K-Clique Is Hard on Average for Regular Resolution

Ilario Bonacina

bonacina@cs.upc.edu

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Dagstuhl, January 30 2018

Joint work with A. Atserias, S. de Rezende, M. Lauria, J. Nordström, A. Razborov

Motivations

- k-clique is a fundamental NP-complete problem (related to FPT vs W[1])
- regular resolution captures the reasoning power of state-of-the-art algorithms to find k-cliques
- for k small (say $k < \sqrt{n}$) the usual tools from proof complexity fail

Main Result (*Informal*)

Main Theorem (informal)
Let $\boldsymbol{G}$ be an Erdős-Rényi random graph with n vertices (and edge density s.t. $\boldsymbol{G}$ has no k-clique) and $k = o(n^{1/4})$. W.h.p. every regular resolution proof of the fact that $\boldsymbol{G}$ does not contain a k-clique has size $\geq n^{\Omega(k)}$

K-Clique Formula

$G = (V, E)$ graph with $V = V_1 \sqcup V_2 \sqcup \cdots \sqcup V_k$ and $|V_i| = n/k$

$x_v = 1$ iff "v belongs to a k-clique (that respects the partition of V)"

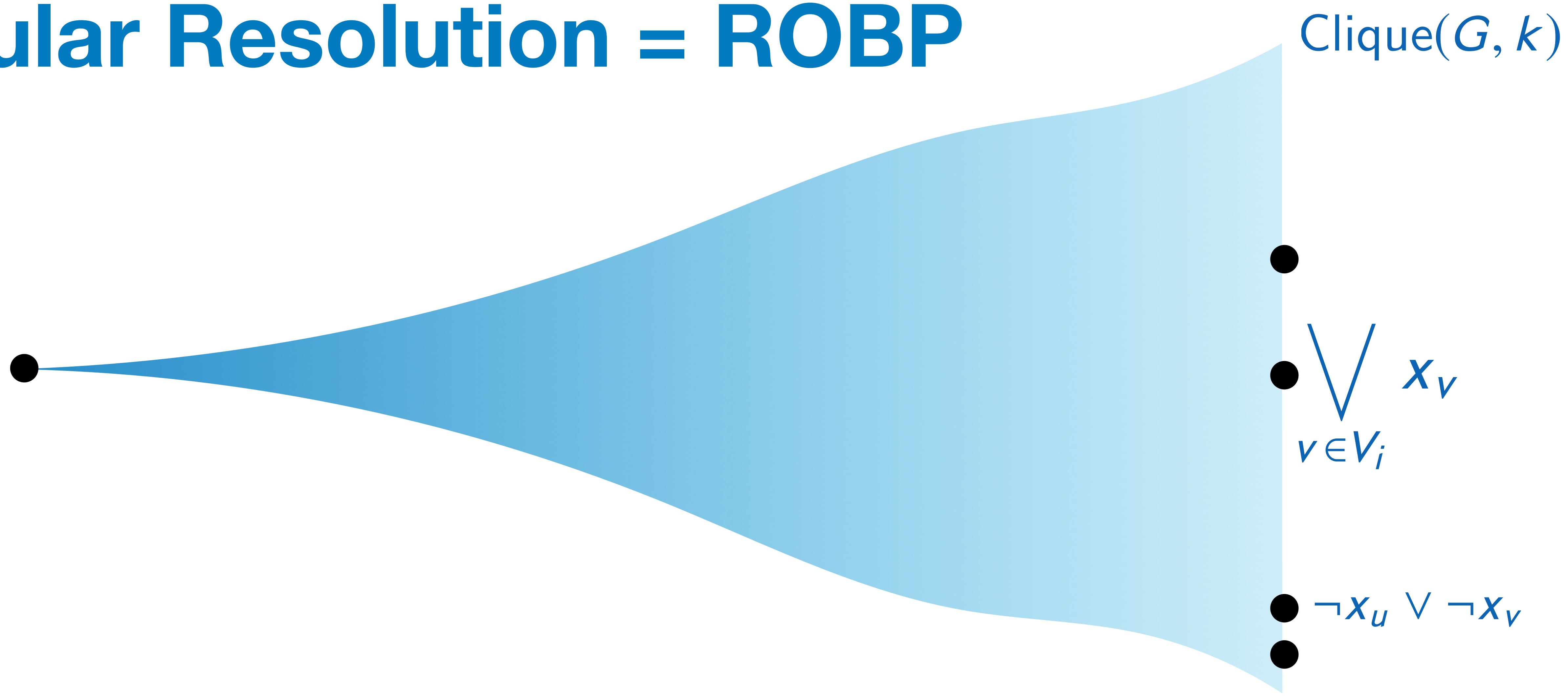
Definition

Clique(G, k) is the conjunction of

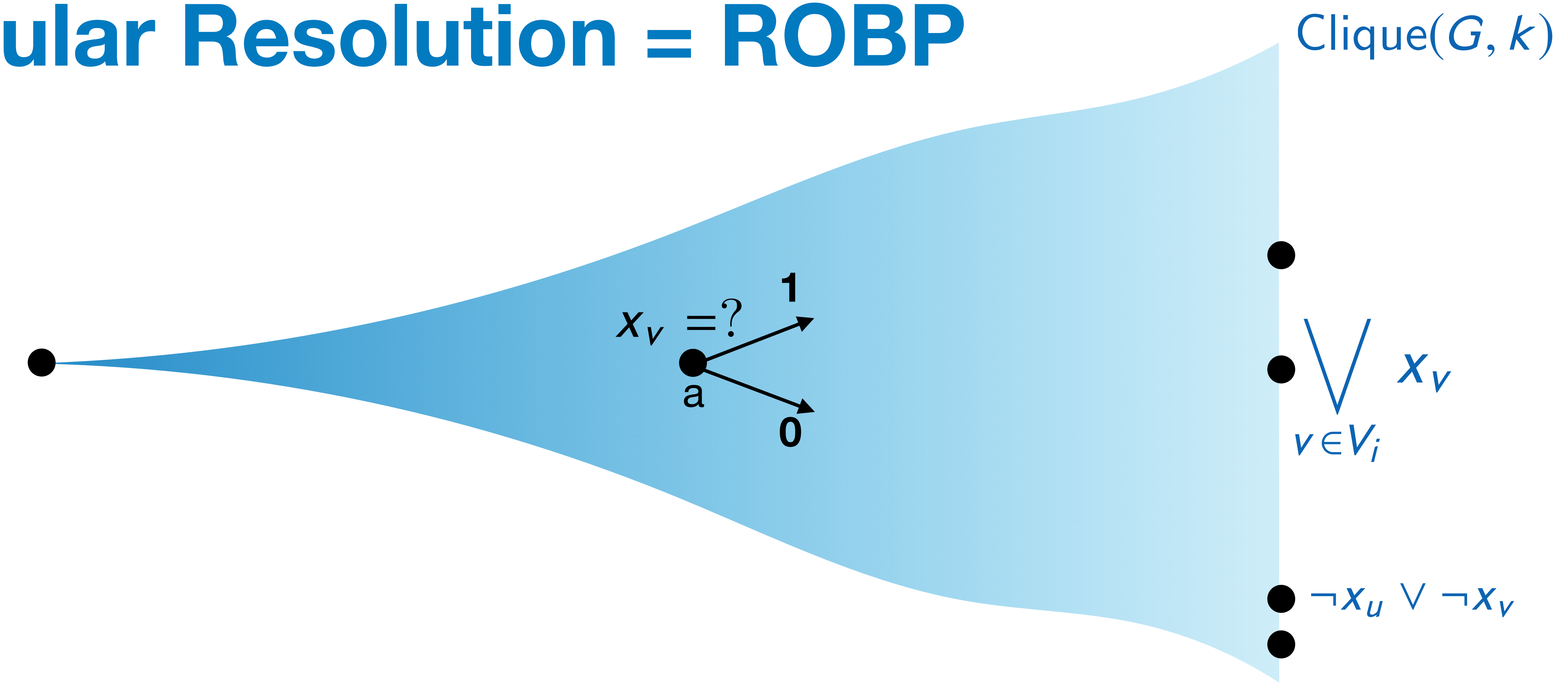
$$\bigvee_{v \in V_i} x_v \qquad \text{for } i \in [k];$$

$$\neg x_u \vee \neg x_v \qquad \text{for } u, v \in V,\ \{u, v\} \notin E \text{ or exists } i \in [k]\ u, v \in V_i$$

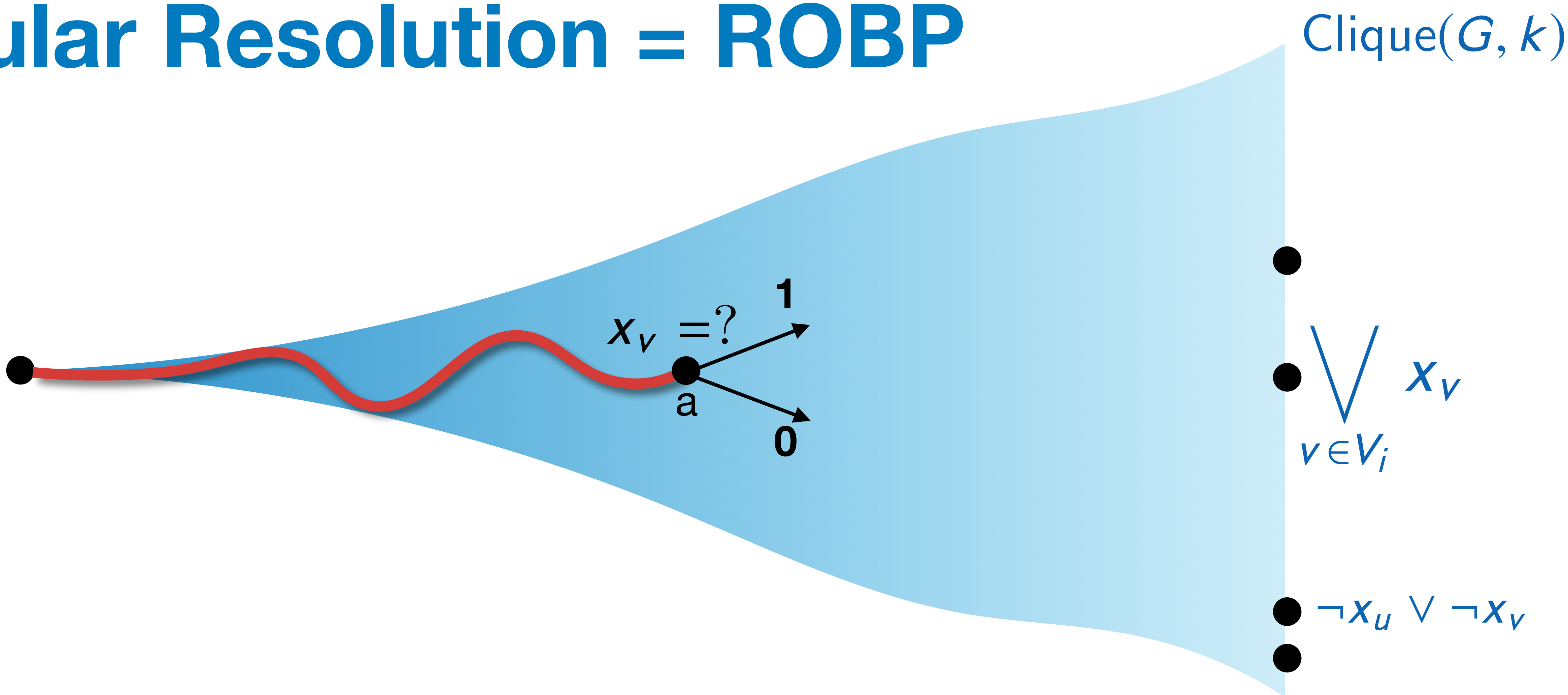
Regular Resolution = ROBP



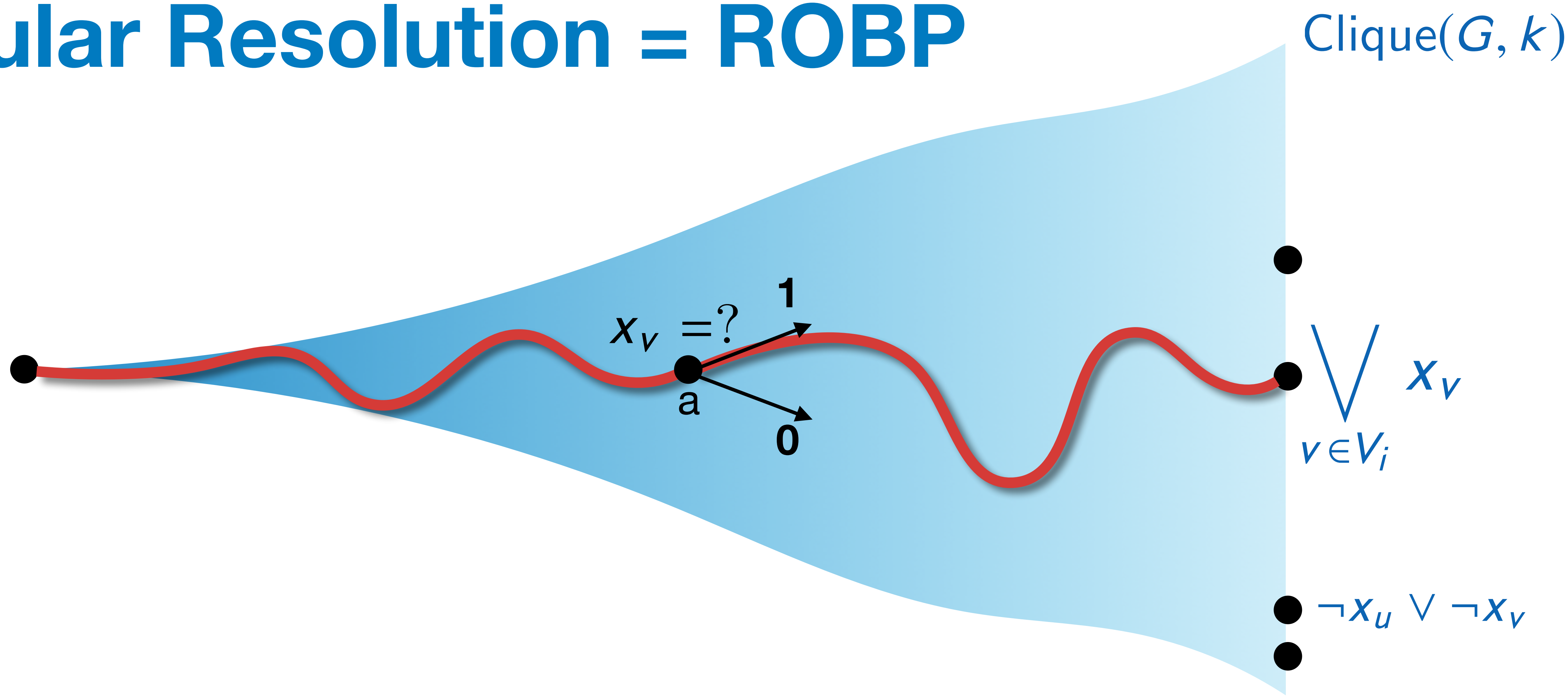
Regular Resolution = ROBP



Regular Resolution = ROBP



Regular Resolution = ROBP



Some Background

- Clique(G, k) has resolution refutations of size $\leq (n/k)^{O(k)}$
- Clique(G, k) has resolution refutations of width $\leq k$. So the size-width inequality (at best) implies $2^{\Omega(k^2/n)}$ lower bounds.

  for $n^{5/6} \ll k < \frac{n}{3}$ and $\boldsymbol{G}$ an Erdős-Rényi random graph with n vertices (and suitable edge density), w.h.p. all resolution refutations of Clique$(\boldsymbol{G}, k)$ have size $2^{n^{\Omega(1)}}$ [BIS'07]

Some Background

- Clique(G, k) has resolution refutations of size $\leq (n/k)^{O(k)}$
- Clique(G, k) has resolution refutations of width $\leq k$. So the size-width inequality (at best) implies $2^{\Omega(k^2/n)}$ lower bounds.

  for $n^{5/6} \ll k < \frac{n}{3}$ and $\boldsymbol{G}$ an Erdős-Rényi random graph with n vertices (and suitable edge density), w.h.p. all resolution refutations of Clique($\boldsymbol{G}, k$) have size $2^{n^{\Omega(1)}}$ [BIS'07]

- regular resolution has short (i.e. $f(k)n^{O(1)}$) refutations of Clique(G, k) when G is the $(k-1)$-partite graph; this is not the case for tree-like resolution [BGL'13]

Main Result

Main Theorem
Let $\boldsymbol{G} \sim \mathcal{G}(n, p)$ be an Erdős-Rényi random graph with $p \ll n^{-2/(k-1)}$.
W.h.p. every regular resolution proof of Clique$(\boldsymbol{G}, k)$ has size $\geq n^{\Omega(k)}$

Main Result

Main Theorem
Let $\boldsymbol{G} \sim \mathcal{G}(n, p)$ be an Erdős-Rényi random graph with $p \ll n^{-2/(k-1)}$.
W.h.p. every regular resolution proof of Clique$(\boldsymbol{G}, k)$ has size $\geq n^{\Omega(k)}$

- The lower bound degrades nicely for smaller edge density and holds whenever $k = o(n^{1/4})$
- For $\boldsymbol{G} \sim \mathcal{G}(n, \frac{1}{2})$ and $k \approx \log n$ the lower bound is $n^{\Omega(\log n)}$


PROOF

Proof Idea

Lemma 1
If the graph $G = (V_1 \sqcup V_2 \sqcup \cdots \sqcup V_k, E)$ satisfies the property $P(k, r, s, \epsilon)$, then every regular resolution refutation of Clique(G, k) has size $\geq \frac{1}{\sqrt{2}} s^{\epsilon r/2}$

Proof Idea

Lemma 1
If the graph $G = (V_1 \sqcup V_2 \sqcup \cdots \sqcup V_k, E)$ satisfies the property $P(k, r, s, \epsilon)$, then every regular resolution refutation of $\mathrm{Clique}(G, k)$ has size $\geq \frac{1}{\sqrt{2}} s^{\epsilon r/2}$

Lemma 2
The Erdős-Rényi random graph $\boldsymbol{G} \sim \mathcal{G}(n, p)$ with $p = n^{-4/(k-1)}$ w.h.p. satisfies the property $P(k, r, s, \epsilon)$ with

$$r = \frac{k}{2^{16}} \qquad s = \sqrt{n} \qquad \epsilon = \frac{1}{8}$$

Whenever $k \leq n^{1/8}/\log n$.

(similar parameters work for $p = n^{-2\eta/(k-1)}$ and $k \leq n^{1/4-\xi}/\log n$ with $\eta > 1$ and $\xi > 0$)

Proof Idea

property $P(k, r, s, \epsilon)$:
there are $t, q \in \mathbb{R}^+$ s.t.
(1) ....
(2) ....

Lemma 1
If the graph $G = (V_1 \sqcup V_2 \sqcup \cdots \sqcup V_k, E)$ satisfies the property $P(k, r, s, \epsilon)$, then every regular resolution refutation of Clique(G, k) has size $\geq \frac{1}{\sqrt{2}} s^{\epsilon r/2}$

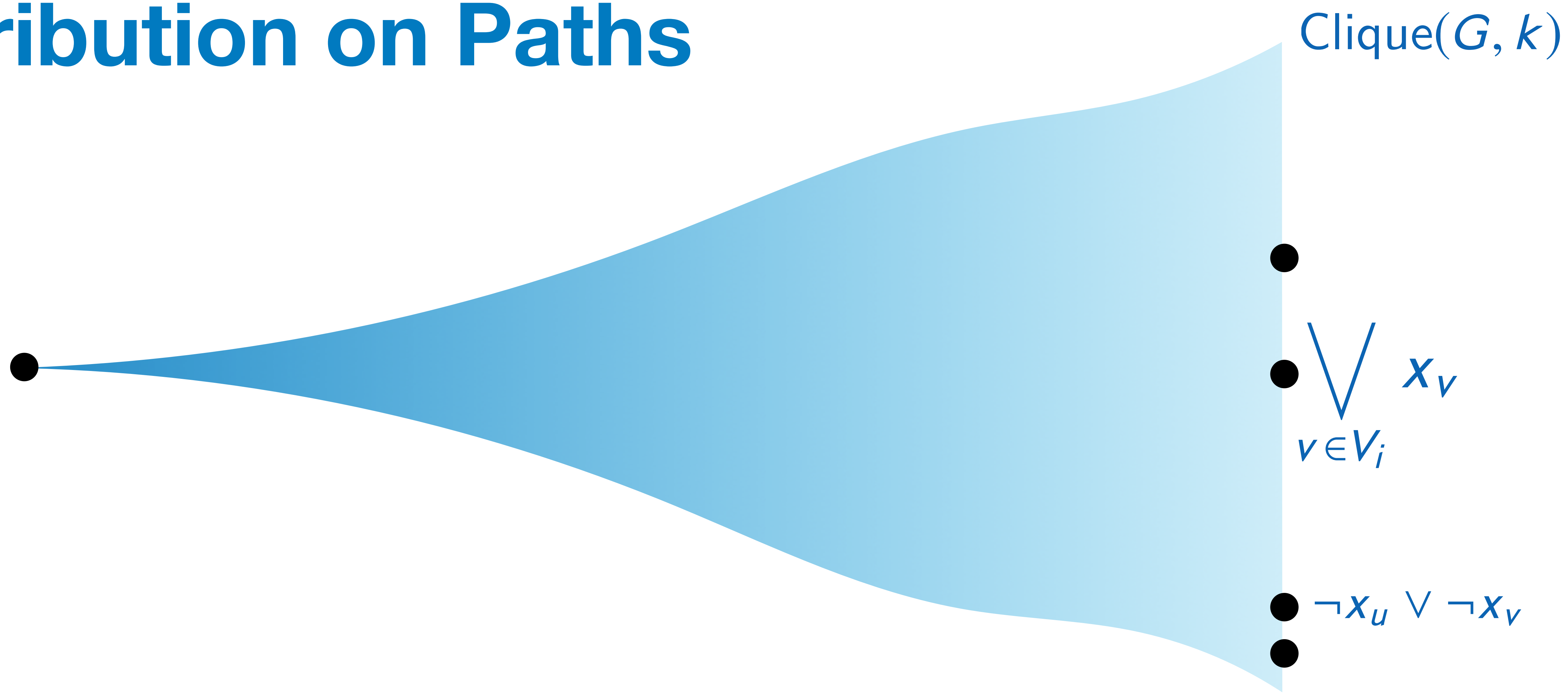
Lemma 2
The Erdős-Rényi random graph $\boldsymbol{G} \sim \mathcal{G}(n, p)$ with $p = n^{-4/(k-1)}$ w.h.p. satisfies the property $P(k, r, s, \epsilon)$ with

$$r = \frac{k}{2^{16}} \qquad s = \sqrt{n} \qquad \epsilon = \frac{1}{8}$$

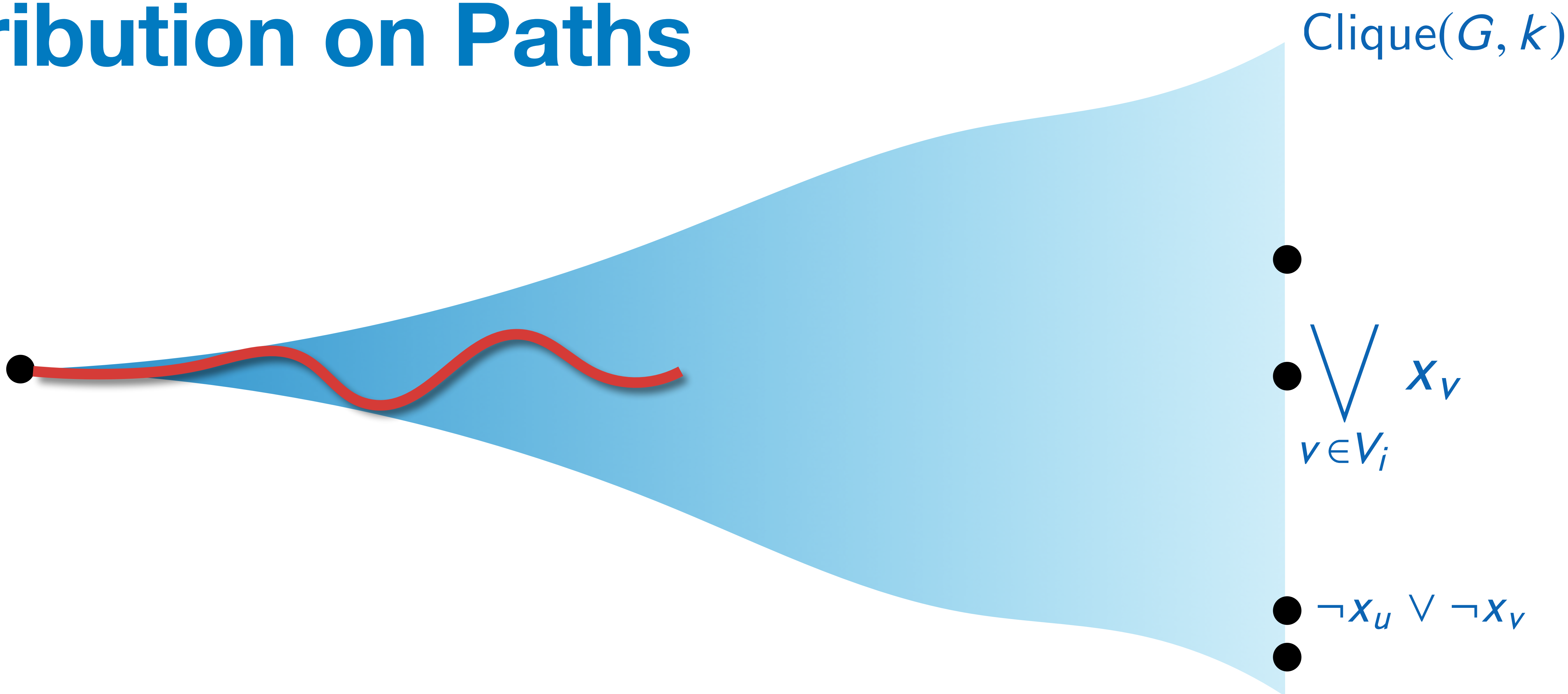
Whenever $k \leq n^{1/8}/\log n$.

(similar parameters work for $p = n^{-2\eta/(k-1)}$ and $k \leq n^{1/4-\xi}/\log n$ with $\eta > 1$ and $\xi > 0$)

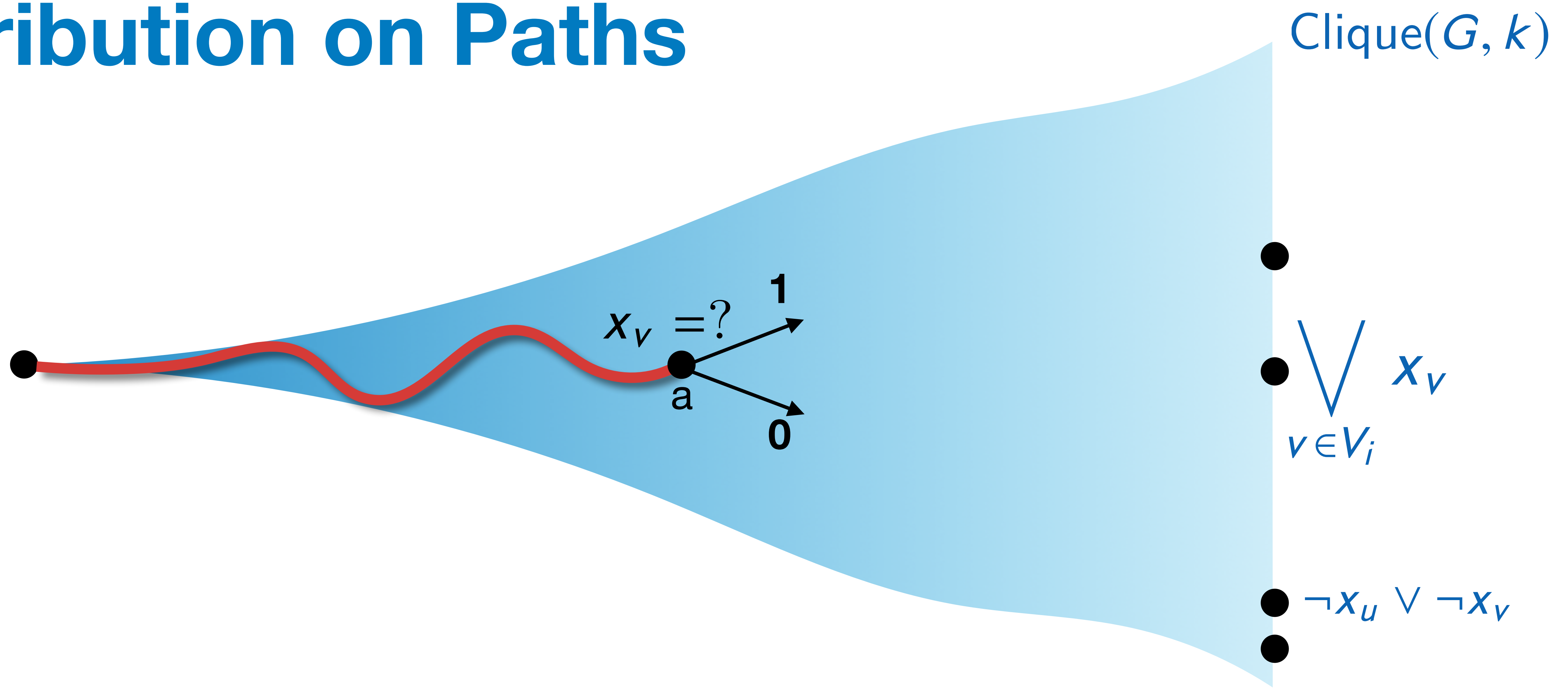
Distribution on Paths



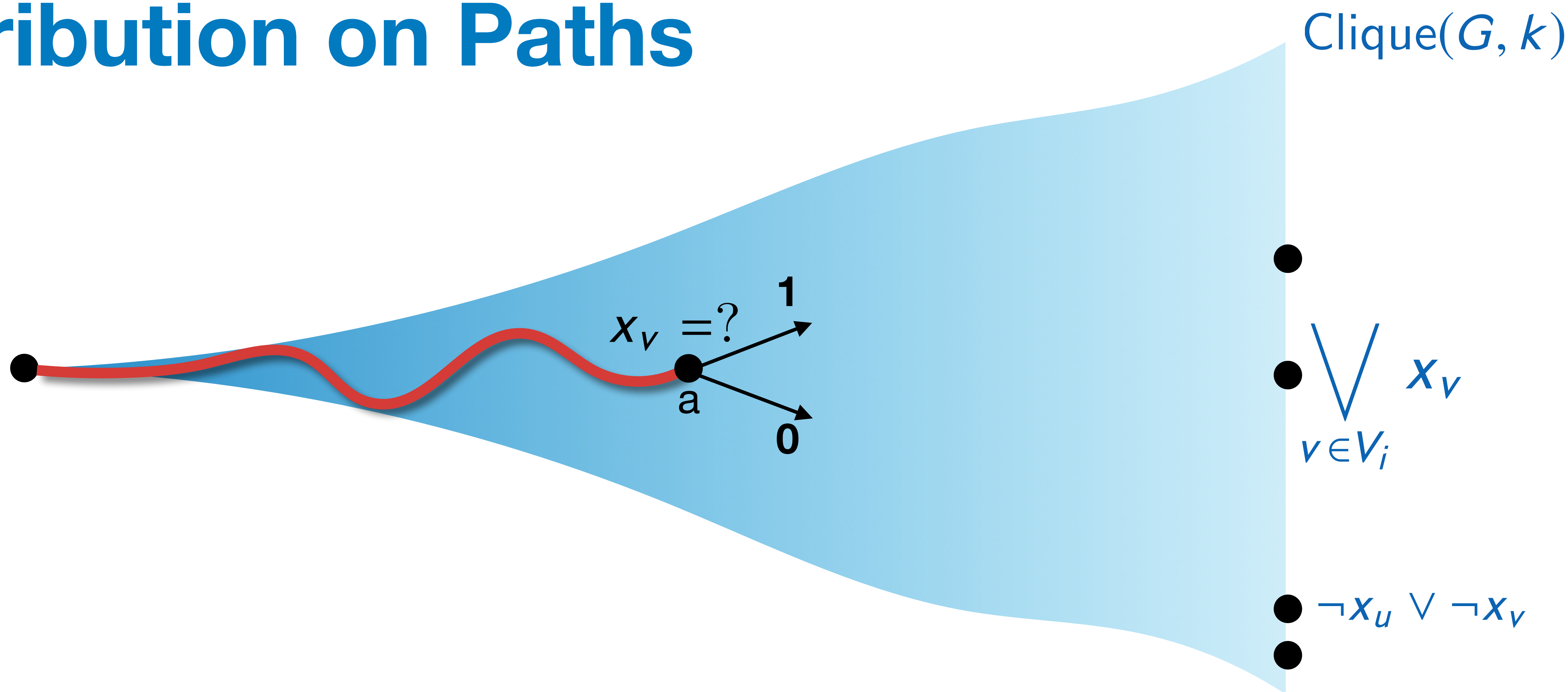
Distribution on Paths



Distribution on Paths



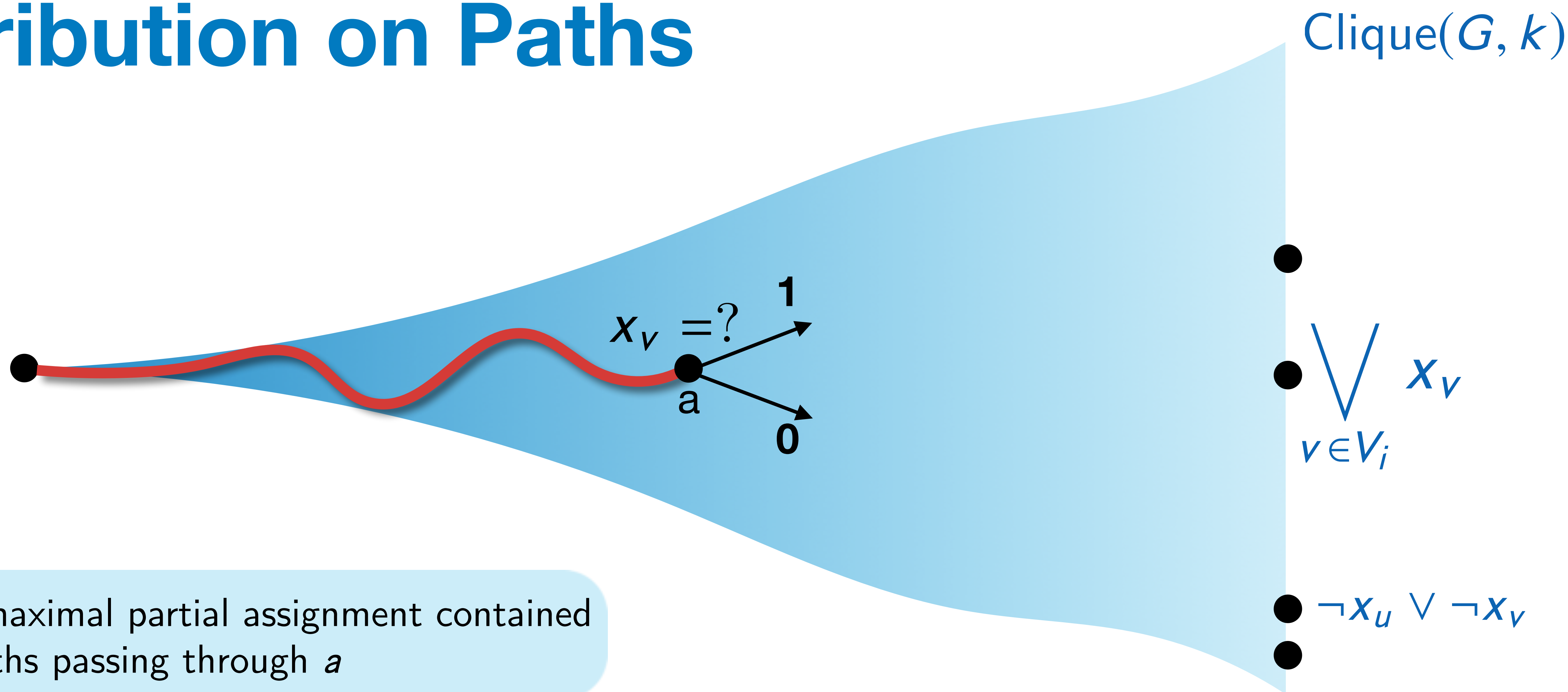
Distribution on Paths



$\boldsymbol{\alpha} \sim \mathcal{D}$ if it is constructed as follows:

- if $v \in V_i$ with i forgotten at a or $\beta(a) \cup \{x_v = 1\}$ falsifies a short axiom of $\text{Clique}(G,k)$ then continue with $x_v = 0$
- otherwise toss a coin and with prob $s^{-1/(1-\epsilon)}$ continue with $x_v = 1$

Distribution on Paths

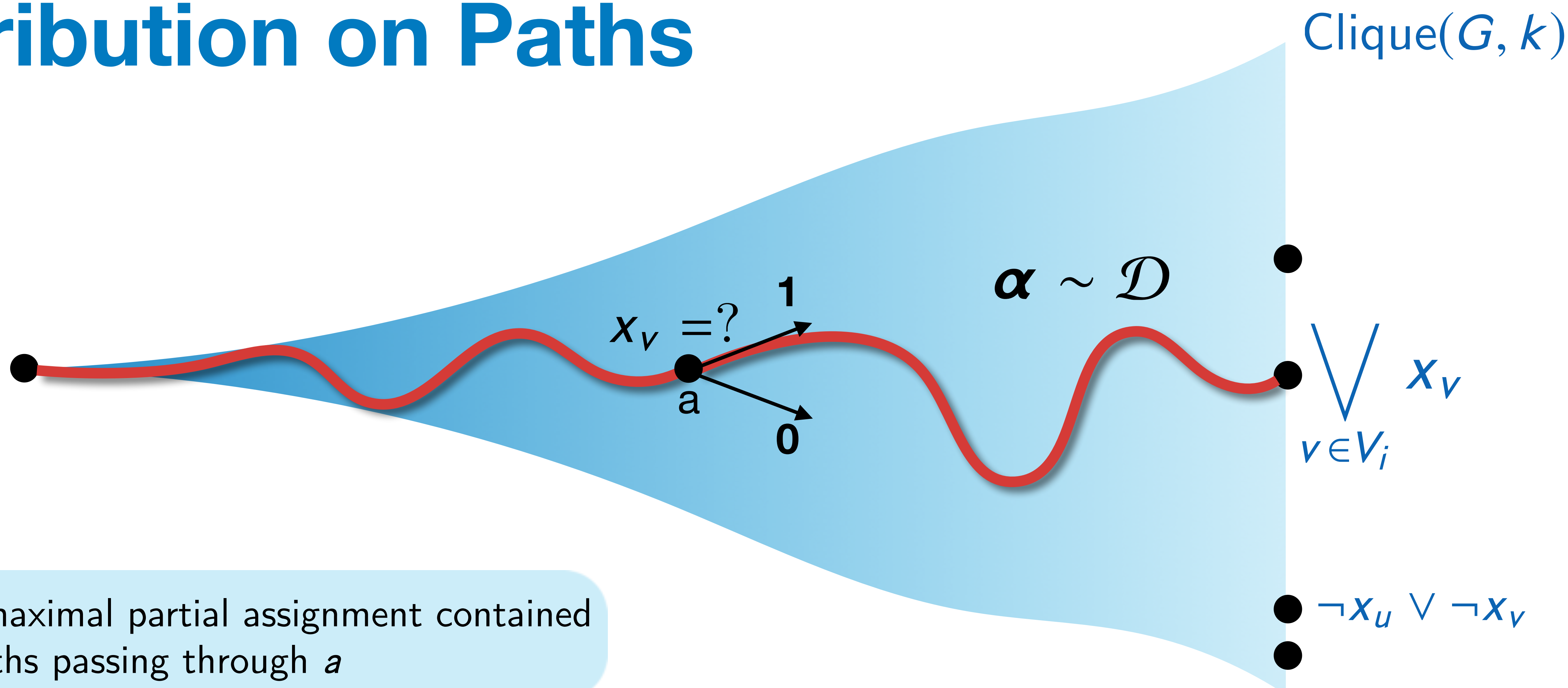


$\beta(a)$ = maximal partial assignment contained in all paths passing through a

$\boldsymbol{\alpha} \sim \mathcal{D}$ if it is constructed as follows:

- if $v \in V_i$ with i forgotten at a or $\beta(a) \cup \{x_v = 1\}$ falsifies a short axiom of Clique(G, k) then continue with $x_v = 0$
- otherwise toss a coin and with prob $s^{-1/(1-\epsilon)}$ continue with $x_v = 1$

Distribution on Paths

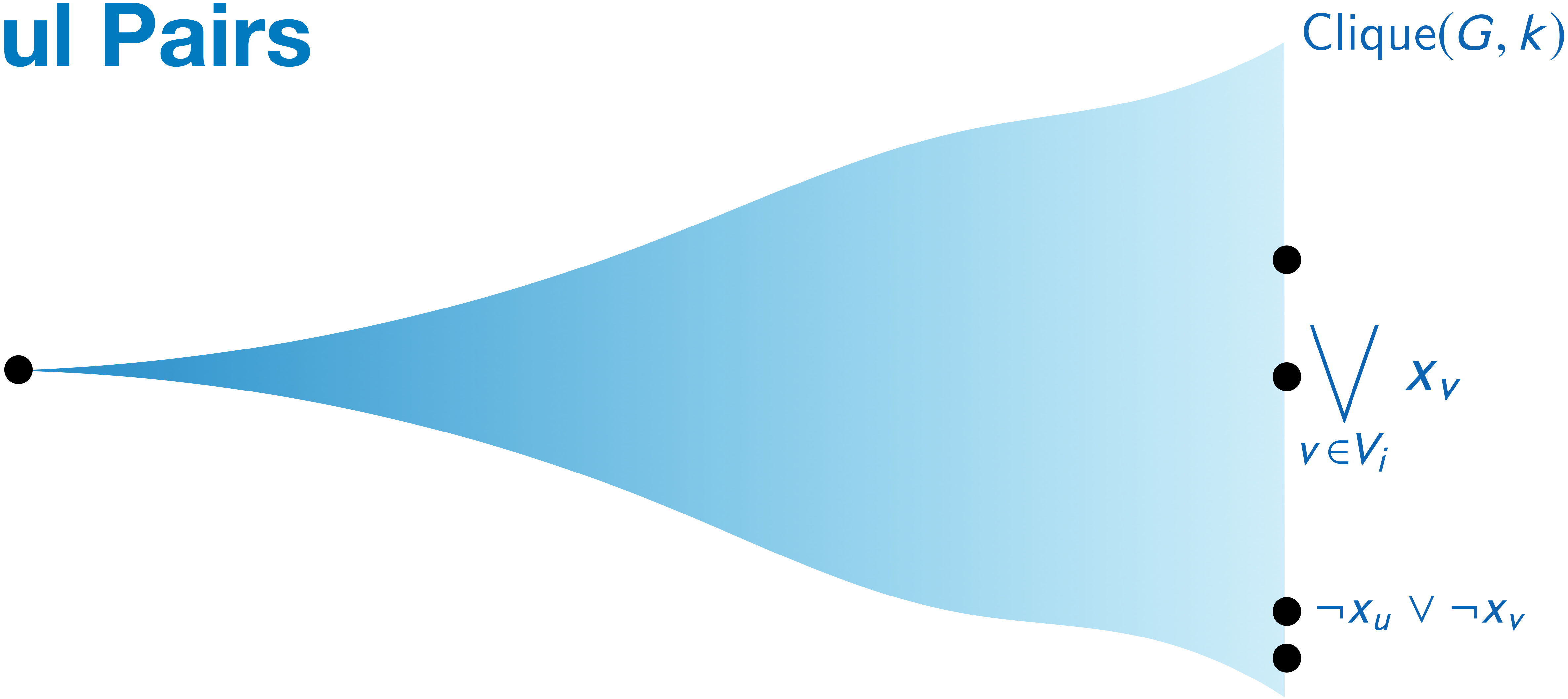


$\beta(a)$ = maximal partial assignment contained in all paths passing through a

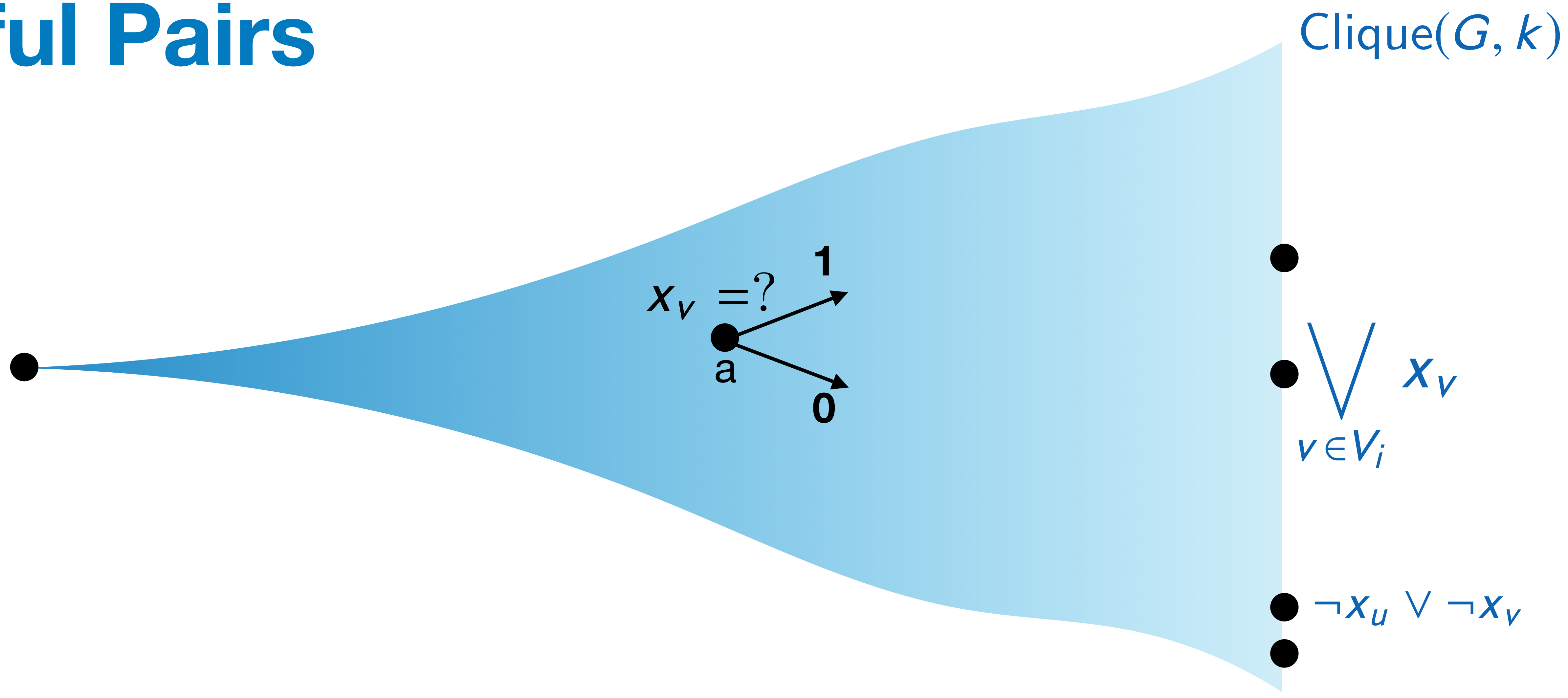
$\boldsymbol{\alpha} \sim \mathcal{D}$ if it is constructed as follows:

- if $v \in V_i$ with i forgotten at a or $\beta(a) \cup \{x_v = 1\}$ falsifies a short axiom of Clique(G, k) then continue with $x_v = 0$
- otherwise toss a coin and with prob $s^{-1/(1-\epsilon)}$ continue with $x_v = 1$

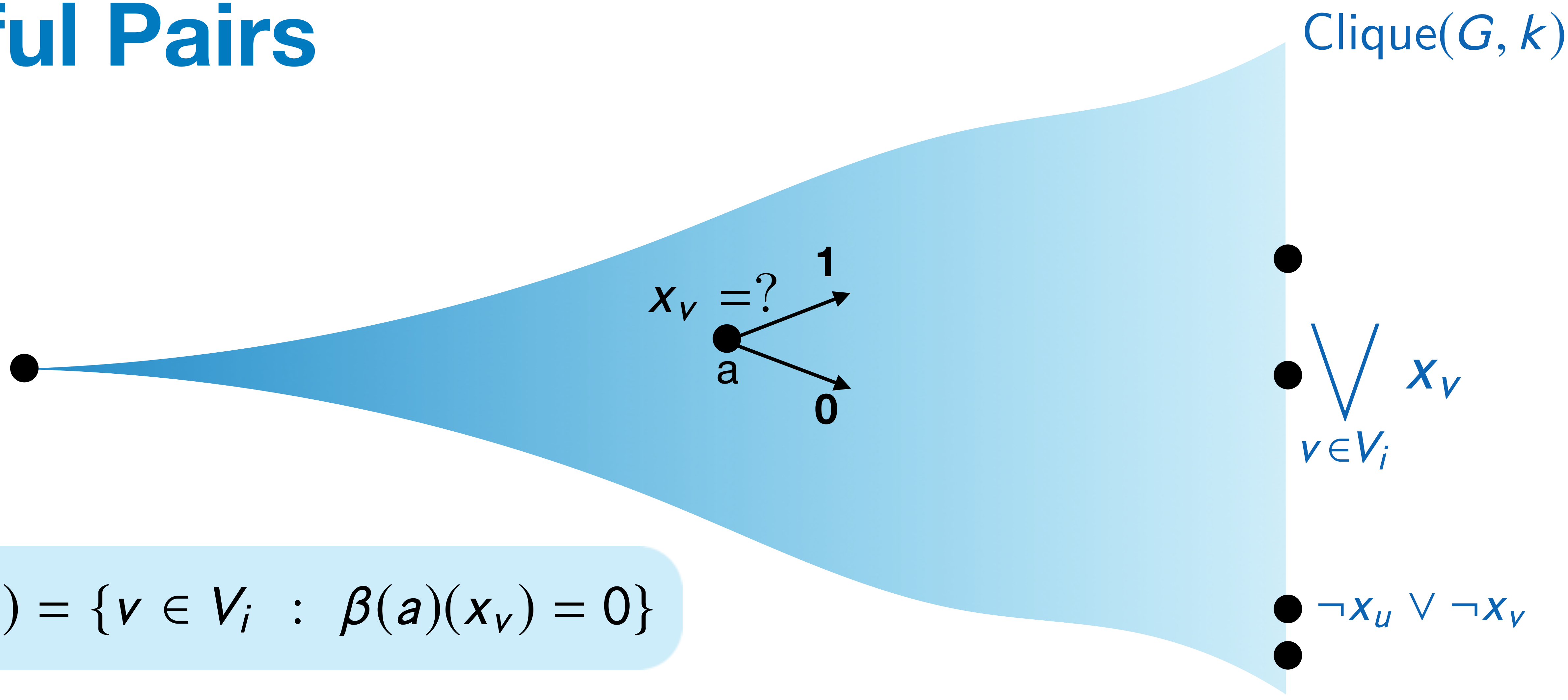
Useful Pairs



Useful Pairs

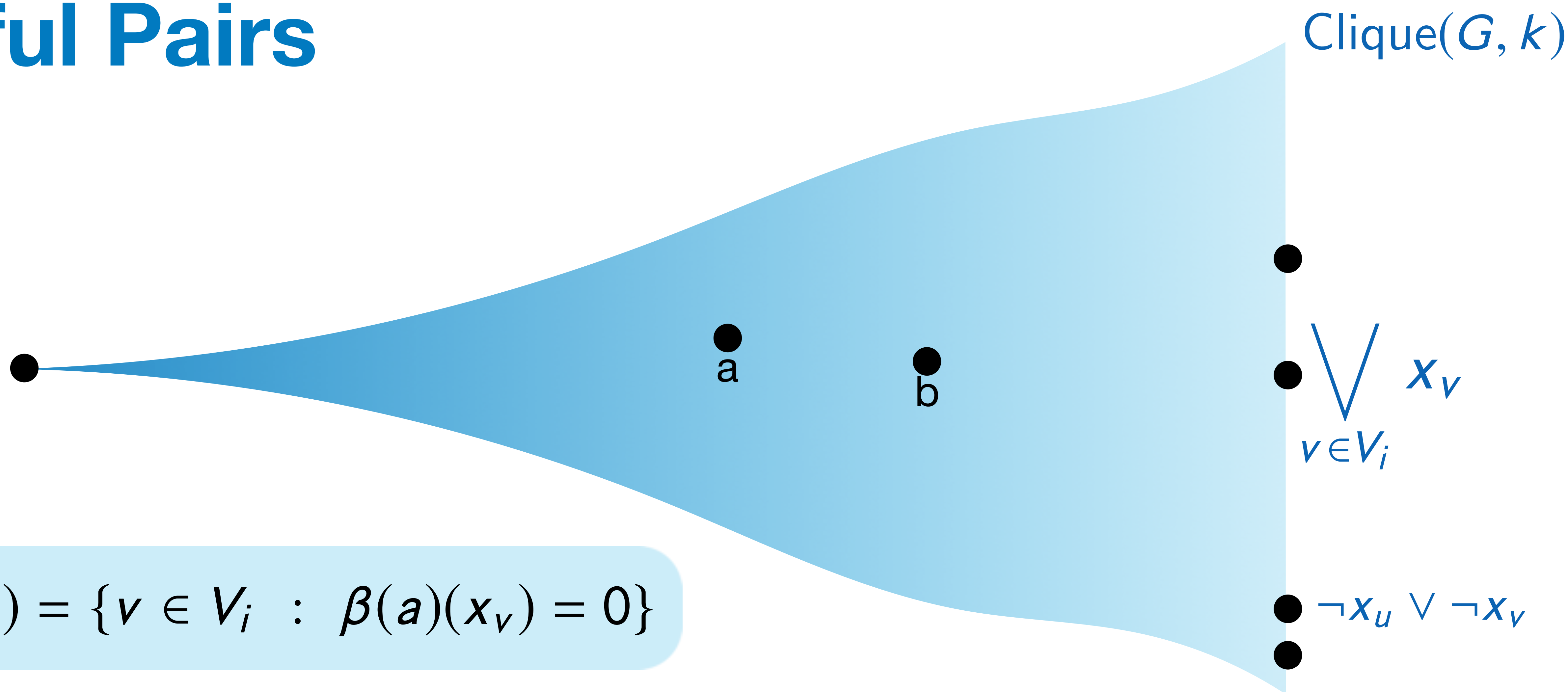


Useful Pairs



$$V_i^0(a) = \{v \in V_i \;:\; \beta(a)(x_v) = 0\}$$

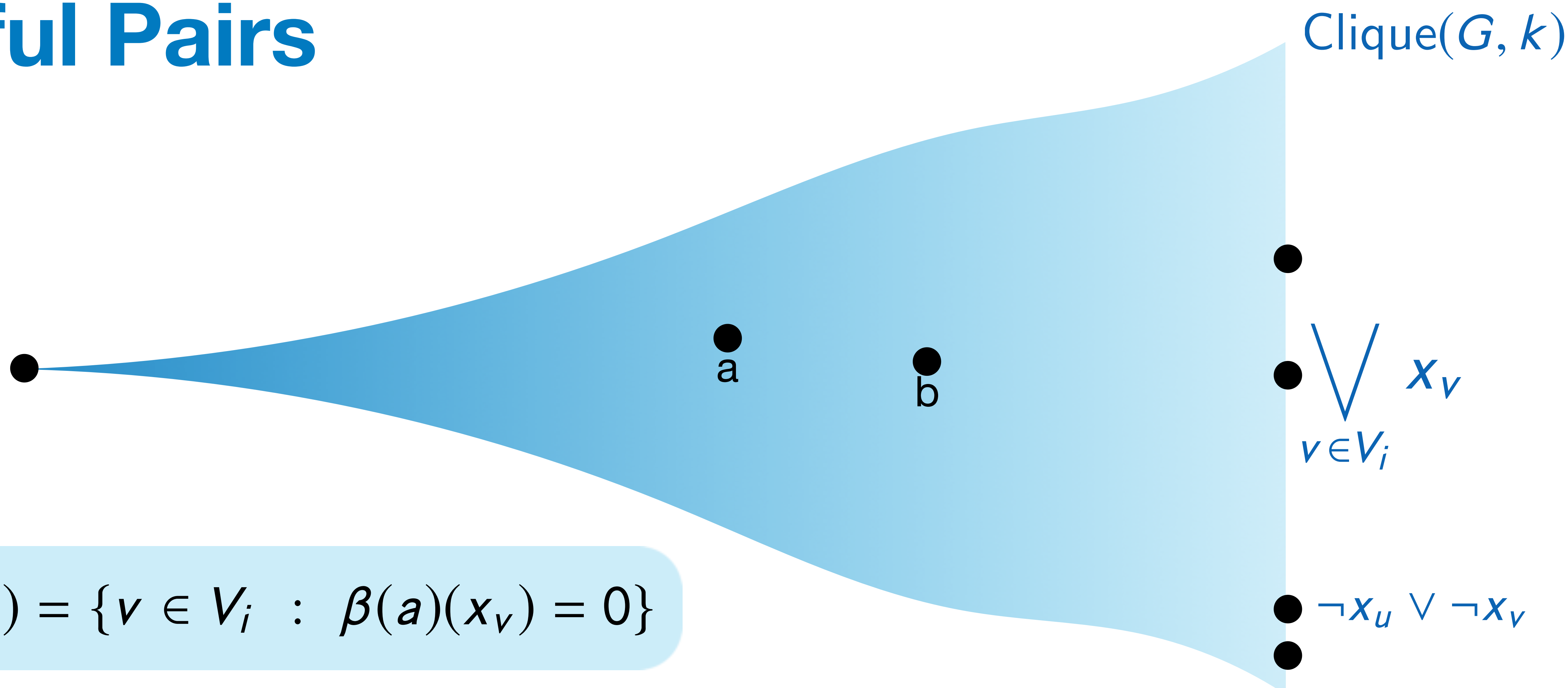
Useful Pairs



$$V_i^0(a) = \{v \in V_i \;:\; \beta(a)(x_v) = 0\}$$

(a, b) is **useful** if exists $i^* \in [k]$ is not forgotten in b st $V_{i^*}^0(b) \setminus V_{i^*}^0(a)$ is (r, q)-dense

Useful Pairs

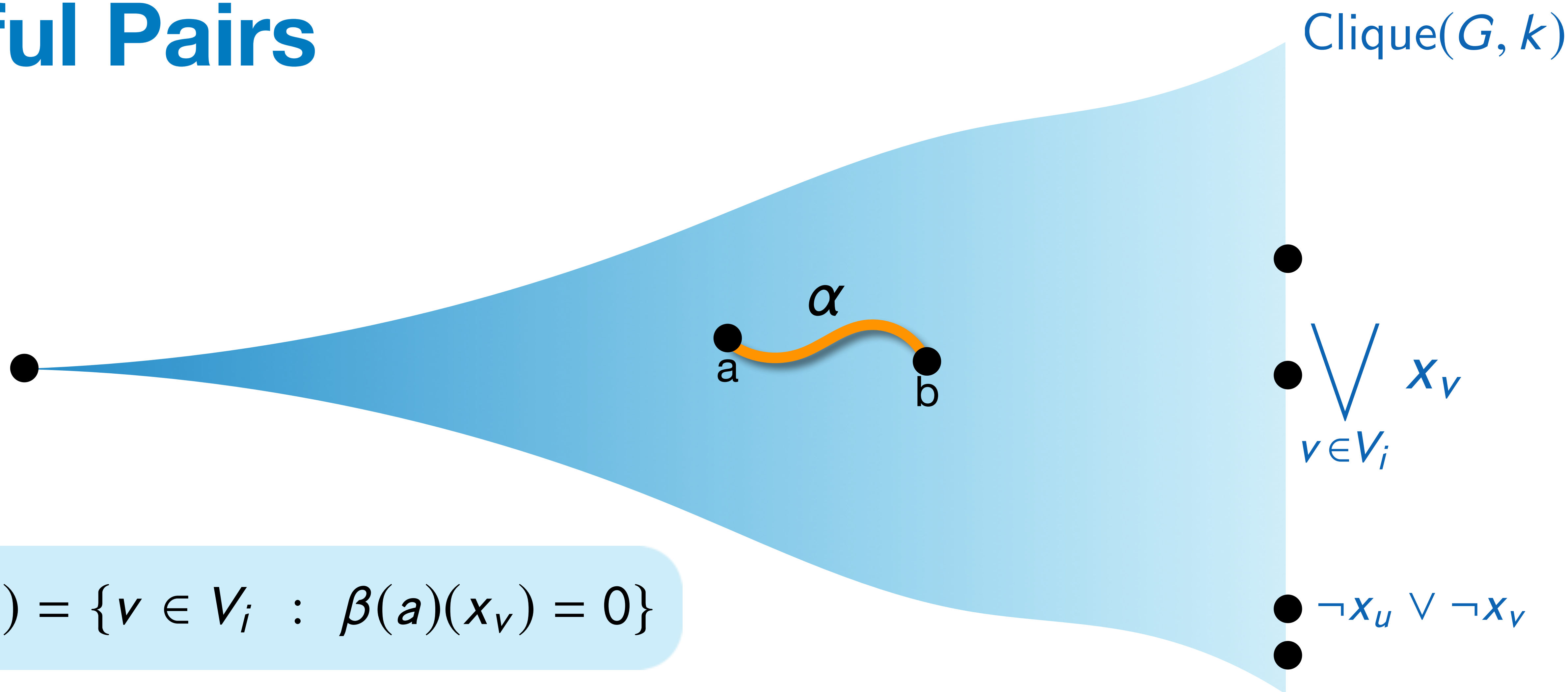


$V_i^0(a) = \{v \in V_i \;:\; \beta(a)(x_v) = 0\}$

(a, b) is **useful** if exists $i^* \in [k]$ is not forgotten in b st
$V_{i^*}^0(b) \setminus V_{i^*}^0(a)$ is (r, q)-dense

W is (r, q)-**dense** if for every $R \subseteq V$ with $|R| \leq r$
it holds that $|\Gamma_W(R)| \geq q$

Useful Pairs



$V_i^0(a) = \{v \in V_i \;:\; \beta(a)(x_v) = 0\}$

(a, b) is **useful** if exists $i^* \in [k]$ is not forgotten in b st $V_{i^*}^0(b) \setminus V_{i^*}^0(a)$ is (r, q)-dense

W is (r, q)-**dense** if for every $R \subseteq V$ with $|R| \leq r$ it holds that $|\Gamma_W(R)| \geq q$

α **usefully** traverses (a, b) if α sets $\leq \lceil k/t \rceil$ variables to 1 between a and b

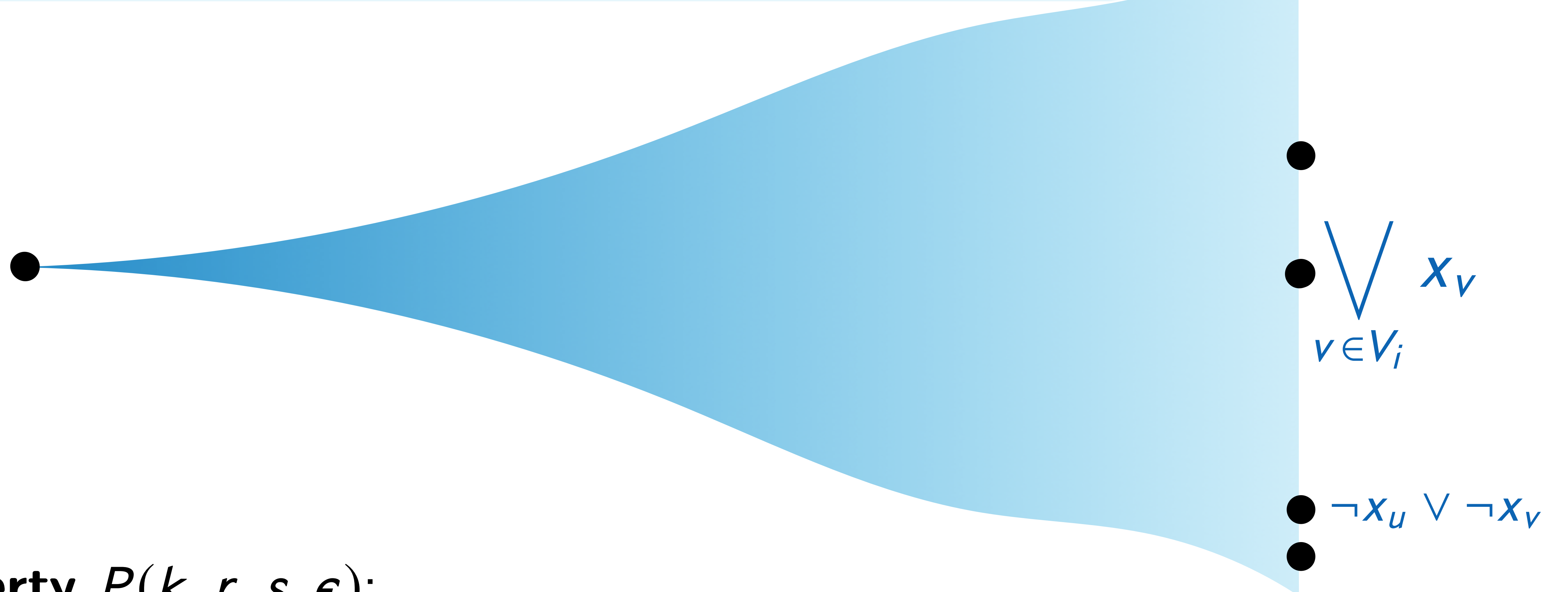
A Bottleneck Counting

Claim 1. Every $\alpha \sim \mathcal{D}$ usefully traverses a useful pair

Claim 2. For every useful pair (a, b), the probability that $\boldsymbol{\alpha} \sim \mathcal{D}$ usefully traverses (a, b) is $\leq 2s^{-\epsilon r}$

Hence the size of the ROBP is $\geq \frac{1}{\sqrt{2}} s^{\epsilon r/2}$ $\square$

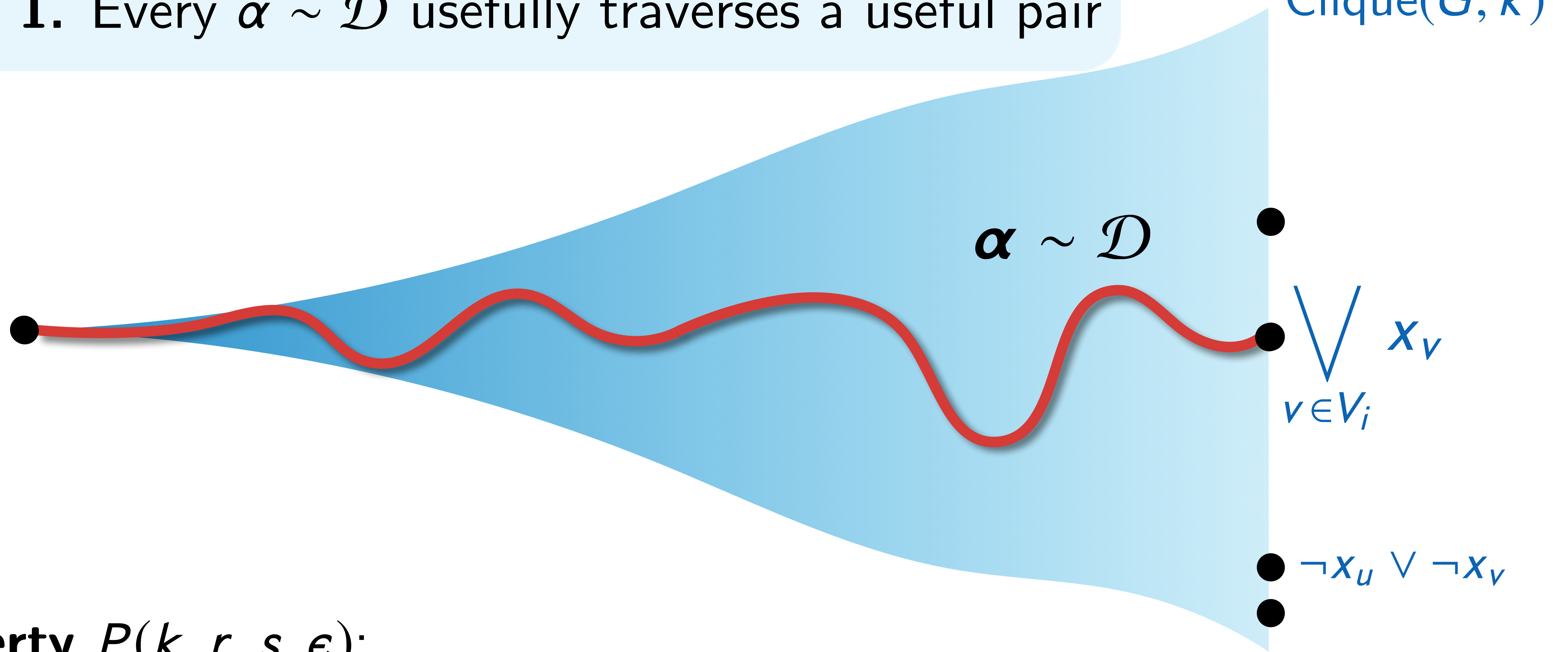
Claim 1. Every $\alpha \sim \mathcal{D}$ usefully traverses a useful pair



property $P(k, r, s, \epsilon)$:
there are $t, q \in \mathbb{R}^+$ s.t.
(1) V_i is (tr, tq)-dense for every $i \in [k]$;
(2) ....

Reminder
- (a, b) is **useful** if exists $i^* \in [k]$ not forgotten in b and $V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ is (r, q)-dense.
- W is (r, q)-**dense** if for every $R \subseteq V$, $|R| \leq r \rightarrow |\Gamma_W(R)| \geq q$.
- α **usefully** traverses (a, b) if α sets $\leq \lceil k/t \rceil$ variables to 1 between a and b

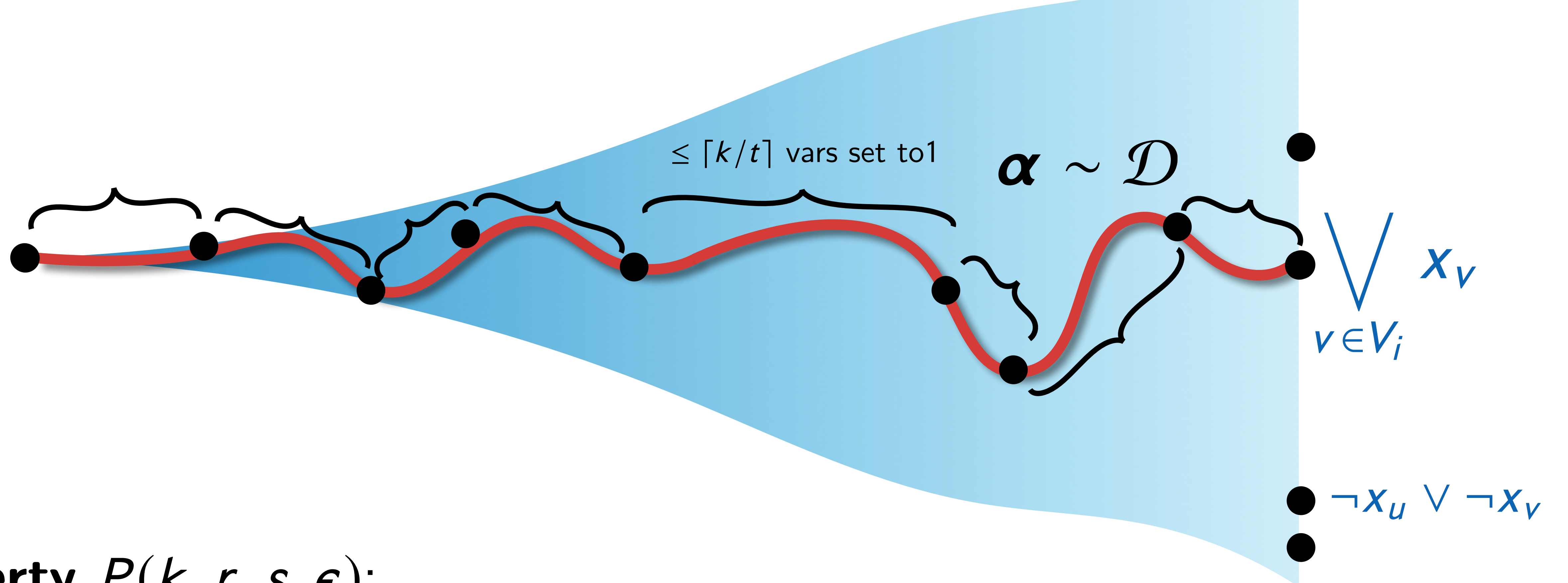
Claim 1. Every $\alpha \sim \mathcal{D}$ usefully traverses a useful pair



property $P(k, r, s, \epsilon)$:
there are $t, q \in \mathbb{R}^+$ s.t.
(1) V_i is (tr, tq)-dense for every $i \in [k]$;
(2) ....

Reminder
- (a, b) is **useful** if exists $i^* \in [k]$ not forgotten in b and $V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ is (r, q)-dense.
- W is (r, q)-**dense** if for every $R \subseteq V$, $|R| \leq r \rightarrow |\Gamma_W(R)| \geq q$.
- α **usefully** traverses (a, b) if α sets $\leq \lceil k/t \rceil$ variables to 1 between a and b

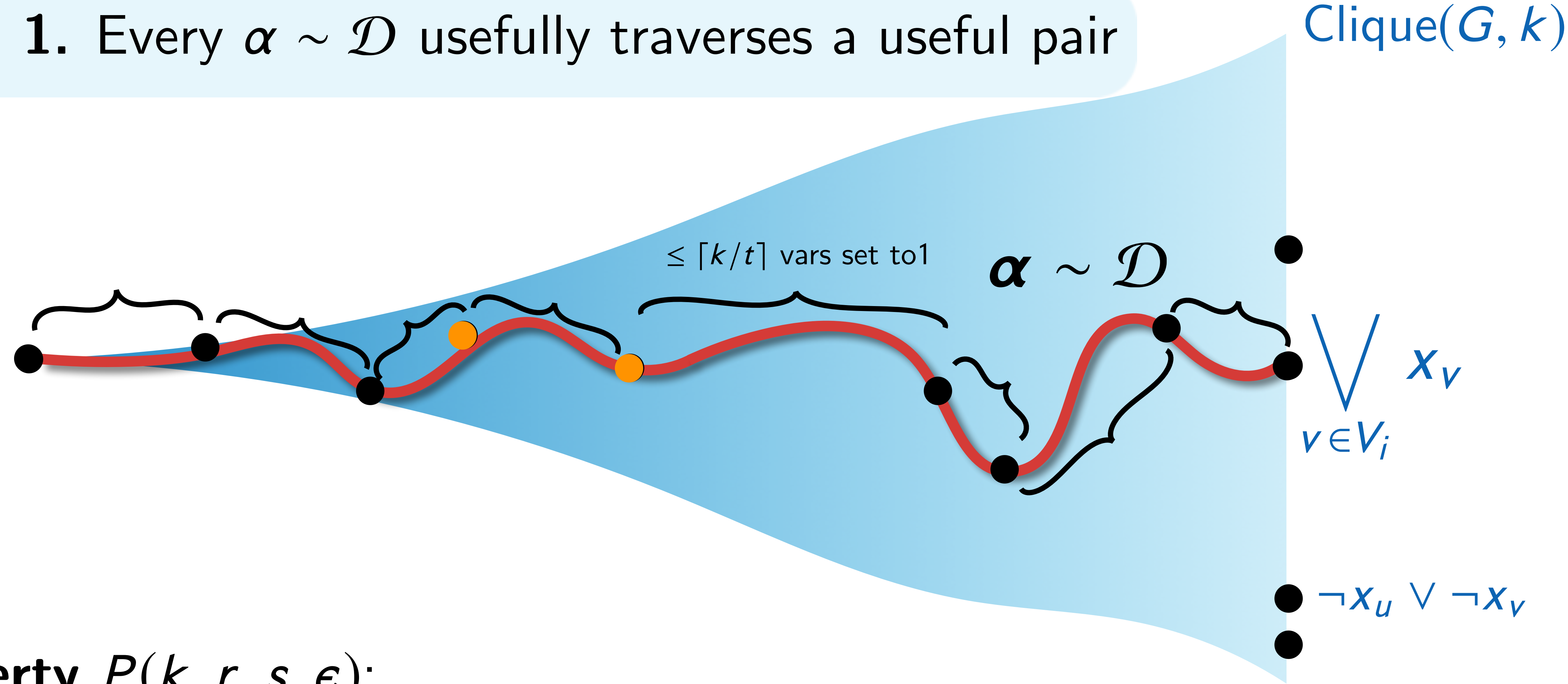
Claim 1. Every $\alpha \sim \mathcal{D}$ usefully traverses a useful pair



property $P(k, r, s, \epsilon)$:
there are $t, q \in \mathbb{R}^+$ s.t.
(1) V_i is (tr, tq)-dense for every $i \in [k]$;
(2) ....

Reminder
- (a, b) is **useful** if exists $i^* \in [k]$ not forgotten in b and $V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ is (r, q)-dense.
- W is (r, q)-**dense** if for every $R \subseteq V$, $|R| \leq r \rightarrow |\Gamma_W(R)| \geq q$.
- α **usefully** traverses (a, b) if α sets $\leq \lceil k/t \rceil$ variables to 1 between a and b

Claim 1. Every $\alpha \sim \mathcal{D}$ usefully traverses a useful pair



property $P(k, r, s, \epsilon)$:
there are $t, q \in \mathbb{R}^+$ s.t.
(1) V_i is (tr, tq)-dense for every $i \in [k]$;
(2) ....

Reminder
- (a, b) is **useful** if exists $i^* \in [k]$ not forgotten in b and $V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ is (r, q)-dense.
- W is (r, q)-**dense** if for every $R \subseteq V$, $|R| \leq r \rightarrow |\Gamma_W(R)| \geq q$.
- α **usefully** traverses (a, b) if α sets $\leq \lceil k/t \rceil$ variables to 1 between a and b

Claim 2. For every useful pair (a, b), the probability that $\boldsymbol{\alpha} \sim \mathcal{D}$ usefully traverses (a, b) is $\leq 2s^{-\epsilon r}$

CASE 1. $|V^1(a)| = |\{v \in V \;:\; \beta(a)(x_v) = 1\}|$ is large.

CASE 2. $|V^1(a)|$ is not large (let $W = V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ and $V^1(\alpha) =$ 1s set by α between a and b)

Reminder
- (a, b) is **useful** if exists $i^* \in [k]$ not forgotten in b and $V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ is (r, q)-dense.
- W is (r, q)-**dense** if for every $R \subseteq V$, $|R| \leq r \to |\Gamma_W(R)| \geq q$.
- α **usefully** traverses (a, b) if α sets $\leq \lceil k/t \rceil$ variables to 1 between a and b

Claim 2. For every useful pair (a, b), the probability that $\boldsymbol{\alpha} \sim \mathcal{D}$ usefully traverses (a, b) is $\leq 2s^{-\epsilon r}$

Case 1. $|V^1(a)| = |\{v \in V \ : \ \beta(a)(x_v) = 1\}|$ is large.

$\Pr(E) \leq s^{-\epsilon r}$ since in the distribution $\mathcal{D}$ choosing 1s is very unlikely

Case 2. $|V^1(a)|$ is not large (let $W = V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ and $V^1(\alpha)$ = 1s set by α between a and b)

Reminder

- (a, b) is **useful** if exists $i^* \in [k]$ not forgotten in b and $V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ is (r, q)-dense.
- W is (r, q)-**dense** if for every $R \subseteq V$, $|R| \leq r \rightarrow |\Gamma_W(R)| \geq q$.
- α **usefully** traverses (a, b) if α sets $\leq \lceil k/t \rceil$ variables to 1 between a and b

Claim 2. For every useful pair (a, b), the probability that $\boldsymbol{\alpha} \sim \mathcal{D}$ usefully traverses (a, b) is $\leq 2s^{-\epsilon r}$

CASE 1. $|V^1(a)| = |\{v \in V \ : \ \beta(a)(x_v) = 1\}|$ is large.

$\Pr(E) \leq s^{-\epsilon r}$ since in the distribution $\mathcal{D}$ choosing 1s is very unlikely

CASE 2. $|V^1(a)|$ is not large (let $W = V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ and $V^1(\alpha) =$ 1s set by α between a and b)

$$\Pr(E) = \Pr(E \wedge |\Gamma_W(V^1(a) \cup V^1(\boldsymbol{\alpha}))| \text{ is large}) \tag{1}$$
$$+ \Pr(E \wedge |\Gamma_W(V^1(a) \cup V^1(\boldsymbol{\alpha}))| \text{ is not large}) \tag{2}$$

Reminder
- (a, b) is **useful** if exists $i^* \in [k]$ not forgotten in b and $V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ is (r, q)-dense.
- W is (r, q)-**dense** if for every $R \subseteq V$, $|R| \leq r \rightarrow |\Gamma_W(R)| \geq q$.
- α **usefully** traverses (a, b) if α sets $\leq \lceil k/t \rceil$ variables to 1 between a and b

Claim 2. For every useful pair (a, b), the probability that $\boldsymbol{\alpha} \sim \mathcal{D}$ usefully traverses (a, b) is $\leq 2s^{-\epsilon r}$

CASE 1. $|V^1(a)| = |\{v \in V \;:\; \beta(a)(x_v) = 1\}|$ is large.

$\Pr(E) \leq s^{-\epsilon r}$ since in the distribution $\mathcal{D}$ choosing 1s is very unlikely

CASE 2. $|V^1(a)|$ is not large (let $W = V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ and $V^1(\alpha) =$ 1s set by α between a and b)

$$\Pr(E) = \Pr(E \wedge |\Gamma_W(V^1(a) \cup V^1(\boldsymbol{\alpha}))| \text{ is large}) \tag{1}$$
$$+ \Pr(E \wedge |\Gamma_W(V^1(a) \cup V^1(\boldsymbol{\alpha}))| \text{ is not large}) \tag{2}$$

(1) $\leq s^{-\epsilon r}$ from the fact that many 0s in W are coin tosses
(2) $\leq s^{-\epsilon r}$ from $P(k, r, s, \epsilon)$: the ones in $V^1(\alpha)$ "are concentrated"

Reminder
- (a, b) is **useful** if exists $i^* \in [k]$ not forgotten in b and $V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ is (r, q)-dense.
- W is (r, q)-**dense** if for every $R \subseteq V$, $|R| \leq r \rightarrow |\Gamma_W(R)| \geq q$.
- α **usefully** traverses (a, b) if α sets $\leq \lceil k/t \rceil$ variables to 1 between a and b

Claim 2. For every useful pair (a, b), the probability that $\boldsymbol{\alpha} \sim \mathcal{D}$ usefully traverses (a, b) is $\leq 2s^{-\epsilon r}$

Case 1: $|V^1(a)| \geq \epsilon r$

$$\Pr_{\boldsymbol{\alpha} \sim \mathcal{D}}(\boldsymbol{\alpha} \text{ passes through } a) \leq (s^{-1/(1-\epsilon)})^{\epsilon r} \leq s^{-\epsilon r}$$

Reminder
- (a, b) is **useful** if exists $i^* \in [k]$ not forgotten in b and $V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ is (r, q)-dense.
- W is (r, q)-**dense** if for every $R \subseteq V$, $|R| \leq r \to |\Gamma_W(R)| \geq q$.
- α **usefully** traverses (a, b) if α sets $\leq \lceil k/t \rceil$ variables to 1 between a and b

Claim 2. For every useful pair (a, b), the probability that $\boldsymbol{\alpha} \sim \mathcal{D}$ usefully traverses (a, b) is $\leq 2s^{-\epsilon r}$

CASE 2.1: $|V^1(a)| < \epsilon r$

$$
\begin{aligned}
\Pr_{\boldsymbol{\alpha}\sim\mathcal{D}}(\ E \ \wedge |\Gamma_W(V^1(a) \cup V^1(\boldsymbol{\alpha}))| \leq rs^{1/(1-\epsilon)} \log s\ ) \\
\leq \Pr(\ |V^1(\boldsymbol{\alpha}) \cap S| \geq (1-\epsilon)r\ ) \\
\leq \binom{|S|}{(1-\epsilon)r} (s^{-1/(1-\epsilon)})^{(1-\epsilon)r} \\
\leq |S|^{(1-\epsilon)r} s^{-r} \\
\leq s^{-\epsilon r}
\end{aligned}
$$

property $P(k, r, s, \epsilon)$:
there are $t, q \in \mathbb{R}^+$ s.t.
(1) V_i is (tr, tq)-dense for every $i \in [k]$;
(2) for every $W \subseteq V$ (r, q)-dense there is a set $S \subseteq V$ with $|S| \leq s$ s.t. every $R \subseteq V$ with $|R| \leq \epsilon r + \lceil k/t \rceil$ and $|\Gamma_W(R)| \leq rs^{1/(1-\epsilon)} \log s$ we have that $|R \cap S| \geq r$

Reminder
- (a, b) is **useful** if exists $i^* \in [k]$ not forgotten in b and $V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ is (r, q)-dense.
- W is (r, q)-**dense** if for every $R \subseteq V$, $|R| \leq r \to |\Gamma_W(R)| \geq q$.
- α **usefully** traverses (a, b) if α sets $\leq \lceil k/t \rceil$ variables to 1 between a and b

Claim 2. For every useful pair (a, b), the probability that $\boldsymbol{\alpha} \sim \mathcal{D}$ usefully traverses (a, b) is $\leq 2s^{-\epsilon r}$

CASE 2.2: $|V^1(a)| < \epsilon r$

$$\Pr_{\boldsymbol{\alpha}\sim\mathcal{D}}(\ E \ \wedge |\Gamma_W(V^1(a) \cup V^1(\boldsymbol{\alpha}))| \geq r s^{1/(1-\epsilon)} \log s\ )$$
$$\leq (1 - s^{-1/(1-\epsilon)})^{r s^{1/(1-\epsilon)} \log s}$$
$$\leq e^{-r \log s}$$
$$\leq s^{-\epsilon r}$$

property $P(k, r, s, \epsilon)$:
there are $t, q \in \mathbb{R}^+$ s.t.
(1) V_i is (tr, tq)-dense for every $i \in [k]$;
(2) for every $W \subseteq V$ (r, q)-dense there is a set $S \subseteq V$ with $|S| \leq s$ s.t. every $R \subseteq V$ with $|R| \leq \epsilon r + \lceil k/t \rceil$ and $|\Gamma_W(R)| \leq r s^{1/(1-\epsilon)} \log s$ we have that $|R \cap S| \geq r$

Reminder
- (a, b) is **useful** if exists $i^* \in [k]$ not forgotten in b and $V^0_{i^*}(b) \setminus V^0_{i^*}(a)$ is (r, q)-dense.
- W is (r, q)-**dense** if for every $R \subseteq V$, $|R| \leq r \rightarrow |\Gamma_W(R)| \geq q$.
- α **usefully** traverses (a, b) if α sets $\leq \lceil k/t \rceil$ variables to 1 between a and b

Conclusions

Take Away Message

- k-clique a fundamental problem
- $n^{\Omega(k)}$ l.b. for small-ish k in regular resolution
- w.h.p. for Erdős-Rényi random graphs

bonacina@cs.upc.edu

Conclusions

Take Away Message

- k-clique a fundamental problem
- $n^{\Omega(k)}$ l.b. for small-ish k in regular resolution
- w.h.p. for Erdős-Rényi random graphs

Open Problems

- Ramsey graphs
- General resolution (and stronger systems)

bonacina@cs.upc.edu

Conclusions

Take Away Message

- k-clique a fundamental problem
- $n^{\Omega(k)}$ l.b. for small-ish k in regular resolution
- w.h.p. for Erdős-Rényi random graphs

Open Problems

- Ramsey graphs
- General resolution (and stronger systems)

Thanks!

bonacina@cs.upc.edu