Lecture 1 (30-07-2021)

30 July 2021 09:28

Automata on infinite words

Some notations

- Let Σ be a finite nonempty set (called alphabet).
- A finite word (over Σ) is a finite (possibly empty) sequence of letters from Σ.

$$w = a_0 a_1 \cdots a_n, \qquad a_i \in \Sigma.$$

ϵ is the empty word.
Σ^* is the set of all finite words (over Σ).

- An infinite word over Σ is an infinite sequence of letters from Σ.

$$\alpha = a_0 a_1 a_2 \cdots, \qquad a_n \in \Sigma \quad \forall n \in \mathbb{N}_0.$$

(Different formality: $\mathbb{N}_0 = \{0, 1, \dots\}$ and $\alpha : \mathbb{N}_0 \to \Sigma^*$)

Also, $\omega := \mathbb{N}_0$.

Σ^ω = all infinite words (on Σ)

(In general, given sets X and Y, Y^X denotes the set of all functions $X \to Y$)

Examples ① $\Sigma = \{a, b\}$

$\alpha = a\ b\ ab\ ab \cdots$

or: $\alpha(n) = \begin{cases} a & ; 2 \mid n \\ b & ; 2 \nmid n \end{cases}$

② $\alpha = abb\ abb\ abb$

$\alpha(n) = \begin{cases} a & ; 3 \mid n \\ b & ; 3 \nmid n \end{cases}$

$\alpha = (abb)^\omega$

③ $\gamma : \omega \to \{a, b\}$

$\gamma(n) = \begin{cases} a & ; n \text{ is prime} \\ b & ; \text{otherwise} \end{cases}$

$$\gamma = \underset{0}{b}\,\underset{1}{b}\,\underset{2}{a}\,\underset{3}{a}\,\underset{4}{b}\,\underset{5}{a}\,\underset{6}{b}\,\underset{7}{a}\,\underset{8}{b}\,\underset{9}{b}\,\underset{10}{b}\,\underset{11}{a} \cdots$$

γ has infinitely many 'a's and 'b's.
(Can't write as compactly as before.)

④ $\Sigma = \{a\}$, $\quad \Sigma^\omega = \{a^\omega\}$. $\quad (|\Sigma^\omega| = 1.)$
But if $|\Sigma| > 1$, then Σ^ω is <u>not</u> a countable set.
OTOH, Σ^* is always a countable set. $\quad (1 \le |\Sigma| < \infty)$

<u>Automata</u>:

$A = (Q, \Sigma, q_0, \Delta \subseteq Q \times \Sigma \times Q,$ "Acceptance condition")

→ a finite set of states
→ $q_0 \in Q$ → the initial state (unique)
→ $\Delta \subseteq Q \times \Sigma \times Q$ → the transition relation
$$(q, a, q') \in \Delta \equiv q \xrightarrow{a} q'$$
(Non-determinism here is fine)

Now, let $\alpha = a_0 a_1 a_2 \cdots \in \Sigma^\omega$ be given.
<u>A</u> run ρ of A on α is an infinite sequence of states

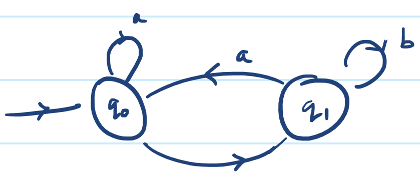
(run)

$$\rho = q_0 q_1 q_2 \cdots$$

Such that "q_0" is indeed the intial state and
$$\forall i \in \omega : \quad (q_i, a_i, q_{i+1}) \in \Delta$$

(In terms of functions: Given $\alpha : \omega \to \Sigma$, we have
$\rho : \omega \to \Sigma$ s.t. $\rho(0) = q_0$ and $(\rho(n), \alpha(n), \rho(n+1)) \in \Delta \ \forall n \in \omega$.)

Example.



$\alpha = (ab)^\omega$
$\rho = q_0 (q_0 q_1)^\omega$

$$\rho = q_0 (q_0\, q_1)^\omega$$

"Acceptance condition": (Büchi automata)

$\alpha \to$ input word

$\rho \to$ a run of A on α

$\mathrm{Inf}(\rho) :=$ the set of states which occur infinitely often along ρ

$$= \{ q \in Q : \exists^\infty i \in \omega \text{ s.t. } \rho(i) = q \}$$

Obs. $\mathrm{Inf}(\rho) \neq \emptyset$. (There are only finitely many states.)

Büchi automaton (BA): Fix $G \subseteq Q$ called the "good states".

A run ρ is accepted by a BA if $\mathrm{Inf}(\rho) \cap G \neq \emptyset$.

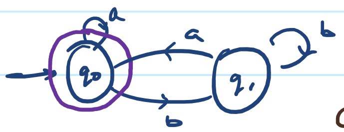
(Thus, some good state appears infinitely often.)

A word $\alpha \in \Sigma^\omega$ is accepted by A if α has an accepting run ρ on the word α.

$$L(A) := \{ \alpha \in \Sigma^\omega : A \text{ accepts } \alpha \}$$

↳ Language of A

Example

A= 

$G = \{q_0\}$, $\Sigma = \{a, b\}$

Claim. $L(A) = \{ \alpha \in \Sigma^\omega :$ α has inf.

many 'a' }.

Proof. Let the right side be L.

- $L(A) \subseteq L$:

  $\alpha \in L(A)$, $\alpha \equiv a_0 a_1 a_2 \cdots$

  Note that A is deterministic, thus α has a unique run ρ, which is accepted.

  $\rho \equiv q_0 q_1' q_2' q_3' \cdots$

  Thus, q_0 appear inf. often above. Since it only receives 'a', we see that 'a' appears inf. often.

- $L \subseteq L(A)$:

  Let $\alpha \in L$. It has a unique run ρ.

  Then, since α has inf. many 'a's, ρ will have inf. many 'q_0's. ∎

Can also write $L = (b^*a)^\omega$ once we have defined what that means.

Question What about $\bar{L} = \Sigma^\omega \setminus L$? Can that be accepted by a Büchi automaton?

Lecture 2 (04-08-2021)

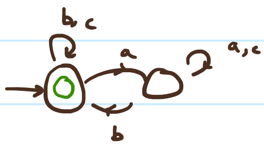
04 August 2021 09:31

Note. We do NOT allow ε transitions in this course.

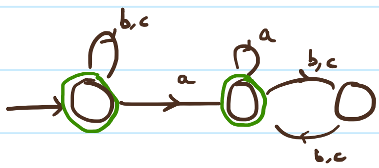
Fact. Even though we insisted on single initial state, the expressive power does not change if we allow more. (It is simply for convenience.)

Examples (1) L_1 over $\Sigma = \{a, b, c\}$.

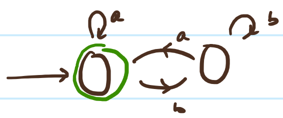
L_1 = every 'a' is eventually followed by a 'b'



(2) L_2 = any two occurences of 'a' are separated by even no. of other (b, c) letters

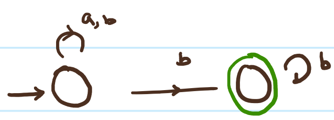


(3) $\Sigma = \{a, b\}$, L = inf. many 'a's



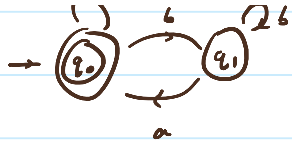
Complement : $\bar{L} = \Sigma^\omega \setminus L$ = finitely many 'a's

Q. What is a BA for $\bar{L}$?



Q. Do we have a deterministic Büchi automaton (DBA) for $\bar{L}$?

Note that we had an DBA for L : 

Note that we had an DBA for L : 

A : $G = \{q_0\}$

Toggle states : A' : $G = \{q_1\}$

But $L(A') \supsetneq \bar{L}$.

infinitely many b

eventually b

$(ab)^\omega \in L(A')$ but $(ab)^\omega \notin \bar{L}$

Complementing the good state of a DBA A does <u>NOT</u> complement the accepted language.

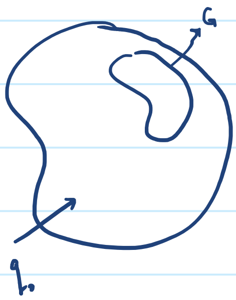
<u>Claim.</u> There is No DBA for $\bar{L} = \{\alpha \in \Sigma^\omega : \alpha$ has finitely many 'a'$\}$.

Thus, as opposed to finite languages, non-determinism actually gives us more languages.

<u>Proof.</u> We prove this by contradiction.

For the sake of contradiction, assume that $\exists$ DBA A such that $L(A) = \bar{L}$.

Suppose A has m states.



$\alpha_0 = b^\omega = b\,bb\cdots \in \bar{L}$

$\rho_0 = q_0\, q_1 q_2 \cdots$

↳ unique run of α_0

Since ρ_0 is accepting, $\exists\, n_1$ s.t. $q_{n_1+1} \in G$.

Pick the smallest such n_1.

$\underbrace{b\ b\ \cdots\ b}_{n_1} \mid b\ b\ \cdots$

$\rho_0 =$ $\qquad\boxed{}$

↑ first good state

Define $a_1 := b^{n_1}\, a\, b^\omega \in \bar{L}$.

$\alpha_1 = b \cdots b^{n_1}\ a\ b\ b \cdots$

$\rho_1 = \square \cdots \square\ \underset{\in G}{\square} \cdots \square$ again a good state

Then, we can get n_2 s.t. $b^{n_1} a b^{n_2} a$ ends at a good state.

Then, $\alpha_2 \cdot b^{n_1} a b^{n_2} a b^{\omega} \in L$.

Its unique run ρ_2 matches ρ_1 until $b^{n_1} a b^{n_2} a$.

Keep getting $n_1, n_2, n_3, \cdots, n_{m+1}$.

$\alpha_m = b^{n_1} a b^{n_2} a \cdots b^{n_{m+1}} a b^{\omega} \in \bar{L}$.

$\rho_m = \underbrace{\underset{\in G}{\square}\ \underset{\in G}{\square} \quad \underset{\in G}{\square}}_{m+1 \text{ states}}$

By PHP, two of these $m+1$ good states are equal. Loop between them to get a word which is accepted but has inf. many 'a's. ☒

Cor. DBA $\subsetneq$ NBA in terms of expressiveness.

Def^n A language $L \subseteq \Sigma^{\omega}$ is said to be ω-regular if there exists a (possibly non-deterministic) Büchi automaton A such that $L(A) = L$.

Closure Properties of ω-Regular Languages

1) closure under union:

$L_1 = L(A_1)$, $\quad A_1 = (Q_1, q_0^1, \Sigma, \Delta_1, G_1)$,

$L_2 = L(A_2)$, $\quad A_2 = (Q_2, q_0^2, \Sigma, \Delta_2, G_2)$.

To-do: Construct a BA A s.t. $L(A) = L_1 \cup L_2$.

We do the usual product construction.

$$\left(Q_1 \times Q_2,\ (q_0^1, q_0^2),\ \Sigma,\ \Delta,\ G_1 \times Q_2 \cup Q_1 \times G_2\right)$$

$$(q_1, q_2) \xrightarrow{a} (q_1', q_2')$$

iff $q_1 \xrightarrow{a} q_1'$ and $q_2 \xrightarrow{a} q_2'$.

$\alpha = a_0\ a_1\ a_2\ \cdots$

$\rho^1 = q_0^1\ q_1^1\ q_2^1\ \cdots$ a run of A_1 on α

$\rho^2 = q_0^2\ q_1^2\ q_2^2\ \cdots$ —"— A_2 —"—

"$\rho^1 \times \rho^2$" $= \begin{pmatrix} q_0^1 \\ q_0^2 \end{pmatrix} \begin{pmatrix} q_1^1 \\ q_1^2 \end{pmatrix} \begin{pmatrix} q_2^1 \\ q_2^2 \end{pmatrix} \cdots$ a "product run" on α

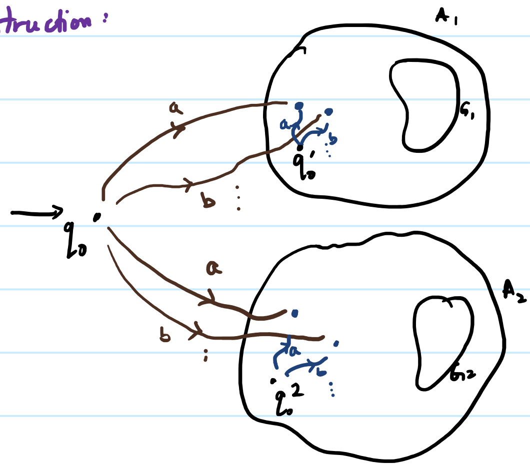
Here we assume that each $\alpha \in \Sigma^\omega$ has at least one run on both A_i. (Can always ensure this by adding a dead state)

With the above assumption,

$$G = (G_1 \times Q_2) \cup (Q_1 \times G_2) \text{ gives}$$

the language as $L_1 \cup L_2$.

A simpler construction:



Lecture 3 (06-08-2021)

06 August 2021 09:39

Closure under intersection.

Do the same product construction as earlier and put
$$G = G_1 \times G_2.$$

$A \equiv A_1 \times A_2.$

Is: $L(A) = L(A_1) \cap L(A_2)$.

($\subseteq$) If $\rho = \rho_1 \times \rho_2$ is an accepting run, so ρ_1 and ρ_2 both are.

($\supseteq$) Let $\alpha \in L(A_1) \cap L(A_2)$.

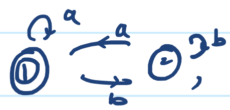
Then there are accepting runs ρ_i on A_i.

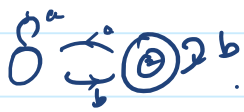
Put $\rho = \rho_1 \times \rho_2$.

But then it is not necessary that ρ is accepting.

For example, ρ_1 has good states at even positions and ρ_2 at odd.

As a concrete example of above:

Take A_1 = 

A_2 = 

Then $(ab)^\omega \in (L(A_1) \cap L(A_2)) \setminus L(A_1 \times A_2)$.

Doesn't work! Slightly modified.

$Q = Q_1 \times Q_2 \times \{1, 2\}$, $\rightarrow$ indicates the component being "searched" for a good state

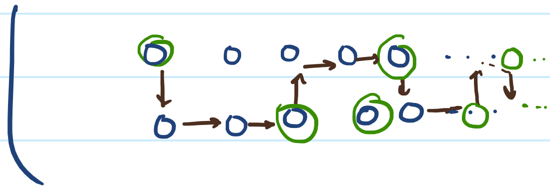
$q_0 = (q_0^1, q_0^2, 1)$

$\Delta = (q_1, q_2, 1) \xrightarrow{a} (q_1', q_2', 1)$ if $q_1 \xrightarrow{a} q_1' \in \Delta_1$, $q_2 \xrightarrow{a} q_2' \in \Delta_2$, $q_1 \notin G_1$

$$(q_1, q_2, 1) \xrightarrow{a} (q_1', q_2', 2) \qquad \begin{array}{l} q_1 \xrightarrow{a} q_1' \\ q_2 \xrightarrow{a} q_2' \\ q_1 \in G_1 \end{array}$$

similarly for $(\, , \, , 2) \to (\, , \, , 2)$
$(\, , \, , 2) \to (\, , \, , 1)$.

$$G = G_1 \times Q_2 \times \{1\}.$$



$$L(A) = L(A_1) \cap L(A_2).$$

Closure under projection:

$\pi : \Sigma_1 \times \Sigma_2 \to \Sigma_1$ induces $\pi : (\Sigma_1 \times \Sigma_2)^\omega \to \Sigma_1^\omega$

$$\binom{a_0}{b_0}\binom{a_1}{b_1}\binom{a_2}{b_2}\cdots \mapsto a_0 a_1 a_2 \cdots$$

If $L \subseteq (\Sigma_1 \times \Sigma_2)^\omega$ is ω-regular, so is $\pi(L)$.

Let $A = (Q, q_0, \Sigma_1 \times \Sigma_2, \Delta, G)$ be a BA with $L(A) = L$.

Goal: Construct B s.t. $L(B) = \pi(L)$.

Define $B = (Q, q_0, \Sigma_1, \Delta', G)$, where

$$\Delta' = \left\{ q \xrightarrow{a} q' \;:\; \begin{array}{l} \exists\, b \in \Sigma_2 \text{ s.t.} \\ q \xrightarrow{(a,b)} q' \text{ in } \Delta \end{array} \right\}.$$

(Take original automata and erase all the second components.)

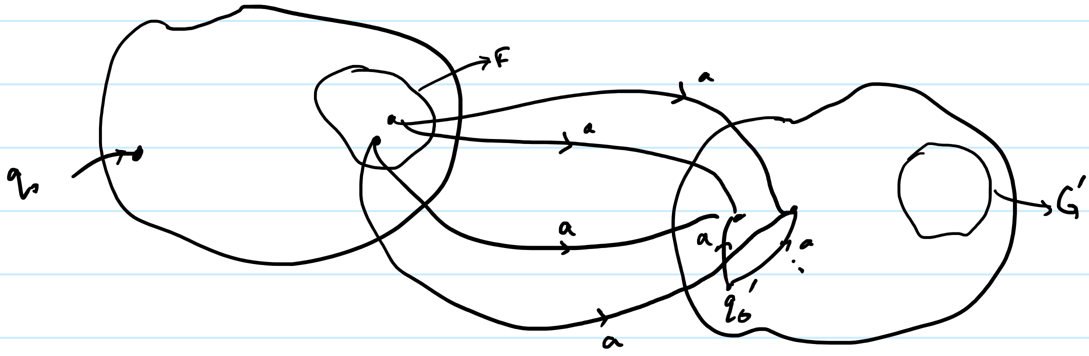
$U \subseteq \Sigma^*$, $L \subseteq \Sigma^\omega$, $U \cdot L \subseteq \Sigma^\omega$.

(The concat. of a finite word followed by an infinite word is defined in the natural way.)

(Nonsense: $\text{Concat} : \Sigma^\omega \times \Sigma^\omega \to \Sigma^\omega$ or $\text{concat} : \Sigma^\omega \times \Sigma^* \to \Sigma^\omega$.)

Closure: $U \subseteq \Sigma^*$ regular $\quad A = (Q_0, q_0, \Sigma, \Delta, F)$, NFA, $L(A)=U$

$L \subseteq \Sigma^\omega$ ω-regular $\quad B = (Q_0', q_0', \Sigma', \Delta', G')$. BA, $L(B)=L$



Keep them disjoint and all possible transitions of the form:

$$q_f \xrightarrow{a} q' \quad \text{where } q_f \in F$$

and $q_0' \xrightarrow{a} q'$ in Δ'.

Keep G as G'. #

Give $U \subseteq \Sigma^*$, define

$$U^\omega = \{ \alpha \in \Sigma^\omega : \alpha \text{ has a factorisation of the form } \alpha = \alpha_0 \alpha_1 \alpha_2 \alpha_3 \cdots \text{ for } \alpha_i \in U. \}$$

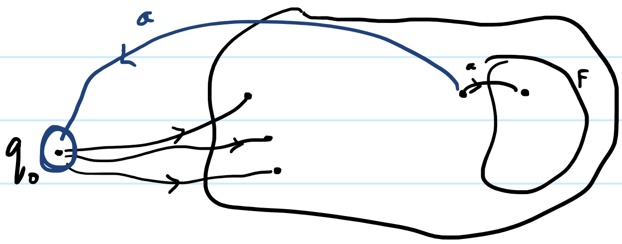
Closure: If $U \subseteq \Sigma^*$ is regular, then U^ω is ω-regular.

Let $A = (Q, q_0, \Sigma, \Delta, F)$ recognise U.

Assume that there are no incoming transitions to q_0 and that $q_0 \notin F$. (Why can we do this?)

(Also note $U^\omega = (U \setminus \{\varepsilon\})^\omega$.)

(Also note $U^\omega = (U \setminus \{\varepsilon\})^\omega$.)



Add all possible transitions of the form:

$$q \xrightarrow{a} q_0 \quad \text{if} \quad \exists q_f \in F \text{ s.t. } q \xrightarrow{a} q_f.$$

Put $G = \{q_0\}$.

Lecture 4 (11-08-2021)

11 August 2021 09:33

To Do : Closure under complementation.

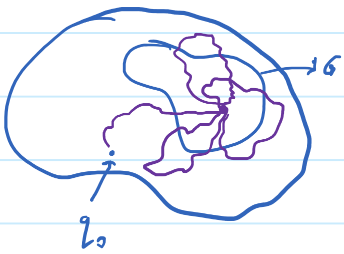
Prop^n. Let L be ω-regular. Then, L can be expressed as

$$L = \bigcup_{i=1}^{n} U_i \cdot V_i^{\omega},$$

where $U_i, V_i \subseteq \Sigma^*$ are regular languages for $i = 1, \ldots, n$.

(By our earlier results, it is clear that any such L is indeed ω-regular.)

Proof. Let A be a BA s.t. $L(A) = L$.
$= (Q, \Sigma, q_0, \Delta, G)$



Given an accepted word $\alpha \in L(A) = L$, $\alpha = a_0 a_1 a_2 \cdots$ with an accepting run $\rho = q_0 q_1 q_2 \cdots$, $\exists\, g \in G$ which occurs i.o.

$$\underbrace{q_0\, q_1\, q_2 \cdots}_{u}\ \ \underbrace{\underset{\uparrow\, g}{|\bigcirc} \cdots}_{v_0}\ \ \underbrace{\underset{\uparrow\, g}{|\bigcirc} \cdots}_{v_1}\ \ \underbrace{\underset{\uparrow\, g}{|\bigcirc} \cdots}_{v_2} \cdots$$

For $g \in G$, define

$$U_g := \{ w \in \Sigma^* : \exists \text{ a run } q_0 \xrightarrow{w} g \}$$
$$V_g := \{ w \in \Sigma^* : \exists \text{ a run } g \xrightarrow{w} g \}.$$

regular since $A_g := (Q, \Sigma, q_0, \Delta, \{g\})$ and $B_g := (Q, \Sigma, \{g\}, \Delta, \{g\})$ accept them

Now, by our earlier observation, it is easy to argue that

$$L = \bigcup_{g \in G} U_g \cdot V_g^{\omega}.$$

Obs. The following problem is decidable: (Non emptiness problem)

- Input :– A → a BA
- Output :– YES if $L(A) \neq \emptyset$,

  NO if $L(A) = \emptyset$.

$\left(L(A) \neq \emptyset \Leftrightarrow \exists g \in G \text{ s.t. } \exists\, q_0 \xrightarrow{w} g \text{ and } \exists\, g \xrightarrow{w} g. \right)$

reachable from initial state

check if part of cycle

both efficient

Obs. If $L(A) \neq \emptyset$, then there exist finite words u and v s.t. $|u|, |v| \leq |Q|$ and $u \cdot v^{\omega} \in L(A)$.

ultimately periodic

Let $A = (Q, \Sigma, q_0, \Delta, G)$ be a BA accepting L.

Goal: To show that $\bar{L} = \Sigma^{\omega} \setminus L$ is also ω-regular.

For $u, v \in \Sigma^*$, define

$u \sim_A v \Leftrightarrow \forall q, q' \in Q$, $q \xrightarrow{u} q'$ iff $q \xrightarrow{v} q'$ and

$q \xrightarrow{u}_G q'$ iff $q \xrightarrow{v}_G q'$.

[Notation: $s \xrightarrow{x}_G s'$ means $\exists$ a run on x from s to s' with an intermediate visit to G.]

Observations:

(i) $\sim_A$ is an equivalence relation on Σ^*

(i) $\sim_A$ is an equivalence relation on Σ^*.

(ii) $\sim_A$ is of finite index, i.e., it has finitely many equivalence classes.

Proof. Fix $q, q' \in Q$.

$$U_{q,q'} = \{ w \in \Sigma^* : q \xrightarrow{w} q' \}.$$

$$V_{q,q'} = \{ w \in \Sigma^* : q \xrightarrow[G]{w} q' \}$$

$2n^2$ such sets. $(n := |Q|)$

For each $u, v \in \Sigma^*$, we can ask $2n^2$ questions about set membership. $u \sim_A v \iff$ they have same answers.

Thus, there are $\leq 2^{2n^2}$ classes.

$$[u]_{\sim_A} = \left(\bigcap_{\substack{q,q' \in Q \\ u \in U_{q,q'}}} U_{q,q'} \right) \cap \left(\bigcap_{\substack{q,q' \in Q \\ u \in V_{q,q'}}} V_{q,q'} \right) \cap \left(\bigcap_{\substack{q,q' \in Q \\ u \notin U_{q,q'}}} \overline{U_{q,q'}} \right)$$

$$\cap \left(\bigcap_{\substack{q,q' \in Q \\ u \notin V_{q,q'}}} \overline{V_{q,q'}} \right).$$

The above discussion also shows that each equivalence class is a regular language.

($U_{q,q'}$ is clearly regular. Same argument shows the same for $V_{q,q'}$.)

Let $U_1, \ldots, U_m$ be the equivalence classes of $\sim_A$.

Lemma Suppose $L \cap (U_i \cdot U_j^{\omega}) \neq \emptyset$ for some i, j, then $U_i \cdot U_j^{\omega} \subseteq L$.

Proof. Let $\alpha \in L \cap (U_i \cdot U_j^{\omega})$.

$$\alpha = a_0 a_1 a_2 a_3 \cdots \in L.$$

Let $\rho = q_0 q_1 q_2 q_3 \cdots$ be an accepting run of A

Let $\rho = q_0\, q_1\, q_2\, q_3 \cdots$ be an accepting run of A on α.

We can also write $\alpha = u \cdot v_0 \cdot v_1 \cdot v_2 \cdots$ s.t. $u \in U_i$ and $v_0, v_1, v_2, \ldots \in U_j$.

$$\rho_\alpha = q_0 \xrightarrow{u} q_1' \xrightarrow{v_0} q_2' \xrightarrow{v_1} q_3' \to \cdots$$

Now, let $\beta \in U_i\, U_j^{\omega}$. Then, $\beta = u'\; v_0'\; v_1' \ldots$

Then, we have a run

$$\rho_B = q_0\, q_1'\, q_2'\, q_3' \cdots$$

by def^n of $\sim_A$.

Moreover if ρ_A saw a good state $q_i' \to q_{i+1}'$, so does ρ_B.

$\therefore\ \beta \in L(A)$. ∎

Lecture 5 (13-08-2021)

13 August 2021 09:36

Ramsey's Theorem

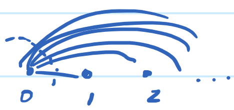
$\mathbb{N} = \{0, 1, 2, \dots\}$
$E = \{(i,j) \in \mathbb{N} \times \mathbb{N} : i < j\}$. } Complete graph on $\mathbb{N}$

$\mathcal{C}$ — a finite set of colours.
$\chi : E \to \mathcal{C}$ is called an edge-colouring of the complete graph on $\mathbb{N}$.

Thm. Given an arbitrary χ, $\exists$ an infinite monochromatic clique in χ.
That is,
$\exists S \subseteq \mathbb{N}$, $|S| = \infty$, $\exists c \in \mathcal{C}$ such that every edge with S is coloured 'c'.

$$(\forall i,j \in S : i < j \Rightarrow \chi((i,j)) = c.)$$

Proof. Fix $\chi : E \to \mathcal{C}$.
$X_0 := \mathbb{N}$, $m_0 := \min(X_0)$ $(= 0)$.



$\exists c_0 \in \mathcal{C}$ s.t. $\exists$ infinitely many x s.t. $\chi((m_0, x)) = c_0$.

Let $X_1 := \{$ neighbours of m_0 in $X_0\} \subseteq X_0 \setminus \{m_0\}$.
Note: $X_1 \subseteq \mathbb{N}$ is infinite.
Let $m_1 := \min(X_1)$ and proceed similarly to pick c_1 and $X_2 \subseteq X_1 \setminus \{m_1\} \dots$

In general, we have an infinite subset X_{k+1} and colour c_k s.t. every element of X_{k+1} is connected to $\min(X_k)$ by c_k.

Define $X_\infty := \{m_0, m_1, m_2, \dots\}$. $(m_0 < m_1 < m_2 < \dots)$
Then, X_∞ is an infinite set s.t. $\forall i,j : \chi((m_i, m_j)) = c_i \ \forall i < j$.

As usual, $\exists c \in \mathcal{C}$ which occurs infinitely many often.
Simply restrict graph to those vertices.

Continuing from last lecture: $U_1, \ldots, U_m$ are equiv. classes of $\sim_A$.
We saw: U_i are regular.

Claim. $\Sigma^\omega = \bigcup_{i,j} U_i \cdot U_j^\omega$.

Proof. Only ($\subseteq$) is to be shown.
Let $\alpha \in \Sigma^\omega$ be arbitrary.
TS: $\exists i,j$ $\alpha = u_0 v_0 v_1 v_2 \cdots$ for $u_0 \in U_i$ and $v_k \in U_j$ $\forall k$.

Write $\alpha = a_0 a_1 a_2 a_3 \cdots \in \Sigma^\omega$ for $a_i \in \Sigma$.

Define the following χ_α on $(\mathbb{N}, \in)$ as:

$$\mathcal{C} = \{U_1, \ldots, U_m\}$$

$$\chi_\alpha((i,j)) = [a_i a_{i+1} \cdots a_{j-1}]_{\sim_A}.$$

equiv class of $a_i a_{i+1} \cdots a_{j-1}$

By Ramsey's theorem, $\exists U_j$ with a clique, i.e., $\exists m_1 < m_2 < m_3 < \cdots$
s.t. $\chi_\alpha((x_k, x_{k+1})) = U_j$ $\forall j$.

Defining $u_0 = a_0 \cdots a_{m_1 - 1}$, $v_0 = a_{m_1} \cdots a_{m_2 - 1}$,
$v_1 = a_{m_2} \cdots a_{m_3 - 1}, \ldots$
does the job. ☒

$$\Sigma^* = U_1 \sqcup U_2 \sqcup \cdots \sqcup U_m,$$
$$\Sigma^\omega = \bigcup_{i,j} U_i \cdot U_j^\omega.$$

Note that U_i are regular. Moreover, we have

$$L \cap (U_i \cdot U_j^\omega) \neq \phi \Rightarrow U_i \cdot U_j^\omega \subseteq L.$$

Thus, $$L = \bigcup_{\text{some } i,j} U_i \cdot U_j^\omega.$$

Thus, $$\Sigma^\omega \setminus L = \bigcup_{i,j : U_i \cdot U_j^\omega \not\subseteq L} U_i \cdot U_j^\omega.$$

Thus, it is again ω-regular. ∎

→ Effective construction of BA for $\bar{L}$.

- Construct automaton for U_i.
- Construct BA for $U_i \cdot U_j^\omega$.
- Take union of those not in L.

(Can effectively check if $L \cap (U_i \cdot U_j^\omega) = \phi$.)

Lecture 6 (18-01-2021)

18 August 2021 09:31

Büchi's Theorem:

Want to talk about properties of words (finite or infinite).

First-order Logic (over words). Fix $\Sigma \to$ alphabet.

First-order variables — $x, y, z, x_1, x_2, x_3, \ldots$ range over positions in the word

Atomic-predicate — $a(x), b(x), \ldots$ $\to$ unary predicate

for $a, b, \ldots \in \Sigma$
and x is a FO variable.

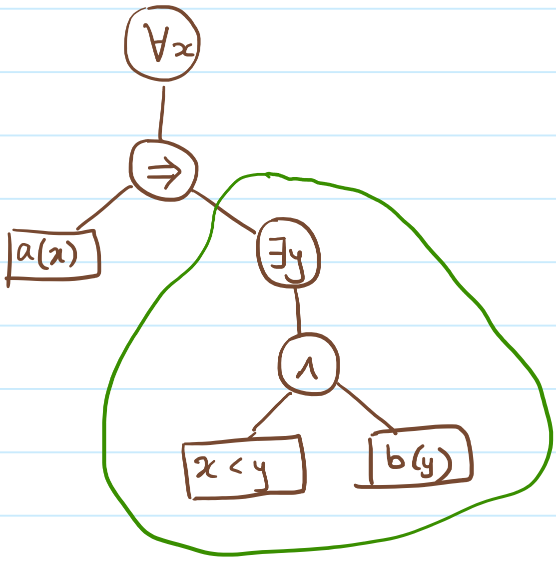
$x < y$ $\to$ binary predicate

Syntax:

$$\varphi \equiv a(x) \mid x < y \mid \neg\varphi \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \exists x . \varphi \mid \forall x . \varphi$$

derived: $\varphi_1 \Rightarrow \varphi_2 \equiv \neg\varphi_1 \vee \varphi_2$

Example: $\varphi_1 \equiv \forall x . [a(x) \Rightarrow \exists y \; (x < y) \wedge b(y)]$



Semantics:

$\varphi(x_1, \ldots, x_m)$ — φ is a formula with free variables

$\varphi(x_1, \dots, x_m)$ — φ is a formula with free variables $x_1, \dots, x_m$

$\varphi' \equiv \exists y[(x<y) \wedge b(y)]$ → x free, y bound

$\varphi(x_1, \dots, x_m)$, $w \to$ word

$w, \; x_1 \leftarrow p_1, \dots, x_m \leftarrow p_m \models \varphi(x_1, \dots, x_m)$

defined by structural induction

1. "$w, x_1 \leftarrow p_1 \models a(x_1)$" iff the letter in w at position p_1 is a

2. "$w, x_1 \leftarrow p_1, x_2 \leftarrow p_2 \models x_1 < x_2$" $\Leftrightarrow$ $p_1 < p_2$

⋮

Example. ① $\varphi_2 \equiv \exists x \, \forall y \, [(x<y) \Rightarrow \neg a(y)]$.

If w $(\neq \varepsilon)$ is finite, then it will satisfy φ_2.

But if w is infinite, then $w \models \varphi_2 \iff w$ has finitely many 'a's.

② $\varphi_3 \equiv \forall x \, \exists y \, (x<y)$

if w is a (nonempty) finite word, then $w \not\models \varphi_3$.
OTOH, all infinite words satisfy this property

Büchi - Elgot Theorem → a logical characterisation of (finite) regular languages

Büchi Theorem → a logical characterisation of ω-regular languages

---

Monadic Second-Order Logic over words

extends FO - over words

position variables — $x, y, x_1, x_2, x_3, \ldots$
sets-of-positions variables — $X, Y, X_1, X_2, X_3, \ldots$
atomic-predicate — $a(x), x < y, X(x)$.

Syntax

$\varphi \equiv$ atomic-predicates $| \neg\varphi | \varphi \vee \varphi | \varphi \wedge \varphi | \exists x \cdot \varphi | \forall x \cdot \varphi | \exists X \cdot \varphi | \forall X \cdot \varphi$

$S(x, y) \equiv$ position y is successor of position x
$\equiv (x < y) \wedge \neg(\exists z \cdot (x < z) \wedge (z < y))$.

$\text{first}(x) \equiv x$ is the first position
$\equiv \forall y \, (x = y \vee x < y)$.

$\text{last}(x) \equiv \ldots$

Remark. In FO, the '<' predicate cannot be expressed using 'S' predicate.

$x < y \Leftrightarrow$ $x \neq y$ and every successor-closed set of positions which contains x, also contains y
↳ can define in MSO

Thus, we can write '<' in terms of 'S' in MSO.

Def^n. Let φ be a MSO sentence.
$L_\varphi = \{\alpha \in \Sigma^\omega : \alpha \models \varphi\}$.
$L \subseteq \Sigma^\omega$ is called MSO-definable if $\exists$ MSO φ s.t. $L = L_\varphi$.

Theorem (Büchi's Theorem)
Let $L \subseteq \Sigma^\omega$.
L is MSO-definable $\Leftrightarrow$ L is ω-regular.

Lecture 7 (20-08-2021)

20 August 2021 09:37

Thm. (Buchi) Let $L \subseteq \Sigma^\omega$.

L is ω-regular $\iff$ L is MSO-definable.

Proof. ($\Rightarrow$) Suppose L is ω-regular, say $L = \mathcal{L}(A)$, where $A = (Q, q_0, \Sigma, \Delta \subseteq Q \times \Sigma \times Q, G)$ is a BA.

Goal: Construct MSO sentence φ_A s.t.

$\forall \alpha \in \Sigma^\omega$: $\alpha \models \varphi_A \iff A$ accepts α.

$\alpha = a_0 a_1 a_2 a_3 a_4 \cdots$

Suppose A accepts α via an accepting run ρ.

$\rho = q_0 q_1 q_2 q_3 q_4 \cdots$

$\forall q \in Q$, $X_q \equiv$ the set of positions in α when this run ρ is in the state 'q'

$= \{i \in \mathbb{N} : q_i \in q\}$. $(0 \in \mathbb{N})$

Note that $\{X_q\}_{q \in Q}$ is a partition of $\mathbb{N}$. (Allowing $\emptyset$ in partition.)

1) $0 \in X_{q_0}$

2) for any two consecutive positions x and y, if $x \in X_q$, $y \in X_{q'}$, then $(q, a, q') \in \Delta$, where a is the letter at position x.

3) for any position x, there is a position y to the right of x such that $y \in X_q$ for some $q \in G$.

Conversely, given a partition with above 3 properties, we can build an accepting run.

For convenience, write $Q = \{0, 1, \ldots, m\}$.
initial

$$\varphi_A \equiv \exists X_0 \, \exists X_1 \, \ldots \, \exists X_m \, . \, \text{partition}(X_0, \ldots, X_m) \wedge$$
$$[\forall x \, . \, \text{first}(x) \Rightarrow X_0(x)] \wedge$$
$$\left[\forall x \forall y \;\; S(x,y) \Rightarrow \left(\bigvee_{(i,a,j) \in \Delta} X_i(x) \wedge X_j(y) \wedge a(x) \right)\right] \wedge$$
$$\left[\forall x \;\; \exists y \;\; (x < y) \wedge \left(\bigvee_{i \in G} X_i(y) \right) \right].$$

$$\text{partition}(X_0, X_1, \ldots, X_m) \equiv \forall x \left(\bigvee_{i \in Q} X_i(x) \;\; \wedge \;\; \bigwedge_{i \neq j} \neg (X_i(x) \wedge X_j(x)) \right).$$

$\text{Length}(\varphi_A) = O(|A|)$.

($\Leftarrow$) Given: MSO sentence φ.

Goal: Construct BA A s.t.

$$L(A) = \{\alpha \in \Sigma^\omega \mid \alpha \models \varphi\}.$$

As in the finite case, we use MSO_0-logic

- substitute position variables by singleton set vars.
- more atomic predicates: $\text{Sing}(X)$, $a(X)$, $S(X, Y)$, $X \subseteq Y$

singleton

X, Y are Sing and the single positions are related by S

these can be defined in MSO.

The converse is true too. Thus, we use them interchangeably.
That is, they have same expressive power.

Lecture 8 (25-08-2021)

25 August 2021 09:39

Goal: Given a MSO_0 formula, construct a BA A s.t. $L(A) = L(\varphi)$.
The construction of A proceeds by structural induction φ.

In fact: Let $\varphi(X_1, \dots, X_n)$ be an MSO_0-formula with free (set-) variables $X_1, \dots, X_n$

$$\alpha, \; X_1 \leftarrow P_1, \dots, X_n \leftarrow P_n \overset{?}{\models} \varphi$$

$P_1 = \{0, 3, 4, \dots\}$

$P_2 = \phi$

$P_n = 2\mathbb{N}$
$= \{0, 2, 4, \dots\}$

$$\begin{array}{ccccccccl}
\alpha & = & a_0 & a_1 & a_2 & a_3 & a_4 & \dots & \\
P_1 & = & 1 & 0 & 0 & 1 & 1 & \dots & \\
P_2 & = & 0 & 0 & 0 & 0 & 0 & \dots & \\
\vdots & & & & & & & & \\
P_n & = & 1 & 0 & 1 & 0 & 1 & \dots &
\end{array} \Bigg\} \text{characteristic vectors}$$

$$\begin{pmatrix} a_0 \\ 1 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \begin{pmatrix} a_1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{pmatrix} a_2 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \begin{pmatrix} a_3 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \begin{pmatrix} a_4 \\ 1 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \dots$$

The model of φ (an inf. word Σ + n sets) can be seen as an inf. word over $\Sigma \times \{0,1\}^n$.

$$\text{Free}(\varphi) = \{X_1, \dots, X_n\}.$$
$$L(\varphi) = \{ \alpha' \in (\Sigma \times \{0,1\}^n)^\omega : \alpha' \models \varphi \}.$$

Claim. $L(\varphi)$ is ω-regular over $\Sigma_n = \Sigma \times \{0,1\}^n$.

Proof. $\varphi \rightsquigarrow A_\varphi$ by structural induction.

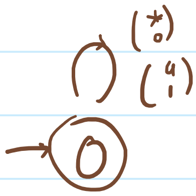
Base. φ — atomic predicate

- $\varphi = \text{Sing}(X_1)$ $\qquad \alpha' = \begin{pmatrix} a_0 \\ b_0 \end{pmatrix} \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \dots \qquad a_i \in \Sigma, \; b_i \in \{0,1\}$

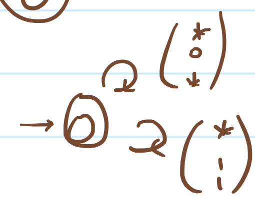
- $\varphi = \mathrm{Sing}(x_1)$ $\quad\quad \alpha' = \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}\begin{pmatrix} a_1 \\ b_1 \end{pmatrix}\begin{pmatrix} a_2 \\ b_2 \end{pmatrix}\cdots$ $\quad\quad a_i \in \Sigma$, $b_i \in \{0,1\}$

- $\varphi = S(x_1, x_2)$; $\Sigma_2 = \Sigma \times \{0,1\} \times \{0,1\}$

- $\varphi = a(x_1)$



- $\varphi = x_1 \subseteq x_2$



<u>Inductive step</u>.

- $\varphi = \varphi_1 \vee \varphi_2$. $\quad\quad \mathrm{Free}(\varphi_1) \subseteq \underbrace{\{x_1, \ldots, x_n\}}_{}$ $\quad$ ($\{x_1,\ldots,x_n\} = \mathrm{Free}(\varphi)$).

WLOG, we may assume $\mathrm{Free}(\varphi_1) = \{x_1, \ldots, x_n\} = \mathrm{Free}(\varphi_2)$.

By induction, we have appropriate automata A_{φ_i} for φ_i. But the alphabet for both is same. Can take union of $\mathcal{BA}$.

- $\varphi = \varphi_1 \wedge \varphi_2$, $\varphi = \neg \varphi_1$ similarly done.

- $\varphi = \exists x_n \ \varphi'(x_1, \ldots, x_n)$ $\quad\quad \mathrm{Free}(\varphi) = \{x_1, \ldots, x_{n-1}\}$

Note: $\alpha' \models \varphi \iff \exists$ a set P_n s.t. $\alpha';\ x_n \leftarrow P_n \models \varphi'$

Consider the projection map

$$\pi : \Sigma \times \{0,1\}^n \longrightarrow \Sigma \times \{0,1\}^{n-1},$$
$$(a, b_1, \dots, b_n) \longmapsto (a, b_1, \dots, b_{n-1}).$$

This induces a map $\pi : (\Sigma_n)^\omega \to (\Sigma_{n-1})^\omega$.

$\alpha' \in (\Sigma_{n-1})^\omega$, $\alpha' \models \varphi \iff \exists\, \alpha'' \in (\Sigma_n)^\omega$ s.t.
$\pi(\alpha'') = \alpha'$ and $\alpha'' \models \varphi'$.

The question is reduced to asking if projection of an ω-regular language is ω-regular.
But this is simple to see. Take an automaton for φ' and erase the last coordinate on all transitions.

- $\varphi = \forall X_n.\ \varphi'$.
  Same as $\neg \exists X_n \neg \varphi'$. ∎

Thus, we are done.

Thm (Büchi's Theorem) Let $L \subseteq \Sigma^\omega$. Then,
L is ω-regular $\iff$ L is MSO-definable.

Moreover, the translations are effective.

The above theorem was proven a few years after the Büchi-Elgot theorem (the analogous theorem about (finite) regular languages).
It is easy to see how MSO-definability translates to ω-words but was not so clear how to extend regularity.

Thus, $MSO(\Sigma)$ is decidable.
Given an MSO-sentence φ, we can check if there

exists an inf. word $\alpha \in \Sigma^\omega$ s.t. $\alpha \models \varphi$.

[$\varphi \rightsquigarrow A_\varphi$ is effective and we can check $L(A_\varphi) \neq \emptyset$.]

In fact, if $L(A_\varphi) \neq \emptyset$, then $\exists\, u, v$ s.t. $uv^\omega \in L(A_\varphi)$ and we can produce the above u, v.

Note: $\varphi \rightsquigarrow A_\varphi$ is NON-elementary.

We cannot bound $|A_\varphi|$ in terms of any (fixed) k-ary exponential of $|\varphi|$.

($n = |\varphi|$, $2^{p(n)}$, $2^{2^{p(n)}}$, ... ← elementary
p ← polynomial
$2^{p(n)}$: singly exp; $2^{2^{p(n)}}$: doubly exp, ..., k-ary exp, ..)

The tower (we get) will have length in terms of n.

↙ can we do better for satisfiability?

FACT. There is a non-elementary type lower bound for MSO-satisfiability problem.

Note: $\varphi \rightsquigarrow A_\varphi \rightsquigarrow \varphi_{A_\varphi}$

↳ This has a nice form $\exists X_1 \cdots \exists X_n$ ("first-order type").

Lecture 9 (27-08-2021)

27 August 2021 09:34

"First-order theory" of arithmetic

$(\mathbb{N}, +, \cdot, 0, 1)$

- $add(x, y, z) \longrightarrow$ asserts $x + y = z$
- $mult(x, y, z) \longrightarrow$ asserts $xy = z$

Usual FO syntax.

- $zero(x) \equiv add(x, x, x)$
- $x < y \equiv \exists z \; add(x, z, y)$
- $S(x, y) \equiv x < y \land \neg \exists z \, (x < z \land z < y)$
- $one(x) \equiv \exists y \, (zero(y) \land S(y, x))$
- $prime(x) \equiv \neg one(x) \land \forall y \forall z \, (mult(y, z, x) \Rightarrow one(y) \lor one(z))$
- $even(x) \equiv \exists y \; add(y, y, x)$.

Goldbach's conjecture:

$\varphi \equiv \forall z \; even(z) \Rightarrow \exists y \exists x \; prime(x) \land prime(y) \land add(x, y, z)$.

Given a sentence φ, we would like to known if φ is true.

Hilbert's belief: Perhaps, we can mechanically figure out the truth/falsity of φ.

? what does this mean?

Church/ Gödel/ Turing : "Computability" ← defined

Moreover, it was shown that:

Moreover, it was shown that:

The first-order theory of arithmetic is undecidable/ non-computable

That is, there is no algorithm s.t.:

Now, let us look at $(\mathbb{N}, +)$ → Presburger arithmetic.
First order and only add (x, y, z).

This IS decidable!

$(\mathbb{N}, +, <)$ → first-order theory

↳ Büchi showed that Presburger arithmetic is decidable using automata theory

$\varphi(x_1, \ldots, x_n)$ → first-order formula

encode $x_1, \ldots, x_n$ in reverse binary order
↳ finite words over $\{0, 1\}^n$.

→ $\underline{S1S}$: $(\mathbb{N}, <)$ or $(\mathbb{N}, S)$

Second order theory of 1 successor

Both same if monadic second order

1960s:

(In fact, MSO + add gives mult, which we know is undecidable)

$\boxed{W}S1S$: subsets are only allowed to be finite subsets

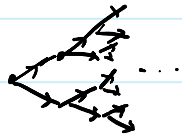
weak

Büchi showed that S1S is decidable

Büchi showed that S1S is decidable

1970s: (Rabin's theorem) S2S is decidable

two successors



MONA: Logic $\longrightarrow$ Automata

$$\bigvee_{i=1}^{k} \left[\left(Inf(\rho) \cap E_i = \emptyset \right) \wedge \left(Inf(\rho) \cap F_i \neq \emptyset \right) \right].$$

Streett: Dual to Rabin.

$\Omega = \{ (E_1, F_1), \ldots, (E_k, F_k) \}$

ρ is accepting if

$$\bigwedge_{i=1}^{k} \left[\left(Inf(\rho) \cap E_i \neq \emptyset \right) \vee \left(Inf(\rho) \cap F_i = \emptyset \right) \right]$$

$$\bigwedge_{i=1}^{k}\left[\left(Inf(\rho)\cap E_i \neq \emptyset\right) \vee \left(Inf(\rho)\cap F_i = \emptyset\right)\right]$$

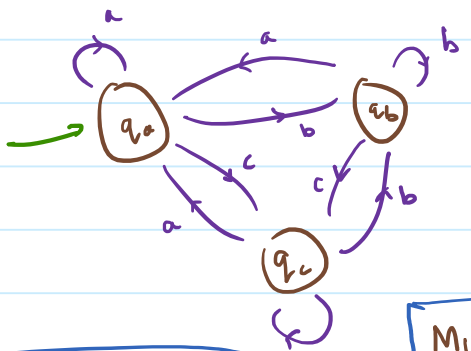
equivalently

$$= \bigwedge_{i=1}^{k}\left(\left[Inf(\rho)\cap F_i \neq \emptyset\right] \Rightarrow \left[Inf(\rho)\cap E_i \neq \emptyset\right]\right).$$

If F_i is visited infinitely often, then so is E_i.

$\Sigma = \{a, b, c\}$

$L = \{\alpha \in \Sigma^\omega \mid$ if 'a' occurs inf. often in α, then so does 'b'$\}$.



Street-condition:

$\Omega = \{(\{q_b\}, \{q_a\})\}$.

Muller-condition

$\mathcal{F} = \{\{q_a, q_b\}, \{q_a, q_b, q_c\}, \{q_c\}, \{q_b\}, \{q_b, q_c\}\}$

$= \{X \subseteq Q : q_a \in X \Rightarrow q_b \in X\} \setminus \{\emptyset\}$.

Note that putting $\emptyset$ in $\mathcal{F}$ makes no difference since $Inf(\rho) \neq \emptyset$ $\forall \rho$.

Rabin-condition

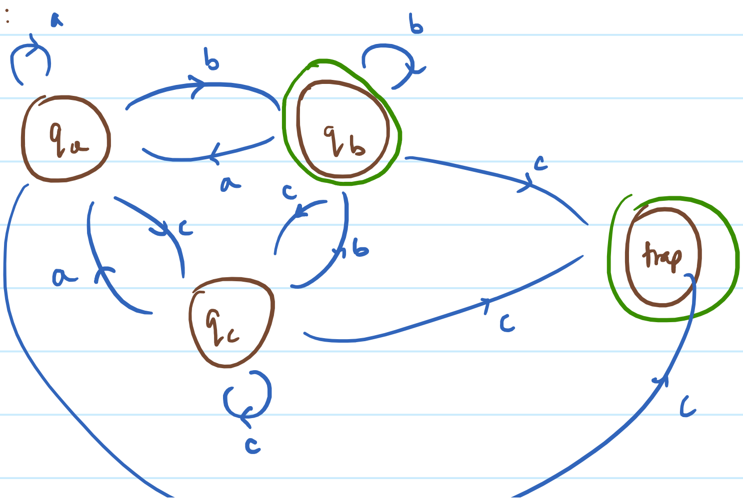
Note:

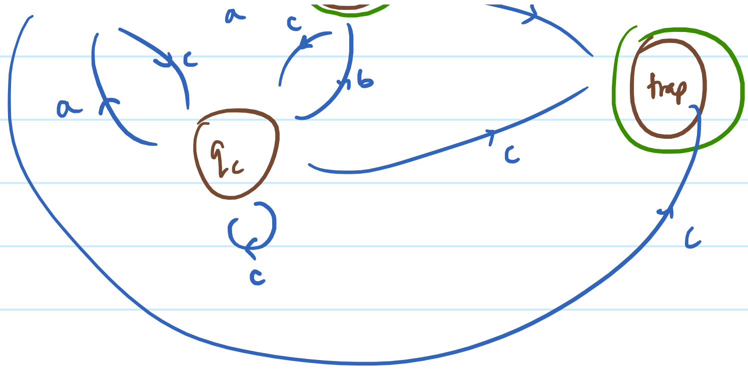
$L = \{\alpha \mid b$ occurs inf. often$\}$

$\cup \{\alpha \mid$ both a & b fin. often$\}$

$\Omega = \{(\emptyset, \{q_b\}), (\{q_a, q_b\}, Q)\}$

Büchi-condition:





Thm (McNaughton) DMA = DRA = DSA = NBA = ω-regular.

D = deterministic

N = non-D

M = Muller, R = Rabin, S = Streeter, B = Büchi

A = Automaton