Automata, Games & Verification

Summary #3

Today at 2:15pm in SR 016:
Seminar “Games, Synthesis, and Robotics”
Synthesis of Reactive(1) Designs

Deterministic Büchi Automata

Theorem 1. *The ω-language $(a + b)^* b^\omega$ is not recognizable by a deterministic Büchi automaton.*

Definition 1. [Substrings] *Let $\alpha \in \Sigma^*$. For two integers $n \leq m$ we define*

$$\alpha(n, m) = \alpha(n)\alpha(n+1)\ldots\alpha(m) \ .$$

Definition 2. [Limit] *For $W \subseteq \Sigma^*$:*

$$\overrightarrow{W} = \{\alpha \in \Sigma^\omega \mid \textit{there exist infinitely many } n \in \omega \textit{ s.t. } \alpha(0, n) \in W\} \ .$$

Theorem 2. *An ω-language $L \subseteq \Sigma^\omega$ is recognizable by a deterministic Büchi automaton iff there is a regular language $W \subseteq \Sigma^*$ s.t. $L = \overrightarrow{W}$.*

Theorem 3. *For any deterministic Büchi automaton $\mathcal{A}$, there exists a Büchi automaton $\mathcal{A}'$ such that $\mathcal{L}(\mathcal{A}') = \Sigma^\omega \setminus \mathcal{L}(\mathcal{A})$.*

Proof: We construct $\mathcal{A}'$ as follows:

- $S' = (S \times \{0\}) \cup ((S \setminus F) \times \{1\})$.
- $I' = I \times \{0\}$.
- $T' = \{((s,0),\sigma,(s',0)) \mid (s,\sigma,s') \in T\}$
  $\cup\ \{((s,0),\sigma,(s',1)) \mid (s,\sigma,s') \in T, s' \in S - F\}$
  $\cup\ \{((s,1),\sigma,(s,1)) \mid (s,\sigma,s') \in T, s' \in S - F\}$.
- $F' = (S - F) \times \{1\}$.

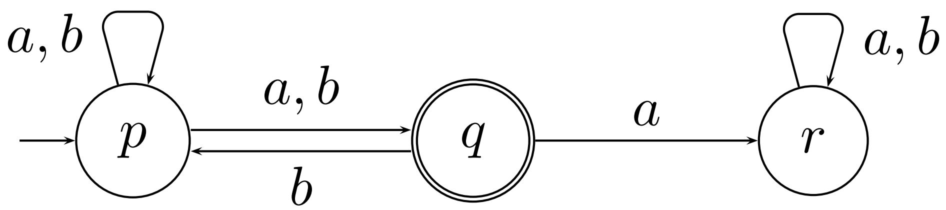
■

Complementation of Nondeterministic Büchi Automata

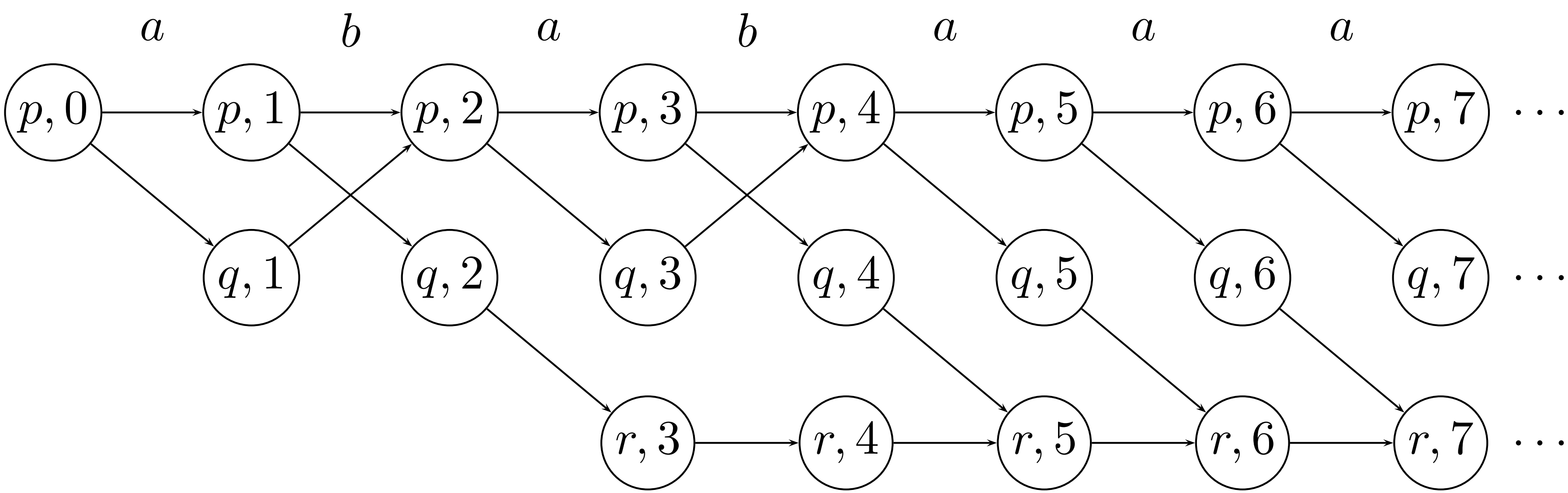
Definition 3. *Let* $\mathcal{A} = (S, I, T, F)$ *be a nondeterministic Büchi automaton. The run DAG of* $\mathcal{A}$ *on a word* $\alpha \in \Sigma^\omega$ *is the directed acyclic graph* $G = (V, E)$ *where*

- $V = \bigcup_{l \geqslant 0} (S_l \times \{l\})$ *where* $S_0 = I$ *and* $S_{l+1} = \bigcup_{s \in S_l, (s, \alpha(l), s') \in T} \{s'\}$
- $E = \{(\langle s, l \rangle, \langle s', l+1 \rangle) \mid l \geqslant 0, (s, \alpha(l), s') \in T\}$

A path in a run DAG is accepting iff it visits F infinitely often.
The automaton accepts α if some path is accepting.



a, b
a, b
a, b
b
a
p
q
r



a
b
a
b
a
a
a
p, 0
p, 1
p, 2
p, 3
p, 4
p, 5
p, 6
p, 7
q, 1
q, 2
q, 3
q, 4
q, 5
q, 6
q, 7
r, 3
r, 4
r, 5
r, 6
r, 7

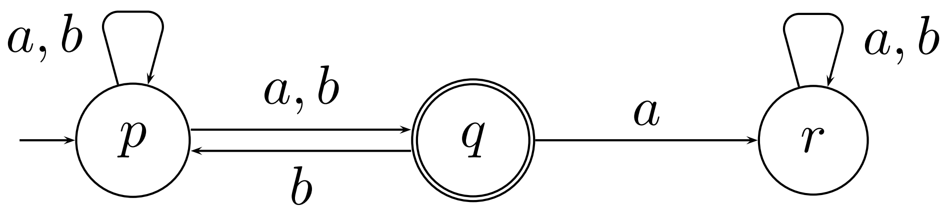
Definition 4. *A ranking for G is a function $f : V \rightarrow \{0, \ldots, 2 \cdot |S|\}$ such that*

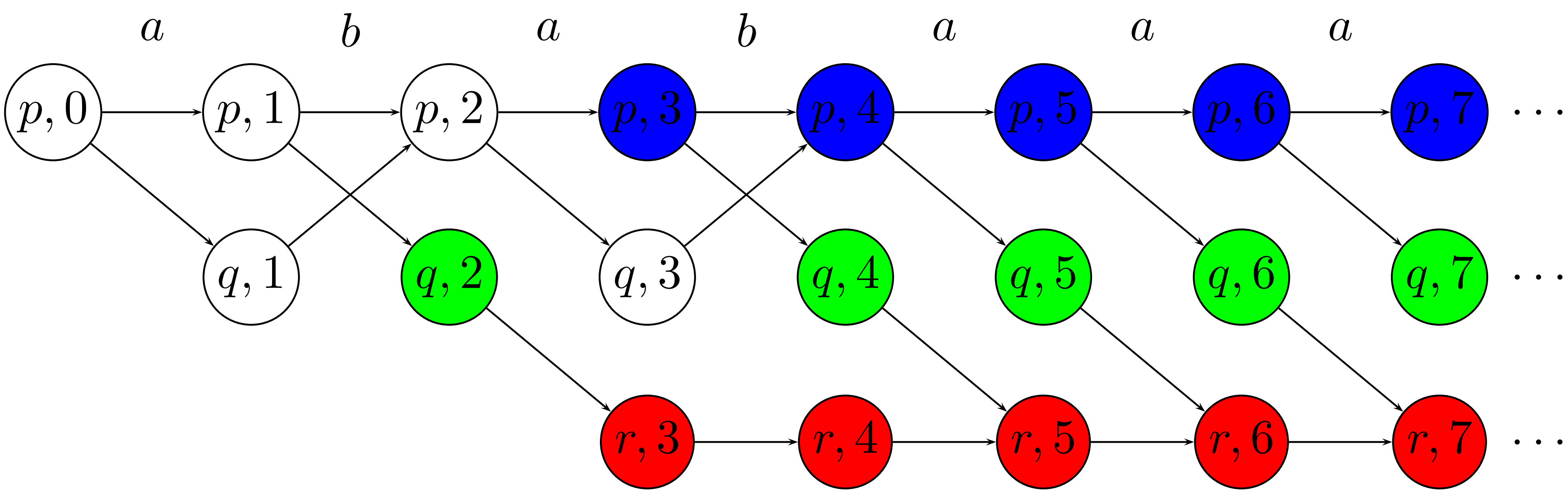
- *for all $\langle s, l \rangle \in V$, if $f(\langle s, l \rangle)$ is odd then $s \notin F$;*
- *for all $(\langle s, l \rangle, \langle s', l' \rangle) \in E$, $f(\langle s', l' \rangle) \leqslant f(\langle s, l \rangle)$.*

A ranking is odd iff for all paths $\langle s_0, l_0 \rangle, \langle s_1, l_1 \rangle, \langle s_2, l_2 \rangle, \ldots$ in G,
there is a $i \geqslant 0$ such that $f(\langle s_i, l_i \rangle)$ is odd and,
for all $j \geqslant 0$, $f(\langle s_{i+j}, l_{i+j} \rangle) = f(\langle s_i, l_i \rangle)$.

Lemma 1.

If there exists an odd ranking for G, then $\mathcal{A}$ does not accept α.





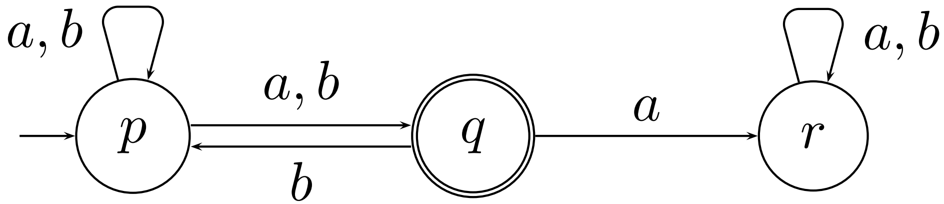
rank 1 — rank 2 — rank 3 — rank 4

Let G' be a subgraph of G. We call a vertex $\langle s, l \rangle$

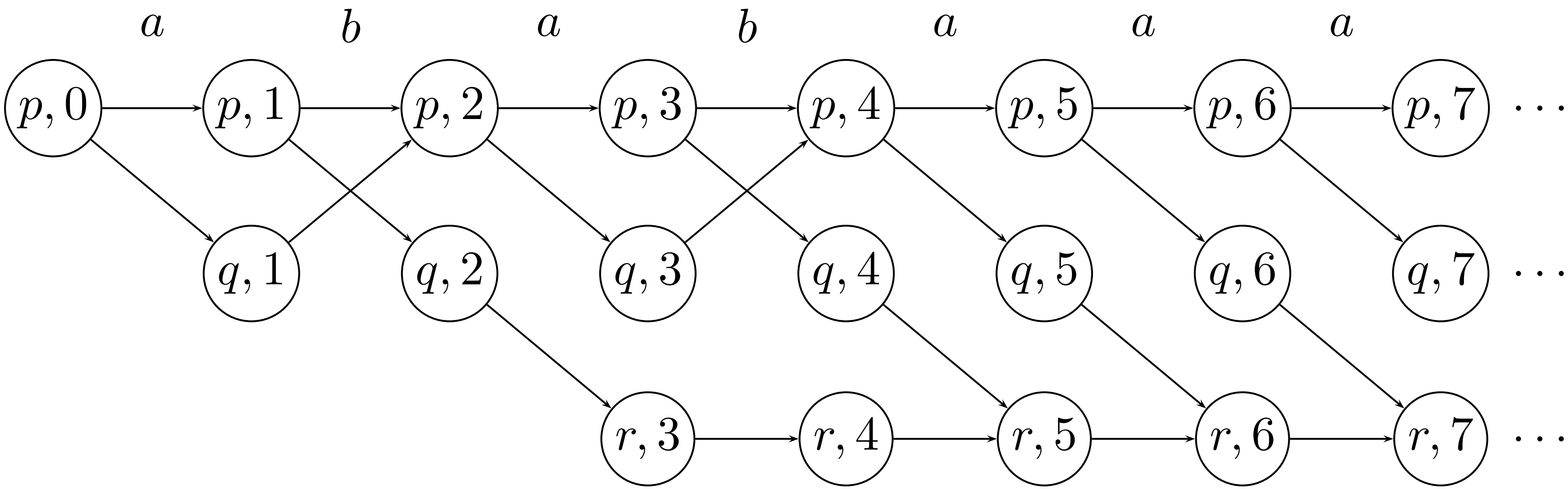
- safe in G' if for all vertices $\langle s', l' \rangle$ reachable from $\langle s, l \rangle$, $s' \notin F$, and
- endangered in G' if only finitely many vertices are reachable.

We define an infinite sequence $G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots$ of DAGs inductively as follows:

- $G_0 = G$
- $G_{2i+1} = G_{2i} \setminus \{\langle s, l \rangle \mid \langle s, l \rangle$ is endangered in $G_{2i}\}$
- $G_{2i+2} = G_{2i+1} \setminus \{\langle s, l \rangle \mid \langle s, l \rangle$ is safe in $G_{2i}\}$.

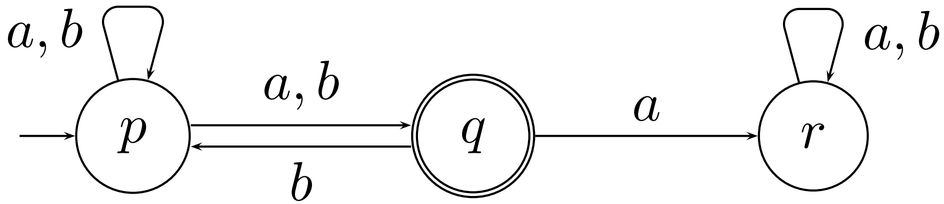


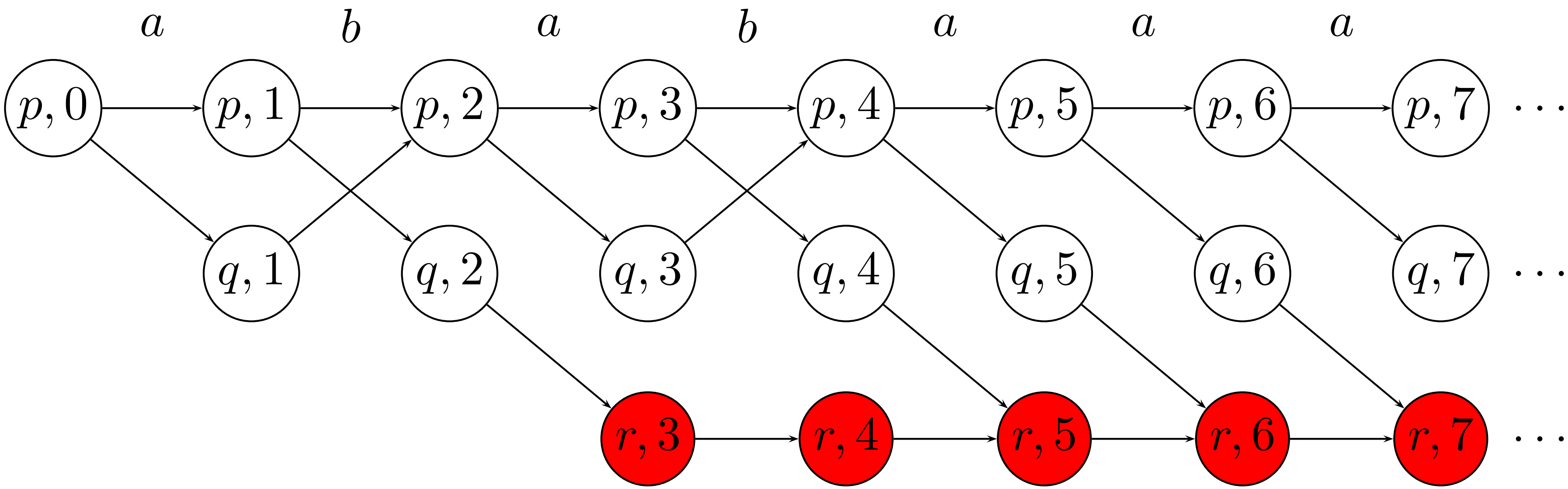
a, b
a, b
p
q
r
b
a
a, b



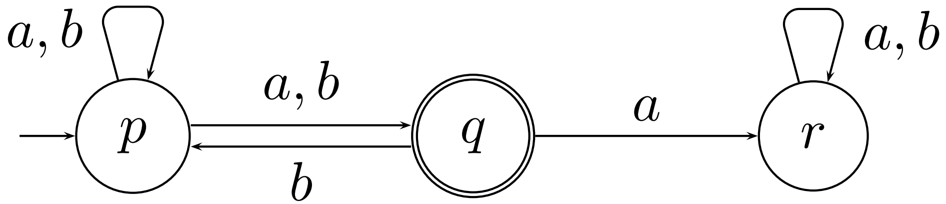
a
b
a
b
a
a
a
p, 0
p, 1
p, 2
p, 3
p, 4
p, 5
p, 6
p, 7
...
q, 1
q, 2
q, 3
q, 4
q, 5
q, 6
q, 7
...
r, 3
r, 4
r, 5
r, 6
r, 7
...

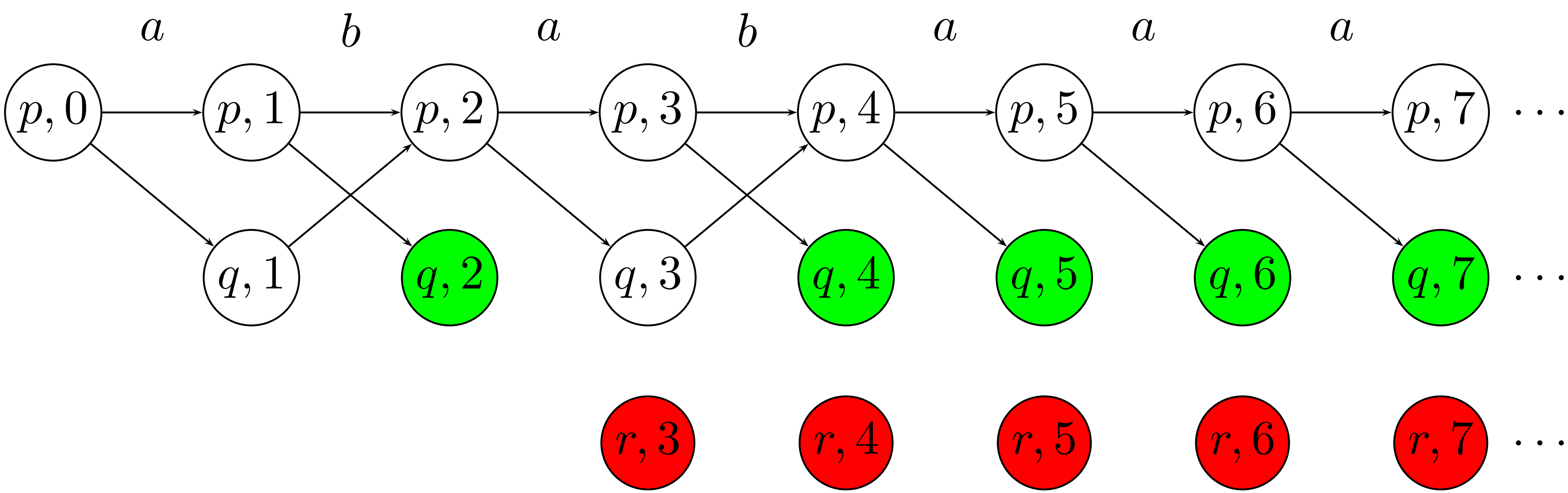
$$G = G_0 = G_1$$


a, b
p
a, b
b
q
a
r
a, b

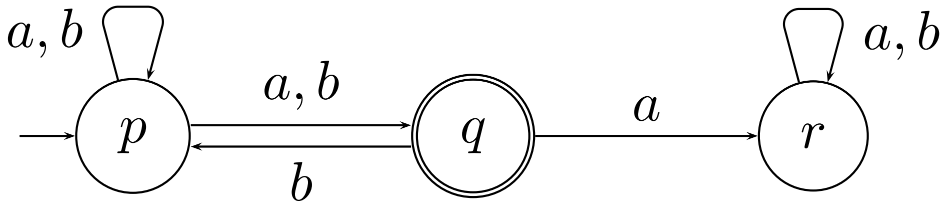

a
b
a
b
a
a
a
p, 0
p, 1
p, 2
p, 3
p, 4
p, 5
p, 6
p, 7
q, 1
q, 2
q, 3
q, 4
q, 5
q, 6
q, 7
r, 3
r, 4
r, 5
r, 6
r, 7

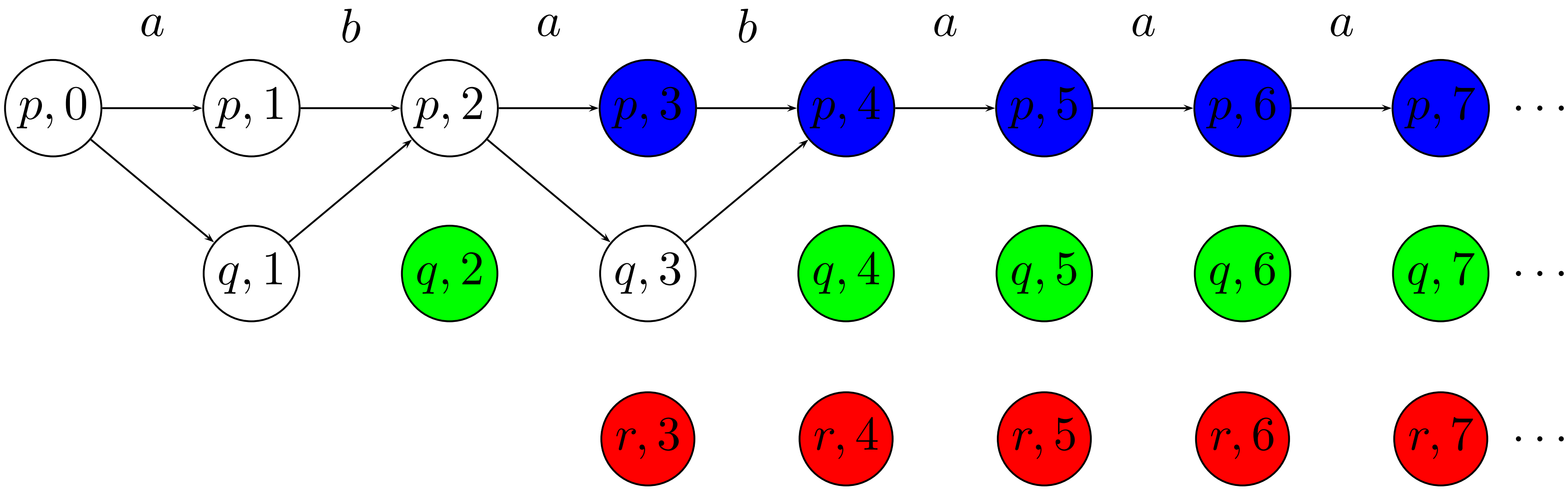
G_1


a, b
a, b
p
q
b
a
r
a, b

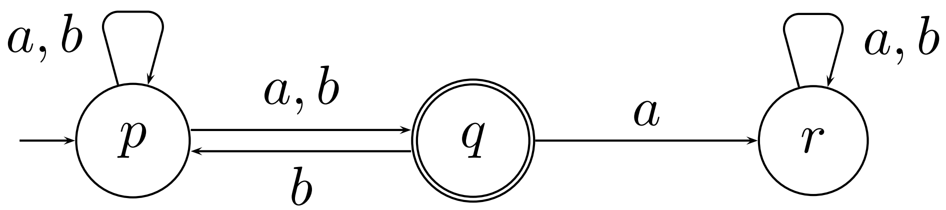

a
b
a
b
a
a
a
p, 0
p, 1
p, 2
p, 3
p, 4
p, 5
p, 6
p, 7
. . .
q, 1
q, 2
q, 3
q, 4
q, 5
q, 6
q, 7
. . .
r, 3
r, 4
r, 5
r, 6
r, 7
. . .

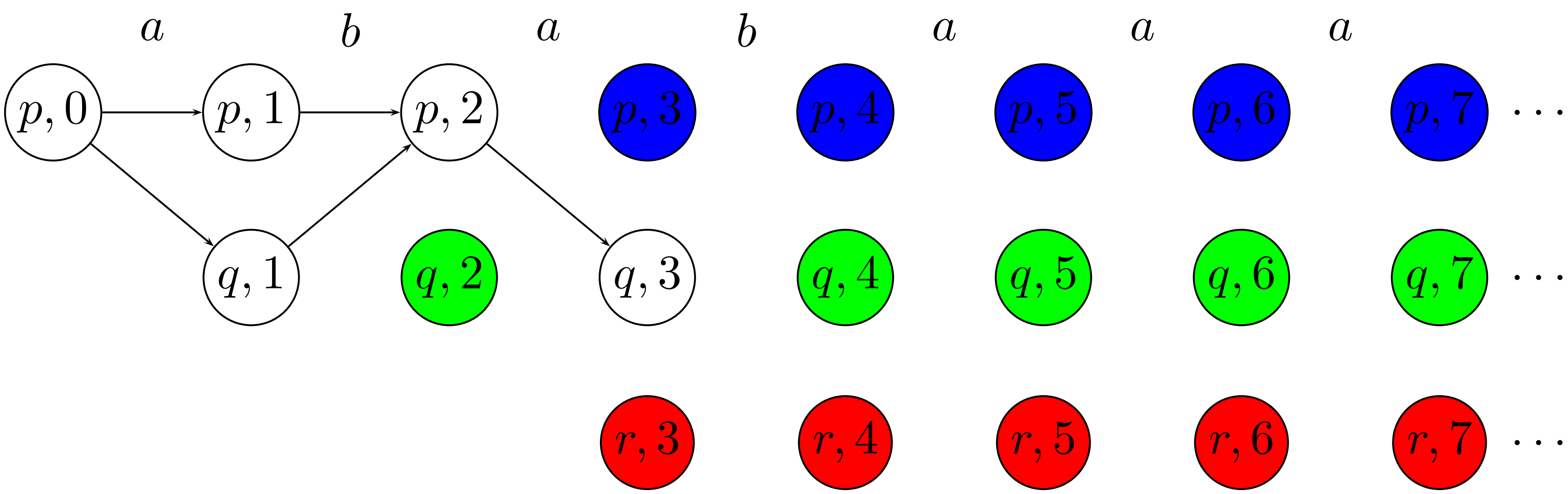
G_2


a, b
a, b
p
q
r
b
a
a, b

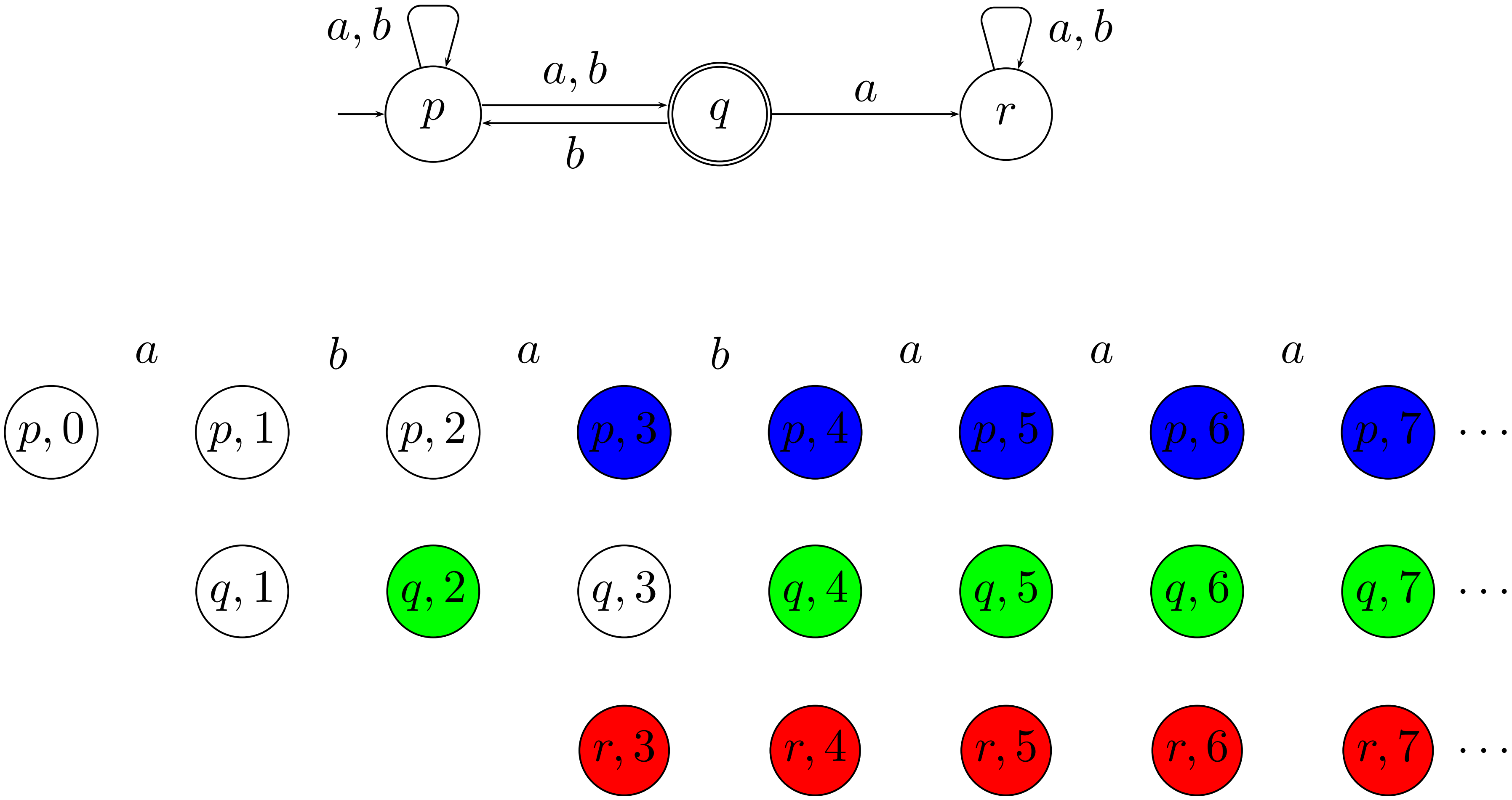

a
b
a
b
a
a
a
p, 0
p, 1
p, 2
p, 3
p, 4
p, 5
p, 6
p, 7
q, 1
q, 2
q, 3
q, 4
q, 5
q, 6
q, 7
r, 3
r, 4
r, 5
r, 6
r, 7

G_3


a, b
a, b
p
q
b
a
r
a, b


a b a b a a a
p, 0
p, 1
p, 2
p, 3
p, 4
p, 5
p, 6
p, 7
q, 1
q, 2
q, 3
q, 4
q, 5
q, 6
q, 7
r, 3
r, 4
r, 5
r, 6
r, 7

G_4


a, b
a, b
a, b
b
a
p
q
r
a b a b a a a
p, 0
p, 1
p, 2
p, 3
p, 4
p, 5
p, 6
p, 7
q, 1
q, 2
q, 3
q, 4
q, 5
q, 6
q, 7
r, 3
r, 4
r, 5
r, 6
r, 7
. . .
. . .
. . .

G_5

Lemma 2.

If $\mathcal{A}$ does not accept α, then the following holds:
For every $i \geqslant 0$ there exists an l_i such that
for all $j \geqslant l_i$ at most $|S| - i$ vertices of the form $\langle \_, j \rangle$ are in G_{2i}.

Proof by induction on i:

- $i = 0$: In G, for every l, there are at most $|S|$ vertices of the form $\langle \_, l \rangle$.
- $i \rightarrow i + 1$:

Proof by induction on i:

- $i = 0$: In G, for every l, there are at most $|S|$ vertices of the form $\langle \_, l \rangle$.
- $i \rightarrow i + 1$:
  - Case G_{2i} is finite: then $G_{2(i+1)}$ is empty.
  - Case G_{2i} is infinite:

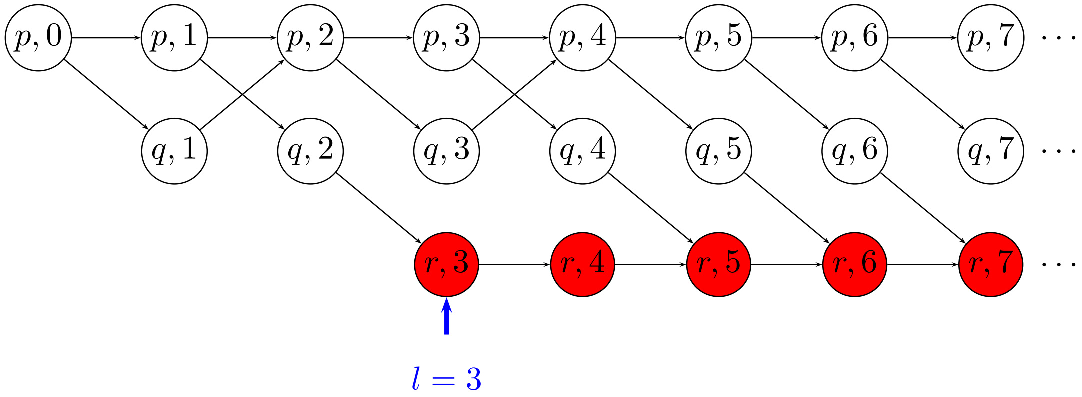
- $G_0 = G$
- $G_{2i+1} = G_{2i} \setminus \{\langle s, l \rangle \mid \langle s, l \rangle$ is endangered in $G_{2i}\}$
- $G_{2i+2} = G_{2i+1} \setminus \{\langle s, l \rangle \mid \langle s, l \rangle$ is safe in $G_{2i}\}$.

Proof by induction on i:

- $i = 0$: In G, for every l, there are at most $|S|$ vertices of the form $\langle \_, l\rangle$.

- $i \rightarrow i+1$:

  – Case G_{2i} is finite: then $G_{2(i+1)}$ is empty.
  – Case G_{2i} is infinite:
    * There must exist a safe vertex $\langle s, l\rangle$ in G_{2i+1}. (Otherwise, we can construct a path in G with infinitely many visits to F).



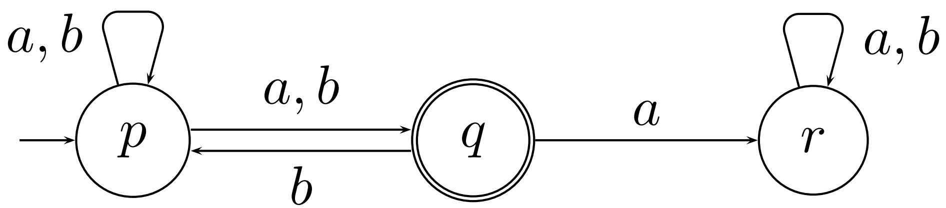
Proof by induction on i:

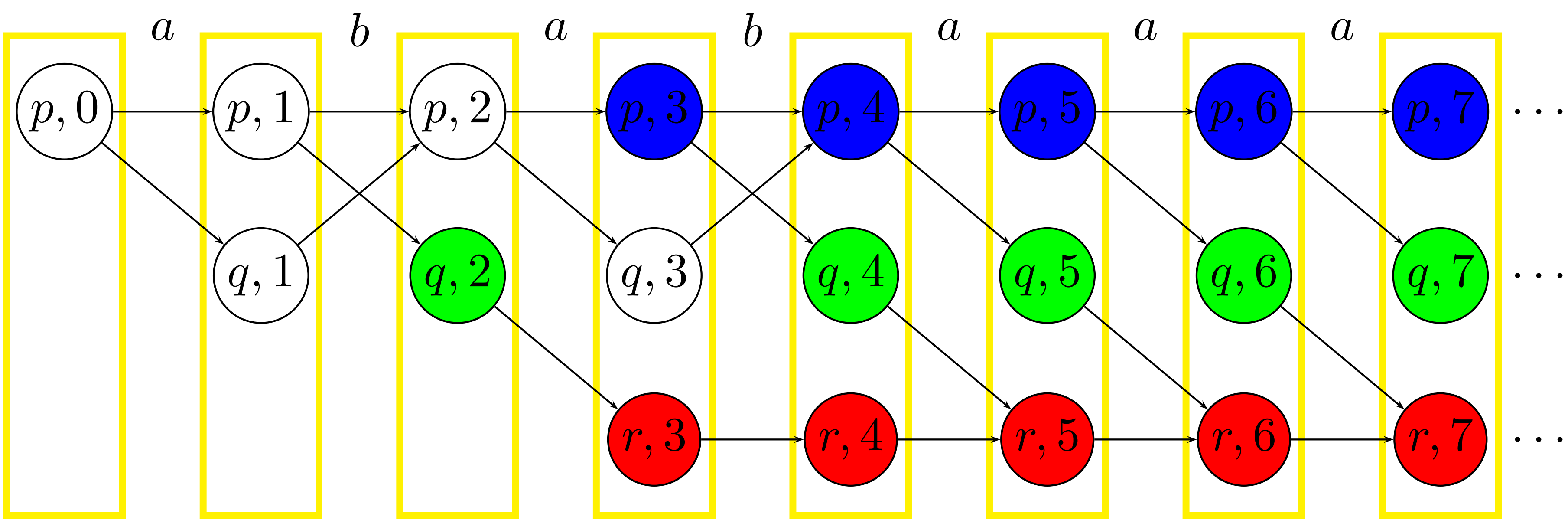
- $i = 0$: In G, for every l, there are at most $|S|$ vertices of the form $\langle \_, l \rangle$.

- $i \to i + 1$:
  - Case G_{2i} is finite: then $G_{2(i+1)}$ is empty.
  - Case G_{2i} is infinite:
    - $*$ There must exist a safe vertex $\langle s, l \rangle$ in G_{2i+1}. (Otherwise, we can construct a path in G with infinitely many visits to F).
    - $*$ We choose $l_{i+1} = l$.
    - $*$ We prove that for all $j \geqslant l$, there are at most $|S| - (i + 1)$ vertices of the form $\langle \_, j \rangle$ in G_{2i+2}.

We prove that for all $j \geqslant l$, there are at most $|S| - (i+1)$ vertices of the form $\langle \_, j \rangle$ in G_{2i+2}.

- Since $\langle s, l \rangle \in G_{2i+1}$, it is not endangered in G_{2i}.
- Hence, there are infinitely many vertices reachable from $\langle s, l \rangle$ in G_{2i}.
- By König's Lemma, there exists an infinite path $p = \langle s, l \rangle, \langle s_1, l + 1 \rangle, \langle s, l + 2 \rangle, \ldots$ in G_{2i}.
- No vertex on p is endangered (there is an infinite path). Therefore, p is in G_{2i+1}.
- All vertices on p are safe ($\langle s, l \rangle$ is safe) in G_{2i+1}. Therefore, none of the vertices on p are in G_{2i+2}.
- Hence, for all $j \geqslant l$, the number of vertices of the form $\langle \_, l \rangle$ in G_{2i+2} is strictly smaller than their number in G_{2i}.


a, b
a, b
p
q
a
r
a, b
b


a
b
a
b
a
a
a
p, 0
p, 1
p, 2
p, 3
p, 4
p, 5
p, 6
p, 7
q, 1
q, 2
q, 3
q, 4
q, 5
q, 6
q, 7
r, 3
r, 4
r, 5
r, 6
r, 7
. . .
. . .
. . .