Local certification of local properties : tight bounds, trade-offs and new parameters

Nicolas Bousquet, Laurent Feuilloley, Sébastien Zeitoun

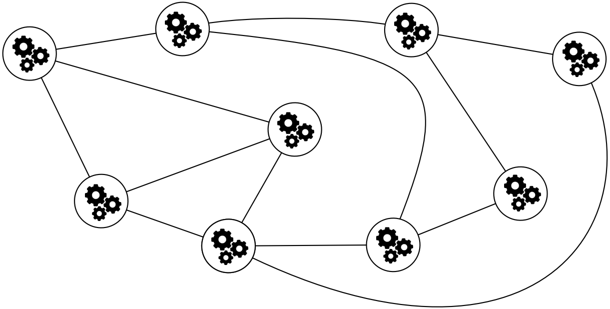
March 13, 2024

Local certification

Local certification

Context : distributed computing

Model : graph, $\begin{cases} \text{vertices} = \text{computation units} \\ \text{edges} = \text{communication channels} \end{cases}$

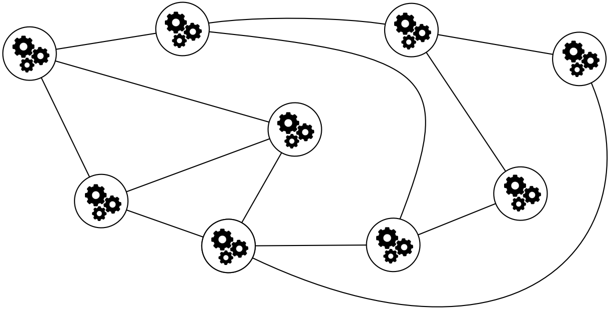


Local certification

Context : distributed computing

Model : graph, $\begin{cases} \text{vertices} = \text{computation units} \\ \text{edges} = \text{communication channels} \end{cases}$

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

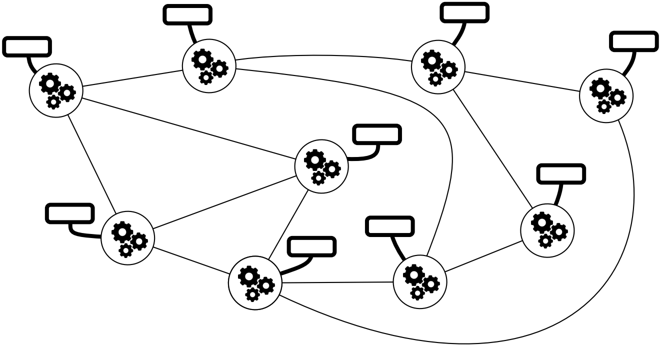


Local certification

Context : distributed computing

Model : graph, $\begin{cases} \text{vertices} = \text{computation units} \\ \text{edges} = \text{communication channels} \end{cases}$

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

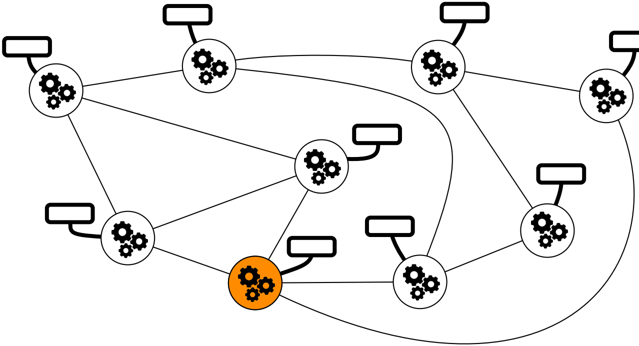


Local certification

Context : distributed computing

Model : graph, $\begin{cases} \text{vertices} = \text{computation units} \\ \text{edges} = \text{communication channels} \end{cases}$

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

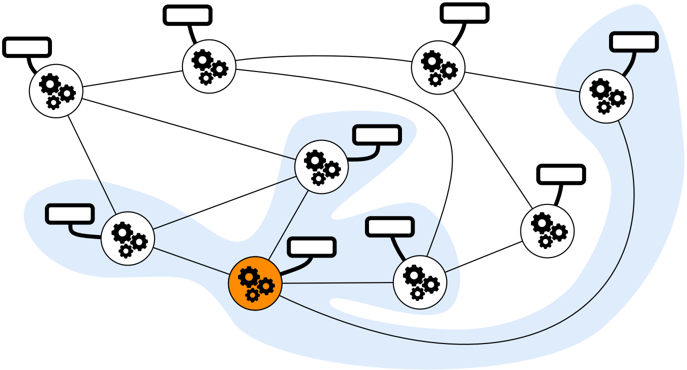


Local certification

Context : distributed computing

Model : graph, $\begin{cases} \text{vertices} = \text{computation units} \\ \text{edges} = \text{communication channels} \end{cases}$

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

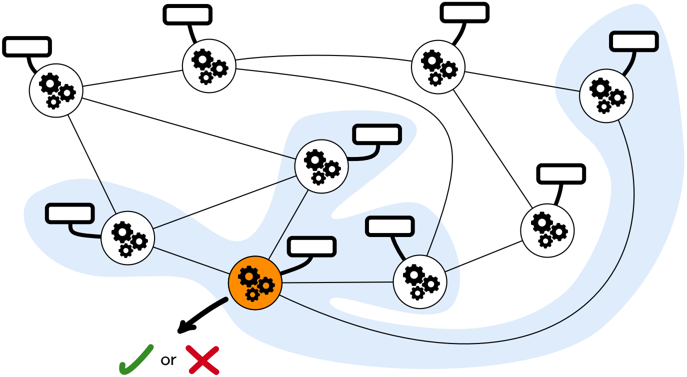


Local certification

Context : distributed computing

Model : graph, $\begin{cases} \text{vertices} = \text{computation units} \\ \text{edges} = \text{communication channels} \end{cases}$

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

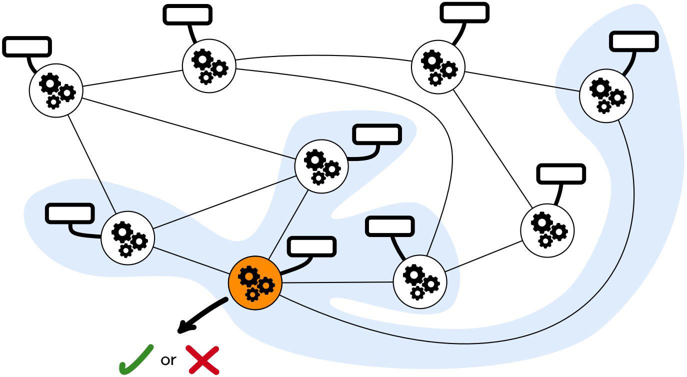


Local certification

Context : distributed computing

Model : graph, $\begin{cases} \text{vertices} = \text{computation units} \\ \text{edges} = \text{communication channels} \end{cases}$

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



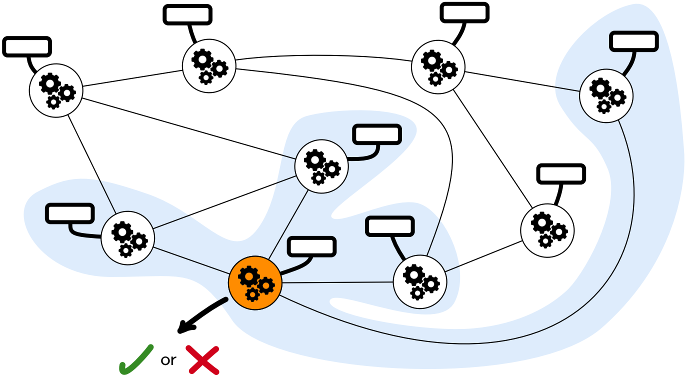
Graph (globally) accepted $\Longleftrightarrow$ all the vertices accept (consensus)

Local certification

Context : distributed computing

Model : graph, $\begin{cases} \text{vertices} = \text{computation units} \\ \text{edges} = \text{communication channels} \end{cases}$

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

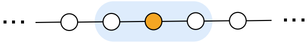


Graph (globally) accepted $\iff$ all the vertices accept (consensus)

G satisfies $\mathcal{P} \iff$ there exists an assignment of the certificates such that G is accepted

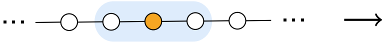
Example : how to certify that a graph is a path ?

Example : how to certify that a graph is a path ?



$\longrightarrow$ Path ? Cycle ?

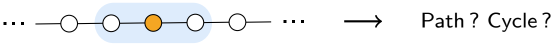
Example : how to certify that a graph is a path ?



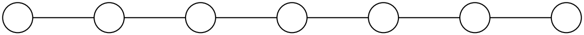
Path ? Cycle ?

Possible way to certify this : certificate = distance to a (fixed) extremity

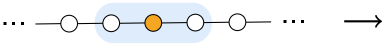
Example : how to certify that a graph is a path ?



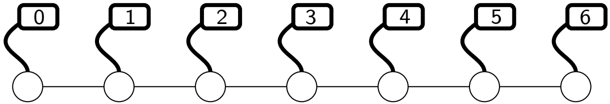
Possible way to certify this : certificate = distance to a (fixed) extremity



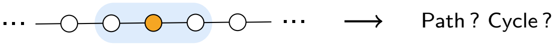
Example : how to certify that a graph is a path ?



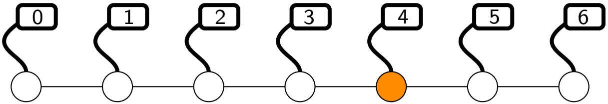
Possible way to certify this : certificate = distance to a (fixed) extremity



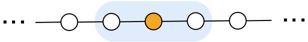
Example : how to certify that a graph is a path ?



Possible way to certify this : certificate = distance to a (fixed) extremity

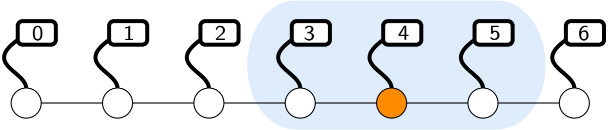


Example : how to certify that a graph is a path ?

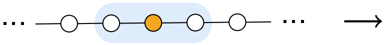


$\longrightarrow$ Path ? Cycle ?

Possible way to certify this : certificate = distance to a (fixed) extremity

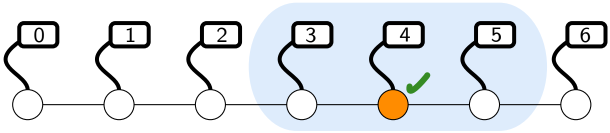


Example : how to certify that a graph is a path ?

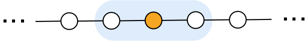


Path ? Cycle ?

Possible way to certify this : certificate = distance to a (fixed) extremity

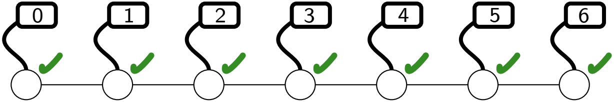


Example : how to certify that a graph is a path ?

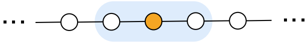


→ Path ? Cycle ?

Possible way to certify this : certificate = distance to a (fixed) extremity

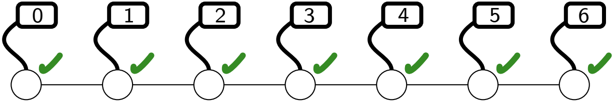


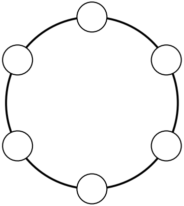
Example : how to certify that a graph is a path ?



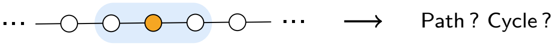
$\longrightarrow$ Path ? Cycle ?

Possible way to certify this : certificate = distance to a (fixed) extremity

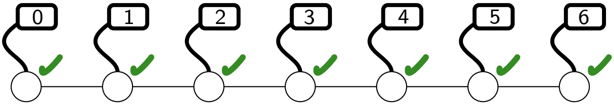


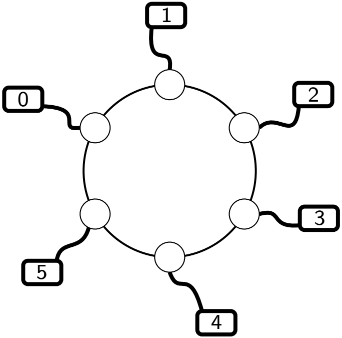


Example : how to certify that a graph is a path ?

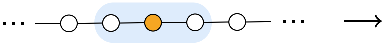


Possible way to certify this : certificate = distance to a (fixed) extremity



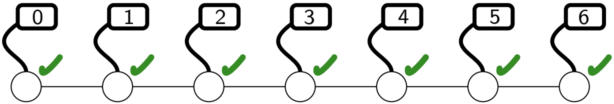


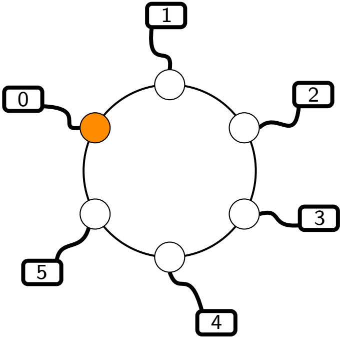
Example : how to certify that a graph is a path ?



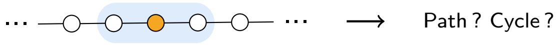
Path ? Cycle ?

Possible way to certify this : certificate = distance to a (fixed) extremity

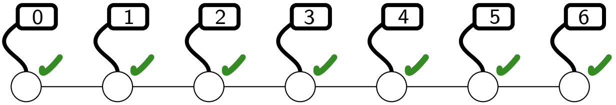


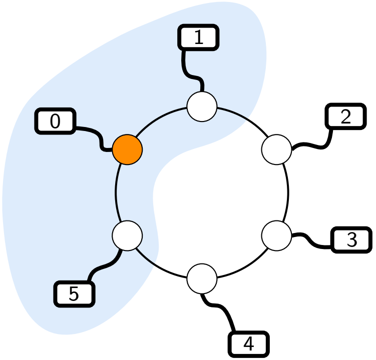


Example : how to certify that a graph is a path ?

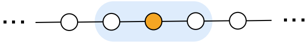


Possible way to certify this : certificate = distance to a (fixed) extremity



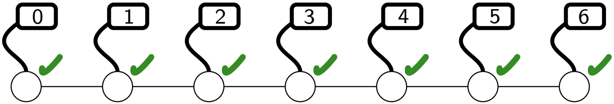


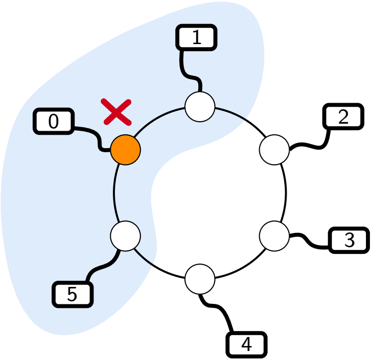
Example : how to certify that a graph is a path ?



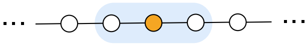
$\longrightarrow$ Path ? Cycle ?

Possible way to certify this : certificate = distance to a (fixed) extremity



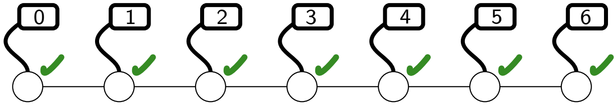


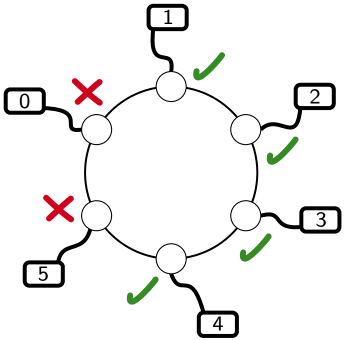
Example : how to certify that a graph is a path ?



$\longrightarrow$ Path ? Cycle ?

Possible way to certify this : certificate = distance to a (fixed) extremity





What should be the minimum size of the certificates?

What should be the minimum size of the certificates ?

Usual parameter : n (number of vertices in the graph)

What should be the minimum size of the certificates ?

Usual parameter : n (number of vertices in the graph)

Optimal size $\leqslant O(n^2)$ for any property

What should be the minimum size of the certificates ?

Usual parameter : n (number of vertices in the graph)

Optimal size $\leqslant O(n^2)$ for any property

Typical size of certificates :

$\tilde{\Theta}(n^2)$	$\Theta(\log n)$

What should be the minimum size of the certificates ?

Usual parameter : n (number of vertices in the graph)

Optimal size $\leqslant O(n^2)$ for any property

Typical size of certificates :

$\tilde{\Theta}(n^2)$	$\Theta(\log n)$
▪ Non-3-colorability ▪ Non-trivial automorphism	

What should be the minimum size of the certificates ?

Usual parameter : n (number of vertices in the graph)

Optimal size $\leqslant O(n^2)$ for any property

Typical size of certificates :

$\tilde{\Theta}(n^2)$	$\Theta(\log n)$
▪ Non-3-colorability	▪ Paths
▪ Non-trivial automorphism	▪ Spanning trees
	▪ Odd number of vertices
	▪ Planar graphs

What should be the minimum size of the certificates ?

Usual parameter : n (number of vertices in the graph)

Optimal size $\leqslant O(n^2)$ for any property

Typical size of certificates :

$\tilde{\Theta}(n^2)$	$\Theta(\log n)$	Independent of n
▪ Non-3-colorability ▪ Non-trivial automorphism	▪ Paths ▪ Spanning trees ▪ Odd number of vertices ▪ Planar graphs	▪ k-colorability ▪ Dominating set at distance t ▪ Perfect matching

What should be the minimum size of the certificates ?

Usual parameter : n (number of vertices in the graph)

Optimal size $\leqslant O(n^2)$ for any property

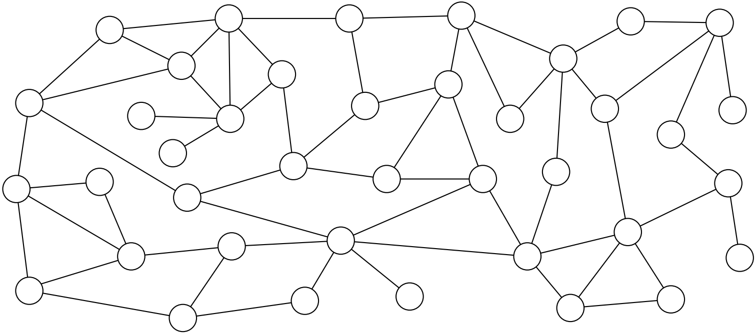
Typical size of certificates :

$\tilde{\Theta}(n^2)$	$\Theta(\log n)$	Independent of n
▪ Non-3-colorability ▪ Non-trivial automorphism	▪ Paths ▪ Spanning trees ▪ Odd number of vertices ▪ Planar graphs	▪ k-colorability ▪ Dominating set at distance t ▪ Perfect matching

Dominating sets at distance t

Dominating sets at distance t

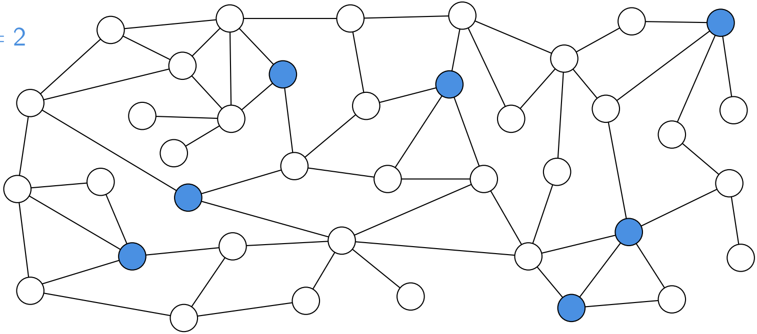
$$S \text{ dominating at distance } t \iff \forall v \in V, \exists u \in S, d(u,v) \leqslant t$$



Dominating sets at distance t

$$S \text{ dominating at distance } t \iff \forall v \in V, \exists u \in S, d(u,v) \leqslant t$$

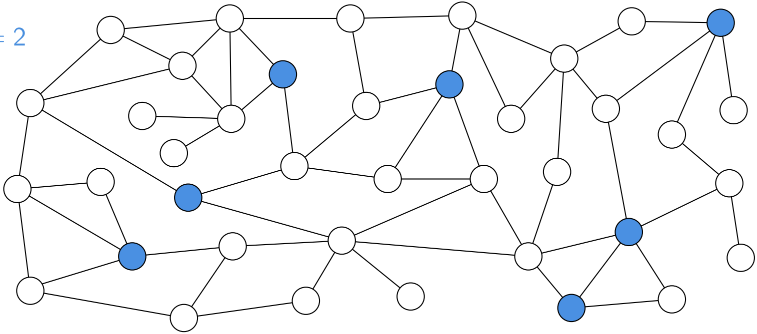
$t = 2$



Dominating sets at distance t

$$S \text{ dominating at distance } t \iff \forall v \in V, \exists u \in S, d(u,v) \leqslant t$$

$t = 2$

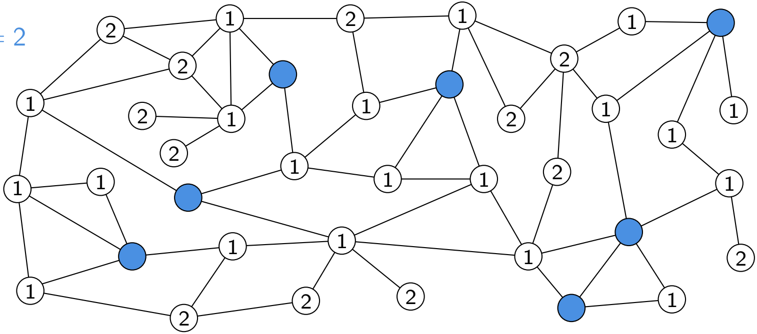


Trivial certification with t certificates (certificate = distance to S).

Dominating sets at distance t

$$S \text{ dominating at distance } t \iff \forall v \in V, \exists u \in S, d(u,v) \leqslant t$$

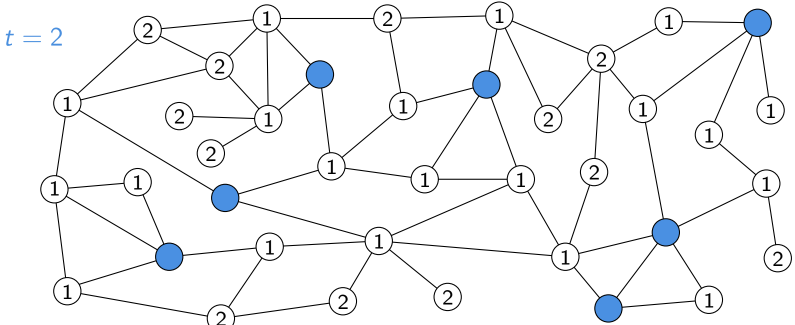
$t = 2$



Trivial certification with t certificates (certificate = distance to S).

Dominating sets at distance t

$$S \text{ dominating at distance } t \iff \forall v \in V, \exists u \in S, d(u,v) \leqslant t$$

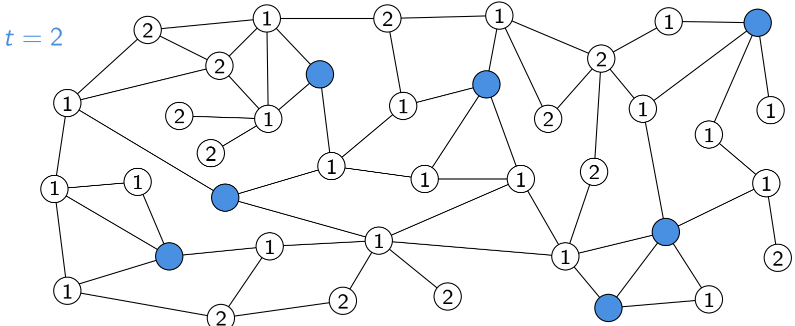


Trivial certification with t certificates (certificate = distance to S).

Optimal ?

Dominating sets at distance t

S dominating at distance $t \iff \forall v \in V, \exists u \in S, d(u,v) \leqslant t$



Trivial certification with t certificates (certificate = distance to S).

Optimal ? No.

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Lower bound : $\Omega(\sqrt{t})$ are necessary.

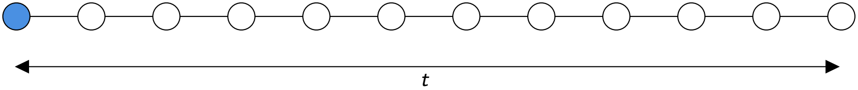
Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Lower bound : $\Omega(\sqrt{t})$ are necessary.

Proof : by contradiction. Assume that $< \sqrt{t}$ certificates are sufficient.



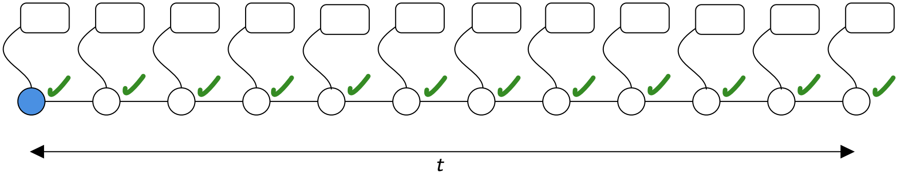
Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Lower bound : $\Omega(\sqrt{t})$ are necessary.

Proof : by contradiction. Assume that $< \sqrt{t}$ certificates are sufficient.



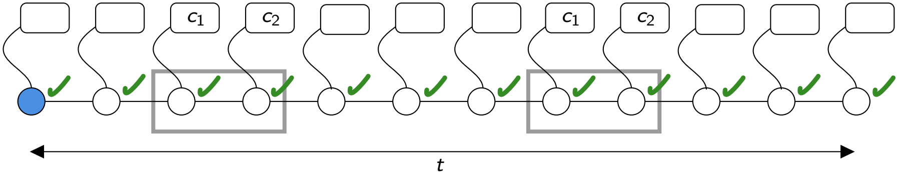
Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Lower bound : $\Omega(\sqrt{t})$ are necessary.

Proof : by contradiction. Assume that $< \sqrt{t}$ certificates are sufficient.



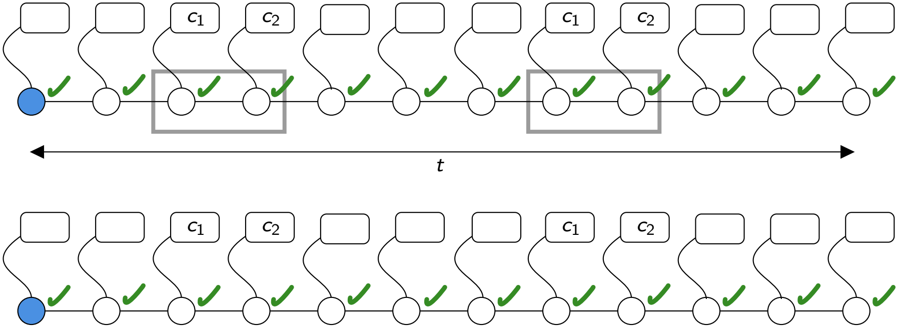
Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Lower bound : $\Omega(\sqrt{t})$ are necessary.

Proof : by contradiction. Assume that $< \sqrt{t}$ certificates are sufficient.



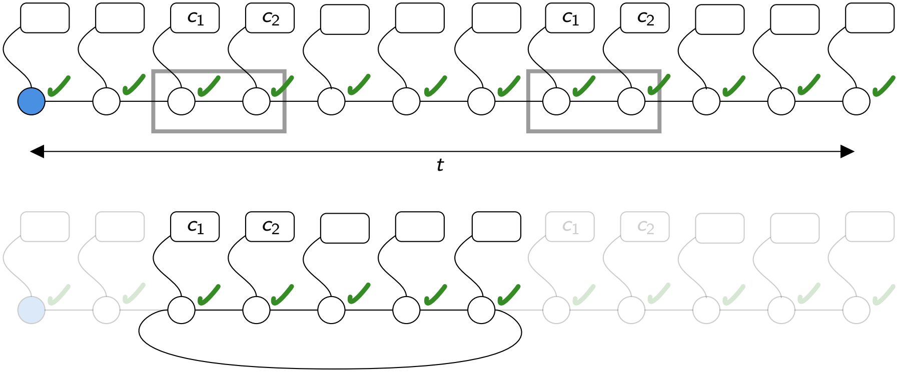
Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Lower bound : $\Omega(\sqrt{t})$ are necessary.

Proof : by contradiction. Assume that $< \sqrt{t}$ certificates are sufficient.



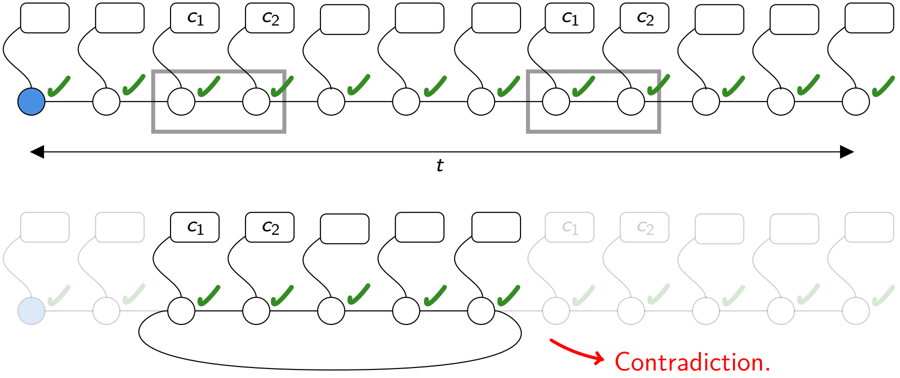
Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Lower bound : $\Omega(\sqrt{t})$ are necessary.

Proof : by contradiction. Assume that $< \sqrt{t}$ certificates are sufficient.



Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

Idea : use De Bruijn words.

Definition

A De Bruijn word on the alphabet $\{1, \ldots, \lceil \sqrt{t} \rceil\}$ is a word ω of length t such that each word of length 2 appears at most once as a factor of ω.

Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

Idea : use De Bruijn words.

Definition

A De Bruijn word on the alphabet $\{1, \ldots, \lceil \sqrt{t} \rceil\}$ is a word ω of length t such that each word of length 2 appears at most once as a factor of ω.

Certification : $\underset{(S = \text{pointed vertices})}{d(u,S) = i} \longrightarrow u$ gets the certificate $(\omega_i, i \mod 3)$

Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

Idea : use De Bruijn words.

Definition

A De Bruijn word on the alphabet $\{1, \ldots, \lceil \sqrt{t} \rceil\}$ is a word ω of length t such that each word of length 2 appears at most once as a factor of ω.

Certification : $d(u, S) = i \longrightarrow u$ gets the certificate $(\omega_i, i \mod 3)$
(S = pointed vertices)

Verification :

Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

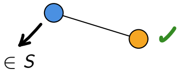
Idea : use De Bruijn words.

Definition

A De Bruijn word on the alphabet $\{1, \ldots, \lceil \sqrt{t} \rceil\}$ is a word ω of length t such that each word of length 2 appears at most once as a factor of ω.

Certification : $d(u, S) = i \longrightarrow u$ gets the certificate $(\omega_i, i \mod 3)$
(S = pointed vertices)

Verification :



Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

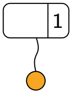
Idea : use De Bruijn words.

Definition

A De Bruijn word on the alphabet $\{1, \dots, \lceil\sqrt{t}\rceil\}$ is a word ω of length t such that each word of length 2 appears at most once as a factor of ω.

Certification : $d(u, S) = i \longrightarrow u$ gets the certificate $(\omega_i, i \mod 3)$
(S = pointed vertices)

Verification :



Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

Idea : use De Bruijn words.

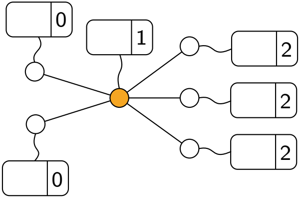
Definition

A De Bruijn word on the alphabet $\{1, \ldots, \lceil \sqrt{t} \rceil\}$ is a word ω of length t such that each word of length 2 appears at most once as a factor of ω.

Certification : $d(u, S) = i \longrightarrow u$ gets the certificate $(\omega_i, i \mod 3)$

(S = pointed vertices)

Verification :



Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

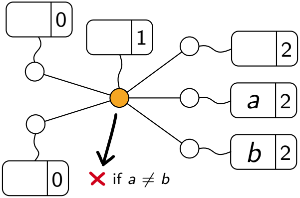
Idea : use De Bruijn words.

Definition

A De Bruijn word on the alphabet $\{1, \dots, \lceil \sqrt{t} \rceil\}$ is a word ω of length t such that each word of length 2 appears at most once as a factor of ω.

Certification : $d(u, S) = i \longrightarrow u$ gets the certificate $(\omega_i, i \mod 3)$
($S =$ pointed vertices)

Verification :



Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

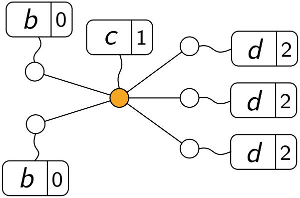
Idea : use De Bruijn words.

Definition

A De Bruijn word on the alphabet $\{1, \ldots, \lceil\sqrt{t}\rceil\}$ is a word ω of length t such that each word of length 2 appears at most once as a factor of ω.

Certification : $d(u, S) = i \longrightarrow u$ gets the certificate $(\omega_i, i \mod 3)$
(S = pointed vertices)

Verification :



Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

Idea : use De Bruijn words.

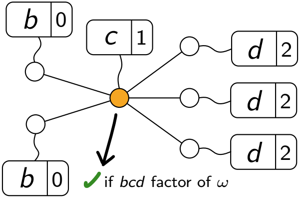
Definition

A De Bruijn word on the alphabet $\{1, \dots, \lceil \sqrt{t} \rceil\}$ is a word ω of length t such that each word of length 2 appears at most once as a factor of ω.

Certification : $d(u, S) = i \longrightarrow u$ gets the certificate $(\omega_i, i \mod 3)$

(S = pointed vertices)

Verification :



Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

Idea : use De Bruijn words.

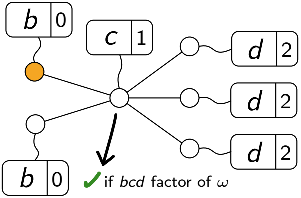
Definition

A De Bruijn word on the alphabet $\{1, \ldots, \lceil\sqrt{t}\rceil\}$ is a word ω of length t such that each word of length 2 appears at most once as a factor of ω.

Certification : $d(u, S) = i \longrightarrow u$ gets the certificate $(\omega_i, i \mod 3)$

(S = pointed vertices)

Verification :



Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

Idea : use De Bruijn words.

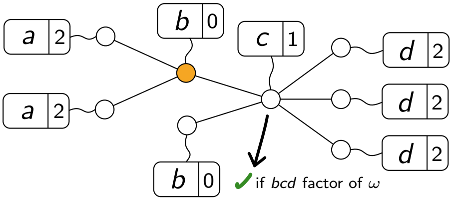
Definition

A De Bruijn word on the alphabet $\{1, \dots, \lceil\sqrt{t}\rceil\}$ is a word ω of length t such that each word of length 2 appears at most once as a factor of ω.

Certification : $d(u, S) = i \longrightarrow u$ gets the certificate $(\omega_i, i \mod 3)$

(S = pointed vertices)

Verification :



Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

Idea : use De Bruijn words.

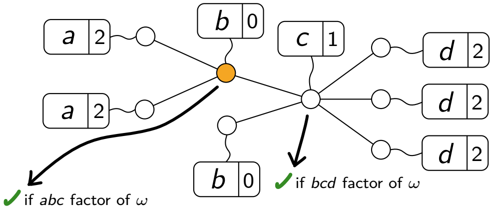
Definition

A De Bruijn word on the alphabet $\{1, \ldots, \lceil\sqrt{t}\rceil\}$ is a word ω of length t such that each word of length 2 appears at most once as a factor of ω.

Certification : $d(u, S) = i \longrightarrow u$ gets the certificate $(\omega_i, i \mod 3)$

(S = pointed vertices)

Verification :



Dominating sets at distance t

Theorem (Bousquet, Feuilloley, Z.)

$\Theta(\sqrt{t})$ certificates are necessary and sufficient to certify a dominating set at distance t.

Upper bound : $O(\sqrt{t})$ are sufficient.

Idea : use De Bruijn words.

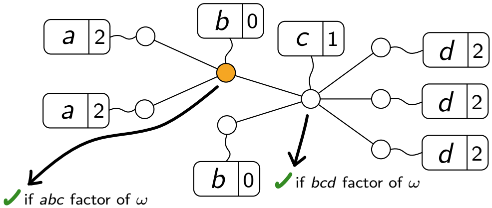
Definition

A De Bruijn word on the alphabet $\{1, \ldots, \lceil\sqrt{t}\rceil\}$ is a word ω of length t such that each word of length 2 appears at most once as a factor of ω.

Certification : $d(u, S) = i \longrightarrow u$ gets the certificate $(\omega_i, i \mod 3)$

(S = pointed vertices)

Verification :



bc appears only once in ω

$\Downarrow$

$\omega = ...abcd.....$

What if vertices can see at distance $d > 1$?

What if vertices can see at distance $d > 1$?

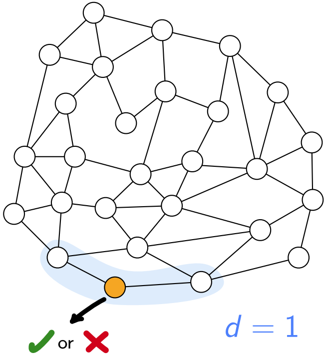
View of a vertex = all the information available at distance $\leqslant d$:

- vertices
- edges
- certificates

What if vertices can see at distance $d > 1$?

View of a vertex = all the information available at distance $\leqslant d$:

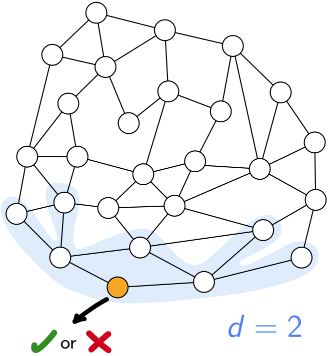
- vertices
- edges
- certificates



What if vertices can see at distance $d > 1$?

View of a vertex = all the information available at distance $\leqslant d$:

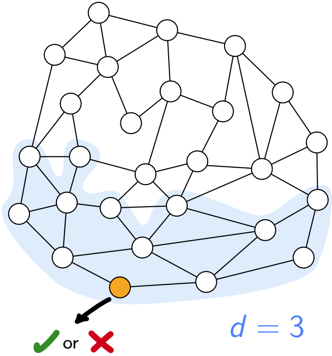
- vertices
- edges
- certificates



What if vertices can see at distance $d > 1$?

View of a vertex = all the information available at distance $\leqslant d$:

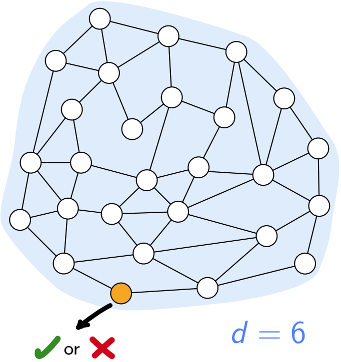
- vertices
- edges
- certificates



What if vertices can see at distance $d > 1$?

View of a vertex = all the information available at distance $\leqslant d$:

- vertices
- edges
- certificates

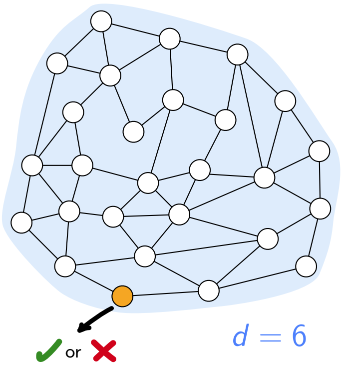


What if vertices can see at distance $d > 1$?

View of a vertex = all the information available at distance $\leqslant d$:

- vertices
- edges
- certificates

Question : How fast does the size of the certificates decreases when d increases ?

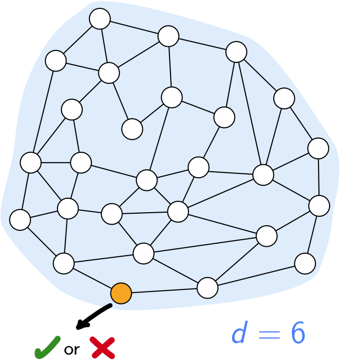


What if vertices can see at distance $d > 1$?

View of a vertex = all the information available at distance $\leqslant d$:

- vertices
- edges
- certificates

Question : How fast does the size of the certificates decreases when d increases ?



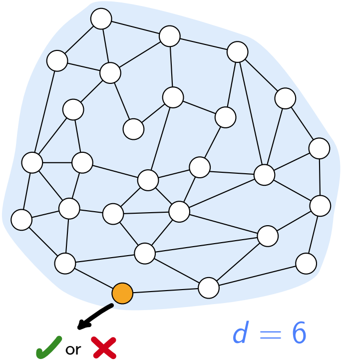
Theorem (Bousquet, Feuilloley, Z.)

If the vertices can see at distance d, $\Theta(\log t/d)$ bits are necessary and sufficient to certify a dominating set at distance t.

What if vertices can see at distance $d > 1$?

View of a vertex = all the information available at distance $\leqslant d$:

- vertices
- edges
- certificates



Question : How fast does the size of the certificates decreases when d increases ?

Theorem (Bousquet, Feuilloley, Z.)

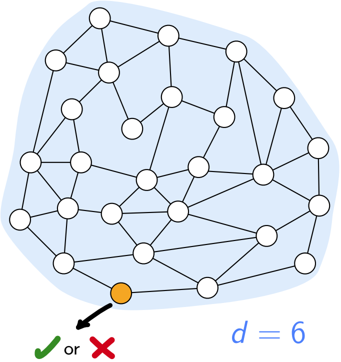
If the vertices can see at distance d, $\Theta(\log t/d)$ bits are necessary and sufficient to certify a dominating set at distance t.

Proof : using De Bruijn words (quite similar).

What if vertices can see at distance $d > 1$?

View of a vertex = all the information available at distance $\leqslant d$:

- vertices
- edges
- certificates



Question : How fast does the size of the certificates decreases when d increases ?

Theorem (Bousquet, Feuilloley, Z.)

If the vertices can see at distance d, $\Theta(\log t/d)$ bits are necessary and sufficient to certify a dominating set at distance t.

Proof : using De Bruijn words (quite similar).

Trade-off conjecture

If s bits are sufficient at distance 1, then $O(s/d)$ bits are sufficient at distance d.

Other results : k-colorability

Other results : k-colorability

Trivial certification with k certificates.

Other results : k-colorability

Trivial certification with k certificates.

Theorem (Ardévol Martínez et al.) (best known lower bound before this paper)

At least 3 different certificates are necessary.

Other results : k-colorability

Trivial certification with k certificates.

Theorem (Ardévol Martínez et al.) (best known lower bound before this paper)

At least 3 different certificates are necessary.

Theorem (Bousquet, Feuilloley, Z.)

If vertices can see at distance 1, k certificates are necessary.

Other results : k-colorability

Trivial certification with k certificates.

Theorem (Ardévol Martínez et al.) (best known lower bound before this paper)

At least 3 different certificates are necessary.

Theorem (Bousquet, Feuilloley, Z.)

If vertices can see at distance 1, k certificates are necessary.

Theorem (Bousquet, Feuilloley, Z.)

If vertices can see at distance d, $\Omega(\log k/d)$ bits are necessary.

Other results : k-colorability

Trivial certification with k certificates.

Theorem (Ardévol Martínez et al.) (best known lower bound before this paper)

At least 3 different certificates are necessary.

Theorem (Bousquet, Feuilloley, Z.)

If vertices can see at distance 1, k certificates are necessary.

Theorem (Bousquet, Feuilloley, Z.)

If vertices can see at distance d, $\Omega(\log k/d)$ bits are necessary.

Question : if vertices can see at distance d, are $\Omega(\log k)$ bits still necessary ?

Other results : k-colorability

Trivial certification with k certificates.

Theorem (Ardévol Martínez et al.) (best known lower bound before this paper)

At least 3 different certificates are necessary.

Theorem (Bousquet, Feuilloley, Z.)

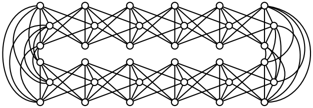
If vertices can see at distance 1, k certificates are necessary.

Theorem (Bousquet, Feuilloley, Z.)

If vertices can see at distance d, $\Omega(\log k/d)$ bits are necessary.

Question : if vertices can see at distance d, are $\Omega(\log k)$ bits still necessary ?

this proof uses uniquely k-colorable graphs :



Other results : k-colorability

Trivial certification with k certificates.

Theorem (Ardévol Martínez et al.) (best known lower bound before this paper)

At least 3 different certificates are necessary.

Theorem (Bousquet, Feuilloley, Z.)

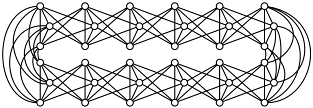
If vertices can see at distance 1, k certificates are necessary.

Theorem (Bousquet, Feuilloley, Z.)

If vertices can see at distance d, $\Omega(\log k/d)$ bits are necessary.

Question : if vertices can see at distance d, are $\Omega(\log k)$ bits still necessary ?

this proof uses uniquely k-colorable graphs :



($k = 3$)

Theorem (Bousquet, Feuilloley, Z.)

If vertices can see at distance d, and if all the balls of radius d are uniquely colorable, then $O(\log k/d)$ bits are sufficient.

Other results : perfect matchings

Other results : perfect matchings

There exists a certification scheme with $O(\Delta)$ certificates.

Other results : perfect matchings

There exists a certification scheme with $O(\Delta)$ certificates.

Theorem (Bousquet, Feuilloley, Z.)

At least Δ certificates are necessary to certify the existence of a perfect matching.

Other results : perfect matchings

There exists a certification scheme with $O(\Delta)$ certificates.

Theorem (Bousquet, Feuilloley, Z.)

At least Δ certificates are necessary to certify the existence of a perfect matching.

Theorem (Bousquet, Feuilloley, Z.)

- $O(\log t)$ bits are sufficient for graphs of treewidth t
- 2 bits are sufficient for planar graphs

Other results : perfect matchings

There exists a certification scheme with $O(\Delta)$ certificates.

Theorem (Bousquet, Feuilloley, Z.)

At least Δ certificates are necessary to certify the existence of a perfect matching.

Theorem (Bousquet, Feuilloley, Z.)

- $O(\log t)$ bits are sufficient for graphs of treewidth t
- 2 bits are sufficient for planar graphs

Question : lower bound at distance $d > 1$?

Thanks for your attention !