COMP-330
Theory of Computation

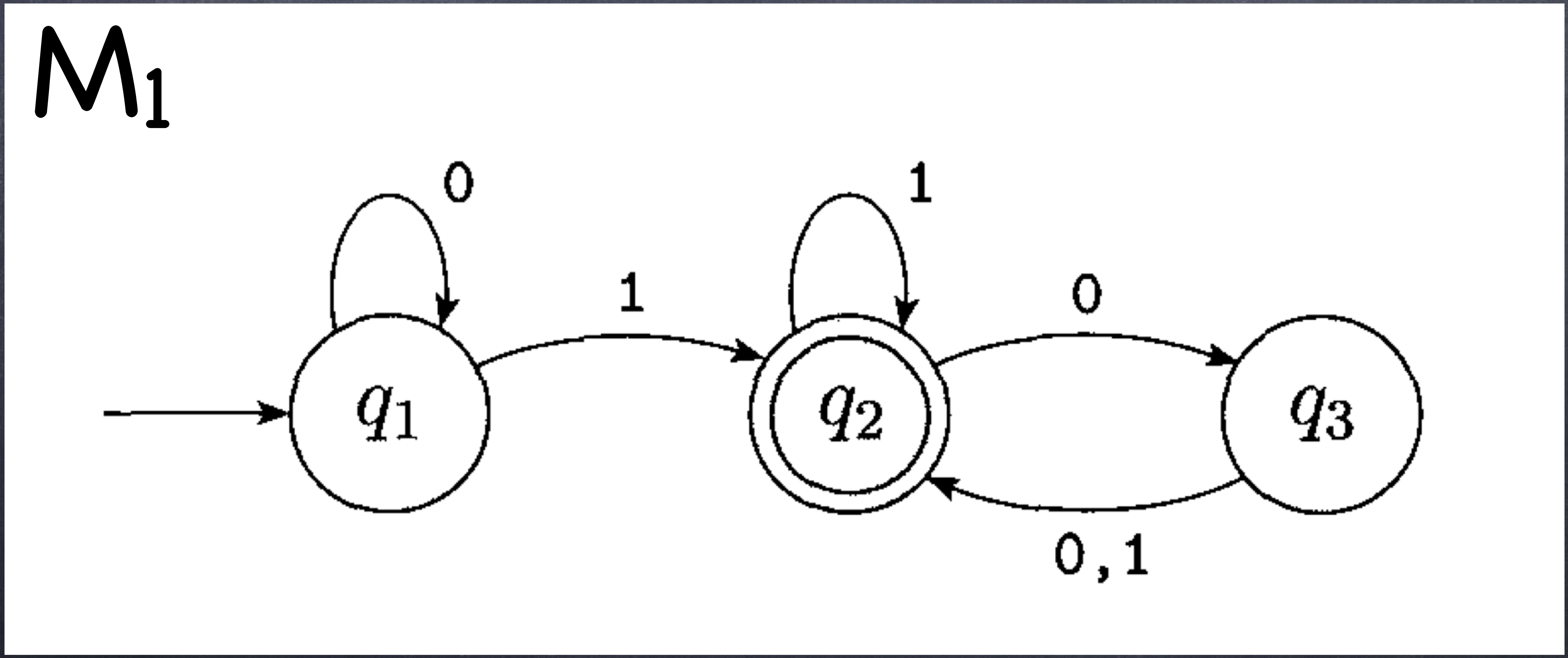
Fall 2019 -- Prof. Claude Crépeau

LECTURE 3 :
Deterministic F A

COMP 330 Fall 2019: Lectures Schedule

1-2. Introduction
    1.5. Some basic mathematics
2-3. Deterministic finite automata +Closure properties,
3-4. Nondeterministic finite automata
5. Minimization+ Myhill-Nerode theorem
6. Determinization+Kleene's theorem
7. Regular Expressions+GNFA
8. Regular Expressions and Languages
9-10. The pumping lemma
11. Duality
12. Labelled transition systems
13. MIDTERM
14. Context-free languages
15. Pushdown automata
16. Parsing
17. The pumping lemma for CFLs
18. Introduction to computability
19. Models of computation
    Basic computability theory
20. Reducibility, undecidability and Rice's theorem
21. Undecidable problems about CFGs
22. Post Correspondence Problem
23. Validity of FOL is RE / Gödel's and Tarski's thms
24. Universality / The recursion theorem
25. Degrees of undecidability
26. Introduction to complexity

DFA: example



Definition of DFA

- States
- Alphabet
- Transition function
- Start state
- Accept states

Definition of DFA

- States

- Alphabet
- Transition function
- Start state
- Accept states

Definition of DFA

- States q_1 q_2 q_3
- Alphabet a,b,c,d
- Transition function
- Start state
- Accept states

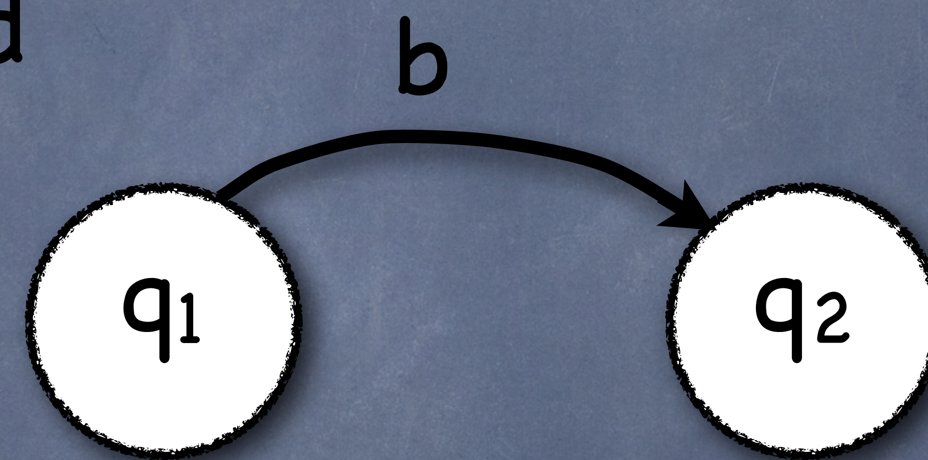
Definition of DFA

- States

- Alphabet

a,b,c,d

- Transition function



- Start state
- Accept states

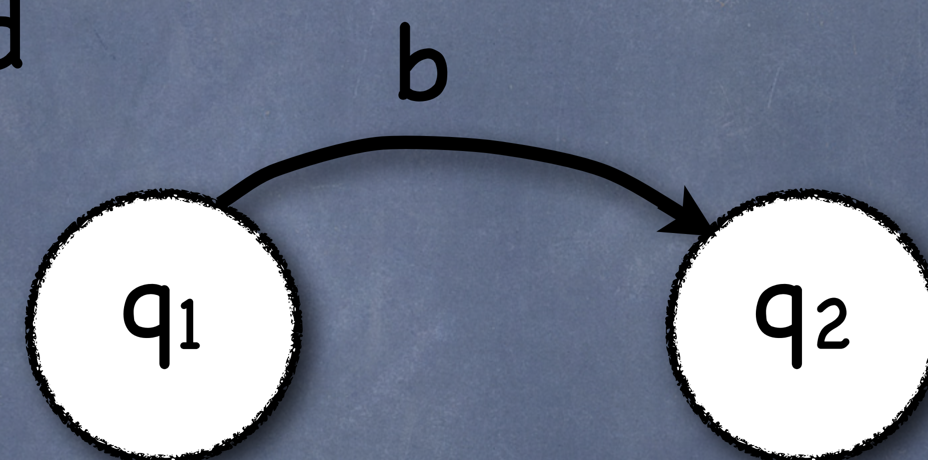
Definition of DFA

- States

- Alphabet

a,b,c,d

- Transition function



- Start state

- Accept states

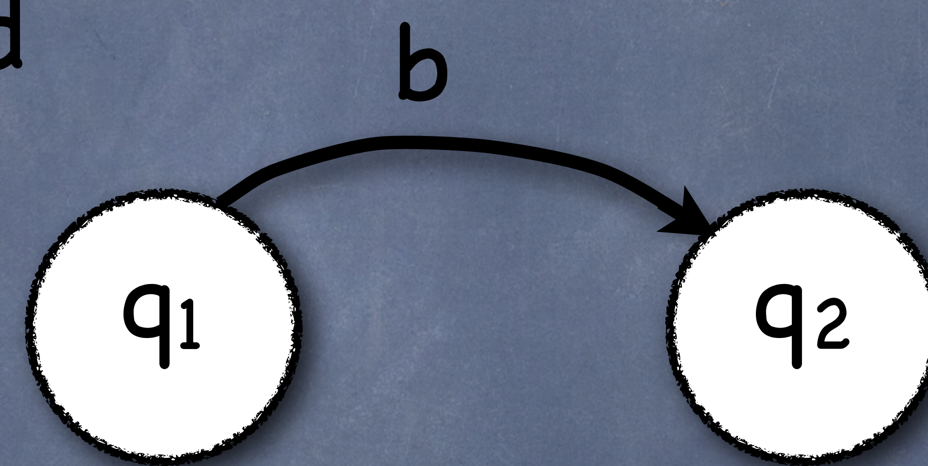
Definition of DFA

- States

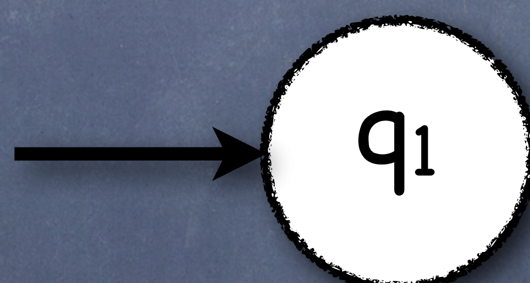
- Alphabet

a,b,c,d

- Transition function



- Start state



- Accept states

Definition of DFA

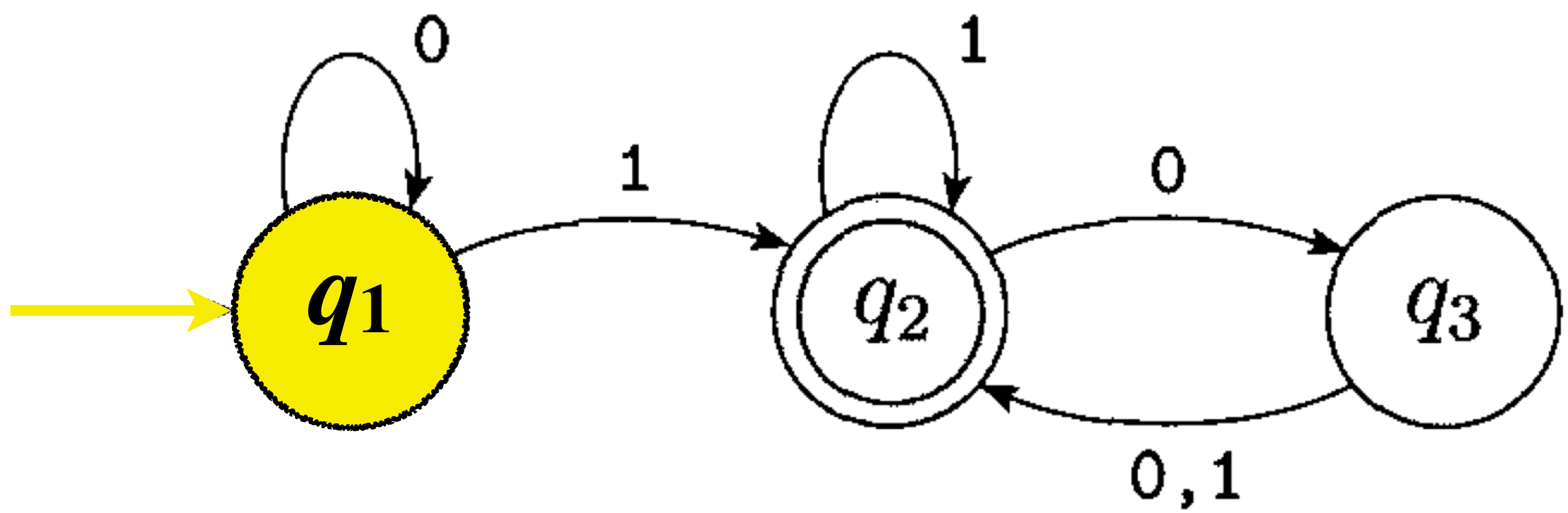
DEFINITION 1.5

A ***finite automaton*** is a 5-tuple $(Q, \Sigma, \delta, q_0, F)$, where

1. Q is a finite set called the ***states***,
2. Σ is a finite set called the ***alphabet***,
3. $\delta \colon Q \times \Sigma \longrightarrow Q$ is the ***transition function***,
4. $q_0 \in Q$ is the ***start state***, and
5. $F \subseteq Q$ is the ***set of accept states***.

M_1

10010101



We can describe M_1 formally by writing $M_1 = (Q, \Sigma, \delta, q_1, F)$, where

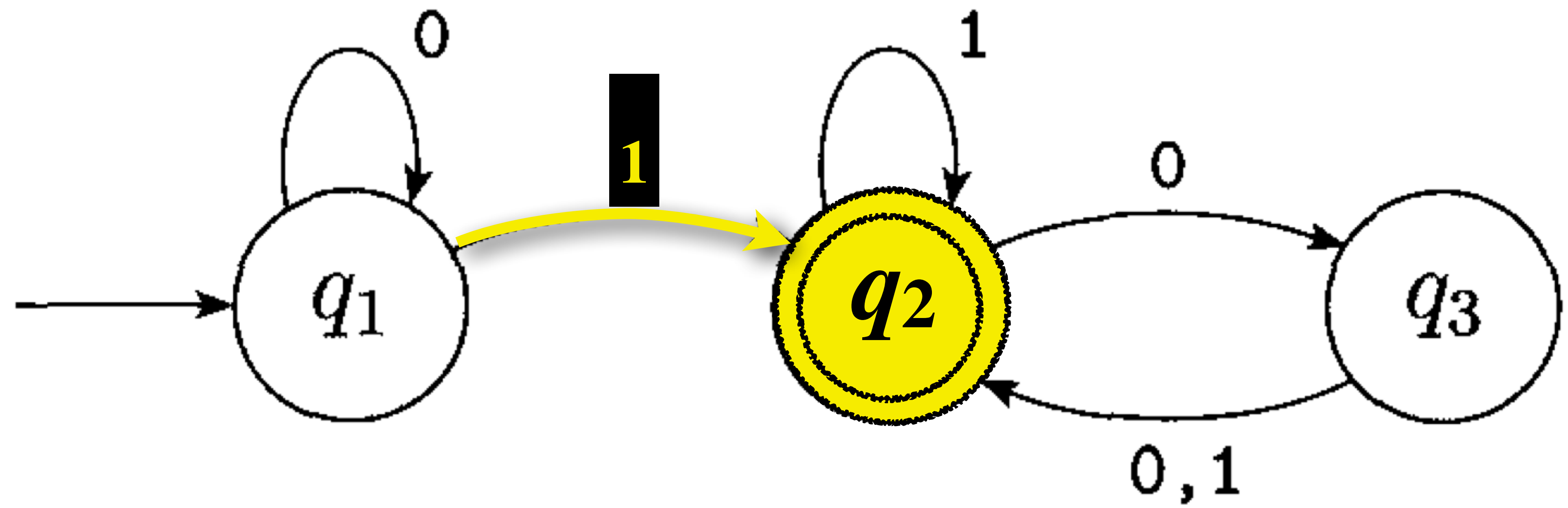
1. $Q = \{q_1, q_2, q_3\}$,
2. $\Sigma = \{0,1\}$,
3. δ is described as

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

4. q_1 is the start state, and
5. $F = \{q_2\}$.

M_1

10010101



We can describe M_1 formally by writing $M_1 = (Q, \Sigma, \delta, q_1, F)$, where

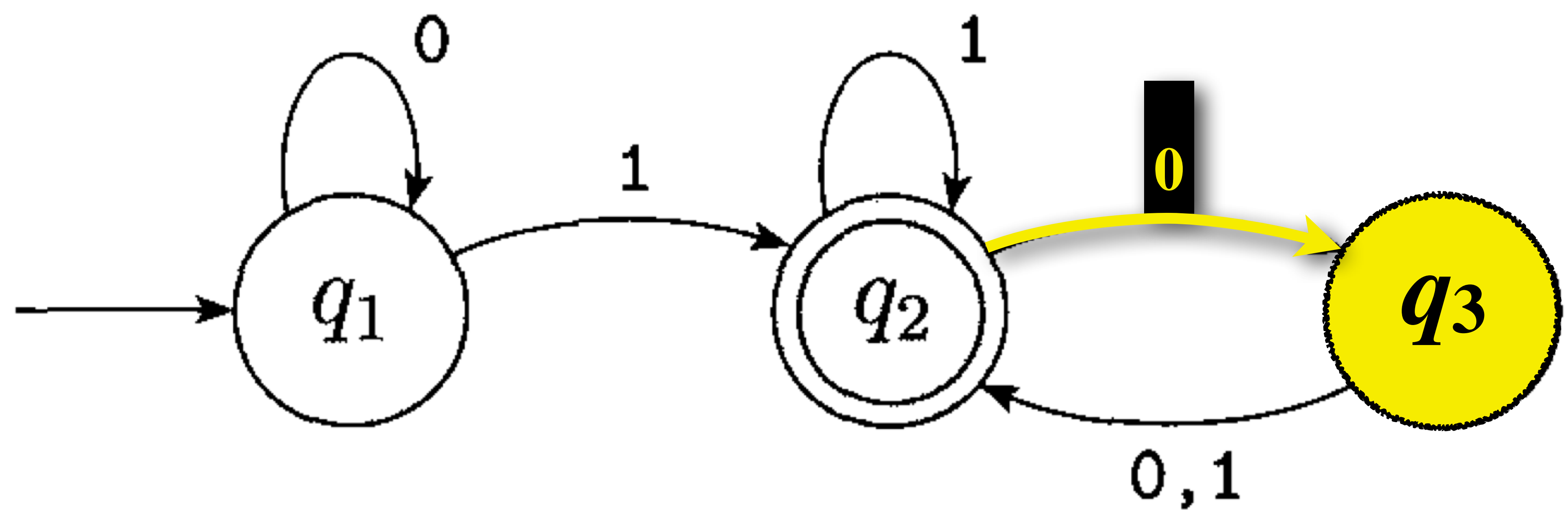
1. $Q = \{q_1, q_2, q_3\}$,
2. $\Sigma = \{0,1\}$,
3. δ is described as

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

4. q_1 is the start state, and
5. $F = \{q_2\}$.

M_1

10010101



We can describe M_1 formally by writing $M_1 = (Q, \Sigma, \delta, q_1, F)$, where

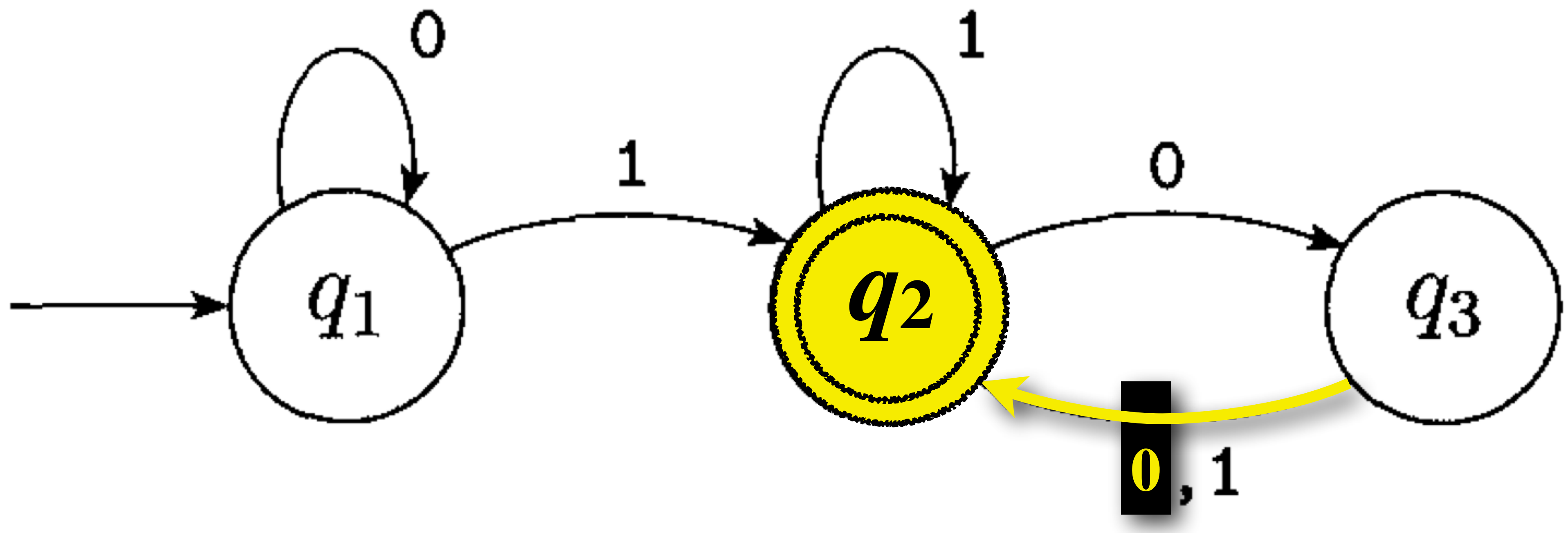
1. $Q = \{q_1, q_2, q_3\}$,
2. $\Sigma = \{0,1\}$,
3. δ is described as

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

4. q_1 is the start state, and
5. $F = \{q_2\}$.

M_1

10010101



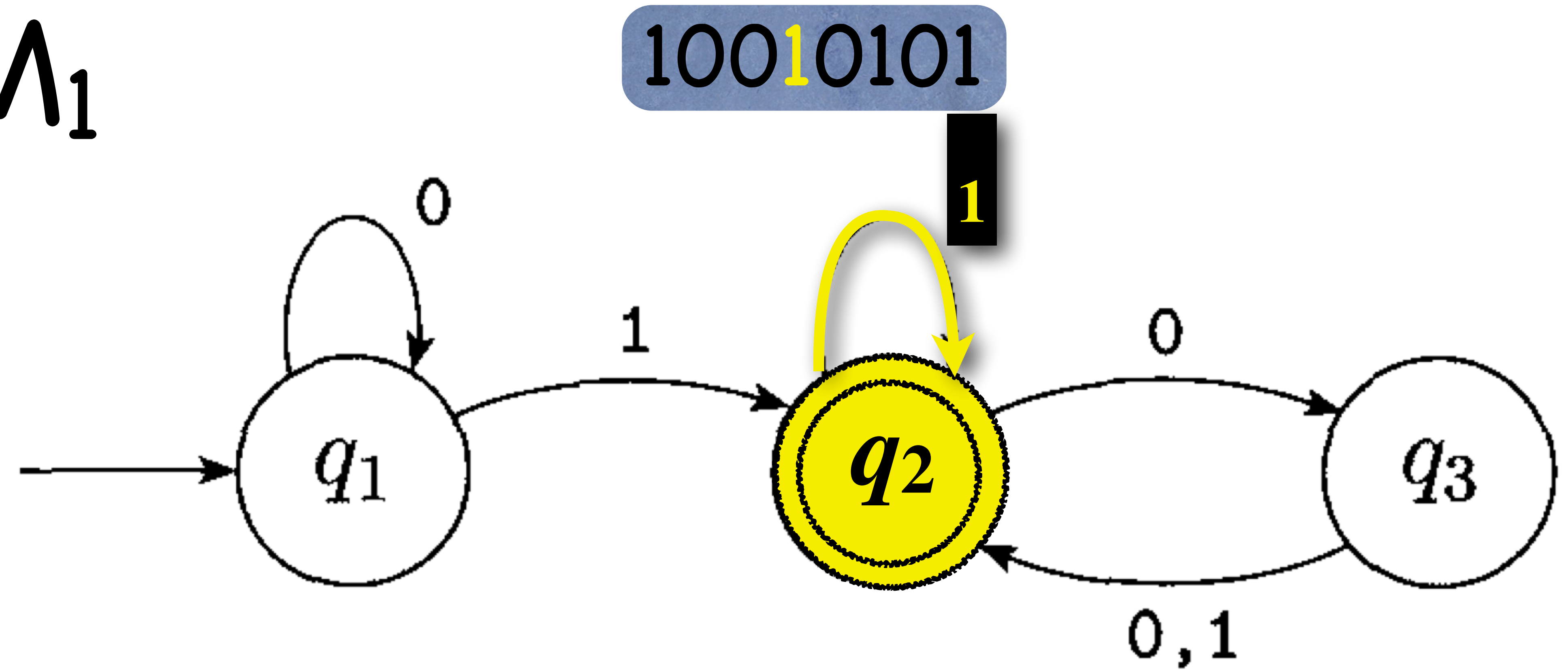
We can describe M_1 formally by writing $M_1 = (Q, \Sigma, \delta, q_1, F)$, where

1. $Q = \{q_1, q_2, q_3\}$,
2. $\Sigma = \{0,1\}$,
3. δ is described as

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

4. q_1 is the start state, and
5. $F = \{q_2\}$.

M_1



We can describe M_1 formally by writing $M_1 = (Q, \Sigma, \delta, q_1, F)$, where

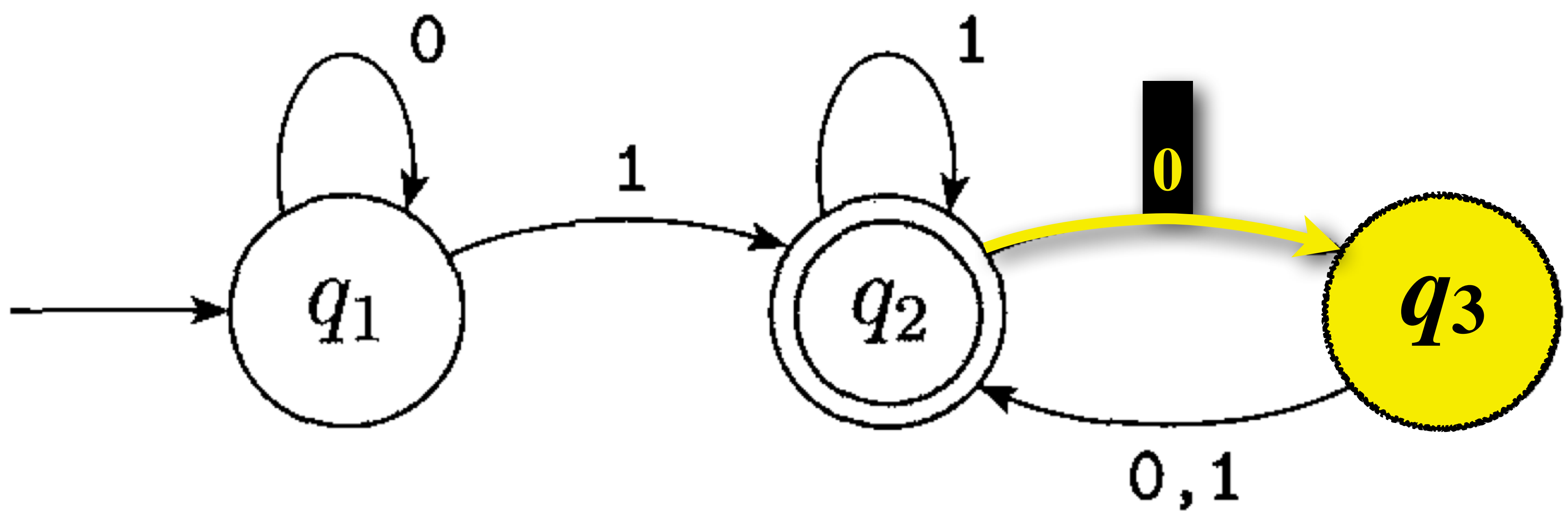
1. $Q = \{q_1, q_2, q_3\}$,
2. $\Sigma = \{0,1\}$,
3. δ is described as

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

4. q_1 is the start state, and
5. $F = \{q_2\}$.

M_1

10010101



We can describe M_1 formally by writing $M_1 = (Q, \Sigma, \delta, q_1, F)$, where

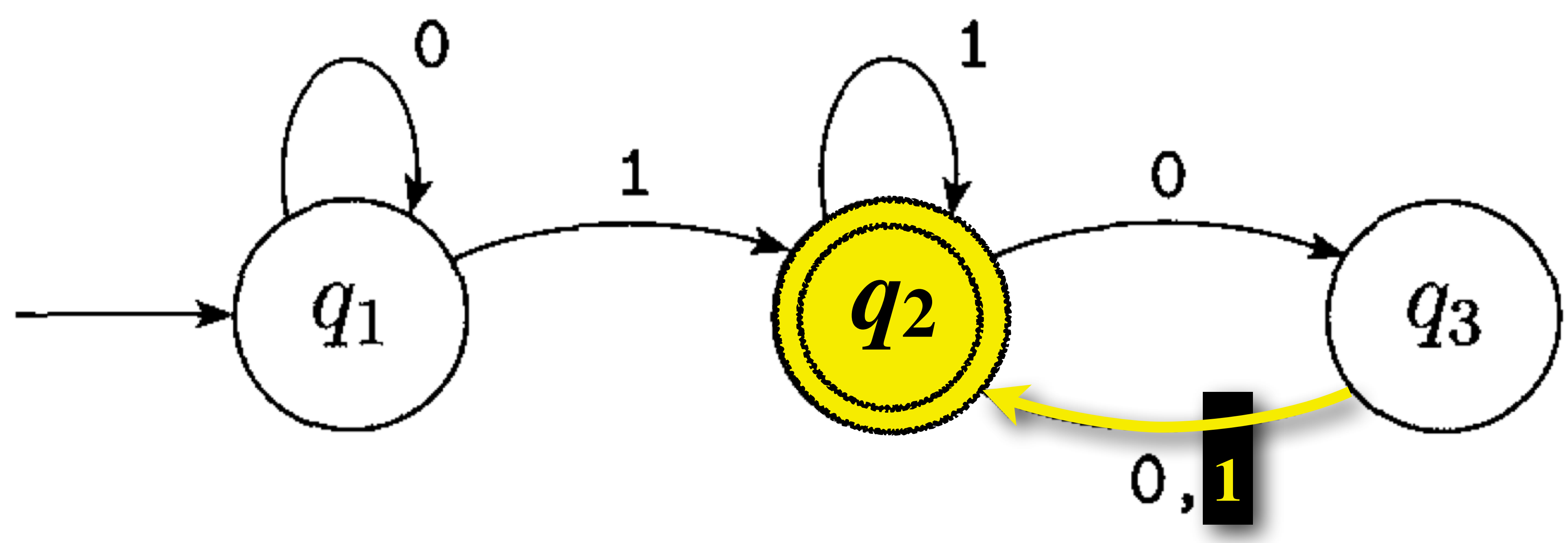
1. $Q = \{q_1, q_2, q_3\}$,
2. $\Sigma = \{0,1\}$,
3. δ is described as

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

4. q_1 is the start state, and
5. $F = \{q_2\}$.

M_1

10010101



We can describe M_1 formally by writing $M_1 = (Q, \Sigma, \delta, q_1, F)$, where

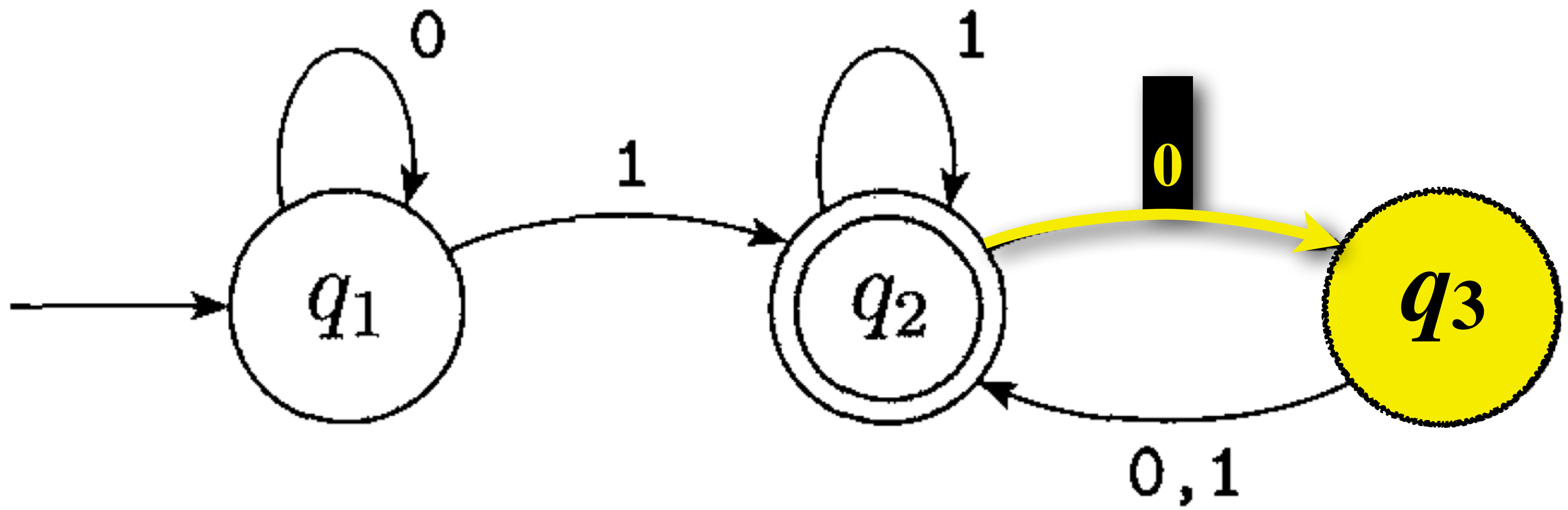
1. $Q = \{q_1, q_2, q_3\}$,
2. $\Sigma = \{0,1\}$,
3. δ is described as

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

4. q_1 is the start state, and
5. $F = \{q_2\}$.

M_1

10010101

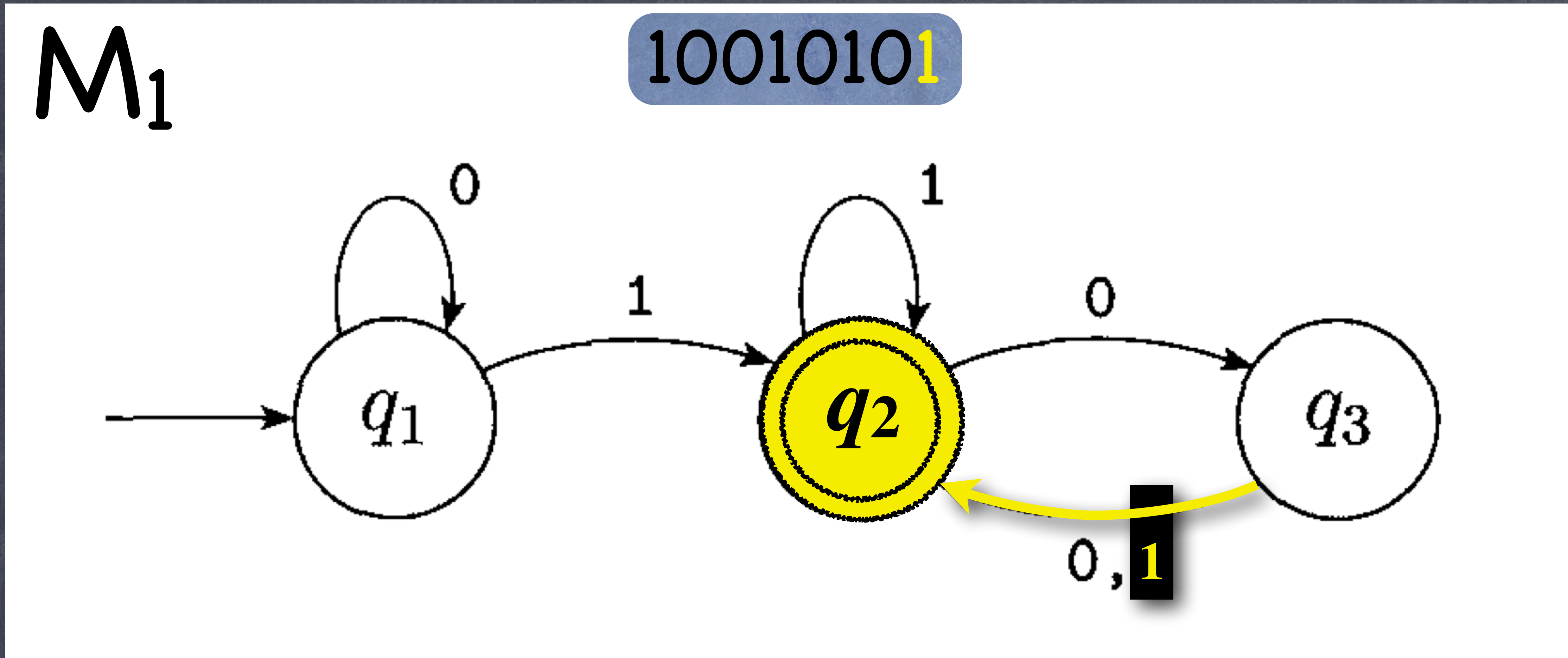


We can describe M_1 formally by writing $M_1 = (Q, \Sigma, \delta, q_1, F)$, where

1. $Q = \{q_1, q_2, q_3\}$,
2. $\Sigma = \{0,1\}$,
3. δ is described as

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

4. q_1 is the start state, and
5. $F = \{q_2\}$.



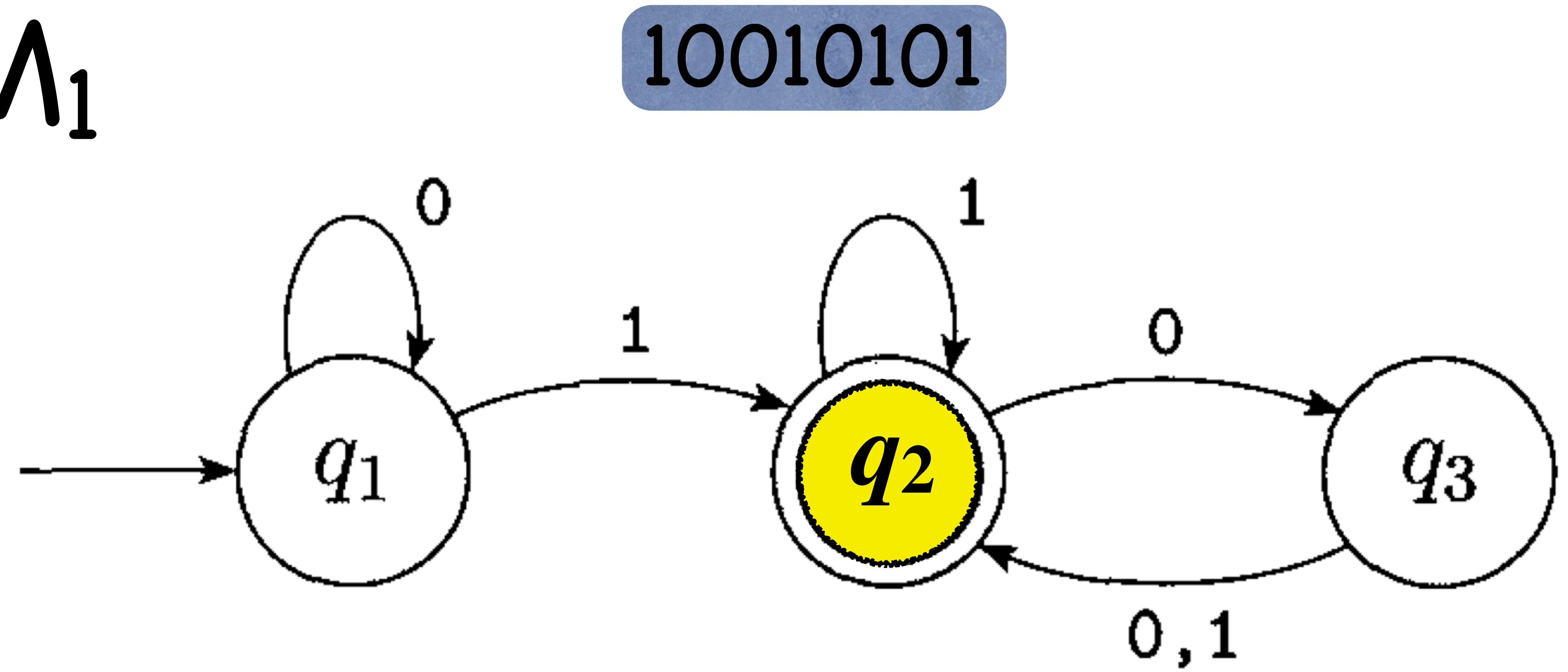
We can describe M_1 formally by writing $M_1 = (Q, \Sigma, \delta, q_1, F)$, where

1. $Q = \{q_1, q_2, q_3\}$,
2. $\Sigma = \{0,1\}$,
3. δ is described as

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

4. q_1 is the start state, and
5. $F = \{q_2\}$.

M_1



We can describe M_1 formally by writing $M_1 = (Q, \Sigma, \delta, q_1, F)$, where

1. $Q = \{q_1, q_2, q_3\}$,
2. $\Sigma = \{0,1\}$,
3. δ is described as

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

4. q_1 is the start state, and
5. $F = \{q_2\}$.

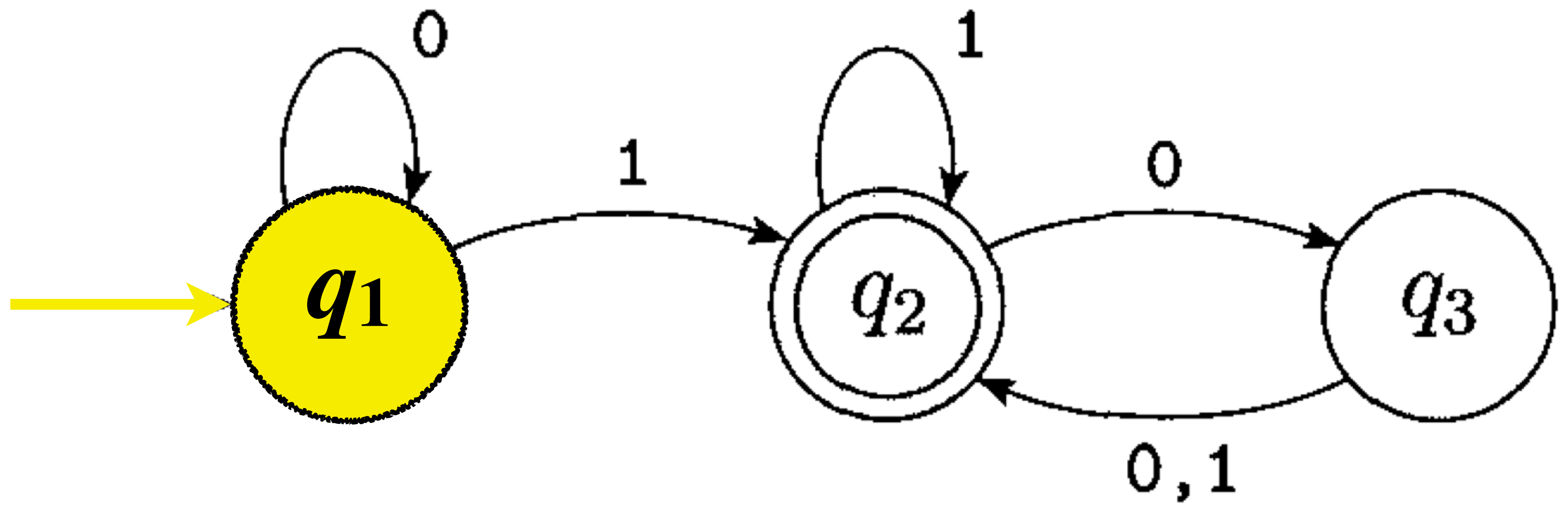
Regular Languages

- Let $M=(Q,\Sigma,\delta,q_0,F)$ be a finite state automaton and let $w=w_1w_2...w_n$ $(n\geq 0)$ be a string where each symbol w_i is from the alphabet Σ.
- M **accepts** w if states $s_0,s_1,\ldots,s_n$ exist s.t.
  1. $s_0 = q_0$
  2. $s_{i+1} = \delta(s_i,w_{i+1})$ for $i = 0 \ldots n-1$, and
  3. $s_n \in F$

Example

M_1

10010101



We can describe M_1 formally by writing $M_1 = (Q, \Sigma, \delta, q_1, F)$, where

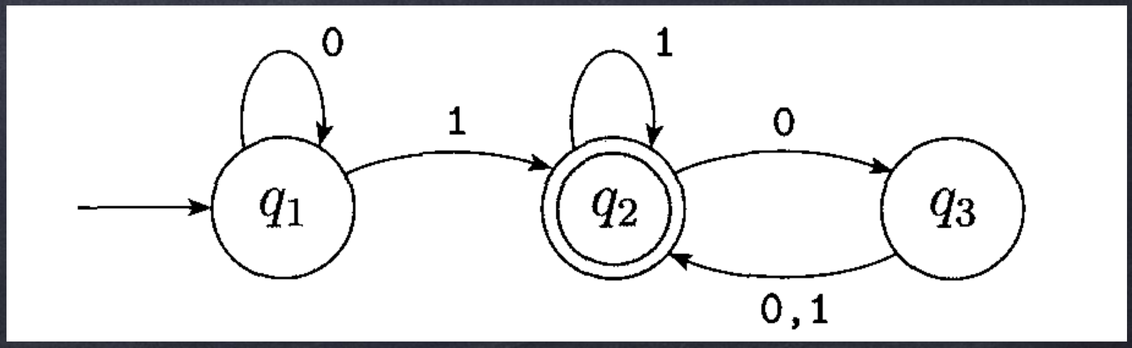
1. $Q = \{q_1, q_2, q_3\}$,
2. $\Sigma = \{0,1\}$,
3. δ is described as

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

4. q_1 is the start state, and
5. $F = \{q_2\}$.

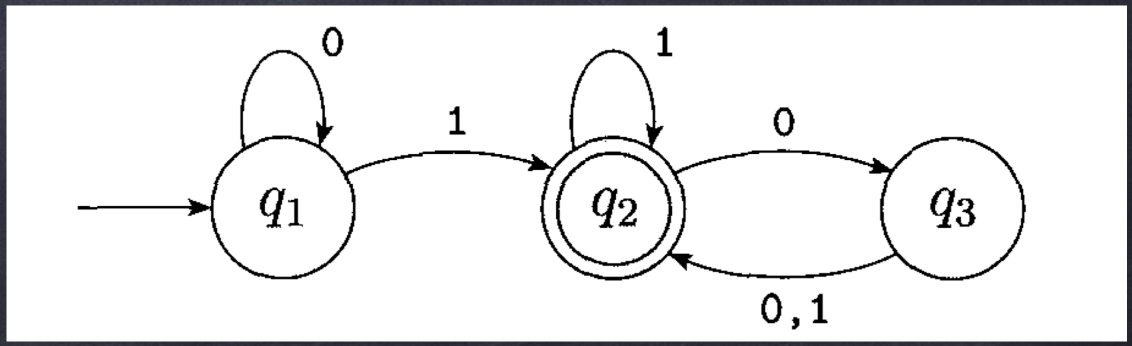
Example

Regular Languages



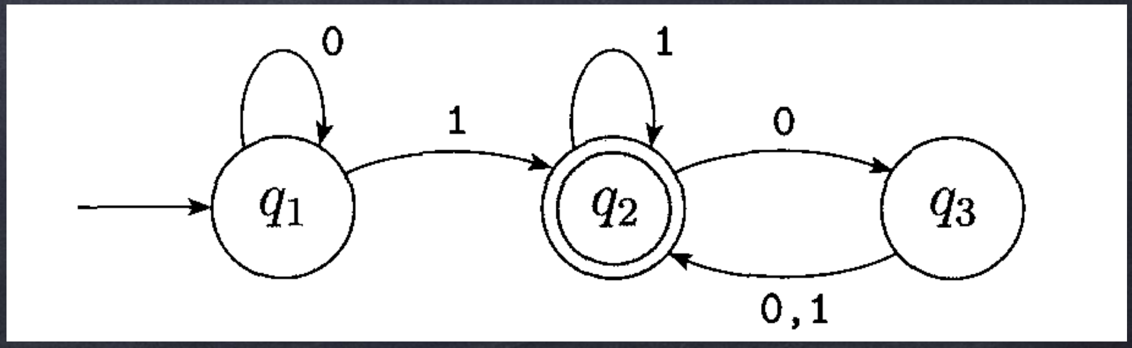
Regular Languages

- M1 **accepts** 10010101 since states $s_0, s_1, \ldots, s_8$ exist s.t.



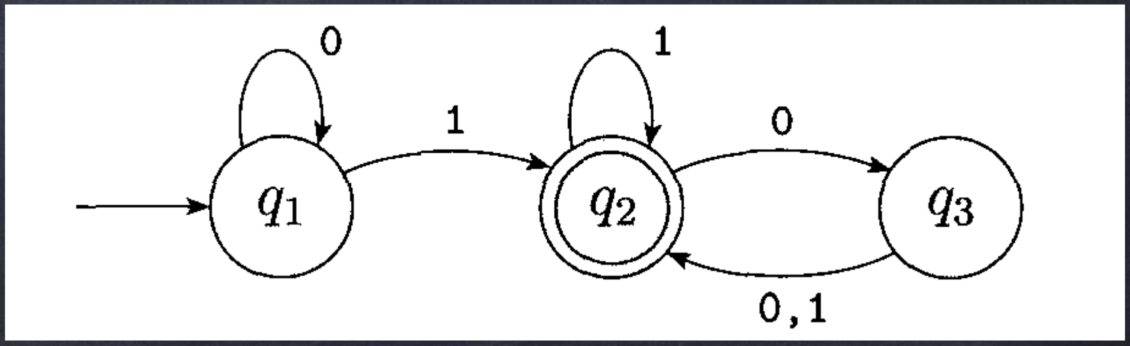
Regular Languages

- M1 **accepts** 10010101 since states $s_0, s_1, \ldots, s_8$ exist s.t.
- 1. $s_0 = q_1$



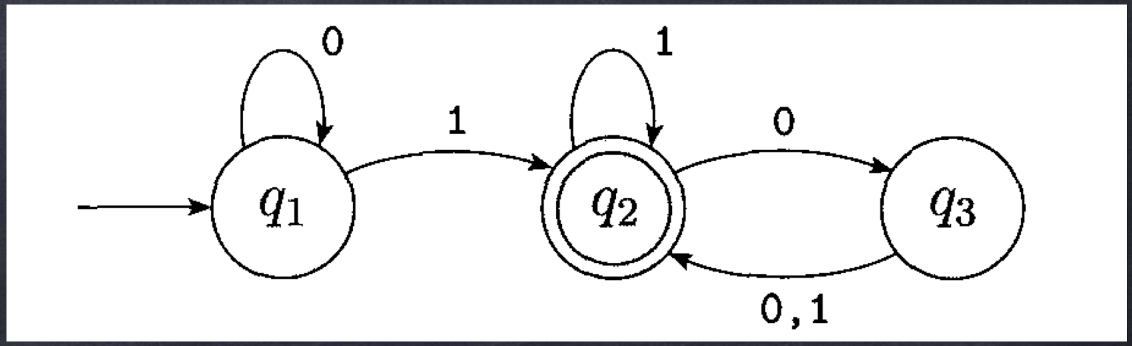
Regular Languages

- M1 **accepts** 10010101 since states $s_0, s_1, \ldots, s_8$ exist s.t.
- 1. $s_0 = q_1$
- 2. $s_1 = q_2 = \delta(q_1,1)$, $s_2 = q_3 = \delta(q_2,0)$,
  $s_3 = q_2 = \delta(q_3,0)$, $s_4 = q_2 = \delta(q_2,1)$,
  $s_5 = q_3 = \delta(q_2,0)$, $s_6 = q_2 = \delta(q_3,1)$,
  $s_7 = q_3 = \delta(q_2,0)$, $s_8 = q_2 = \delta(q_3,1)$



Regular Languages

- M1 **accepts** 10010101 since states $s_0, s_1, \ldots, s_8$ exist s.t.
- 1. $s_0 = q_1$
- 2. $s_1 = q_2 = \delta(q_1,1)$, $s_2 = q_3 = \delta(q_2,0)$,
  $s_3 = q_2 = \delta(q_3,0)$, $s_4 = q_2 = \delta(q_2,1)$,
  $s_5 = q_3 = \delta(q_2,0)$, $s_6 = q_2 = \delta(q_3,1)$,
  $s_7 = q_3 = \delta(q_2,0)$, $s_8 = q_2 = \delta(q_3,1)$
- 3. $s_8 \in F$



Regular Languages

- Let M be a finite state automaton and let $w=w_1w_2...w_n$ $(n \geq 0)$ be a string where each symbol w_i is from the alphabet Σ.
- M **recognizes language** A if

$$A = \{ w \mid M \text{ accepts } w \}$$

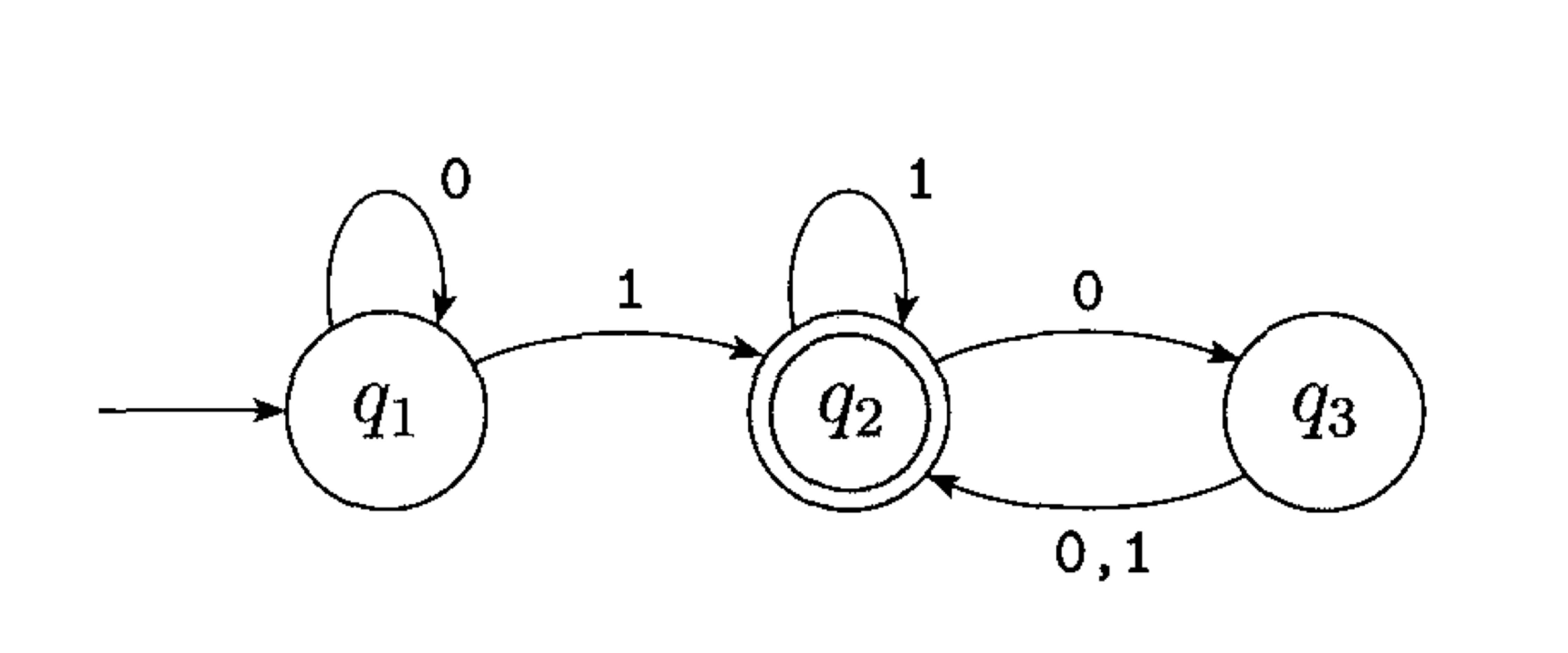
DEFINITION 1.16

A language is called a ***regular language*** if some finite automaton recognizes it.

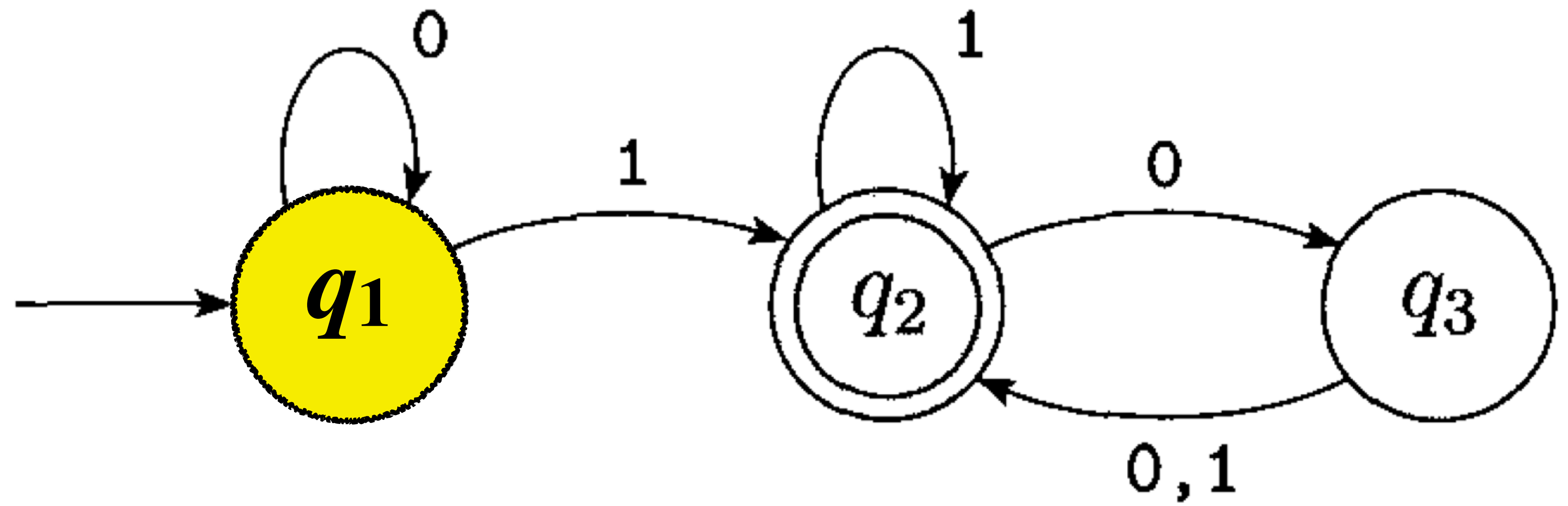
Proving the language M_1 accepts...

- **Theorem 1.A**:

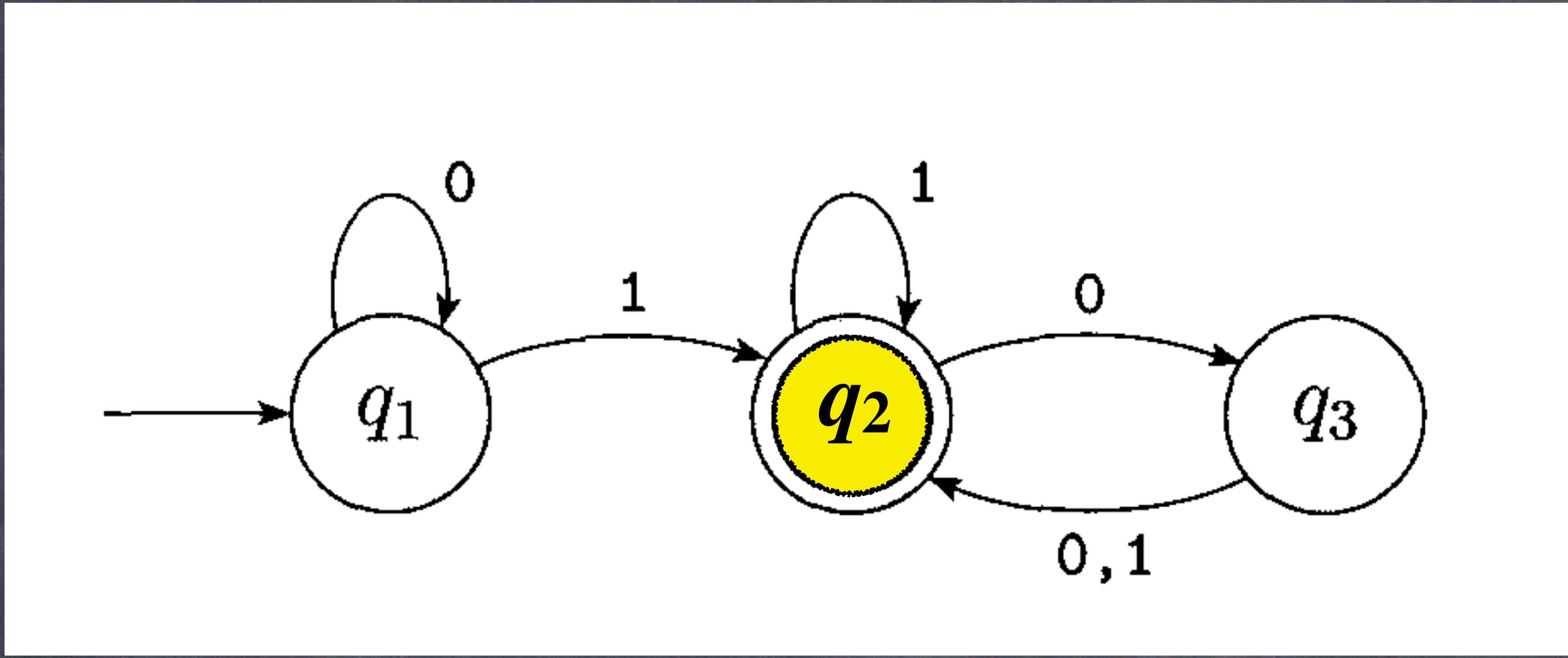
$L(M_1)$ = { All binary strings that contain at least one "1" and end with an even number of "0"s }



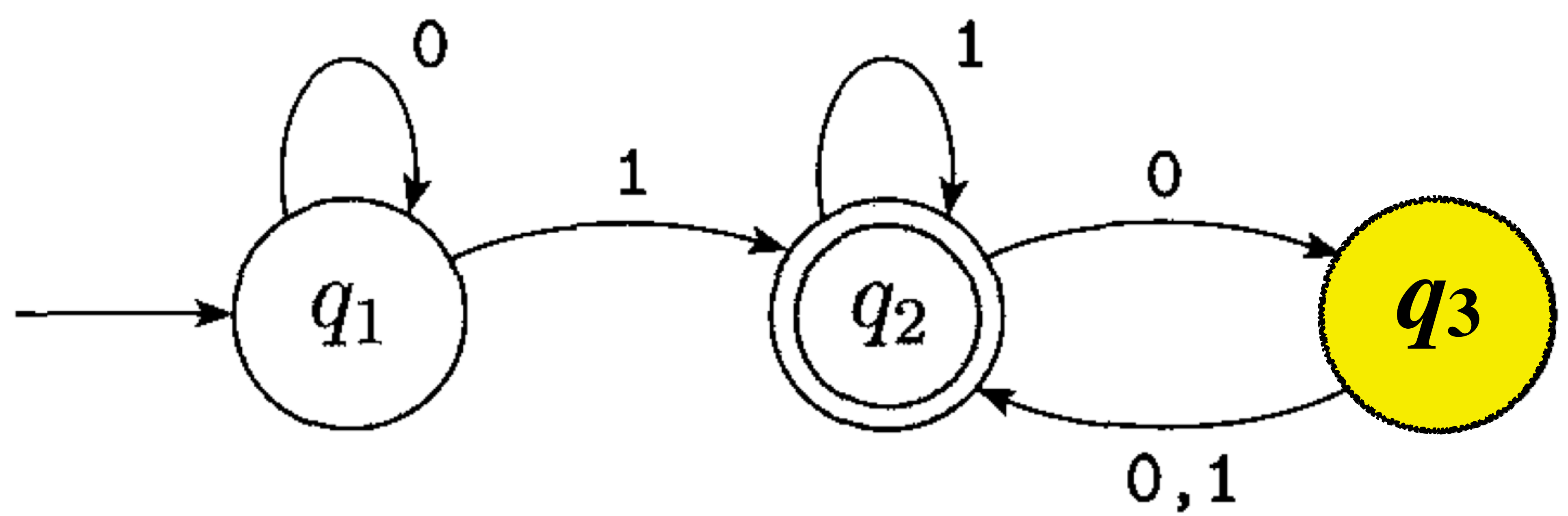
- **Theorem 1.B** : Let $w \in \{0,1\}^*$ be of length $n \geq 0$.
  1) M_1 stops in state q_1 $\Leftrightarrow$ w contains no "1"s.
  2) M_1 stops in state q_2 $\Leftrightarrow$ w contains at least one "1" and ends with an even number of "0"s.
  3) M_1 stops in state q_3 $\Leftrightarrow$ w contains at least one "1" and ends with an odd number of "0"s.



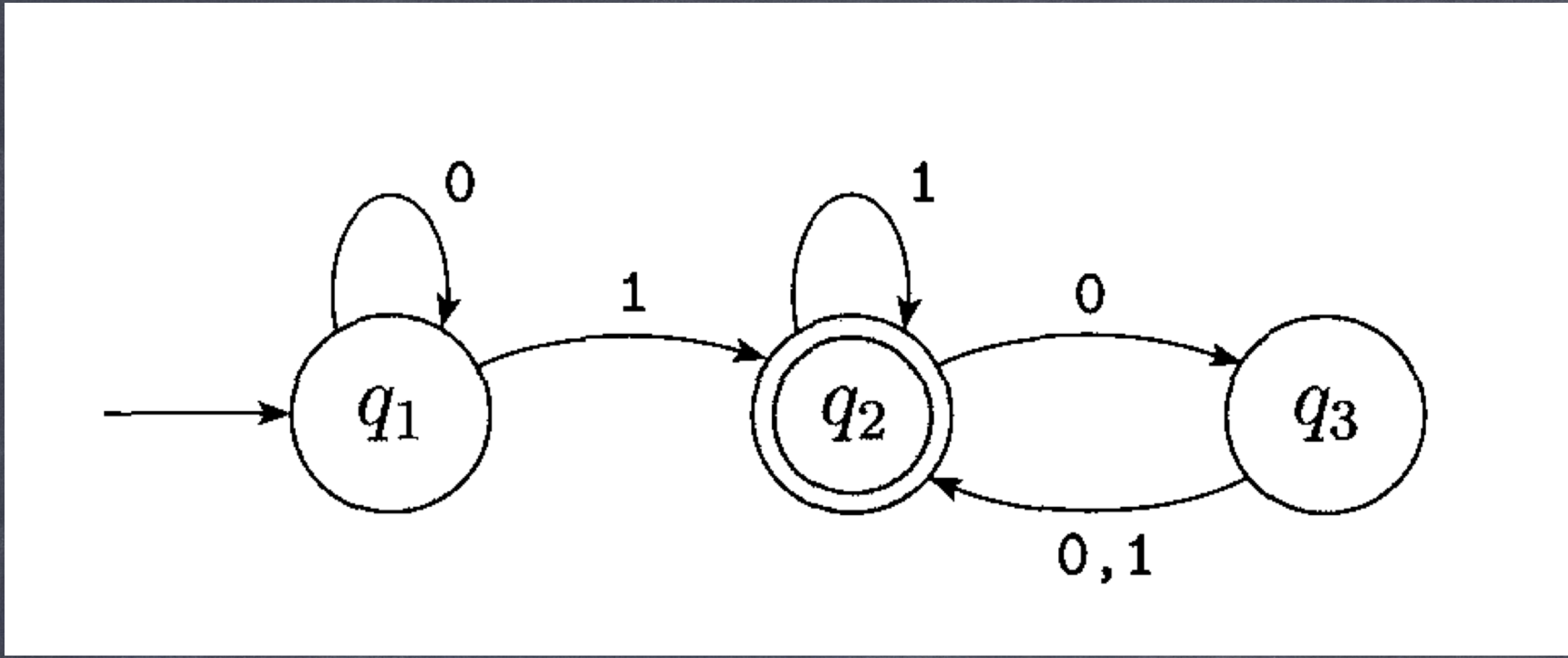
- **Theorem 1.B** : Let $w \in \{0,1\}^*$ be of length $n \geq 0$.
  1) M_1 stops in state $q_1 \Leftrightarrow$ w contains no "1"s.
  2) M_1 stops in state $q_2 \Leftrightarrow$ w contains at least one "1" and ends with an even number of "0"s.
  3) M_1 stops in state $q_3 \Leftrightarrow$ w contains at least one "1" and ends with an odd number of "0"s.



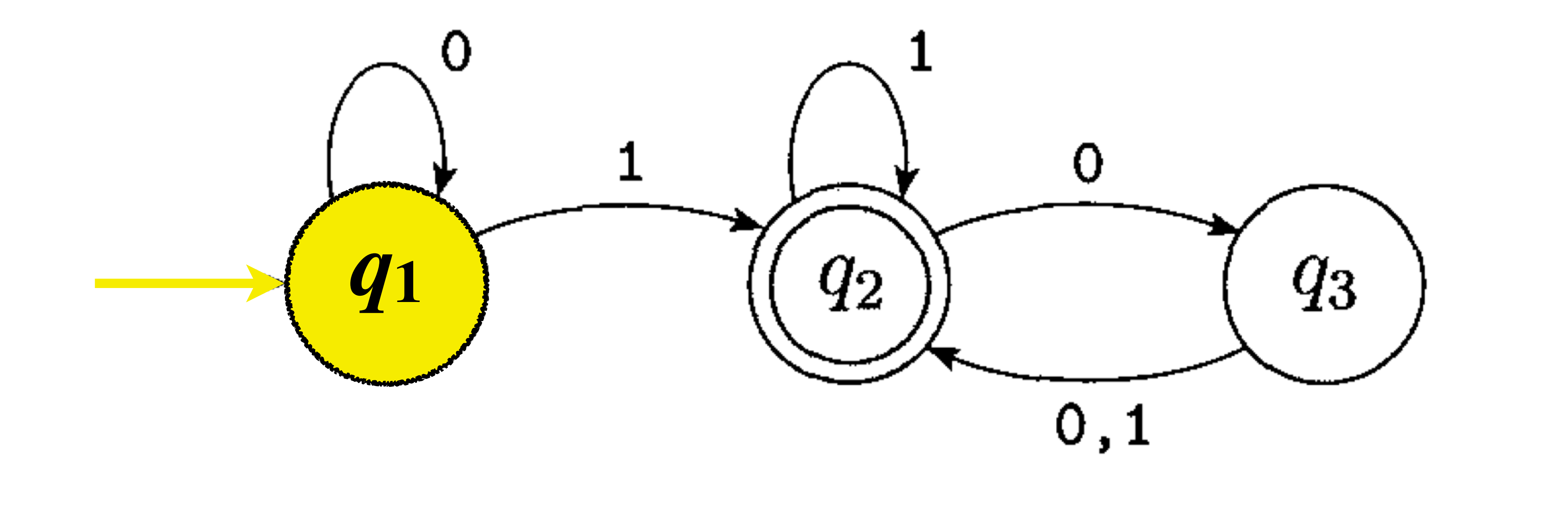
- **Theorem 1.B** : Let $w \in \{0,1\}^*$ be of length $n \geq 0$.
  1) M_1 stops in state q_1 $\Leftrightarrow$ w contains no "1"s.
  2) M_1 stops in state q_2 $\Leftrightarrow$ w contains at least one "1" and ends with an even number of "0"s.
  3) M_1 stops in state q_3 $\Leftrightarrow$ w contains at least one "1" and ends with an odd number of "0"s.



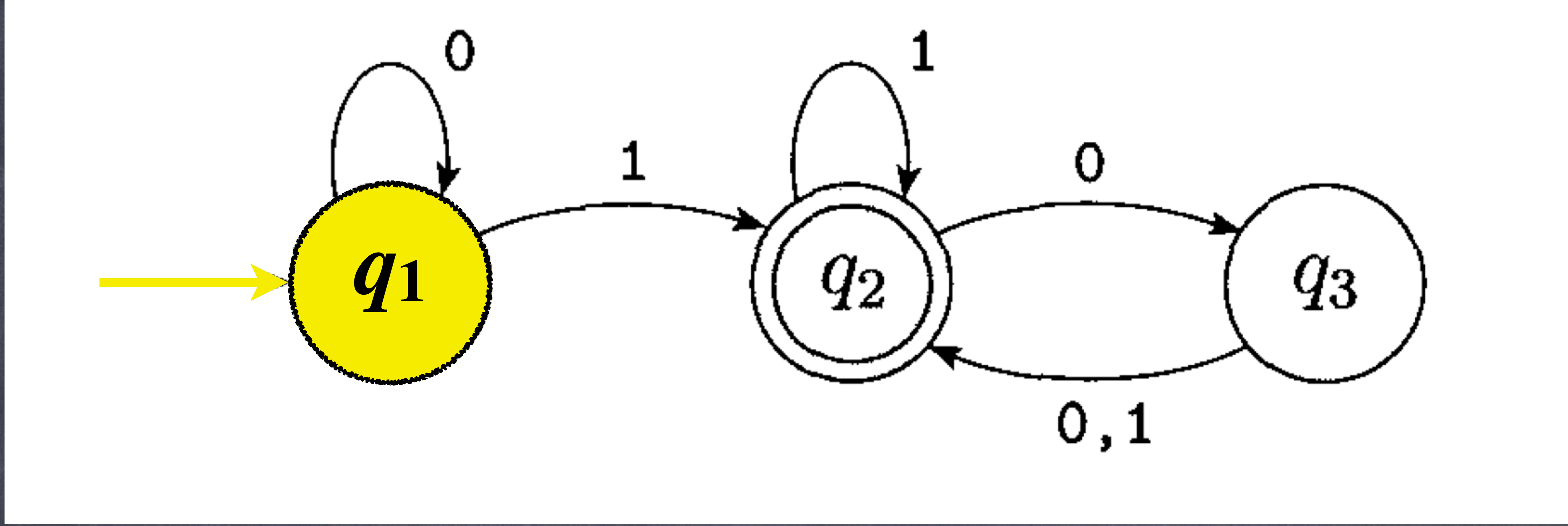
- **Theorem 1.B** : Let $w \in \{0,1\}^*$ be of length $n \geq 0$.
  1) M_1 stops in state $q_1 \Leftrightarrow$ w contains no "1"s.
  2) M_1 stops in state $q_2 \Leftrightarrow$ w contains at least one "1" and ends with an even number of "0"s.
  3) M_1 stops in state $q_3 \Leftrightarrow$ w contains at least one "1" and ends with an odd number of "0"s.



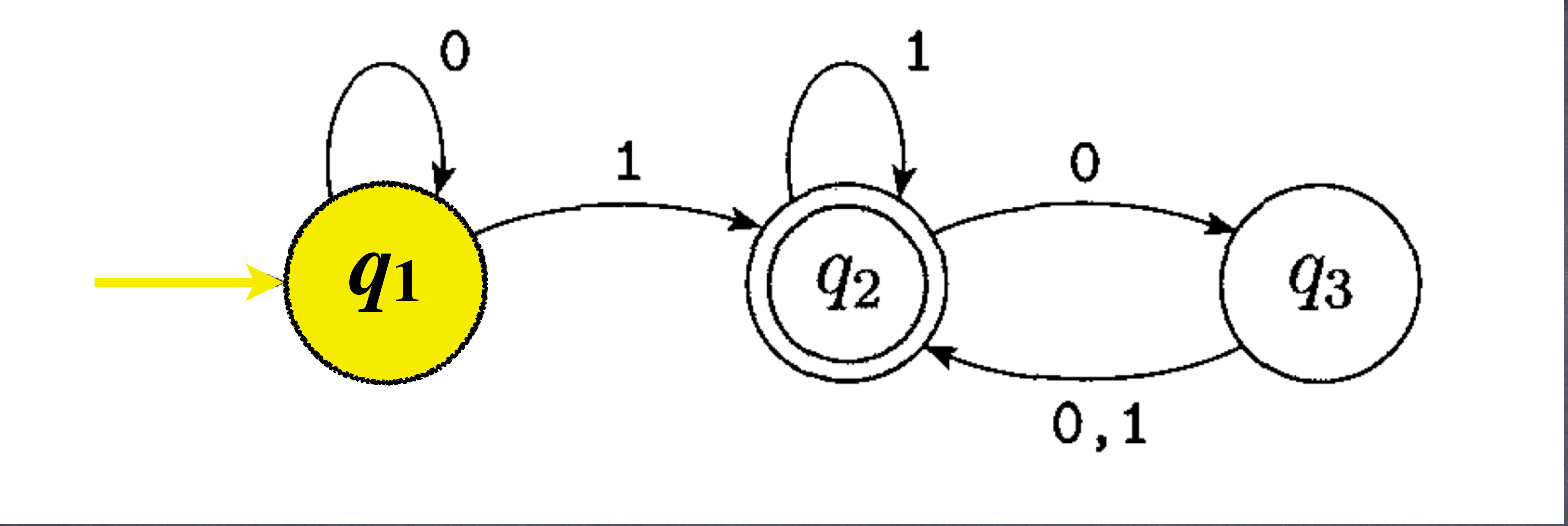
- **Theorem 1.B** $\Longrightarrow$ **Theorem 1.A**
- Proof of **Theorem 1.B** by induction.



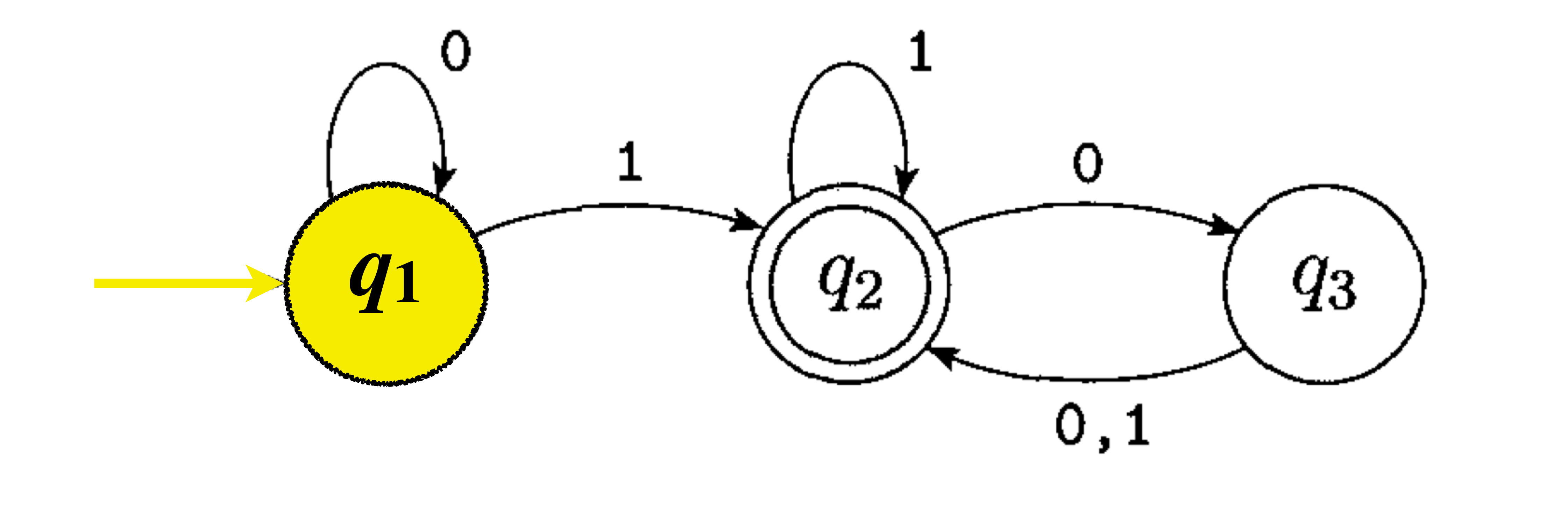
0
1
1
0
q_1
q_2
q_3
0,1



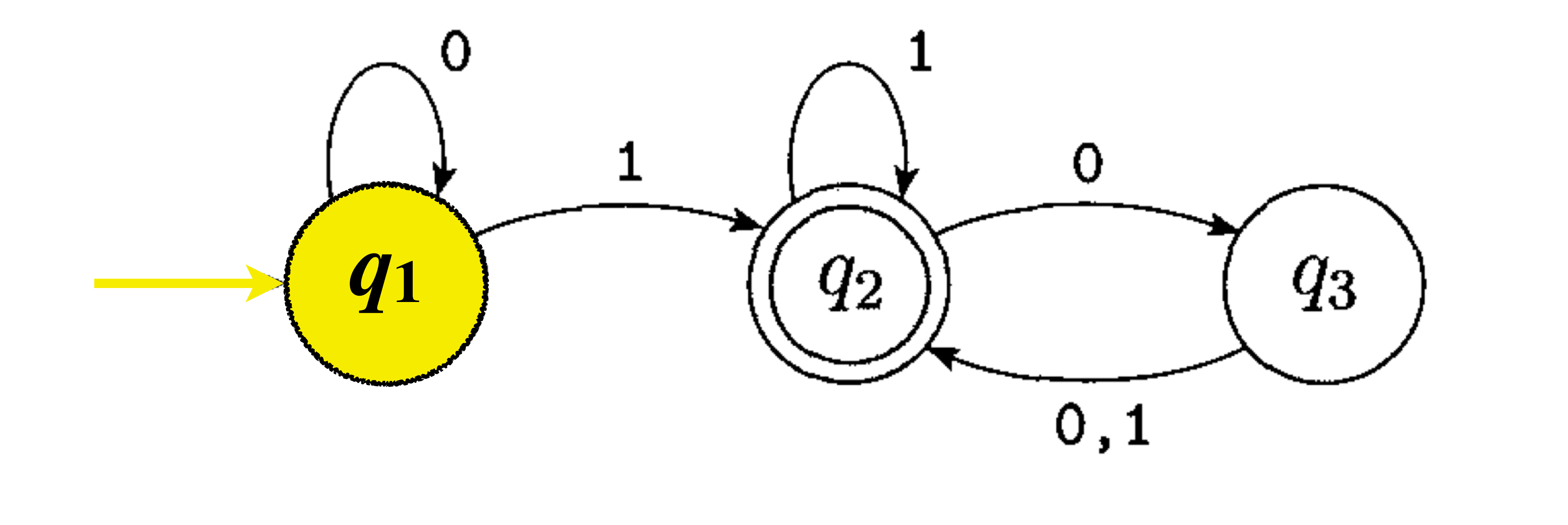
- Induction basis



- Induction basis
- Let $w \in \{0,1\}^*$ be a string of length $n=0$, $w=\varepsilon$.



- Induction basis
- Let $w \in \{0,1\}^*$ be a string of length $n=0$, $w=\varepsilon$.
- The evaluation of w by M_1 stops in state q_1 right after starting and rejects w.



- <u>Induction basis</u>
- Let $w \in \{0,1\}^*$ be a string of length $n=0$, $w=\varepsilon$.
- The evaluation of w by M_1 stops in state q_1 right after starting and rejects w.
- Therefore, 1) is valid because $w=\varepsilon$ does not contain a "1". Since there are no strings containing a "1" and no strings leading to q_2 or q_3, 2) and 3) are also valid.

- 1) M_1 stops in state $q_1 \Leftrightarrow$ w contains no "1"s.
2) M_1 stops in state $q_2 \Leftrightarrow$ w contains at least one "1" and ends with an even number of "0"s.
3) M_1 stops in state $q_3 \Leftrightarrow$ w contains at least one "1" and ends with an odd number of "0"s.

- Induction basis

- Let $w \in \{0,1\}^*$ be a string of length $n=0$, $w=\varepsilon$.

- The evaluation of w by M_1 stops in state q_1 right after starting and rejects w.

- Therefore, 1) is valid because $w=\varepsilon$ does not contain a "1". Since there are no strings containing a "1" and no strings leading to q_2 or q_3, 2) and 3) are also valid.

- 1) M_1 stops in state $q_1 \Leftrightarrow$ w contains no "1"s.
2) M_1 stops in state $q_2 \Leftrightarrow$ w contains at least one "1" and ends with an even number of "0"s.
3) M_1 stops in state $q_3 \Leftrightarrow$ w contains at least one "1" and ends with an odd number of "0"s.

- 1) M_1 stops in state $q_1 \Leftrightarrow$ w contains no "1"s.
  2) M_1 stops in state $q_2 \Leftrightarrow$ w contains at least one "1" and ends with an even number of "0"s.
  3) M_1 stops in state $q_3 \Leftrightarrow$ w contains at least one "1" and ends with an odd number of "0"s.

- Induction Step : Let $w \in \{0,1\}^*$ be a string of length $n>0$.

- 1) M_1 stops in state q_1 ⟺ w contains no "1"s.
  2) M_1 stops in state q_2 ⟺ w contains at least one "1" and ends with an even number of "0"s.
  3) M_1 stops in state q_3 ⟺ w contains at least one "1" and ends with an odd number of "0"s.

- Induction Step : Let $w \in \{0,1\}^*$ be a string of length $n>0$.

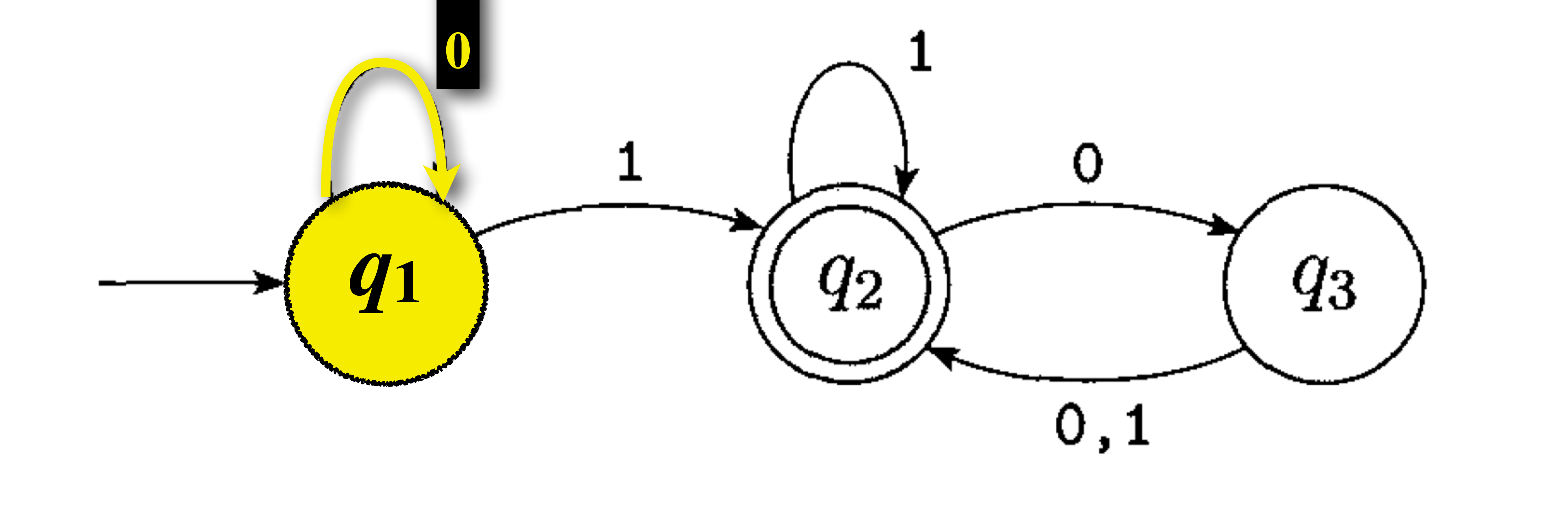
- We assume for Induction Hypothesis that 1), 2), and 3) are valid for n-1 and all strings v of size n-1.

- 1) M_1 stops in state q_1 ⇔ w contains no "1"s.
  2) M_1 stops in state q_2 ⇔ w contains at least one "1" and ends with an even number of "0"s.
  3) M_1 stops in state q_3 ⇔ w contains at least one "1" and ends with an odd number of "0"s.

- Induction Step : Let $w \in \{0,1\}^*$ be a string of length $n>0$.

- We assume for Induction Hypothesis that 1), 2), and 3) are valid for n-1 and all strings v of size n-1.

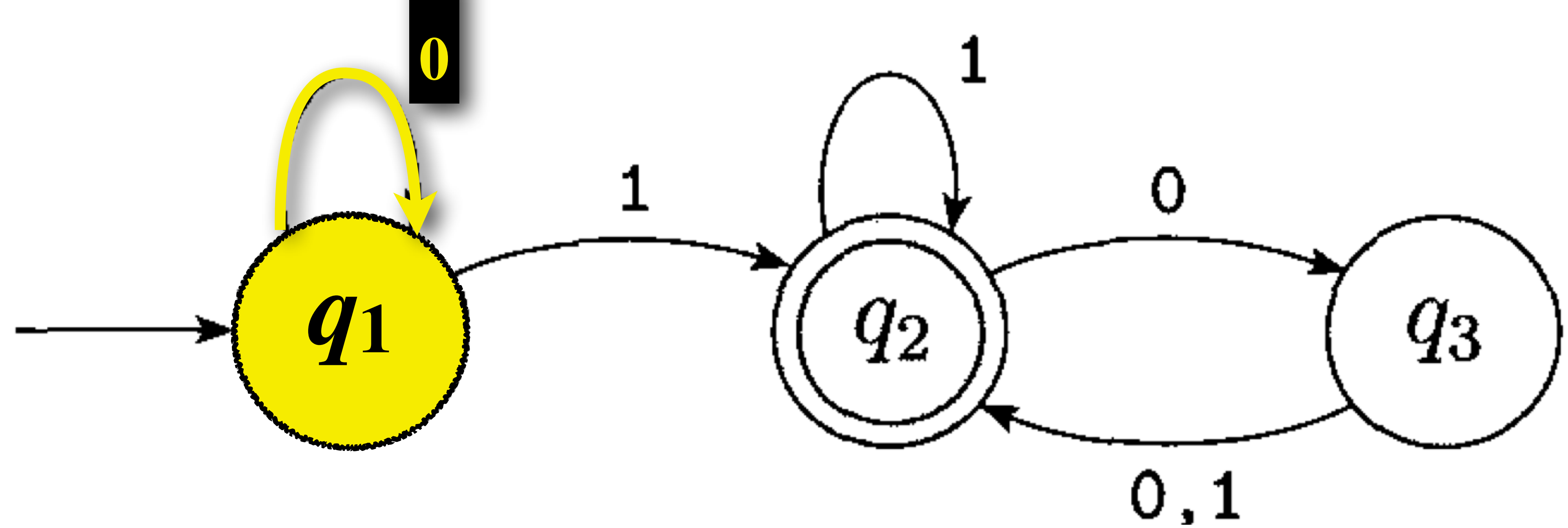
- We now prove that 1), 2), and 3) are also valid for n and all strings w of size n.



- Let $w \in \{0,1\}^*$ be a string of length $n>0$.
- If w ends with a "0" then it means that

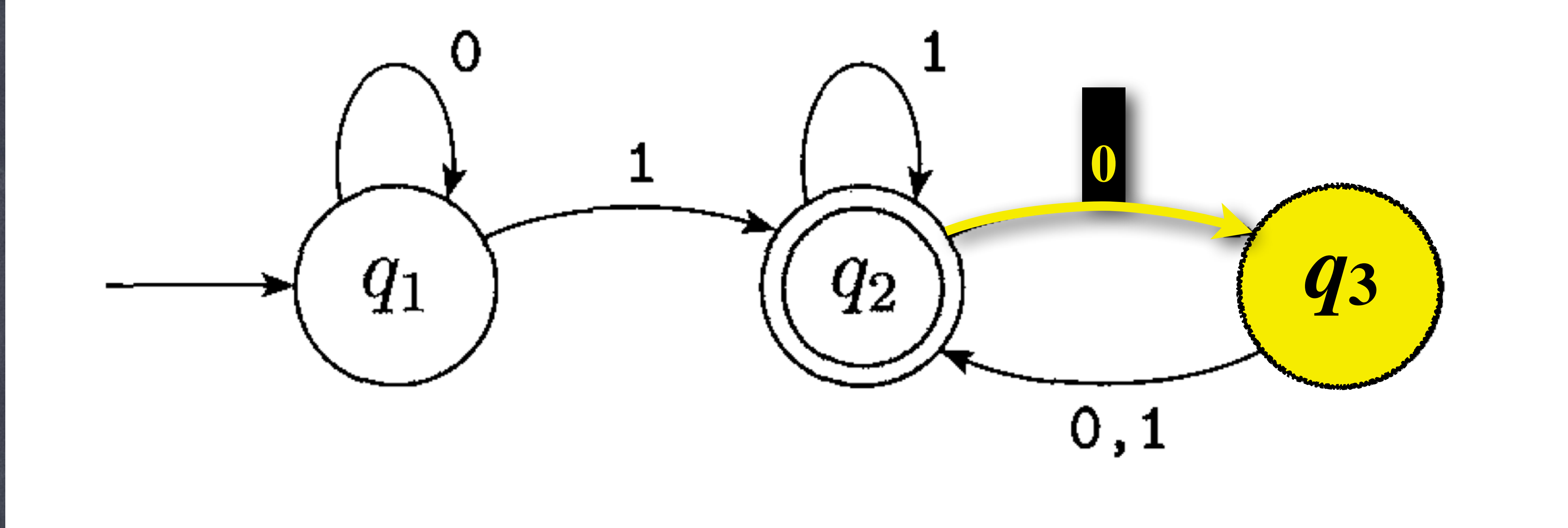
$$w = v0$$

with v a string of length n-1. Let q be the state in which M_1 ends when evaluating v.
- If $q=q_1$ then by induction we have that $v=0^{n-1}$ and therefore $w=0^n$ contains no "1", proving 1).

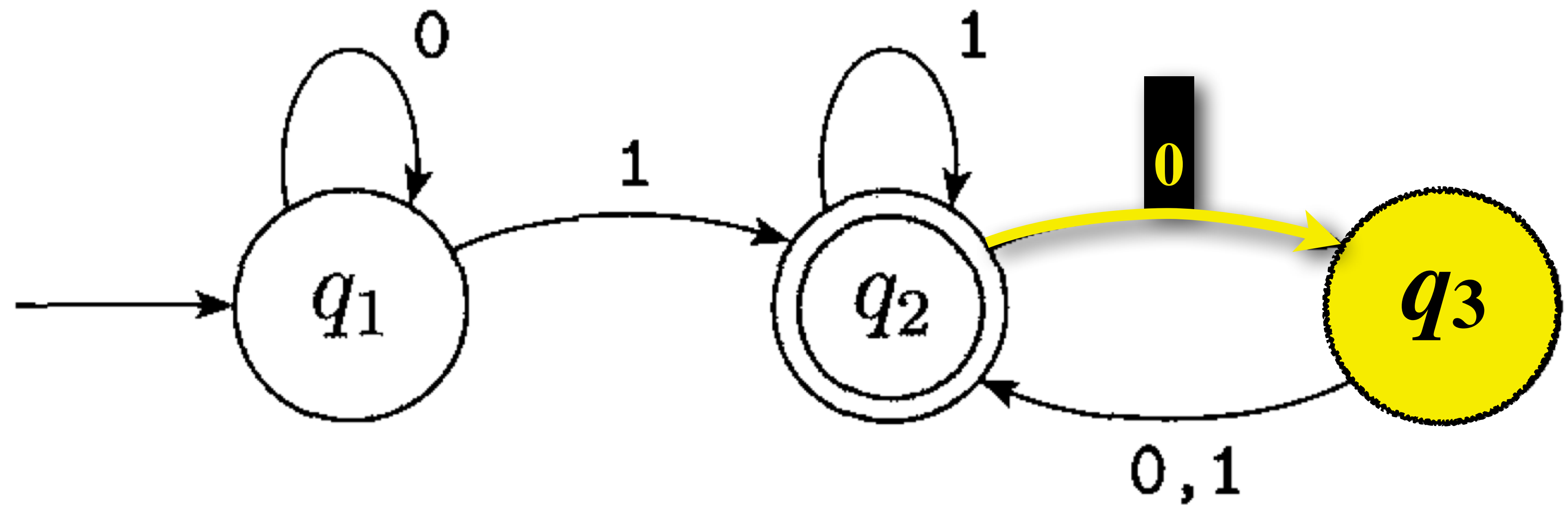


1) M_1 stops in state $q_1 \Leftrightarrow$ w contains no "1"s.

- Let $w \in \{0,1\}^*$ be a string of length $n>0$.
- If w ends with a "0" then it means that
$$w = v0$$
with v a string of length n-1. Let q be the state in which M_1 ends when evaluating v.
- If $q=q_1$ then by induction we have that $v=0^{n-1}$ and therefore $w=0^n$ contains no "1", proving 1).

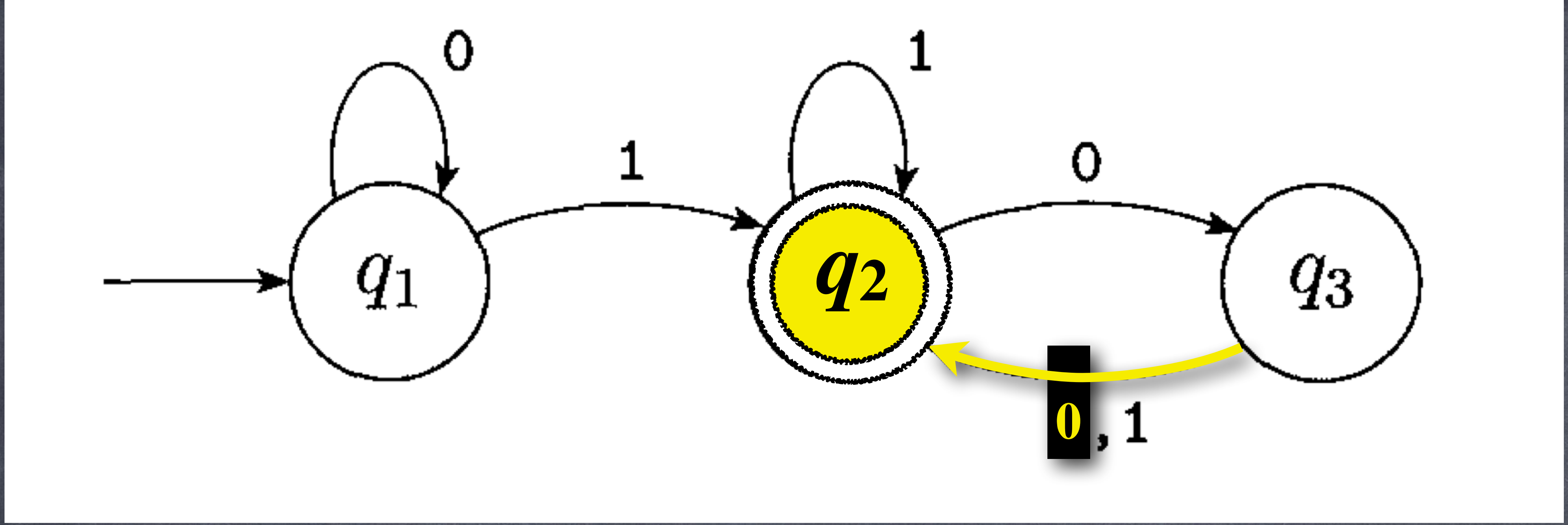


- If $q=q_2$ then by induction we have that v contains at least one "1" and ends with an even number of "0"s.
- Therefore w contains at least one "1" and ends with an odd number of "0"s., proving 3).

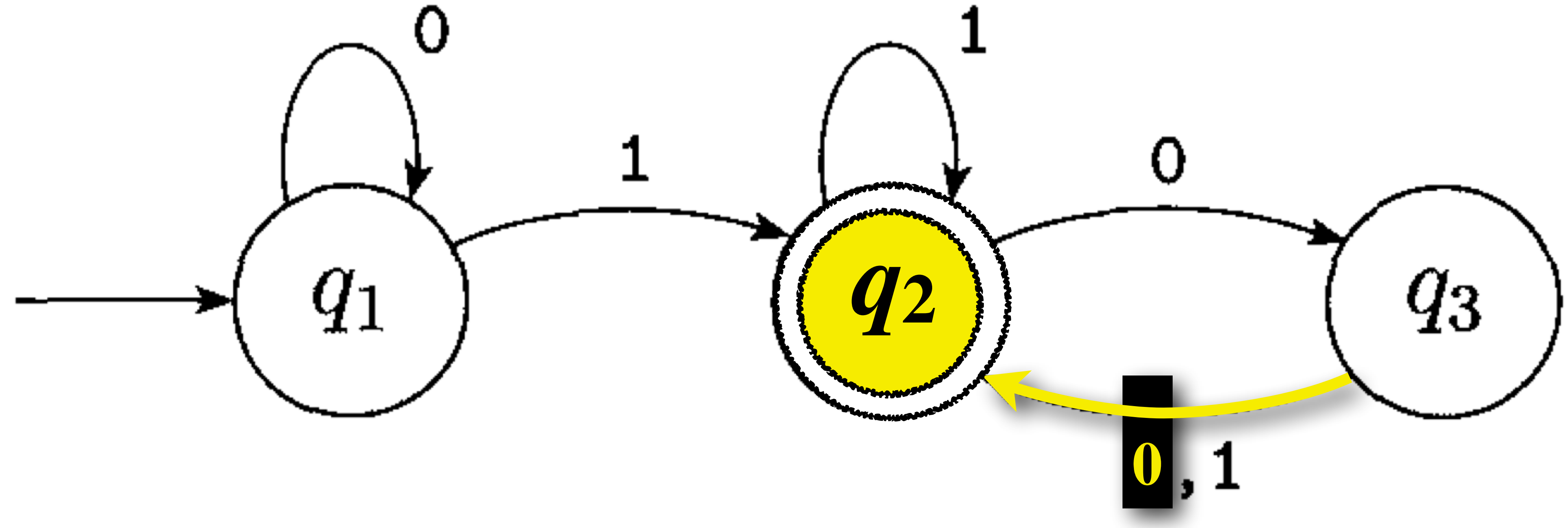


- 3) M_1 stops in state $q_3 \Leftrightarrow$ w contains at least one "1" and ends with an odd number of "0"s.

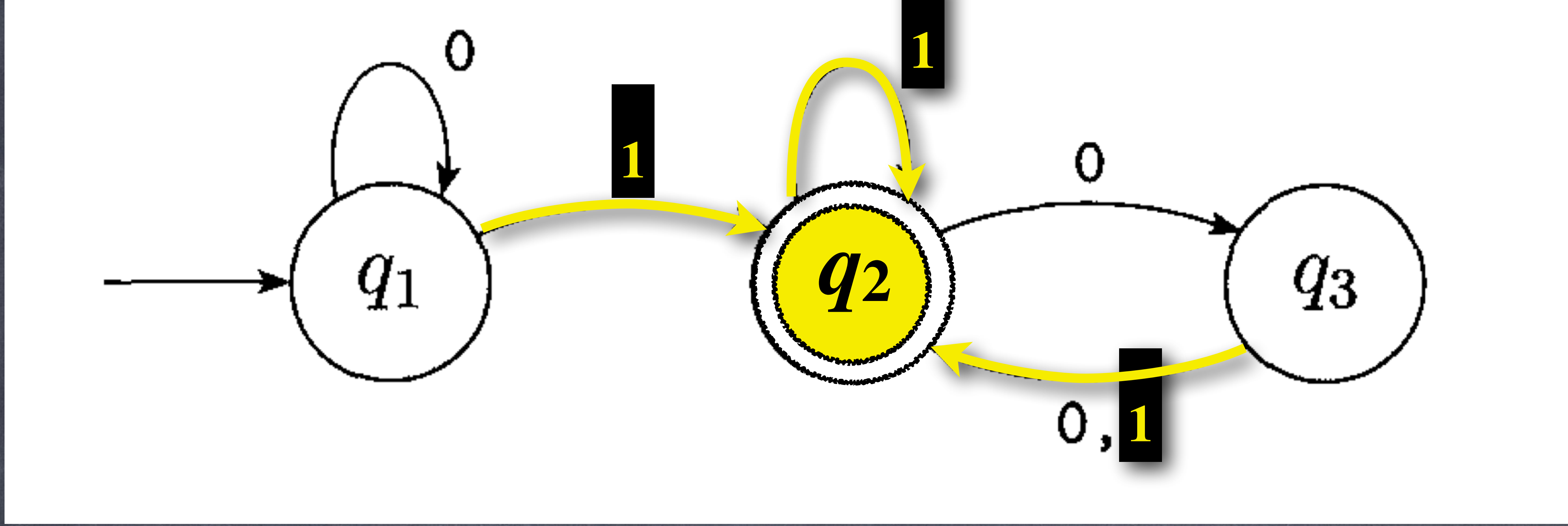
- If $q=q_2$ then by induction we have that v contains at least one "1" and ends with an even number of "0"s.
- Therefore w contains at least one "1" and ends with an odd number of "0"s., proving 3).



- If $q=q_3$ then by induction we have that v contains at least one "1" and ends with an odd number of "0"s.
- Therefore w contains at least one "1" and ends with an even number of "0"s greater than zero, proving part of 2).



- 2) M_1 stops in state q_2 ⟺ w contains at least one "1" and ends with an even number of "0"s.
- If $q=q_3$ then by induction we have that v contains at least one "1" and ends with an odd number of "0"s.
- Therefore w contains at least one "1" and ends with an even number of "0"s greater than zero, proving part of 2).



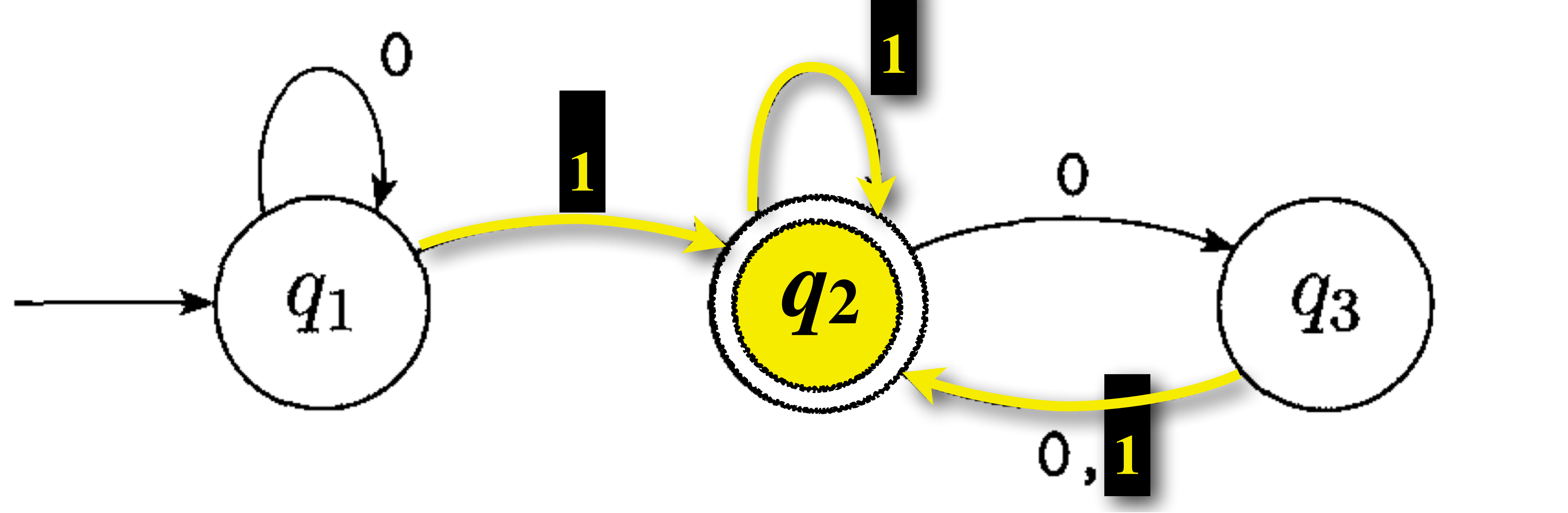
- If w ends with a "1" then it means that

$$w = v1$$

with v a string of length n-1. Let q be the state in which M_1 ends when evaluating v.

- By examination of δ we conclude that for all q, $\delta(q,1)=q_2$. Thus M_1 accepts w and 2) is valid whenever w ends with zero "0"s. This completes the proof of 2) and of the Thm.

QED



- 2) M_1 stops in state q_2 ⇔ w contains at least one "1" and ends with an even number of "0"s.

- If w ends with a "1" then it means that

  w = v1

  with v a string of length n-1. Let q be the state in which M_1 ends when evaluating v.

- By examination of δ we conclude that for all q, $\delta(q,1)=q_2$. Thus M_1 accepts w and 2) is valid whenever w ends with zero "0"s. This completes the proof of 2) and of the Thm.

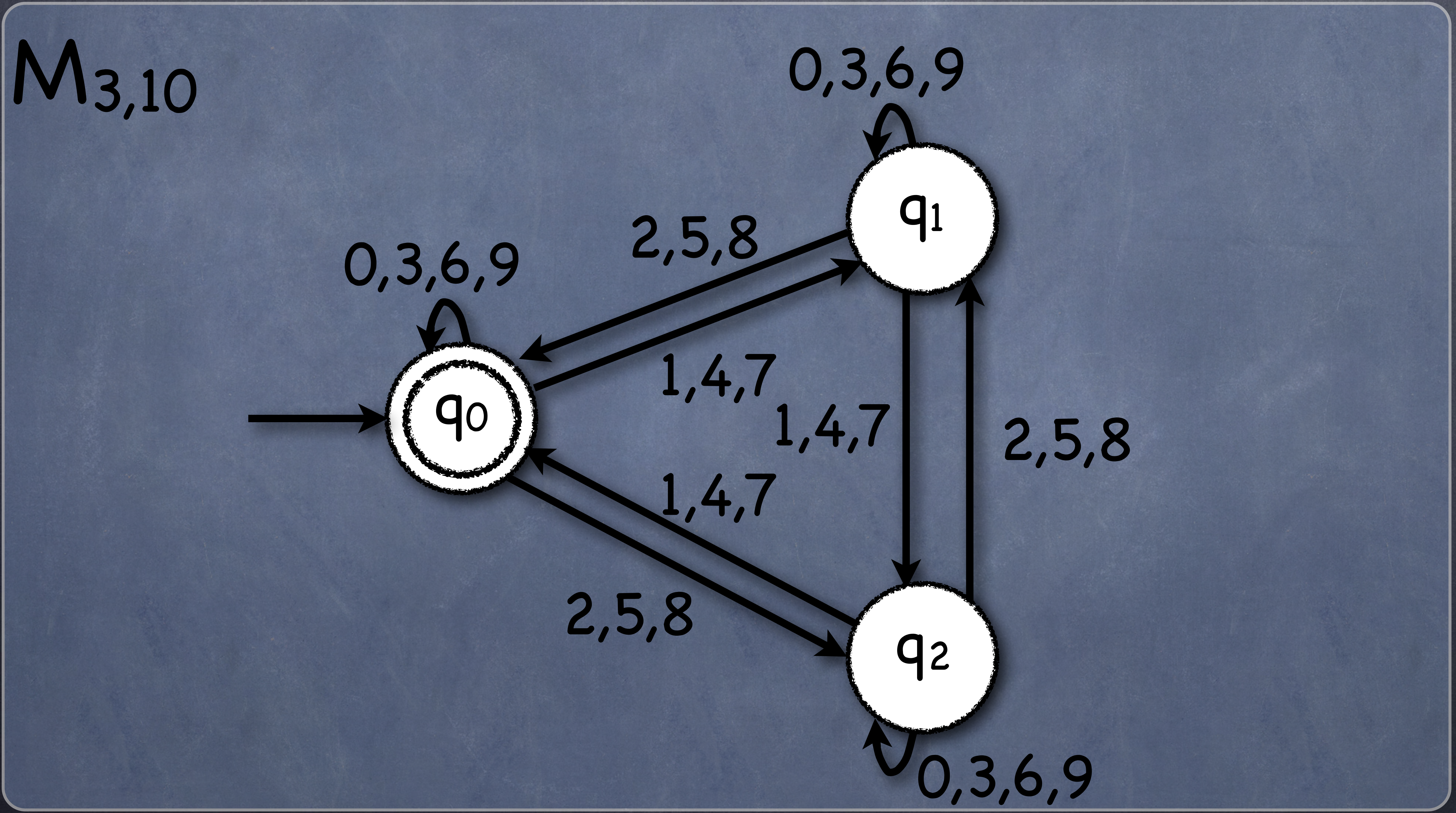
  QED

Another example: multiples of 3...

- Remember what you learned in elementary school: N is a multiple of 3 if N=0,3,6,9 or if the sum of its digits is a multiple of 3...
- Example: 54708 is a multiple of 3 because the sum of its digits 5+4+7+0+8=24 is a multiple of 3. We know that because the sum of its digits 2+4=6 is a multiple of 3.

gcd(B,N) = 1

0 MOD 3 (base 10)



0 MOD 3 (base 10)

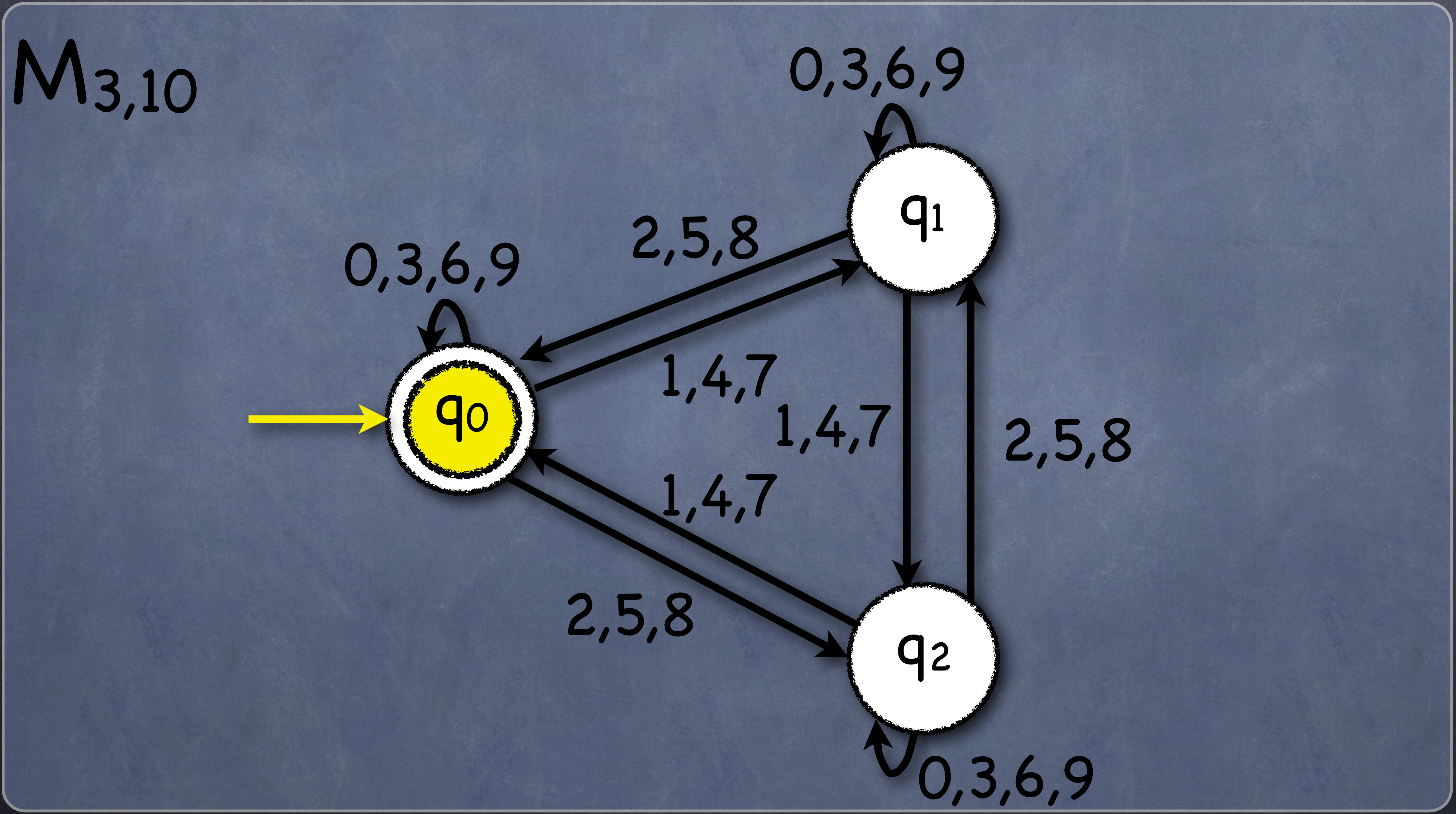
- **<u>Theorem 1.C</u>** :
  Let $w \in \{0,1,\ldots,9\}^*$ be of length $n \geq 0$.

  1) M_1 stops in state $q_0 \Leftrightarrow w = 0 \bmod 3$.

  2) M_1 stops in state $q_1 \Leftrightarrow w = 1 \bmod 3$.

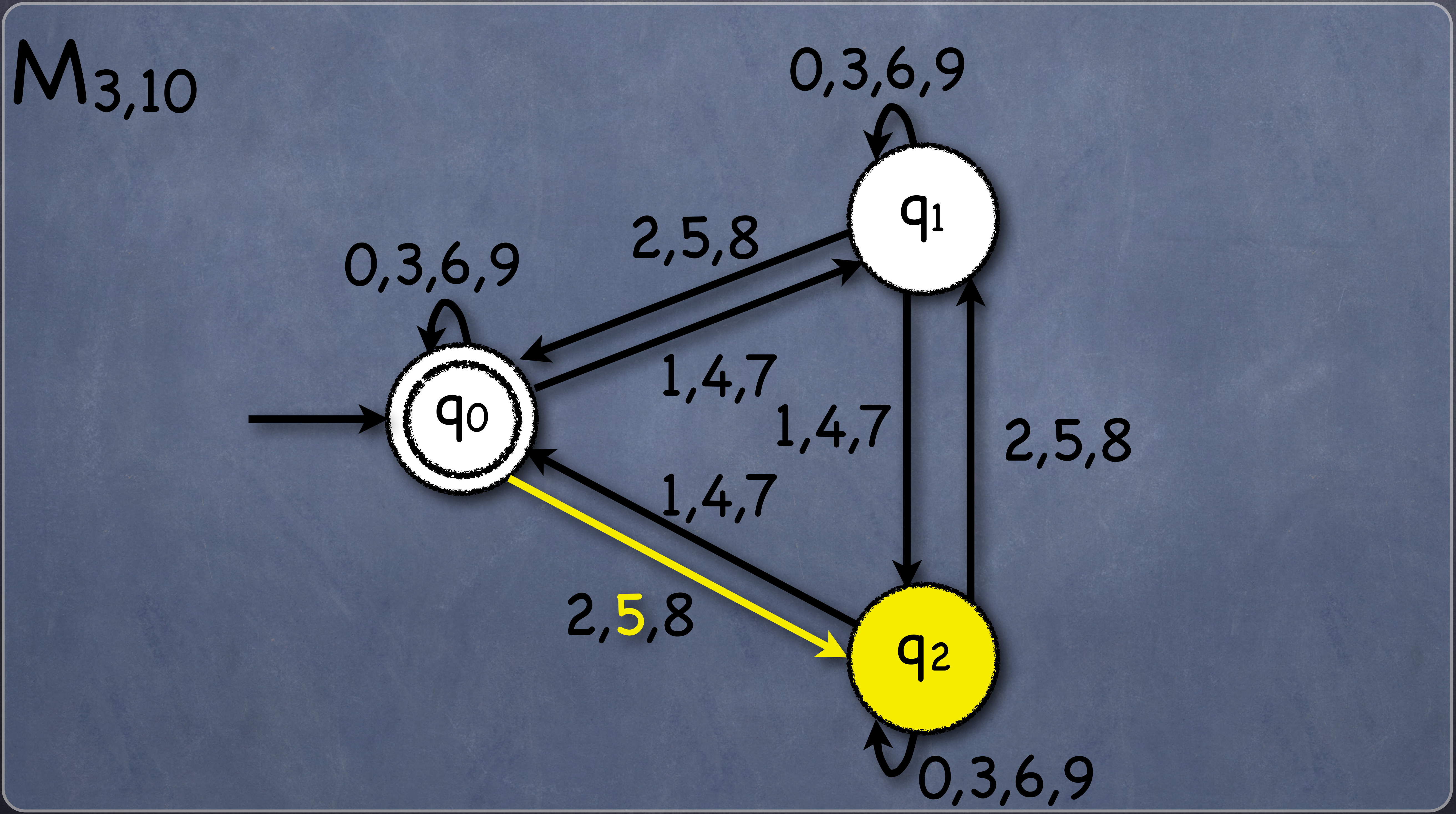
  3) M_1 stops in state $q_2 \Leftrightarrow w = 2 \bmod 3$.

54708



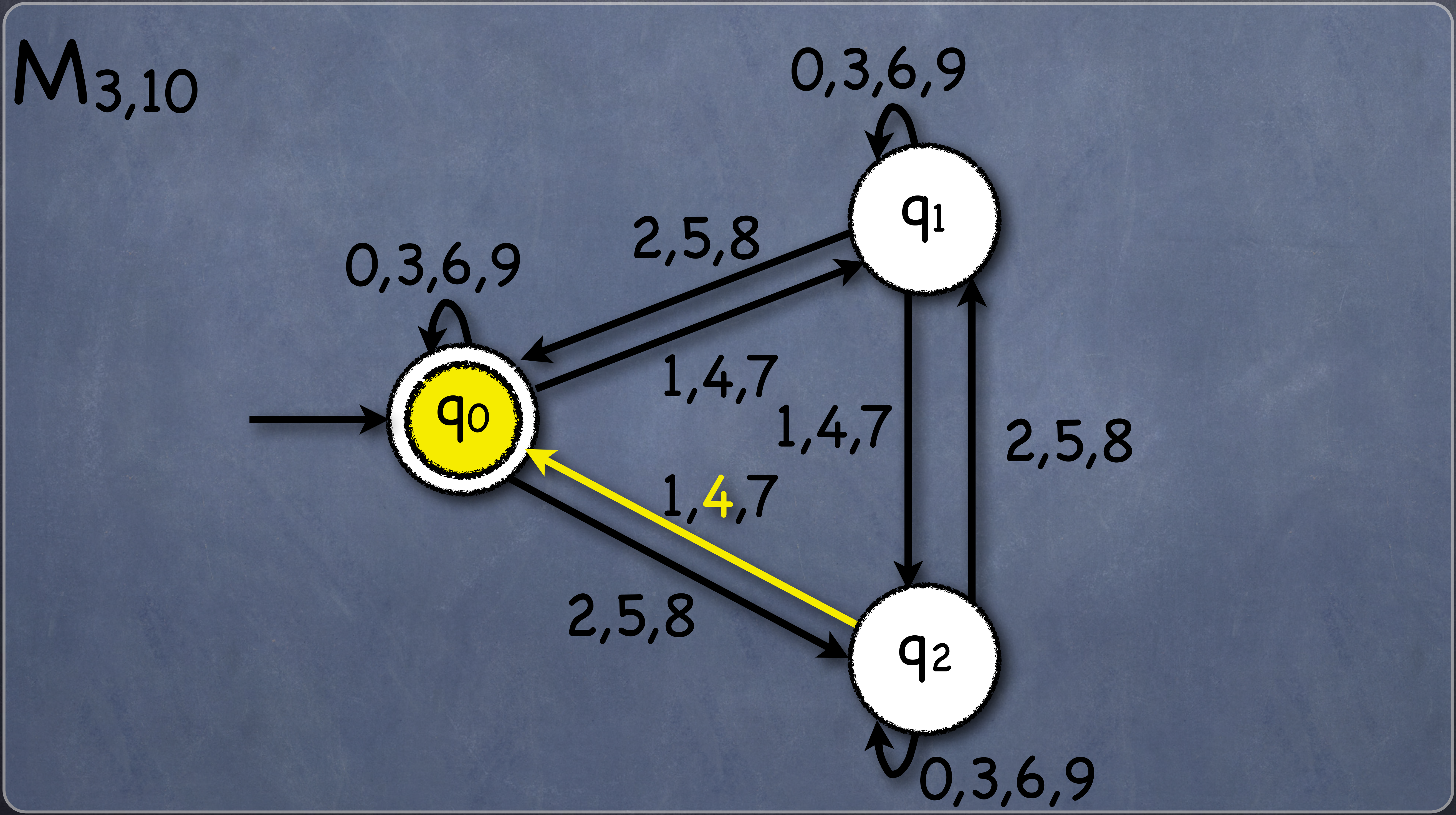
$M_{3,10}$ stops in state $q_r \Leftrightarrow w = r \bmod 3$

54708



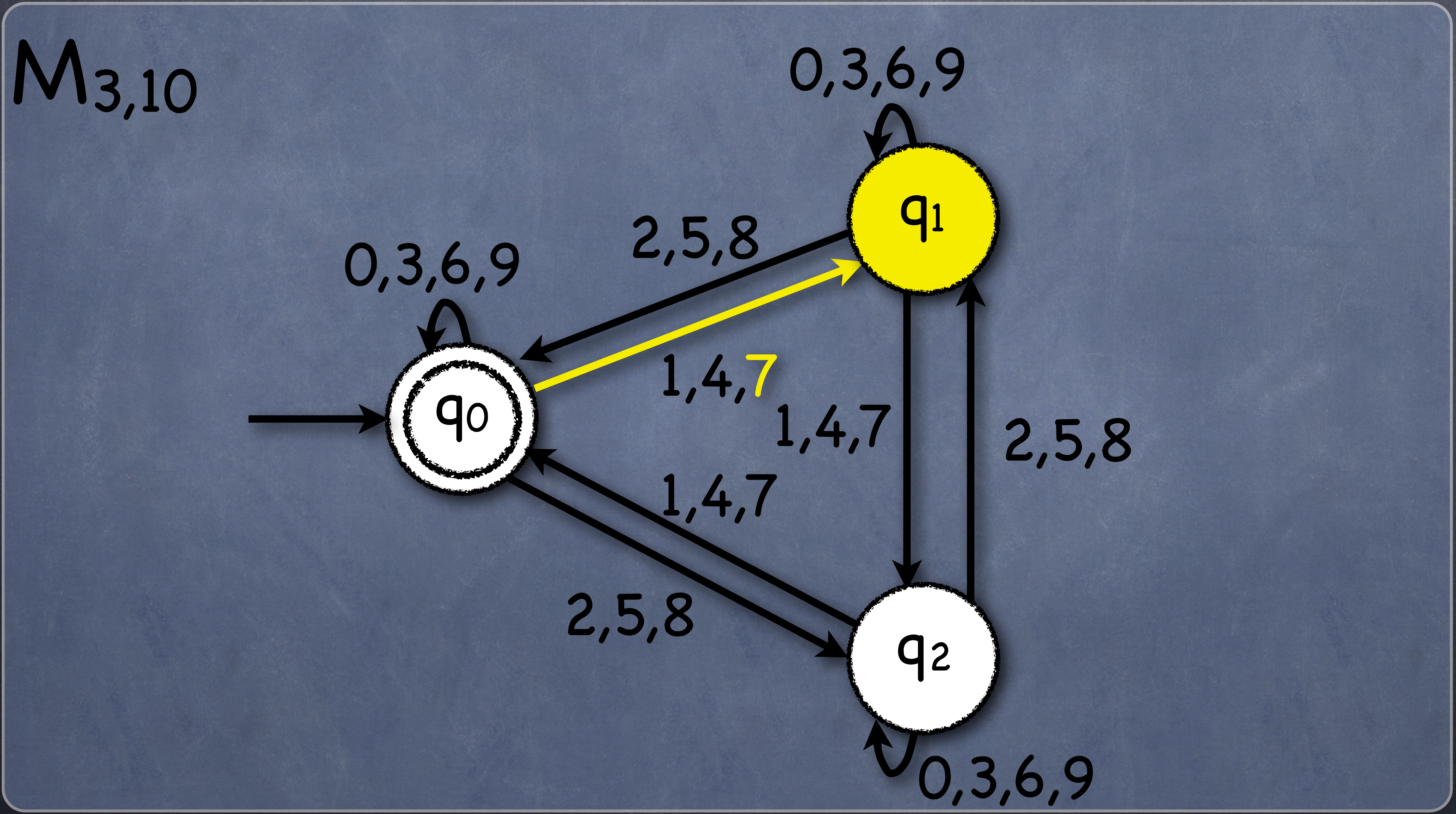
$M_{3,10}$ stops in state $q_r \Leftrightarrow w = r \bmod 3$

54708



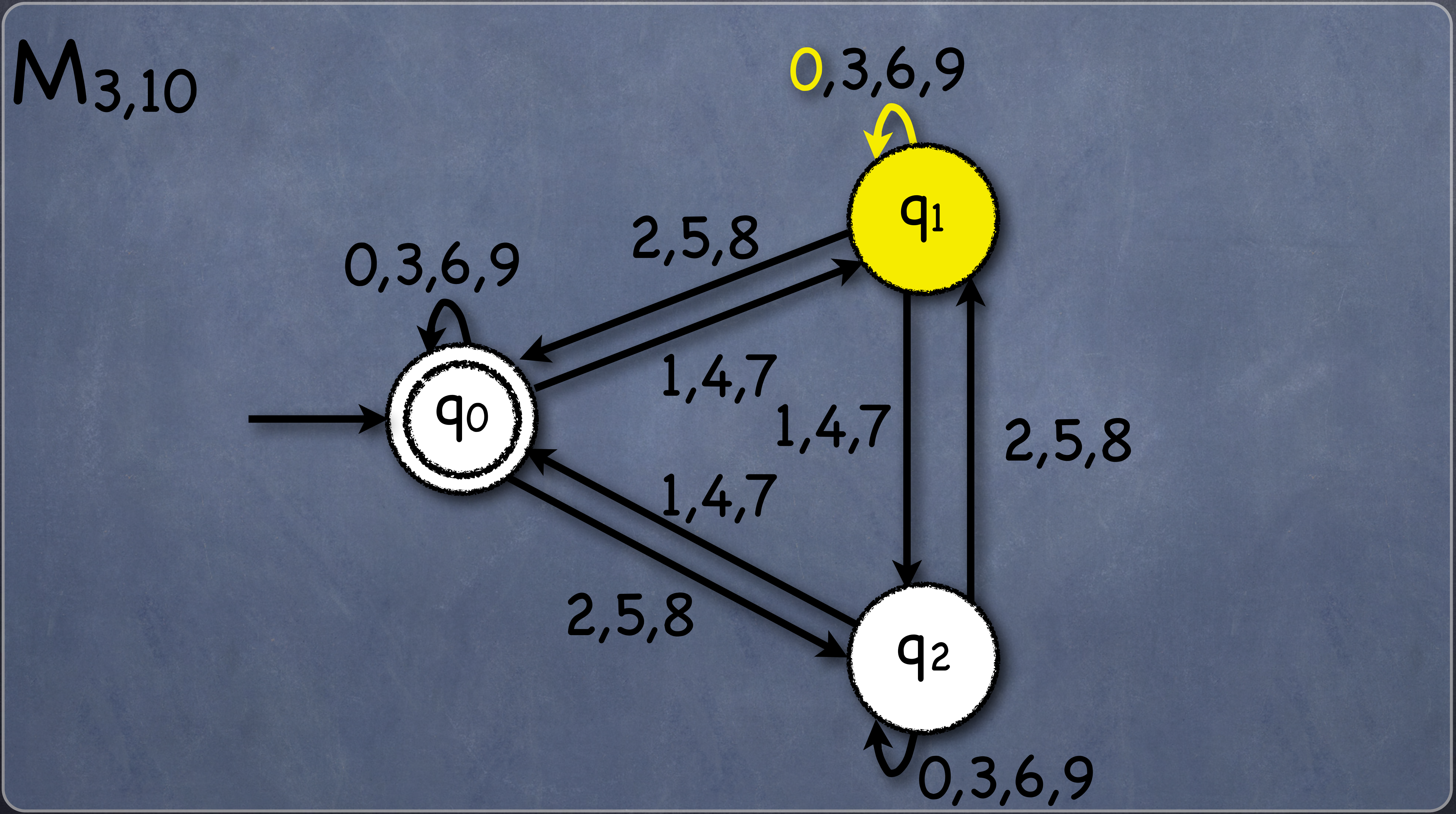
$M_{3,10}$ stops in state $q_r \Leftrightarrow w = r \bmod 3$

54708



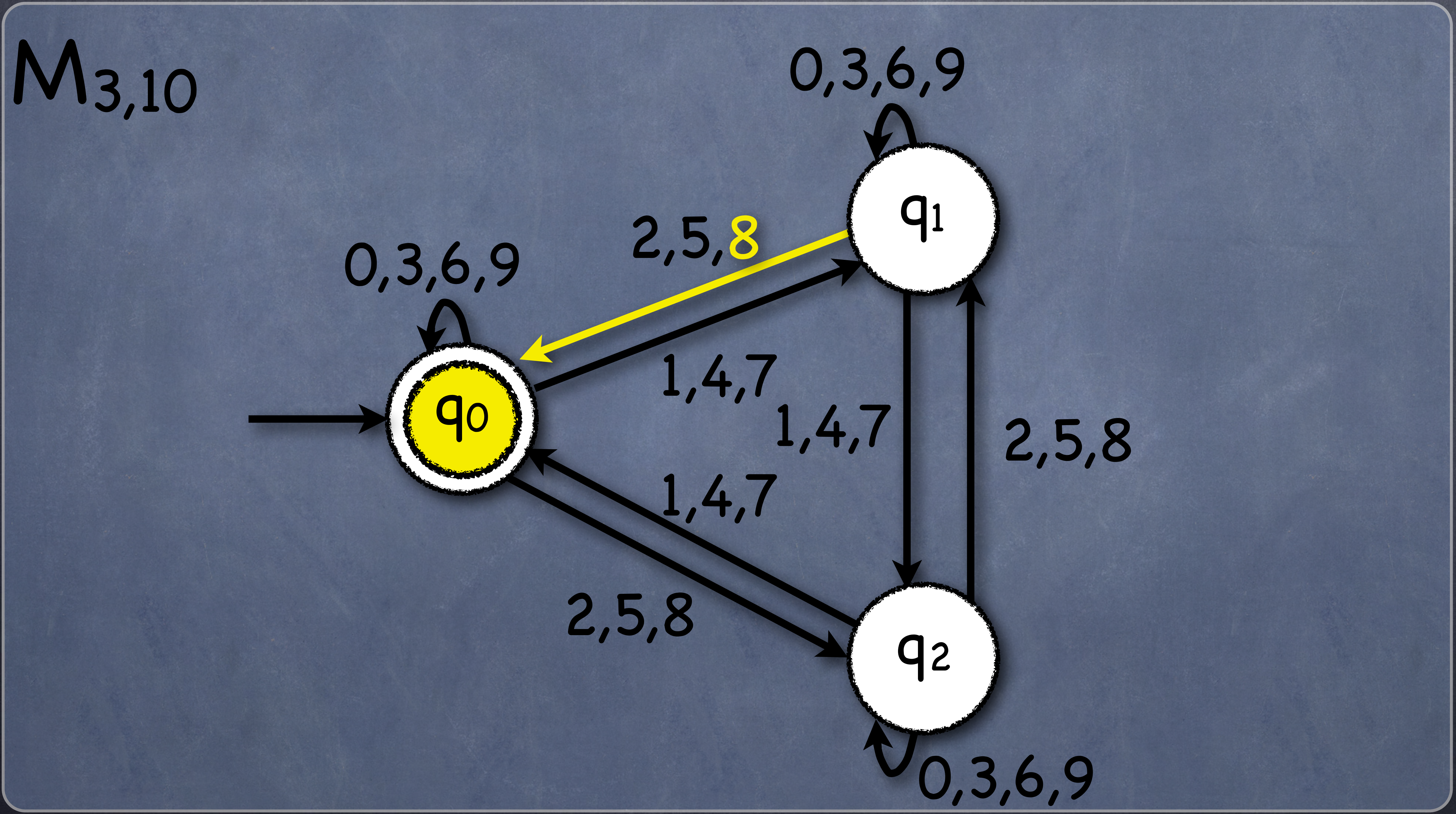
$M_{3,10}$ stops in state $q_r \Leftrightarrow w = r \bmod 3$

54708



$M_{3,10}$ stops in state $q_r \Leftrightarrow w = r \bmod 3$

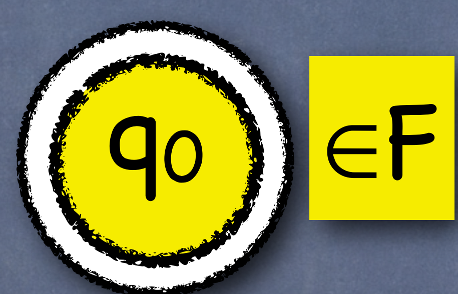
54708



$M_{3,10}$ stops in state $q_r \Leftrightarrow w = r \bmod 3$

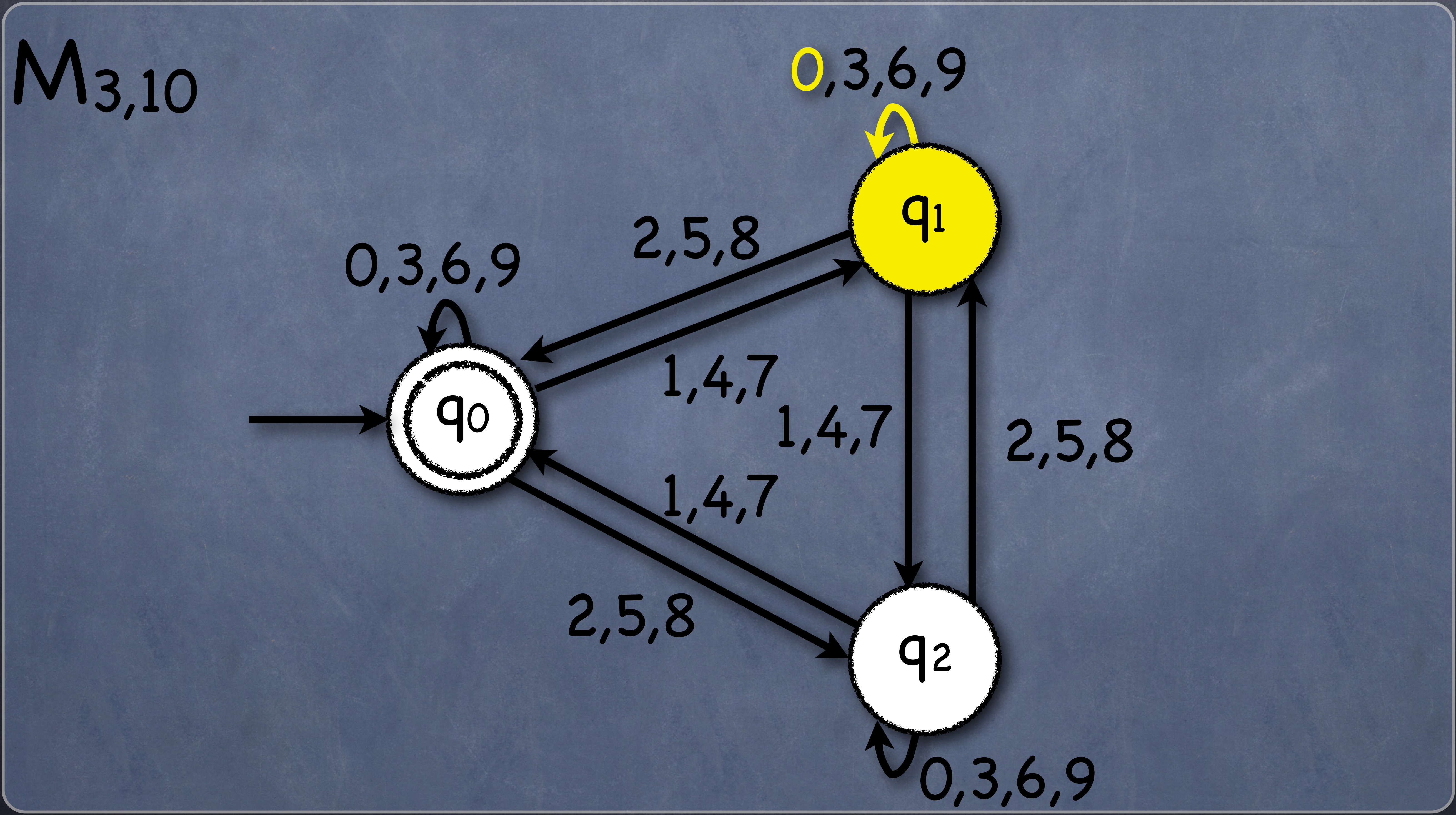
54708

is a multiple of 3



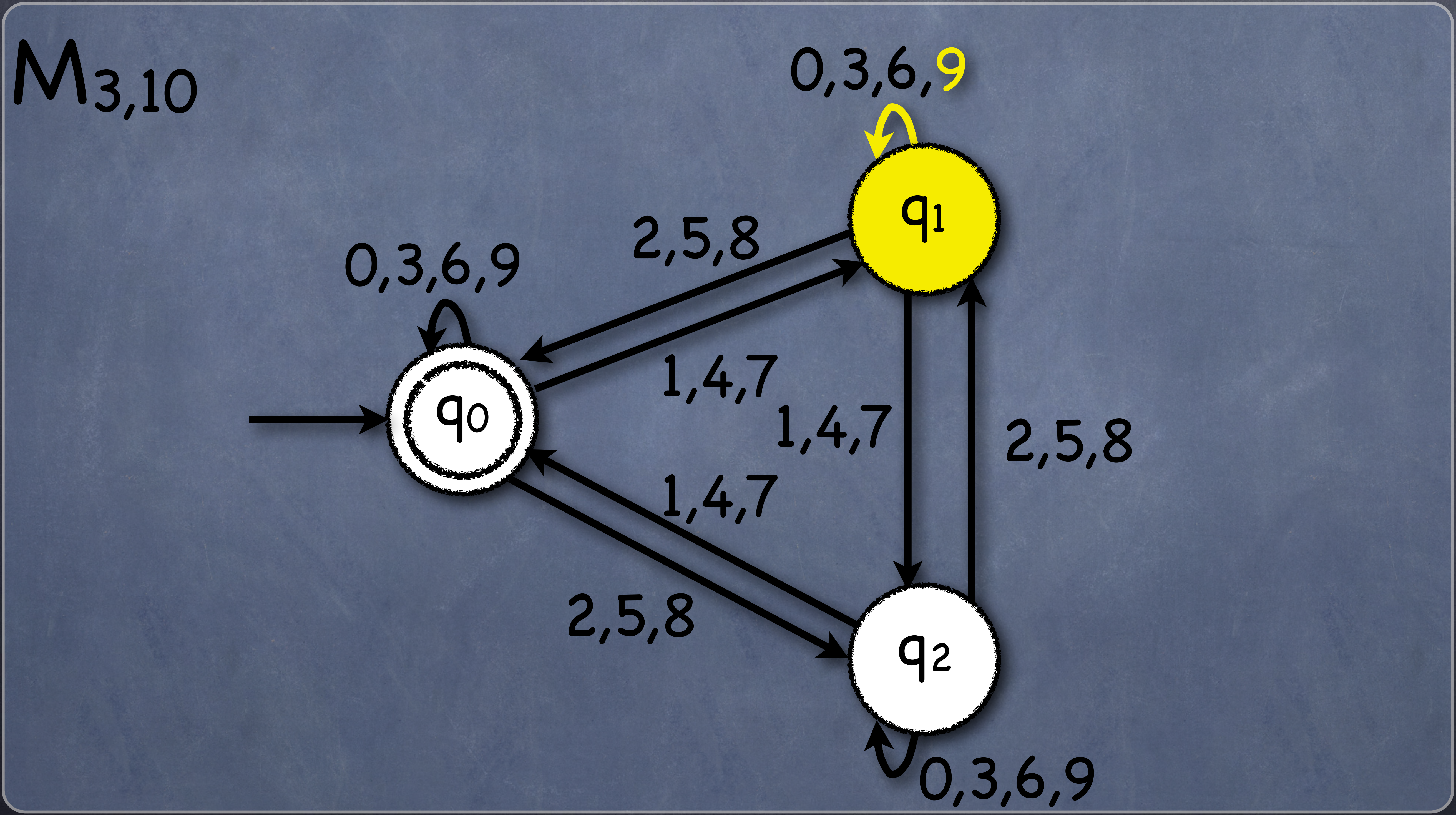
$M_{3,10}$ stops in state $q_r \Leftrightarrow w = r \bmod 3$

54709



$M_{3,10}$ stops in state $q_r \Leftrightarrow w = r \bmod 3$

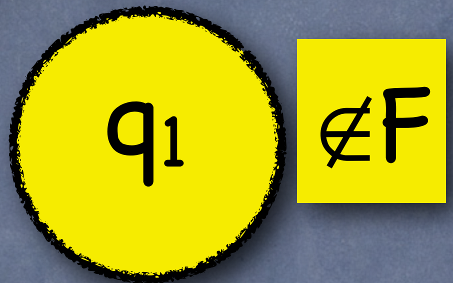
54709



$M_{3,10}$ stops in state $q_r \iff w = r \bmod 3$

54709

is NOT a multiple of 3



$M_{3,10}$ stops in state $q_r \Leftrightarrow w = r \bmod 3$

COMP-330
Theory of Computation

Fall 2019 -- Prof. Claude Crépeau

LECTURE 3 :
Deterministic F A