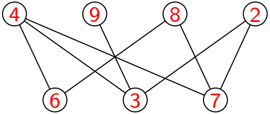
# Conclusion

Before:



# Conclusion

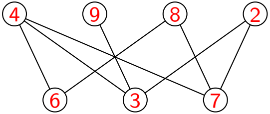
Before:




$2 \longrightarrow 0$
$3 \longrightarrow 1$
$4 \longrightarrow 0$
$6 \longrightarrow 1$
$7 \longrightarrow 1$
$8 \longrightarrow 0$
$9 \longrightarrow 0$

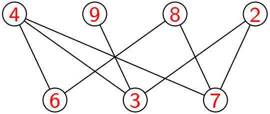
# Conclusion

Before:



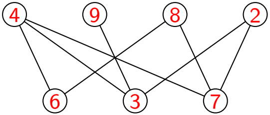

$$\begin{array}{l} 2 \longrightarrow 0 \\ 3 \longrightarrow 1 \\ 4 \longrightarrow 0 \\ 6 \longrightarrow 1 \\ 7 \longrightarrow 1 \\ 8 \longrightarrow 0 \\ 9 \longrightarrow 0 \end{array}$$

Now:



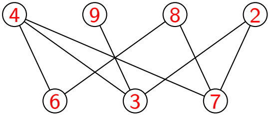
# Conclusion

Before:




$$\begin{array}{l} 2 \longrightarrow 0 \\ 3 \longrightarrow 1 \\ 4 \longrightarrow 0 \\ 6 \longrightarrow 1 \\ 7 \longrightarrow 1 \\ 8 \longrightarrow 0 \\ 9 \longrightarrow 0 \end{array}$$

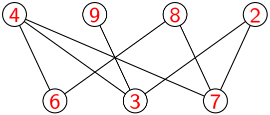
Now:




$$h : \begin{array}{l} 2 \longrightarrow L[4] \\ 3 \longrightarrow L[2] \\ 4 \longrightarrow L[1] \\ 6 \longrightarrow L[5] \\ 7 \longrightarrow L[6] \\ 8 \longrightarrow L[7] \\ 9 \longrightarrow L[3] \end{array} \quad , \quad L = [0, 1, 0, 0, 1, 1, 0]$$

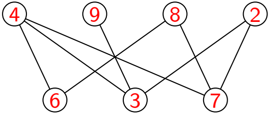
# Conclusion

Before:




$$\begin{aligned} 2 &\longrightarrow 0 \\ 3 &\longrightarrow 1 \\ 4 &\longrightarrow 0 \\ 6 &\longrightarrow 1 \\ 7 &\longrightarrow 1 \\ 8 &\longrightarrow 0 \\ 9 &\longrightarrow 0 \end{aligned}$$

Now:



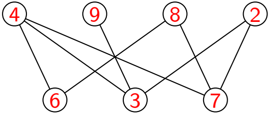

$$h : \begin{array}{l} 2 \longrightarrow L[4] \\ 3 \longrightarrow L[2] \\ 4 \longrightarrow L[1] \\ 6 \longrightarrow L[5] \\ 7 \longrightarrow L[6] \\ 8 \longrightarrow L[7] \\ 9 \longrightarrow L[3] \end{array} \quad , \quad L = [0, 1, 0, 0, 1, 1, 0]$$

**Theorem (Bousquet, Feuilloley, Z.)**

In global certification, $O(n \log k + \log \log M(n))$ bits are sufficient to certify that a graph is $k$-colorable.

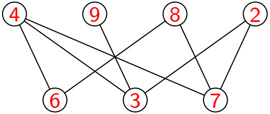
# Conclusion

Before:




$$\begin{array}{l} 2 \longrightarrow 0 \\ 3 \longrightarrow 1 \\ 4 \longrightarrow 0 \\ 6 \longrightarrow 1 \\ 7 \longrightarrow 1 \\ 8 \longrightarrow 0 \\ 9 \longrightarrow 0 \end{array}$$

Now:




$$h : \begin{array}{l} 2 \longrightarrow L[4] \\ 3 \longrightarrow L[2] \\ 4 \longrightarrow L[1] \\ 6 \longrightarrow L[5] \\ 7 \longrightarrow L[6] \\ 8 \longrightarrow L[7] \\ 9 \longrightarrow L[3] \end{array} , \quad L = [0, 1, 0, 0, 1, 1, 0]$$

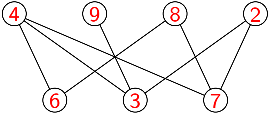
**Theorem (Bousquet, Feuilloley, Z.)**

In global certification, $O(n \log k + \log \log M(n))$ bits are sufficient to certify that a graph is $k$-colorable.

↪ this can be generalized to graph homomorphism

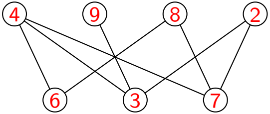
# Conclusion

Before:




$$\begin{array}{l} 2 \longrightarrow 0 \\ 3 \longrightarrow 1 \\ 4 \longrightarrow 0 \\ 6 \longrightarrow 1 \\ 7 \longrightarrow 1 \\ 8 \longrightarrow 0 \\ 9 \longrightarrow 0 \end{array}$$

Now:




$$h : \begin{array}{l} 2 \longrightarrow L[4] \\ 3 \longrightarrow L[2] \\ 4 \longrightarrow L[1] \\ 6 \longrightarrow L[5] \\ 7 \longrightarrow L[6] \\ 8 \longrightarrow L[7] \\ 9 \longrightarrow L[3] \end{array} \quad , \quad L = [0, 1, 0, 0, 1, 1, 0]$$

**Theorem (Bousquet, Feuilloley, Z.)**

In global certification, $O(n \log k + \log \log M(n))$ bits are sufficient to certify that a graph is $k$-colorable.

→ this can be generalized to graph homomorphism

Question: are there other problems for which this hashing technique can be used ?

Thanks for your attention !