Verification in Isabelle/HOL of Hopcroft's algorithm for minimizing DFAs including runtime analysis

Vincent Trélat
supervised by Prof. Dr. Tobias Nipkow and Dr. Peter Lammich

Technical University of Munich
Chair for Logic and Verification

September 2023

Outline

Figure: Location of Munich

Figure: Some photos of Munich

Figure: Technical University of Munich (TUM), Garching campus

Figure: Technical University of Munich (TUM), Garching campus


Kloster
Scheyern
SEIT 1119
KLOSTER-GOLD
DUNKEL


Kloster
Scheyern
KLOSTER-GOLD
DUNKEL


13 28
J.W.
Augustiner-
Bräu München
Edelstoff


Kloster
Scheyern
KLOSTER-GOLD
DUNKEL


13 28
J W
Augustiner-
Bräu München
Edelstoff


Kloster
Scheyern
KLOSTER-GOLD
DUNKEL


Edelstoff
13 28
J W
Augustiner-
Bräu München
Edelstoff


Kloster
Scheyern
KLOSTER-GOLD
DUNKEL


Kloster
Scheyern
KLOSTER-GOLD
DUNKEL


Edelstoff
13 28
J.W.
Augustiner-
Bräu München
Edelstoff


Kloster
Scheyern
KLOSTER-GOLD
DUNKEL


SPEZIAL
HERZOGLICH BAYERISCHES
BRAUHAUS
TEGERNSEE


Kloster
Scheyern
KLOSTER-GOLD
DUNKEL


Edelstoff
13 28
J W
Augustiner-
Bräu München
Edelstoff


Kloster
Scheyern
KLOSTER-GOLD
DUNKEL


SPEZIAL
HERZOGLICH BAYERISCHES
BRAUHAUS
TEGERNSEE


Kloster
Scheyern
KLOSTER-GOLD
DUNKEL


Edelstoff
13 28
J.W.
Augustiner-
Bräu München
Edelstoff


Kloster
Scheyern
KLOSTER-GOLD
DUNKEL


SPEZIAL
BRAUHAUS
TEGERNSEE


WIRTS MADL
Bayrisch Hell
WIRTS MADL
Bayrisch Hell


Kloster
Scheyern
KLOSTER-GOLD
DUNKEL


Edelstoff
13 28
J.W.
Augustiner-
Bräu München
Edelstoff


Kloster
Scheyern
KLOSTER-GOLD
DUNKEL


SPEZIAL
BRAUHAUS
TEGERNSEE


WIRTS MADL
Bayrisch Hell
WIRTS MADL
Bayrisch Hell


HB
HOFBRÄUHAUS

Understanding Refinement

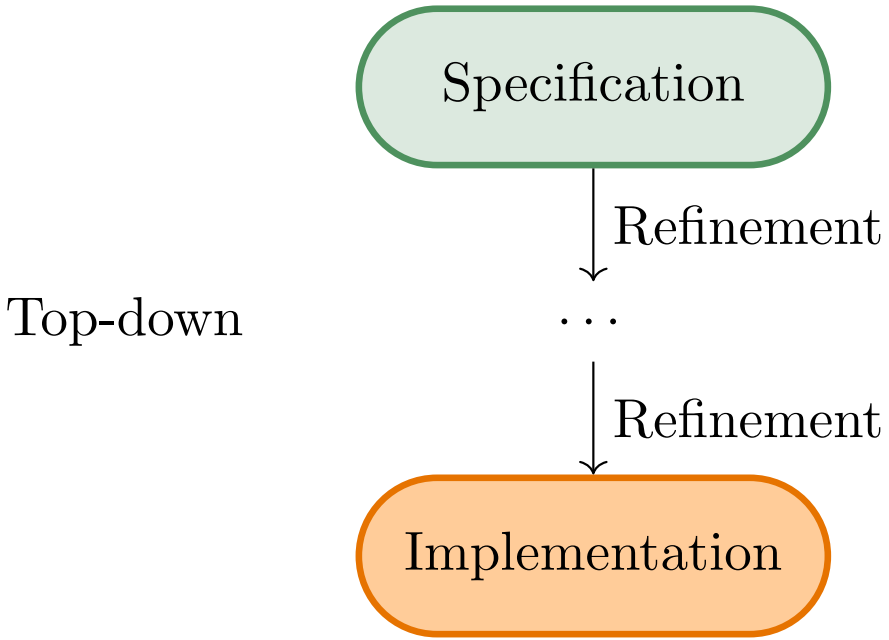
Definition 1

Refinement is a systematic process of refining a high-level abstract specification into a concrete implementation.

Understanding Refinement

Definition 1

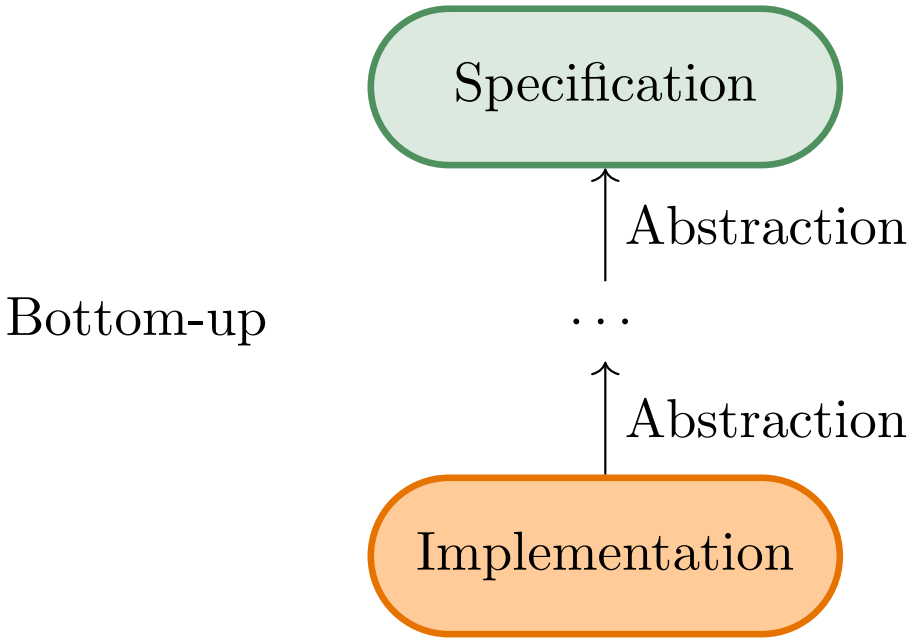
Refinement is a systematic process of refining a high-level abstract specification into a concrete implementation.



Understanding Refinement

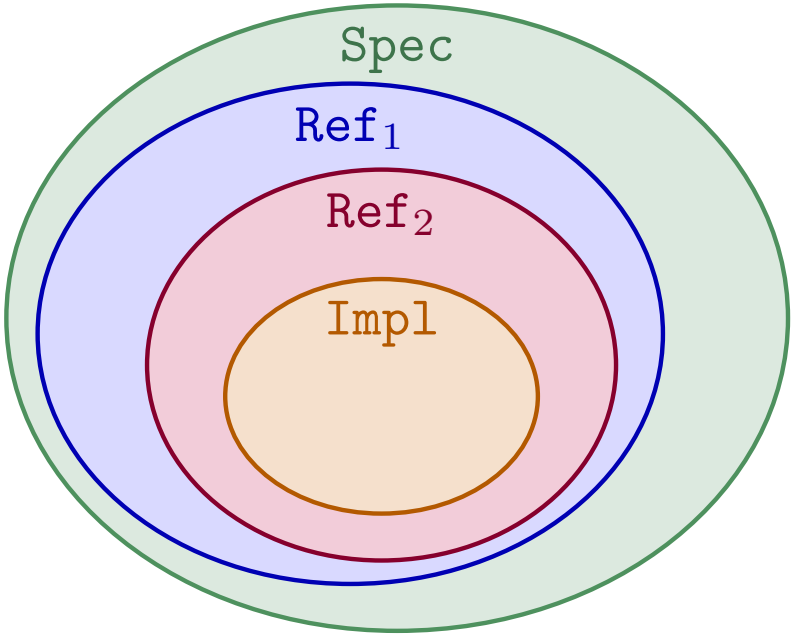
Definition 1

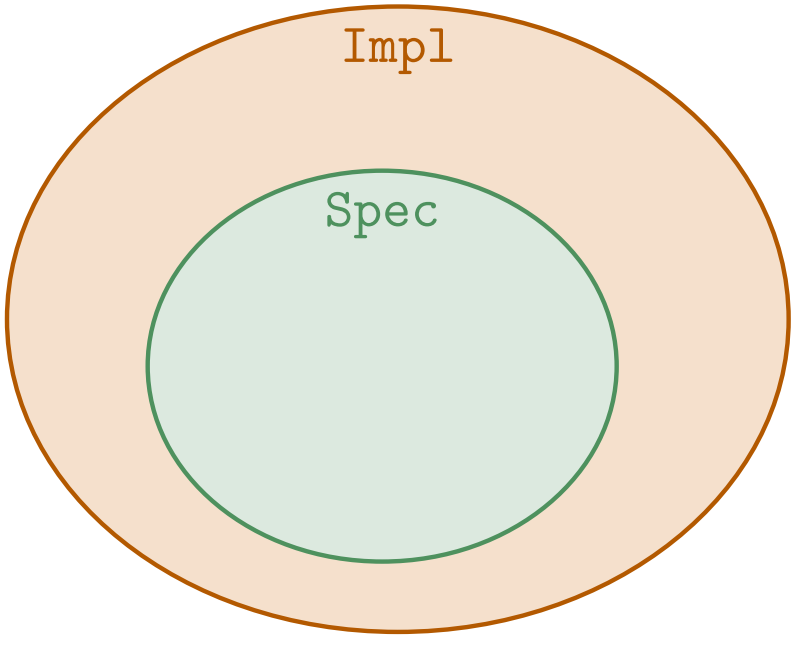
Refinement is a systematic process of refining a high-level abstract specification into a concrete implementation.



Each refinement step preserves the intended behavior.

$$\texttt{Spec} \rightarrow \texttt{Ref}_1 \rightarrow \texttt{Ref}_2 \rightarrow \texttt{Impl}$$



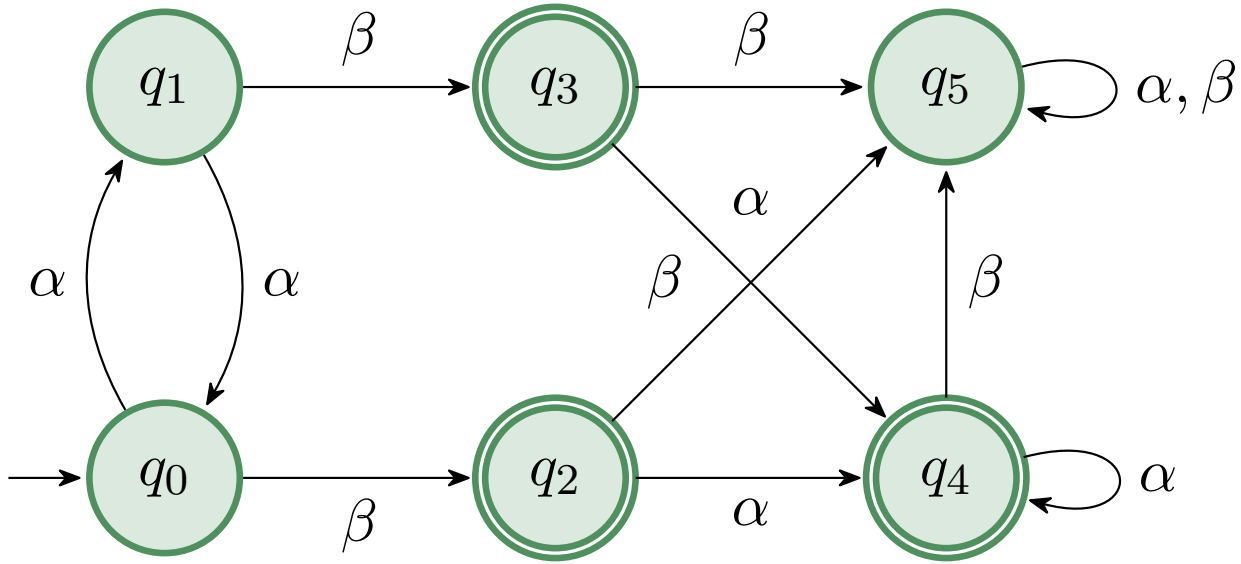


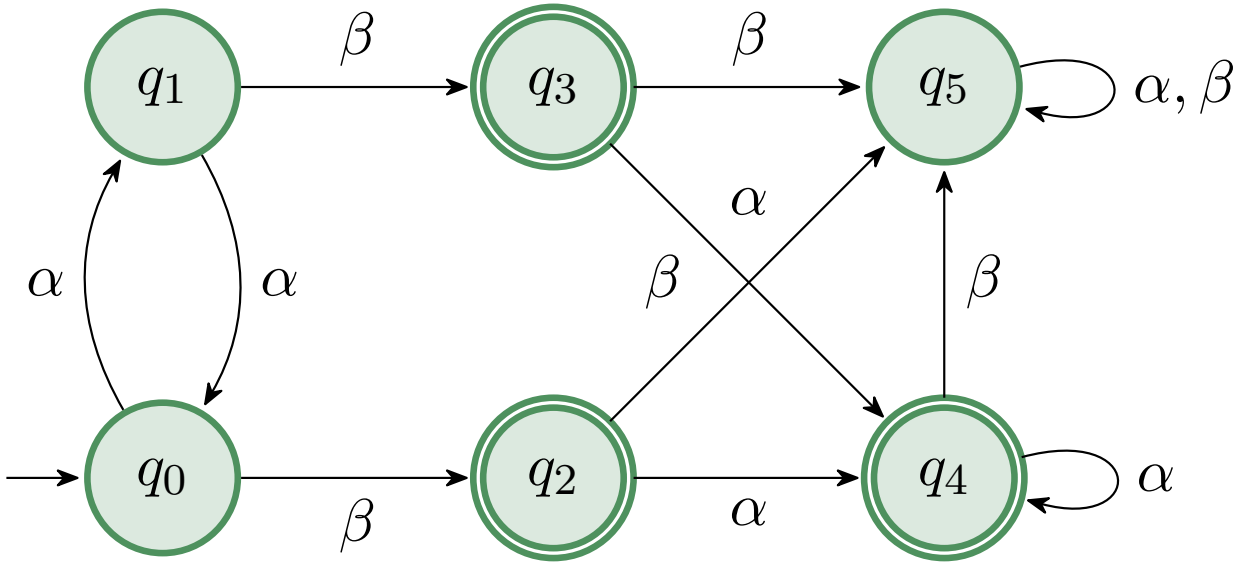
The Isabelle Refinement Framework

Isabelle Refinement Framework

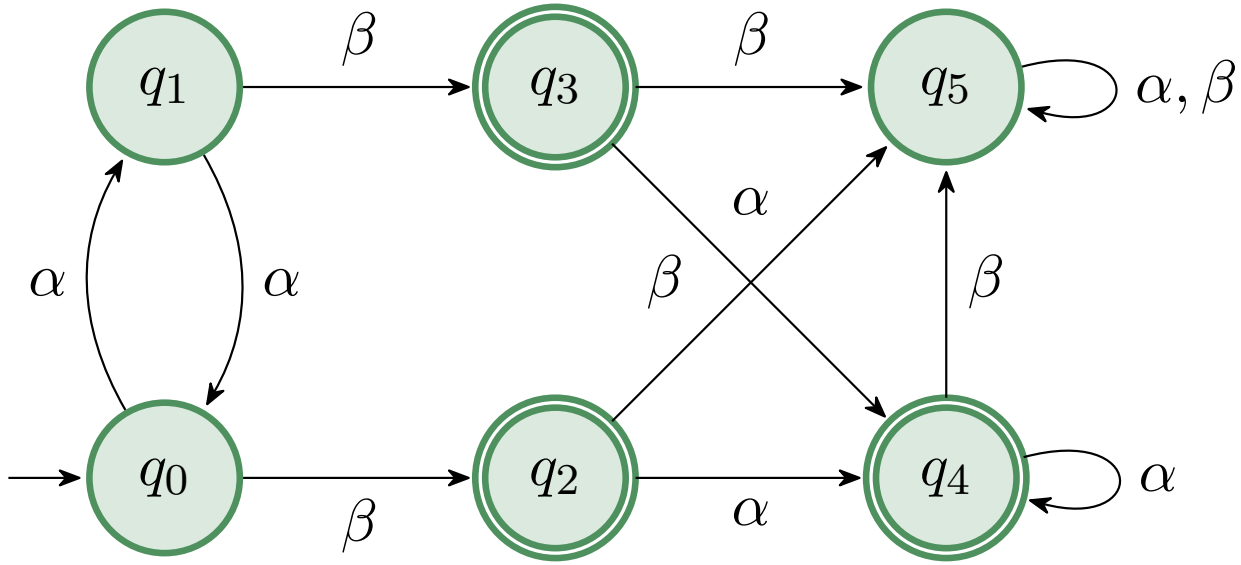
- Stepwise refinement approach to verified program development
- Formal and mathematical
- Ensures correctness at each step

Comes with the Isabelle Collection Framework, which provides an extensive library of reusable verified functional data structures.

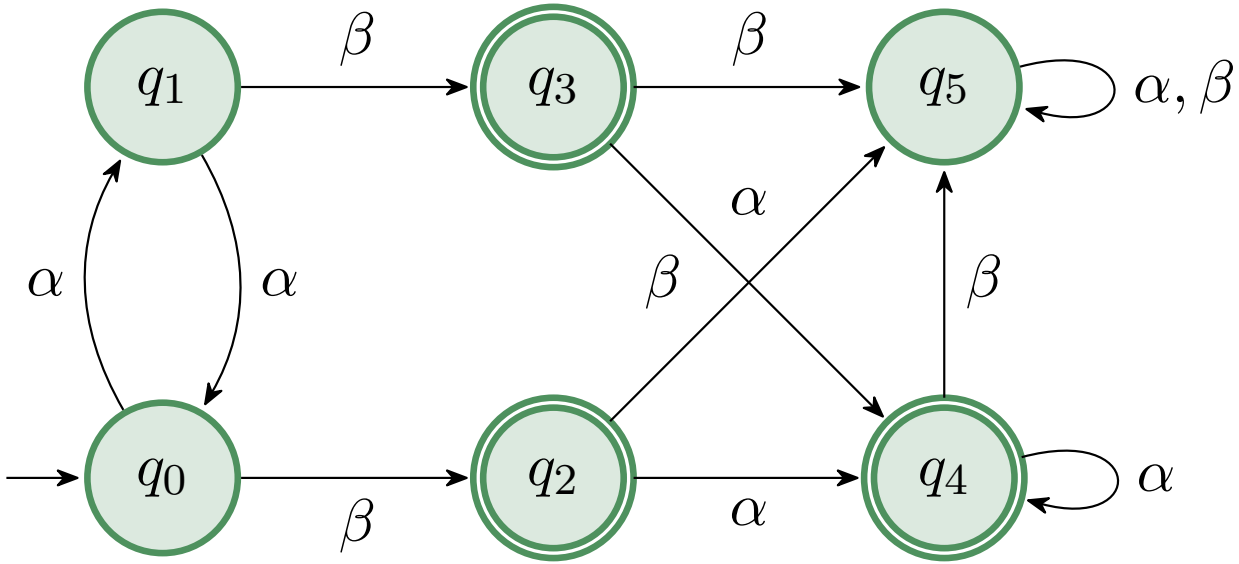

q_1
q_3
q_5
q_0
q_2
q_4
β
β
α, β
α
α
α
β
β
β
α
α



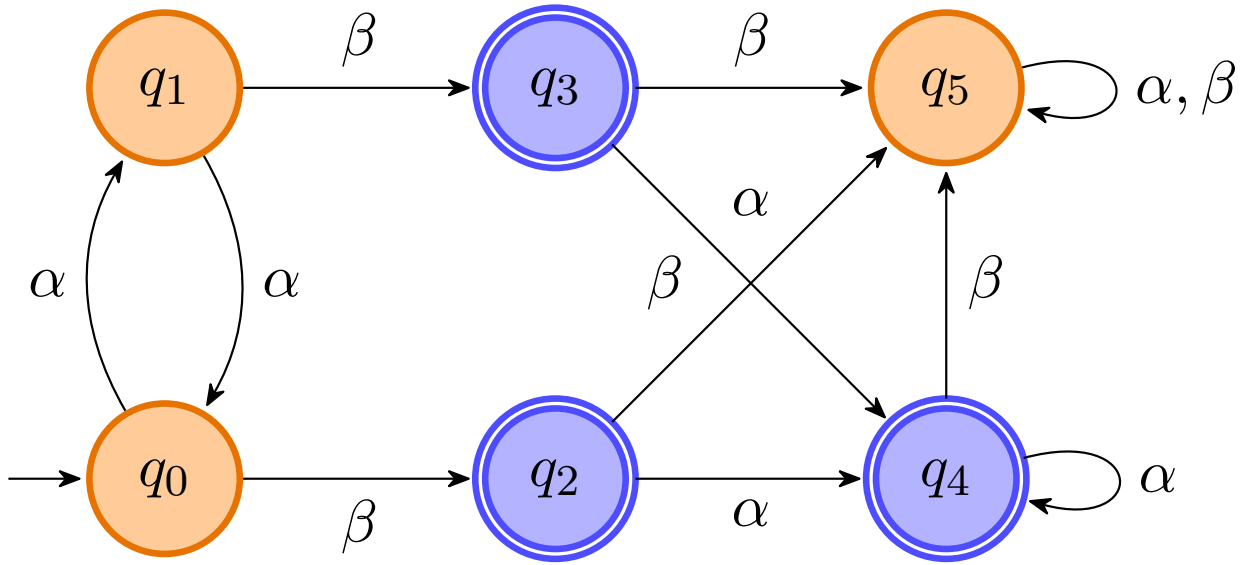
- Successively partitions the set of states into equivalence classes



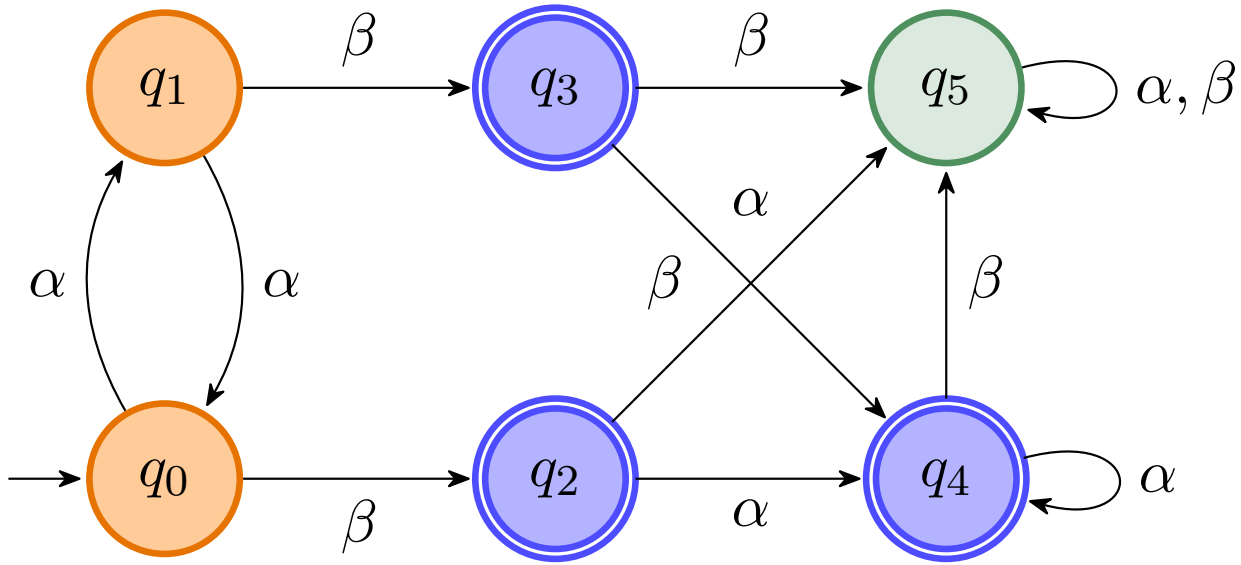
- Successively partitions the set of states into equivalence classes
- Initial partition: accepting and non-accepting states



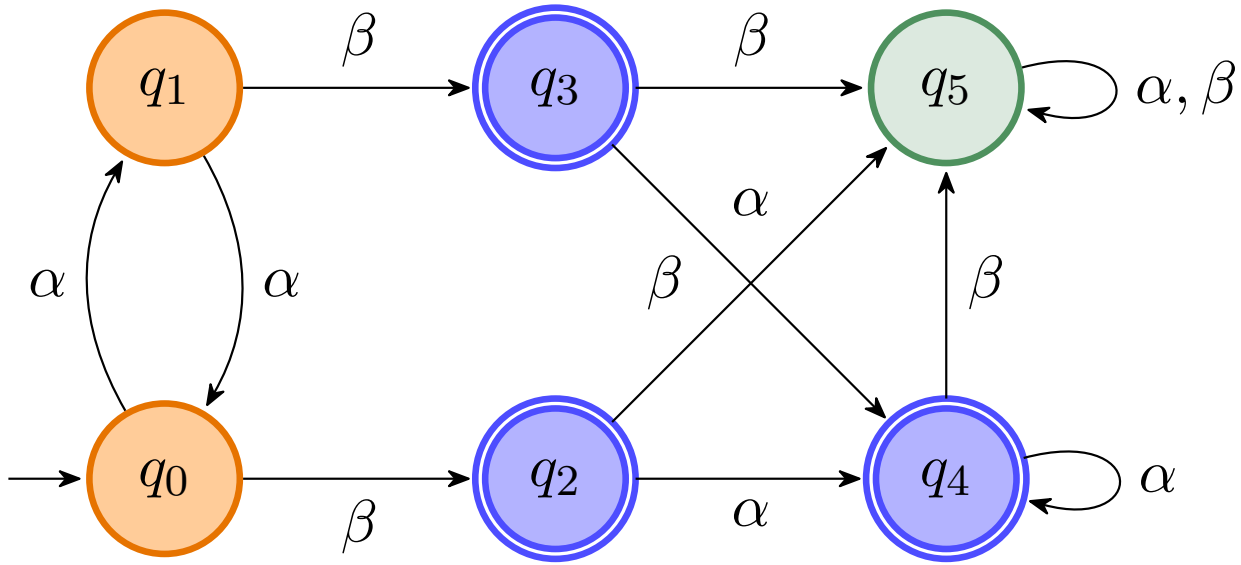
- Successively partitions the set of states into equivalence classes
- Initial partition: accepting and non-accepting states
- Each iteration: pick a splitter and split all blocks of the current partition



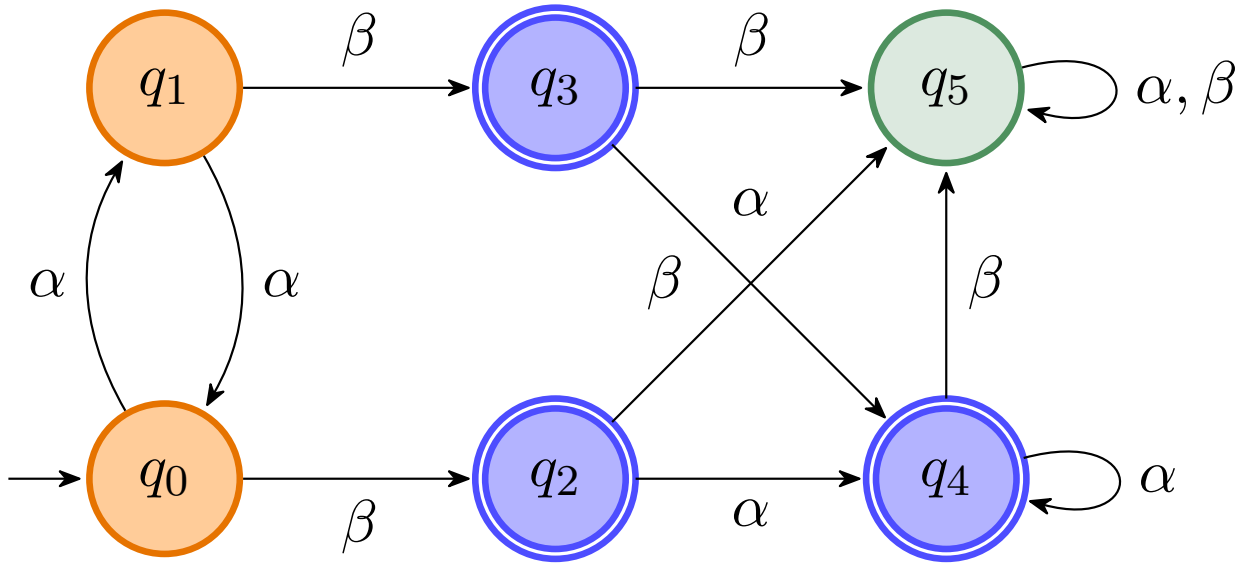
Splitter	Partition	Workset
–	$\{q_0, q_1, q_5\}\{q_2, q_3, q_4\}$	$(\alpha, \{q_0, q_1, q_5\})$ $(\beta, \{q_0, q_1, q_5\})$



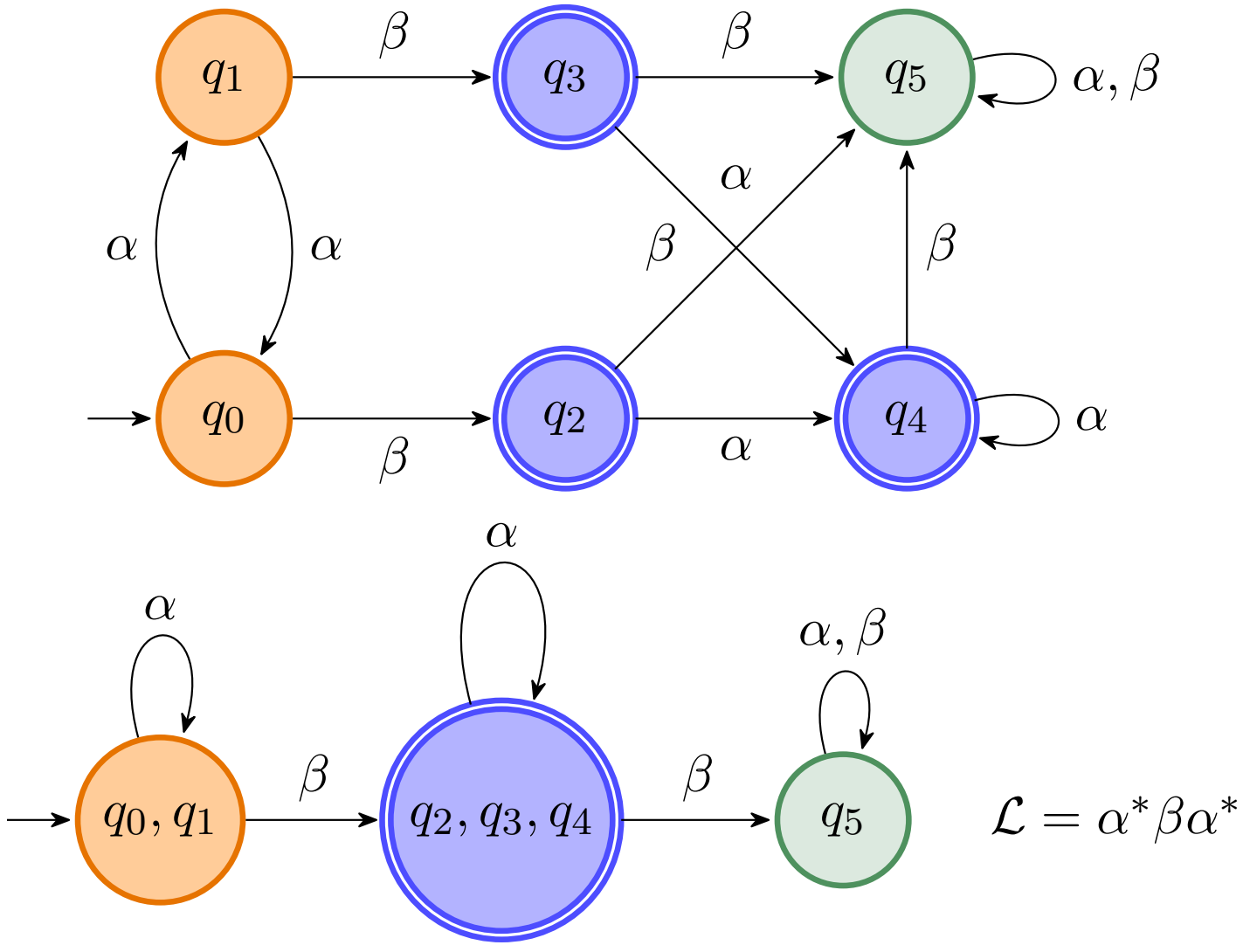
Splitter	Partition	Workset
–	$\{q_0, q_1, q_5\}\{q_2, q_3, q_4\}$	$(\alpha, \{q_0, q_1, q_5\})$ $(\beta, \{q_0, q_1, q_5\})$
$(\beta, \{q_0, q_1, q_5\})$	$\{q_0, q_1\}\{q_5\}\{q_2, q_3, q_4\}$	$(\alpha, \{q_0, q_1\})$ $(\alpha, \{q_5\})$



Splitter	Partition	Workset
–	$\{q_0, q_1, q_5\}\{q_2, q_3, q_4\}$	$(\alpha, \{q_0, q_1, q_5\})\ (\beta, \{q_0, q_1, q_5\})$
$(\beta, \{q_0, q_1, q_5\})$	$\{q_0, q_1\}\{q_5\}\{q_2, q_3, q_4\}$	$(\alpha, \{q_0, q_1\})\ (\alpha, \{q_5\})$
$(\alpha, \{q_0, q_1\})$	$\{q_0, q_1\}\{q_5\}\{q_2, q_3, q_4\}$	$(\alpha, \{q_5\})$



Splitter	Partition	Workset
–	$\{q_0, q_1, q_5\}\{q_2, q_3, q_4\}$	$(\alpha, \{q_0, q_1, q_5\})\ (\beta, \{q_0, q_1, q_5\})$
$(\beta, \{q_0, q_1, q_5\})$	$\{q_0, q_1\}\{q_5\}\{q_2, q_3, q_4\}$	$(\alpha, \{q_0, q_1\})\ (\alpha, \{q_5\})$
$(\alpha, \{q_0, q_1\})$	$\{q_0, q_1\}\{q_5\}\{q_2, q_3, q_4\}$	$(\alpha, \{q_5\})$
$(\alpha, \{q_5\})$	$\{q_0, q_1\}\{q_5\}\{q_2, q_3, q_4\}$	$\varnothing$


q_1
q_3
q_5
q_0
q_2
q_4
β
β
α, β
α
α
β
β
β
α
α
α
α
α, β
q_0, q_1
q_2, q_3, q_4
q_5
β
β
$\mathcal{L} = \alpha^* \beta \alpha^*$

Formalization

Coming soon