可 计 算 理 论

罗 欢

Email：hluo@fzu.edu.cn

学习内容

- 三个模块

- 计算装置
- 可计算性
- 计算复杂性

计算装置

- 有哪些计算装置？能力如何？
  - 有穷自动机
  - 下推自动机
  - 图灵机

  - 正则语言
  - 上下文无关文法
  - 可计算语言、半可计算语言

可计算性

- 什么是计算?
- 哪些问题（不）可计算?
  - 丘奇-图灵论题
  - 通用机
  - 停机问题
  - 规约
  - 递归定理

计算复杂性

- 什么是有效计算？
- 哪些问题（不）可有效计算？
  - 时间复杂性
  - 空间复杂性
  - 多项式时间规约
  - 完全问题

学习目标

- 掌握计算机理论的基础知识，能够初步回答下列问题
  - 什么是计算？
  - 什么是有效计算？
  - 哪些问题（不）可计算？
  - 哪些问题（不）可有效计算？

科学价值

- 优美的理论
  - 优美的定理和证明
  - 非常好的思维训练
- 现代科学的基础
  - 现代密码学
  - 机器学习理论
  - 生物演化理论
  - 经济学、物理学、数学、.....

发展简史

- 1900年希尔伯特：机械化?
- 1930年代图灵：图灵机
  - 通用图灵机、不可计算问题
  - 丘奇-图灵论题
- 1940年代：电子计算机
- 1950年代：乔姆斯基谱系
  - 正则语言、上下文无关文法
- 1960年代：计算复杂性
  - 扩展的丘奇-图灵论题
- 1970年代：NP完全问题
  - PvsNP问题

预备知识

- 离散数学
  - 集合、关系、函数
  - 逻辑运算
  - 图论

参考教材

计 算 机 科 学 丛 书
原书第3版
计算理论导引
[美] 迈克尔·西普塞（Michael Sipser） 著
段磊 唐常杰 等译
Introduction to the Theory of Computation
Third Edition
Introduction to the Theory of Computation
3rd edition
Michael Sipser
机械工业出版社
China Machine Press

北京高等教育精品教材
可计算性与计算复杂性导引
（第3版）
张立昂 编著
高等院校计算机专业及专业基础课系列教材

- 课件位置
  - QQ群：
  - 考核方式（闭卷考试）
  - 成绩：期末考试70%，作业30%

预备知识

字符串(1)

- 字母表: 任意非空有穷集合
  - $\Sigma=\{0,1\}$
  - $\Sigma=\{a,b,c,\ldots,x,y,z,$空格$\}$
- (字符)串:
  - x=01001，w=madam
- 连接:
  - xw=01001madam
  - $xx=x^2=0100101001$

字符串(2)

- 串长度: $|x|=5$, $|w|=5$, $|xw|=10$
- 空串: ε, $|\varepsilon|=0$, $x^0=\varepsilon$
  - 空串≠空格: |空格|=1
- 子串:
  - ada是madam的子串
- 子序列:
  - m,d,m是m,a,d,a,m的子序列

语言(1)

- Σ^* = { x | x是Σ上有穷长度的串 }
- Σ^+ = { x | x是Σ上正有穷长度的串 }
- Σ^∞ = { x | x是Σ上无穷长度的串 }

语言(2)

- 语言: 串的集合
  - $A\subseteq\Sigma^*$
- 空语言: $\varnothing$
  - 空串语言: $\{\varepsilon\}$
  - 空串: ε
- 语言连接:
  - $AB = \{ xy \mid x\in A$ 且 $y\in B \}$
  - $\{\varepsilon\}A=A\{\varepsilon\}=A$
  - $\varnothing A=A\varnothing=\varnothing$.

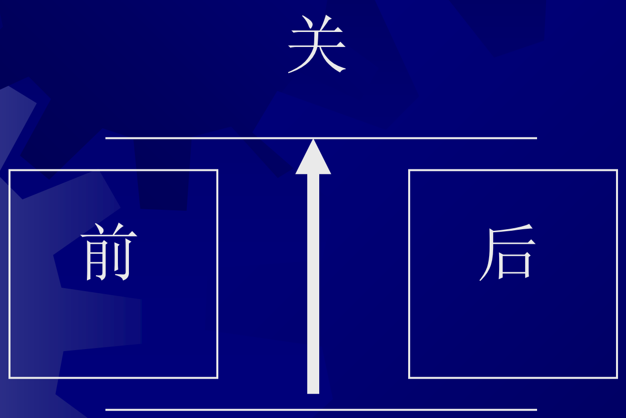
标准序

- 先短后长，等长逐位比较
- $\Sigma_1=\{0,1\}$, $0<1$
- $\Sigma_1^*=\{\varepsilon, 0, 1, 00, 01, 10, 11, 000, 001, \ldots \}$
- $\Sigma_2=\{a,b,c,\ldots,x,y,z\}$, $a<b<c<\ldots<x<y<z$
- $\Sigma_2^*=\{\varepsilon,a,b,c,\ldots,x,y,z, aa,ab,\ldots,ay,az,ba,\ldots,bz, ca,\ldots cz,\ldots,za,\ldots zz,aaa, \ldots,zzz,aaaa,\ldots\}$

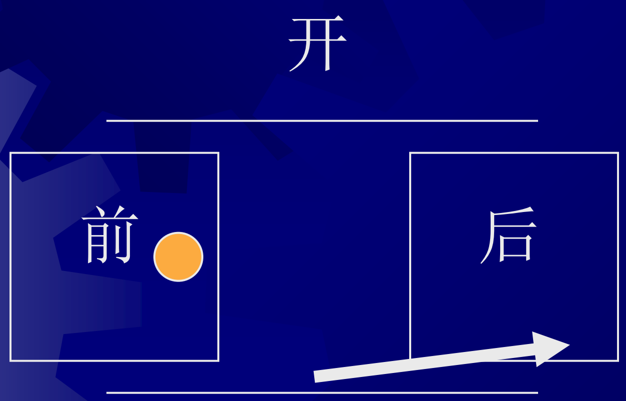
第一讲　　有限状态自动机

商场自动门的例子

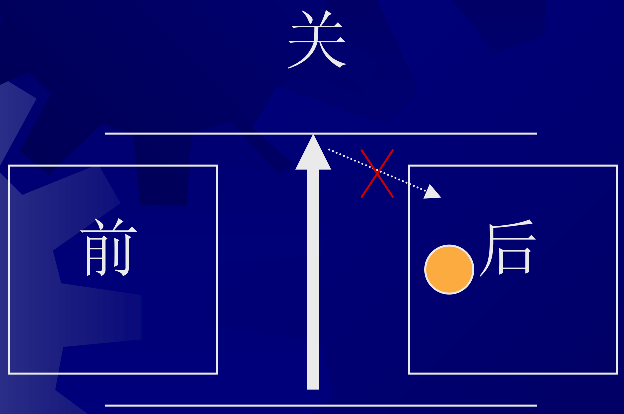
商场自动门(1)



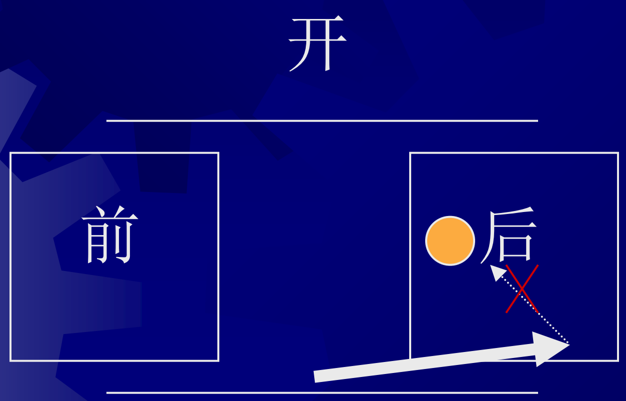
商场自动门(2)



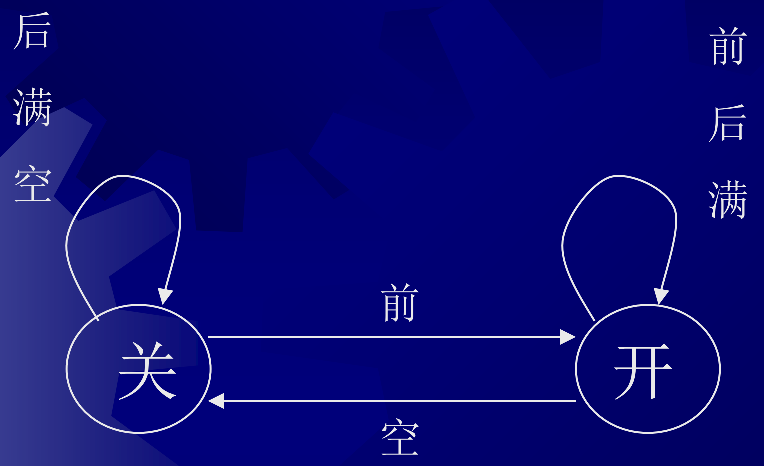
商场自动门(3)



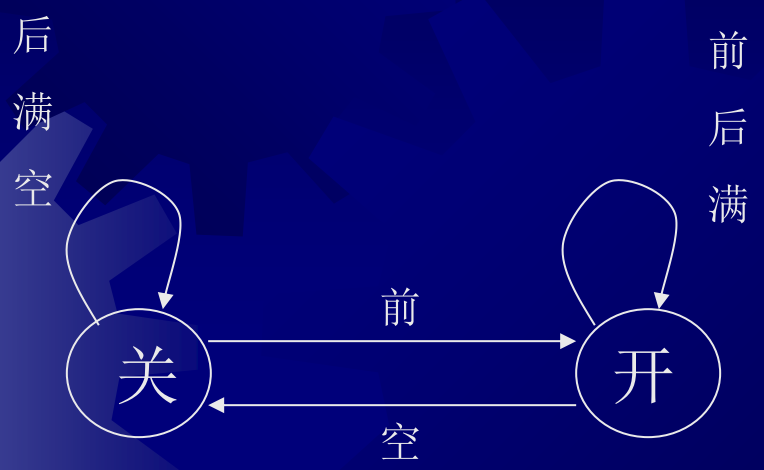
商场自动门(4)



自动门控制器-状态图



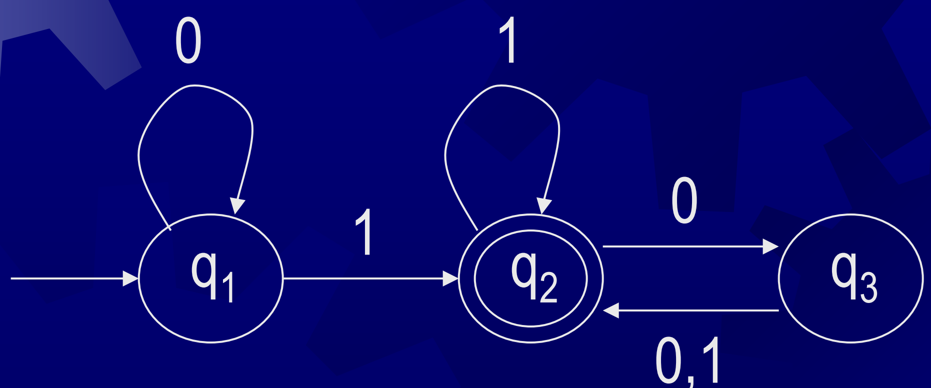
自动门控制器-状态表



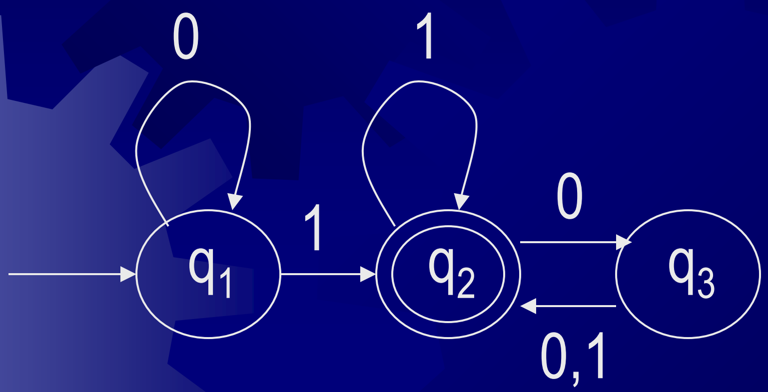
	空	前	后	满
关	关	开	关	关
开	关	开	开	开

有穷自动机

- 状态图
- 状态, 初始状态，接受状态
- 转移, 输入符号



有穷自动机M_1

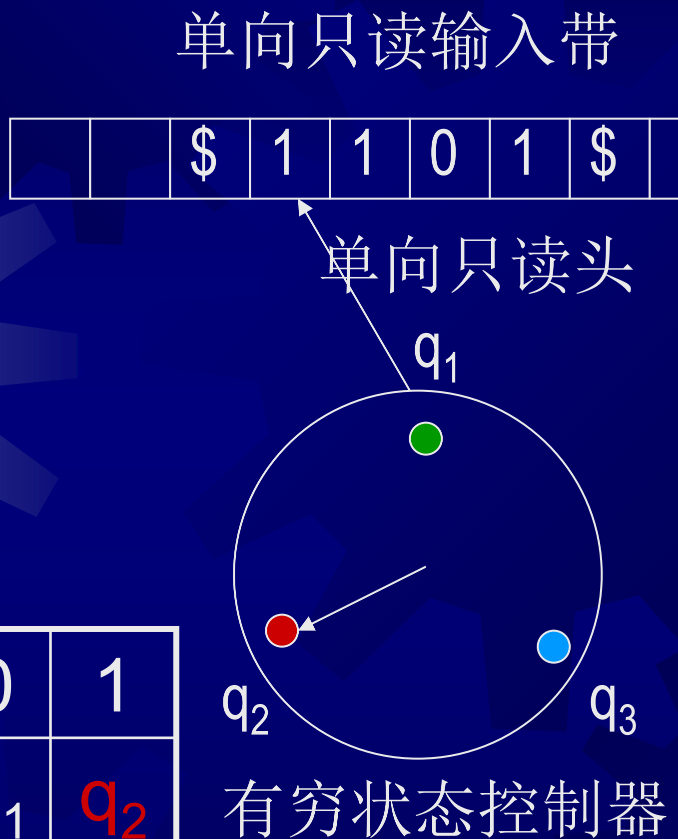


	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

M_1在1101上运行

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

M_1在1101上运行



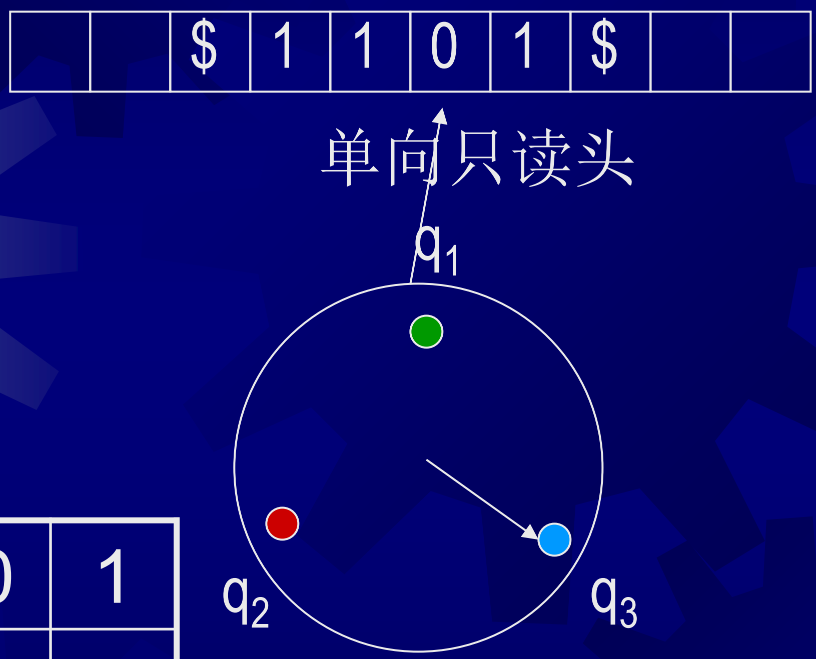
	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

M_1在1101上运行

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

M_1在1101上运行

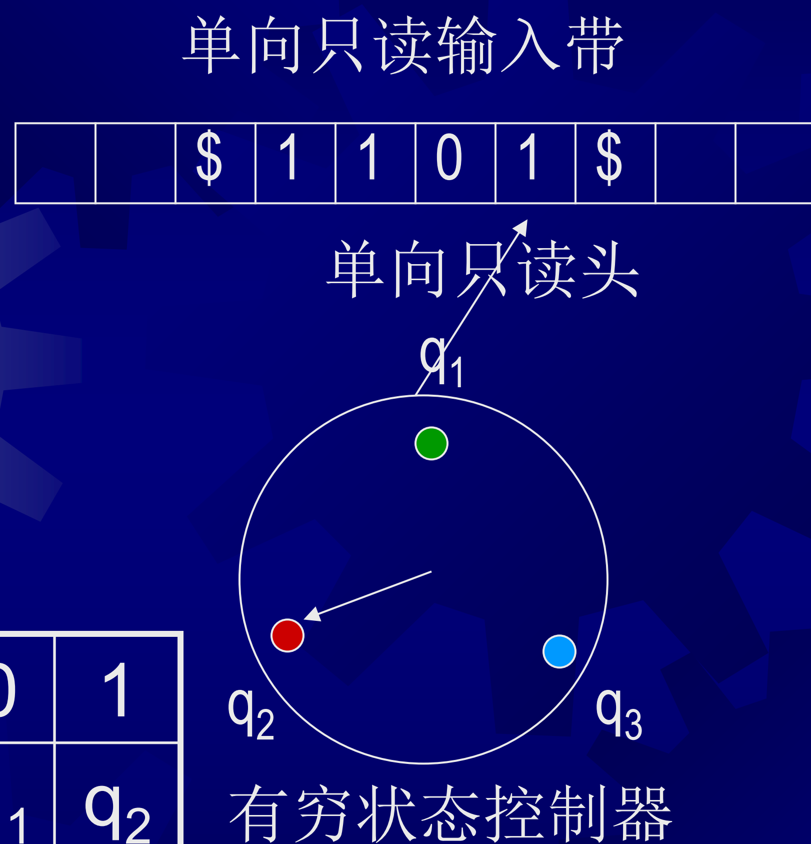
单向只读输入带



有穷状态控制器

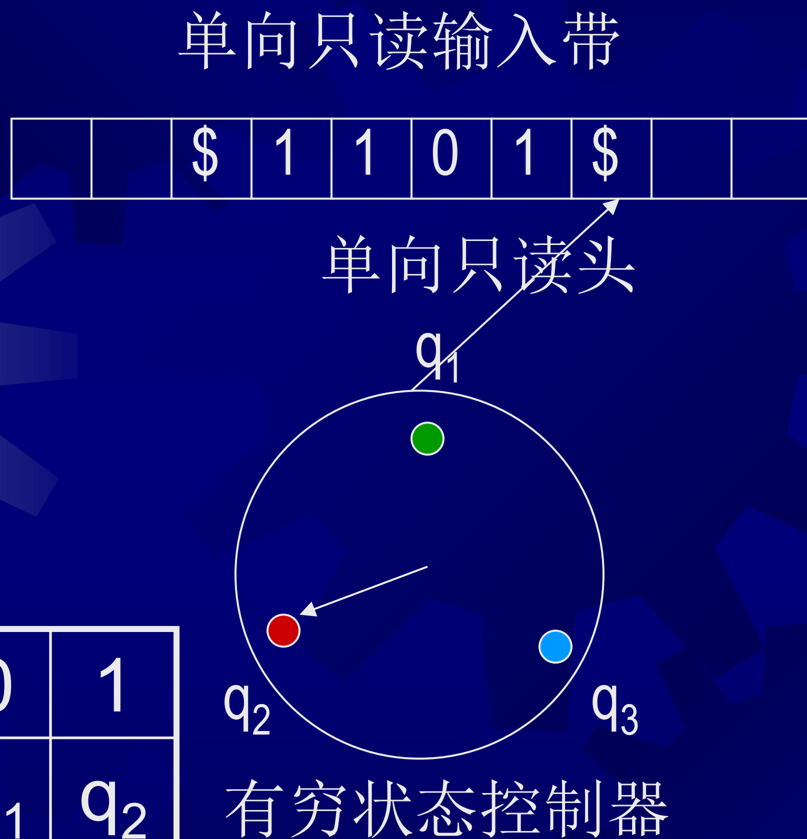
	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

M_1在1101上运行



	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

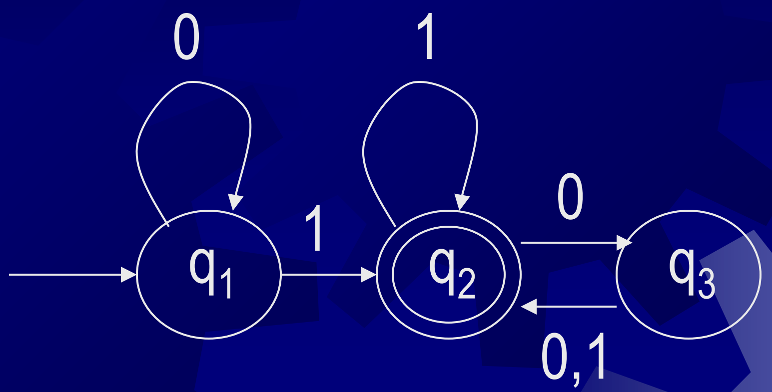
M_1在1101上运行



	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2

M_1接受哪些串?

	0	1
q_1	q_1	q_2
q_2	q_3	q_2
q_3	q_2	q_2



从初始状态到接受状态的路径上标注的字符串

1　　0*1　　0*1 1*　　0*1 1*00　　0*1 1*(00)*

0*1 1*(01)*

有穷自动机的形式定义

- 定义2.1: 有穷自动机

$M=(Q,\Sigma,\delta,q_0,F)$

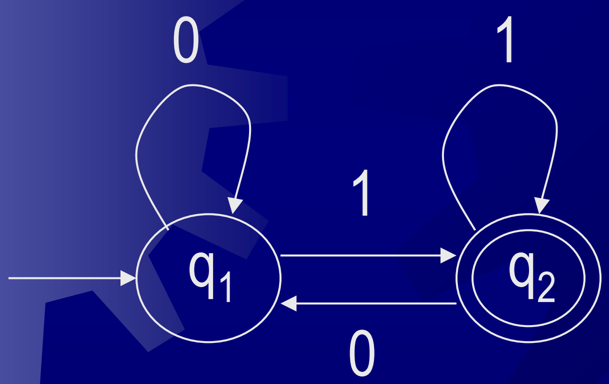
  - Q: 有穷状态集
  - Σ: 输入字母表
  - δ: $Q\times\Sigma\rightarrow Q$, 转移函数

  (δ: $Q\times\Sigma^*\rightarrow Q$, 扩展转移函数)

  - $q_0\in Q$: 初始状态
  - $F\subseteq Q$: 接受状态(终结状态)
- $L(M)=\{w\in\Sigma^* \mid \delta(q_0,w)\in F\}$

例2.2

- $M_2=(\{q_1,q_2\},\{0,1\},\delta, q_1,\{q_2\})$

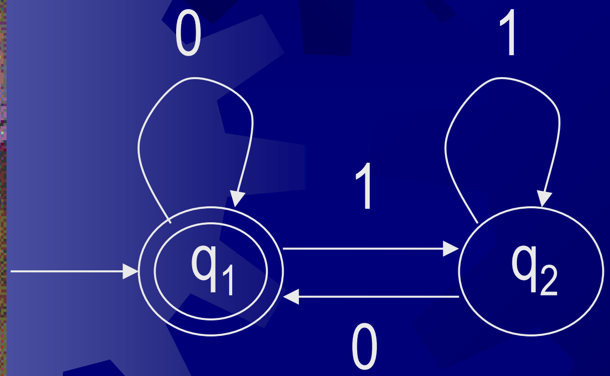


	0	1
q_1	q_1	q_2
q_2	q_1	q_2

$L(M_2) = \{ w \mid w$以1结束 $\}$

例2.3

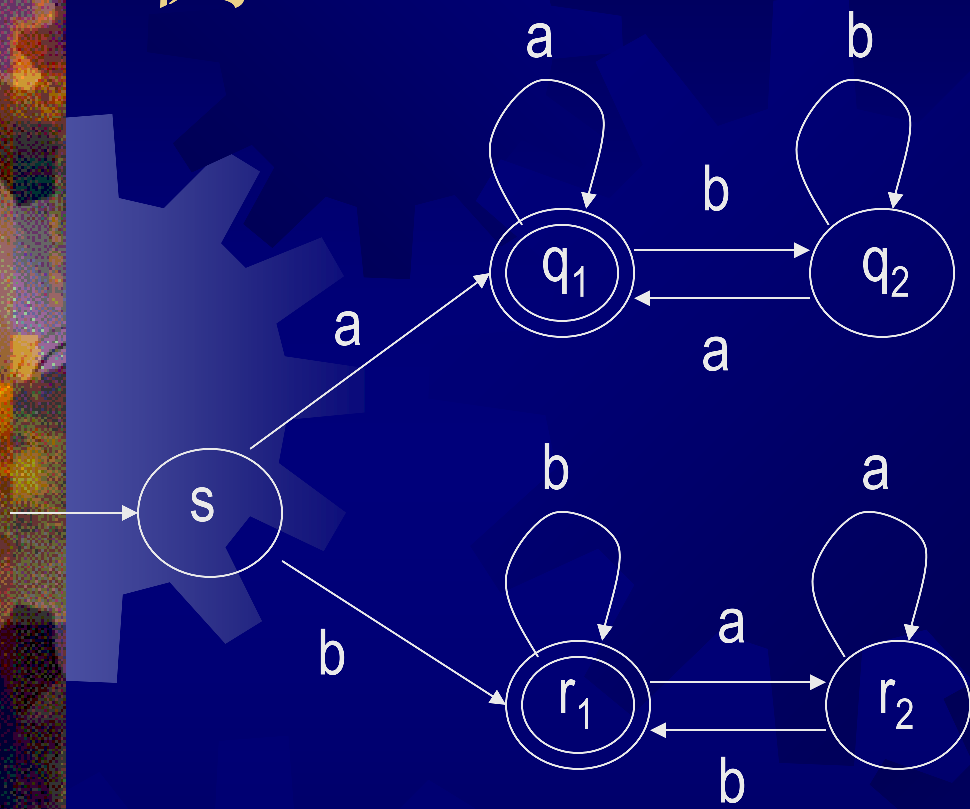
- $M_3=(\{q_1,q_2\},\{0,1\},\delta, q_1,\{q_1\})$



	0	1
q_1	q_1	q_2
q_2	q_1	q_2

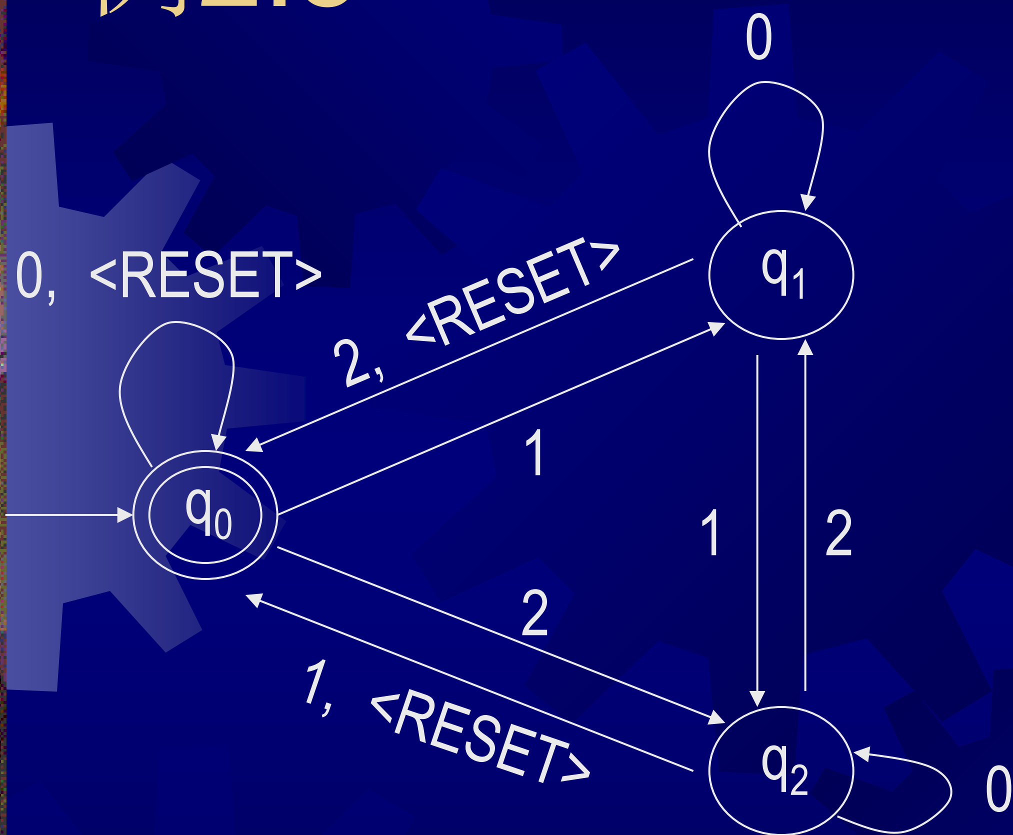
$L(M_3) = \{ w \mid w=\varepsilon$或$w$以0结束 $\}$

例2.4



$L(M_4)$ = { w | w不为空串且开头和结尾符号相同 }

例2.5



$L(M_4)$ = { w | 最后一个<RESET>之后 w的数字之和是3的倍数 }

例2.6(推广例2.5)

- $\Sigma = \{ 0, 1, 2, \text{<RESET>} \}$
- A_i = { w |最后一个<RESET>之后w数字之和是i的倍数 }
- $L(B_i)=A_i$; 自动机 B_i = ?

$B_i = (Q_i, \Sigma, \delta_i, q_0, \{q_0\})$

$Q_i = \{ q_0, q_1, q_2, \ldots , q_{i-1} \}$

$\delta_i(q_k, 0) = q_k$

$\delta_i(q_k, 1) = q_{k+1(\mathrm{mod}\ i)}$

$\delta_i(q_k, 2) = q_{k+2(\mathrm{mod}\ i)}$

$\delta_i(q_k, \text{<RESET>}) = q_0$

计算的形式定义

- $M=(Q,\Sigma,\delta,q_0,F)$;
  - 输入串$w=w_1w_2\ldots w_n$;
- 计算: 状态序列$r_0,r_1,\ldots, r_n$;
  - $r_0=q_0$;
  - $\delta(r_i,w_{i+1})=r_{i+1}$; $(i=0,1,\ldots,n-1)$
- 接受计算: M接受w
  - $r_n\in F$;
- M识别(接受)的语言:
  - L(M)={ x | M接受x }

正则语言

- 正则语言:
  - L=L(M)
  - M是有穷自动机

例2.8(续例2.5)

- $L(M_5)$ = { w | 除了 <RESET>将计数重新置0外, w符号之和模3为0 }

输入: w = 10<RESET>22<RESET>012

计算: q_0, q_1, q_1, q_0, q_2, q_1, q_0, q_0, q_1, q_0

设计有穷自动机

- 状态: 需要记住的东西
- 转移: 根据输入符号, 从一种状态到另一种状态

例

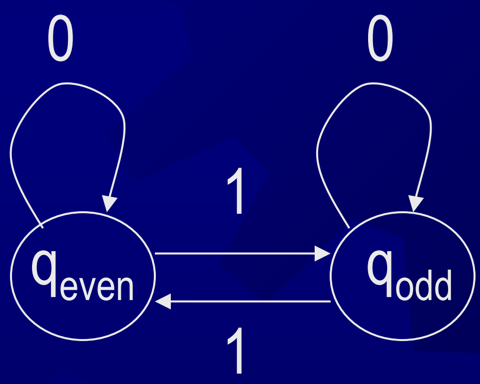
- $L(E_1)$={ w | w中有奇数个1 },
  $\Sigma=\{0,1\}$

例

- $L(E_1)=\{ w \mid w$中有奇数个$1 \}$,
  $\Sigma=\{0,1\}$

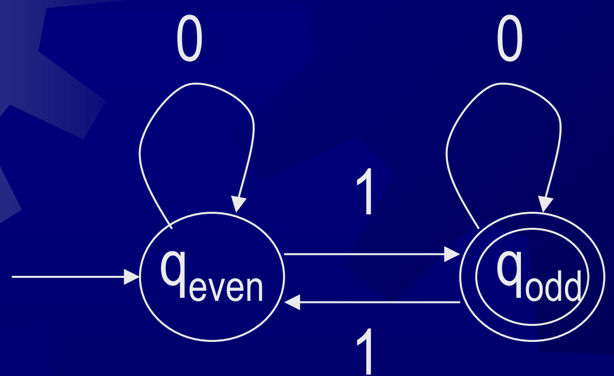
例

- $L(E_1)=\{ w \mid w$中有奇数个$1 \}$, $\Sigma=\{0,1\}$



例

- $L(E_1)=\{ w \mid w$中有奇数个$1 \}$, $\Sigma=\{0,1\}$



例2.9

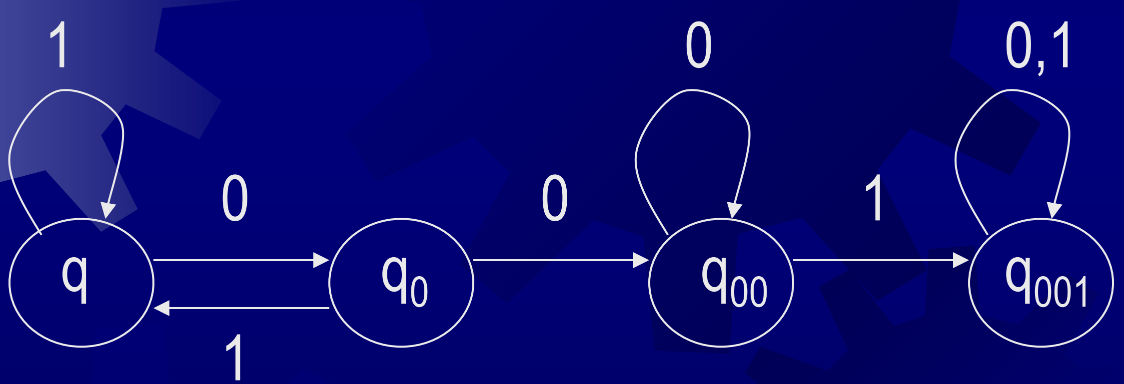
- $L(E_2)=\{ w \mid w$中含有子串$001 \}, \Sigma=\{0,1\}$

例2.9

- $L(E_2)$={ w | w中含有子串001 }, Σ={0,1}

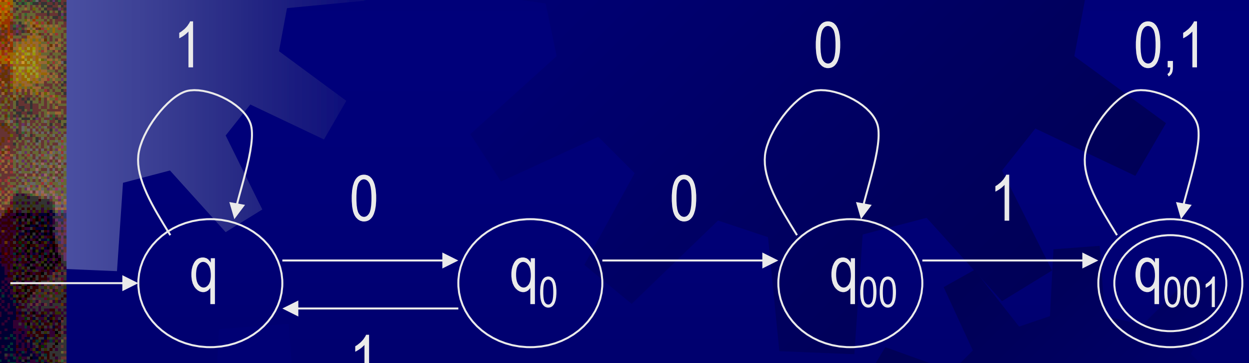
例2.9

- $L(E_2)=\{ w \mid w$中含有子串$001 \}, \Sigma=\{0,1\}$



例2.9

- $L(E_2)$={ w | w中含有子串001 }, Σ={0,1}



正则运算

- 设A,B是两个语言,正则运算是:
  - 并 $A \cup B=\{x \mid x \in A$或$x \in B\}$
  - 连接 $AB=\{xy \mid x \in A$且$y \in B\}$
  - 星号 $A^*=A^0 \cup A^1 \cup A^2 \cup A^3 \cup \ldots$

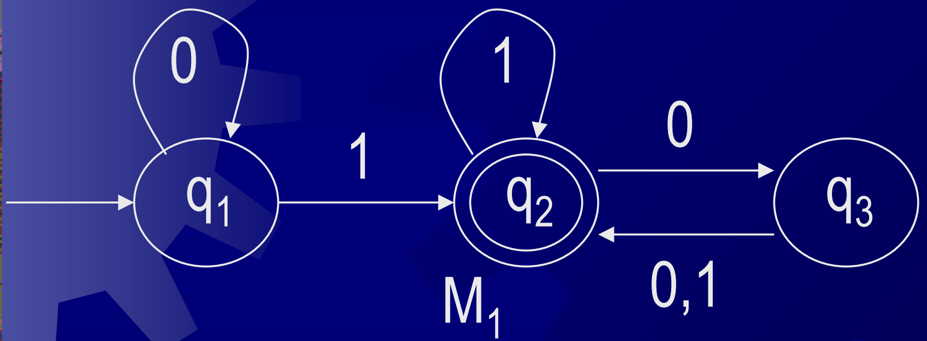
    $=\{\varepsilon\} \cup A \cup AA \cup AAA \cup \ldots$

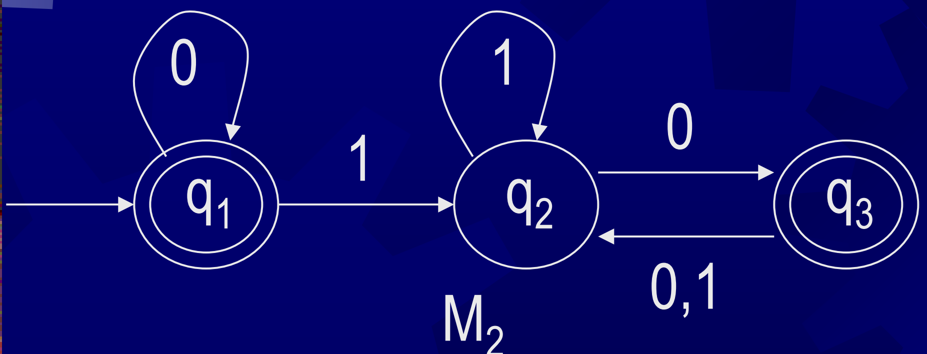
    $=\{x_1x_2\ldots x_k \mid k \geq 0$且每个$x_i \in A\}$

- 定理: 正则语言对正则运算封闭.

对补运算的封闭性

- 定理: 正则语言对补封闭.
- 证明思路





对补运算的封闭性

- 定理: 正则语言对补封闭.
- 证明: 设正则语言$L=L(M)$,

$M=(Q,\Sigma,\delta,q_0,F)$. 令$F'=Q-F$.

$M'=(Q,\Sigma,\delta,q_0,F')$.

扩充定义 $\delta:Q\times\Sigma^*\to Q$.

$\delta(q,a_1\ldots a_k)=\delta(\ldots\delta(\delta(q,a_1),a_2),\ldots,a_k)$

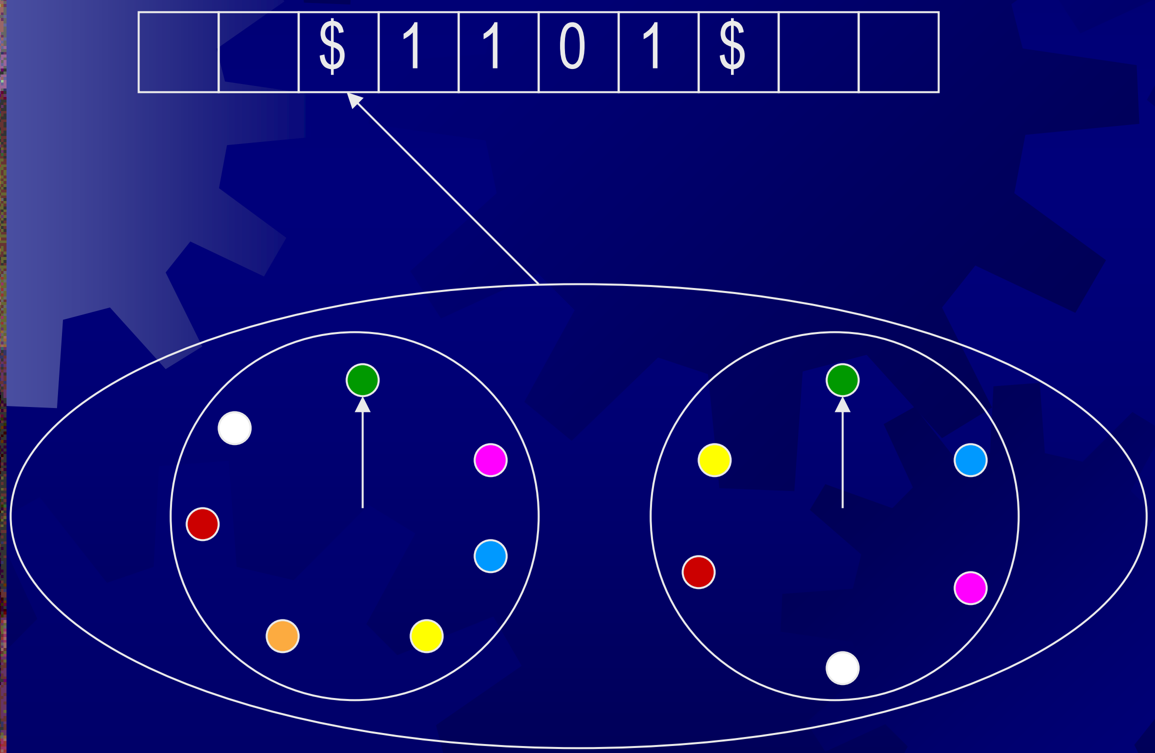
$\forall x,\ x\in L(M) \Leftrightarrow \delta(q_0,x)\in F \Leftrightarrow$

$\delta(q_0,x)\notin F' \Leftrightarrow x\notin L(M')$

$\therefore\ L(M')=\Sigma^*-L(M)=L(M)^c$. #

对并运算的封闭性

- 定理2.12: 正则语言对并封闭.
- 证明思路



对并运算的封闭性

- 定理2.12: 正则语言对并封闭.
- 证明: 设正则语言$L_i=L(M_i)$,

$M_i=(Q_i,\Sigma,\delta_i,q_i,F_i)$, $i=1,2$.

令$Q_3=Q_1\times Q_2$; $q_3=(q_1,q_2)$;

$\delta_3((r_1,r_2),a)=(\delta_1(r_1,a),\delta_2(r_2,a))$;

$F_3=(F_1\times Q_2)\cup(Q_1\times F_2)$.

$M_3=(Q_3,\Sigma,\delta_3,q_3,F_3)$.

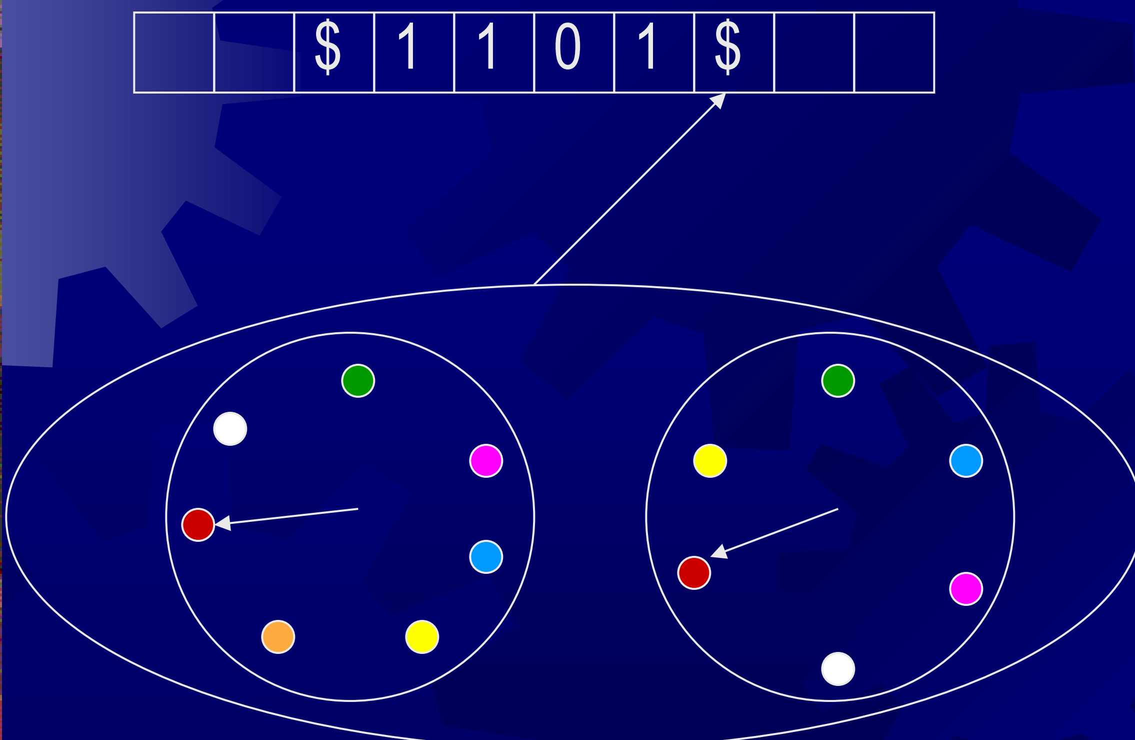
$L_1\cup L_2=L(M_1)\cup L(M_2)=L(M_3)$. #

对交运算的封闭性

- 定理: 正则语言对交封闭.
- 证明思路一:
  - 布尔运算: 交, 并, 补
- 推论:
  - 正则语言对布尔运算封闭.
- 推论:
  - 正则语言对差,对称差封闭.

对交运算的封闭性

- 定理: 正则语言对交封闭.
- 证明思路二:



对交运算的封闭性

- 定理: 正则语言对交封闭.
- 证明: 设$L_i=L(M_i)$,

$M_i=(Q_i,\Sigma,\delta_i,q_i,F_i)$; $i=1,2$.

令$Q_3=Q_1\times Q_2$; $q_3=(q_1,q_2)$;

$\delta_3((r_1,r_2),a)=(\delta_1(r_1,a),\delta_2(r_2,a))$;

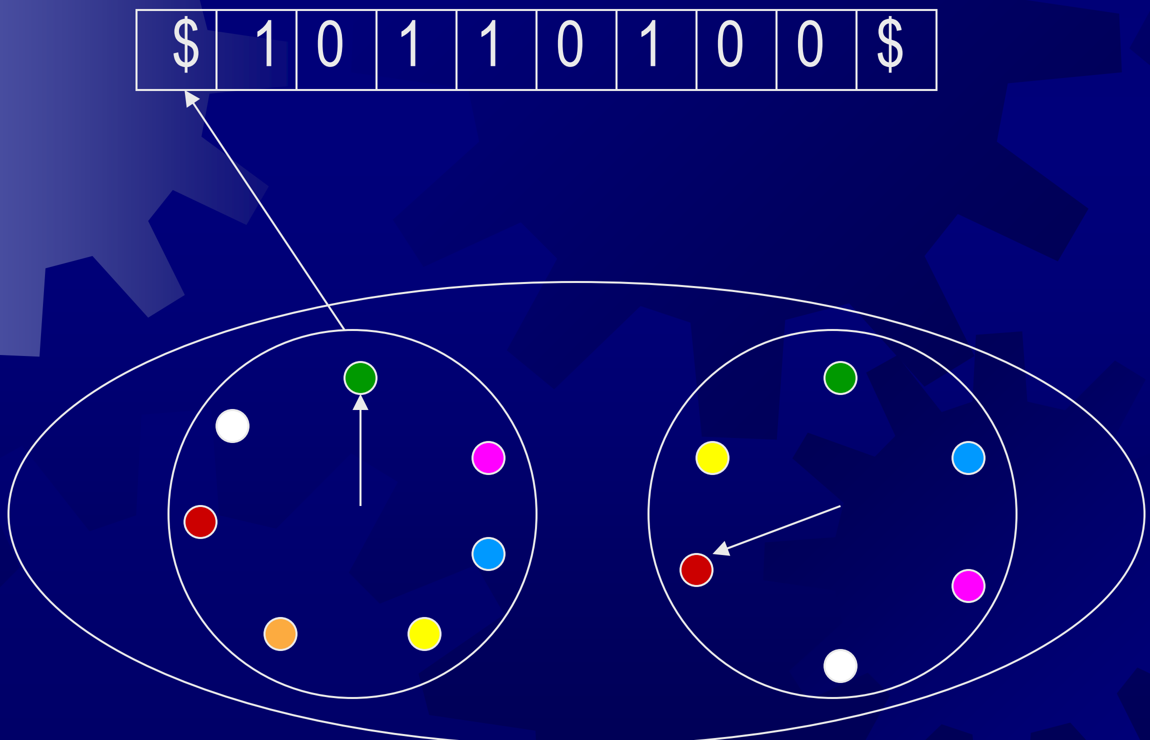
$F_3=F_1\times F_2$.

$M_3=(Q_3,\Sigma,\delta_3,q_3,F_3)$.

$L(M_3)=L(M_1)\cap L(M_2)=L_1\cap L_2$. #

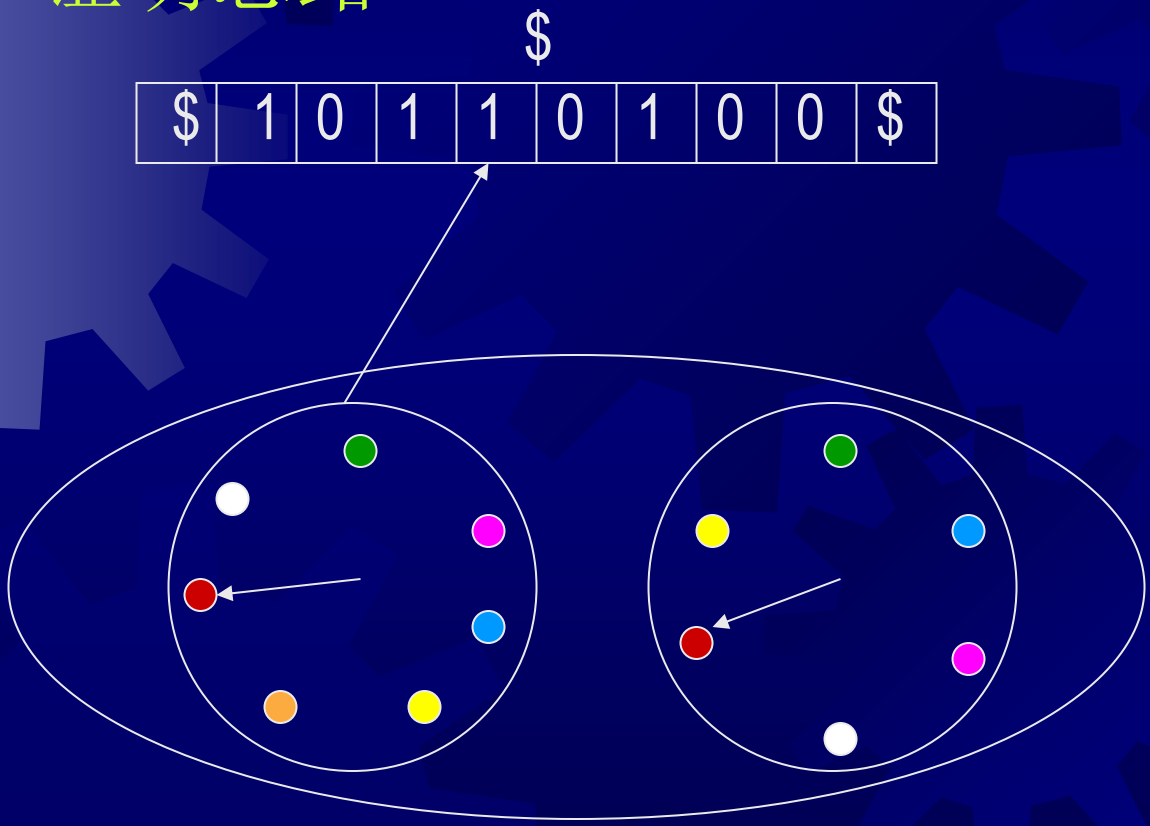
对连接运算的封闭性

- 定理2.13: 正则语言对连接封闭.
- 证明思路



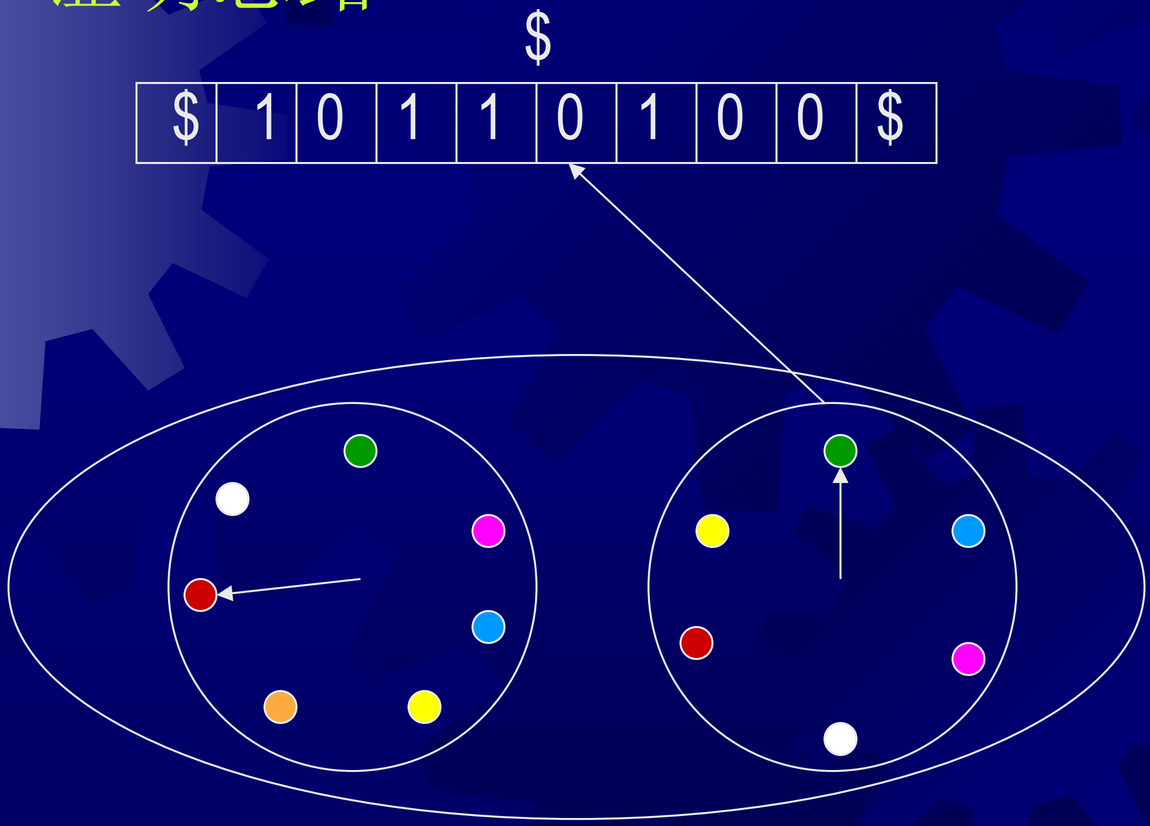
对连接运算的封闭性

- 定理2.13: 正则语言对连接封闭.
- 证明思路



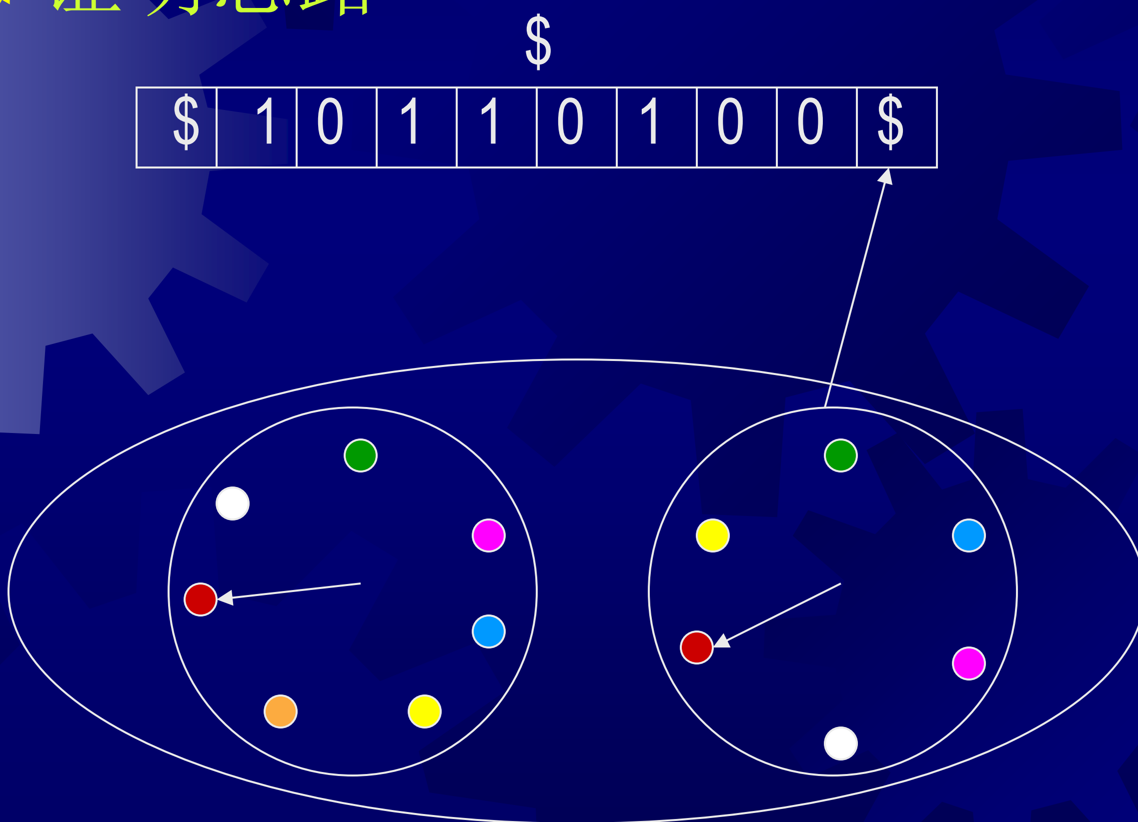
对连接运算的封闭性

- 定理2.13: 正则语言对连接封闭.
- 证明思路



对连接运算的封闭性

- 定理2.13: 正则语言对连接封闭.
- 证明思路



对连接运算的封闭性

- 定理2.13: 正则语言对连接封闭.
- 证明: $M_i=(Q_i,\Sigma,\delta_i,q_i,F_i)$; $i=1,2,3$.

$L(M_3)=L(M_1)L(M_2)$. $Q_3=Q_1\times P(Q_2)$.

扩展定义 $\delta:P(Q)\times\Sigma\to P(Q)$,

$\delta(R,a)=\{\delta(s,a)|s\in R\}$. $q_3=(q_1,s)$.

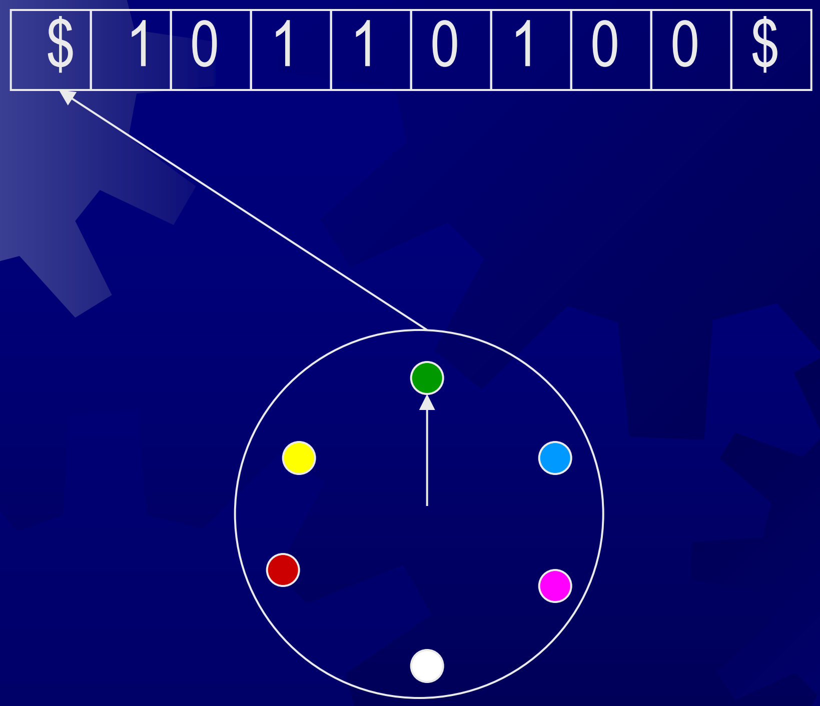
$\delta_3((r_1,r_2),a)=(\delta_1(r_1,a),\delta_2(r_2,a)\cup t)$.

$s=\begin{cases}\{q_2\}, & \text{若 } q_1\in F_1\\ \varnothing, & \text{否则.}\end{cases}$ $t=\begin{cases}\{q_2\}, & \text{若 } \delta_1(r_1,a)\in F_1\\ \varnothing, & \text{否则.}\end{cases}$

$F_3=\{ (r_1,r_2) \mid r_2\cap F_2\neq\varnothing \}$. #

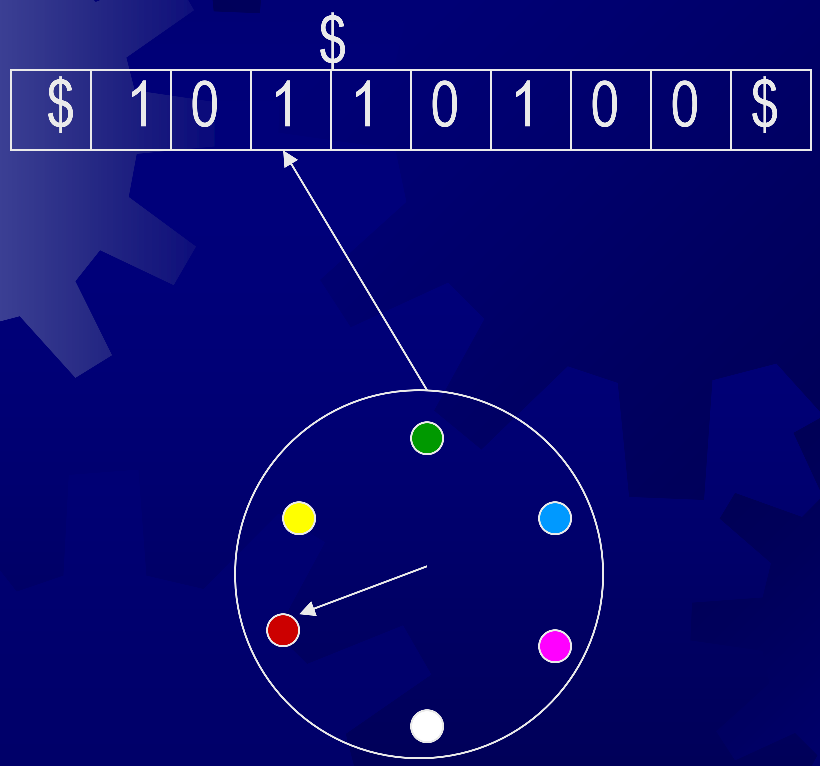
对星号运算的封闭性

- 定理2.24: 正则语言对星号封闭.
- 证明思路



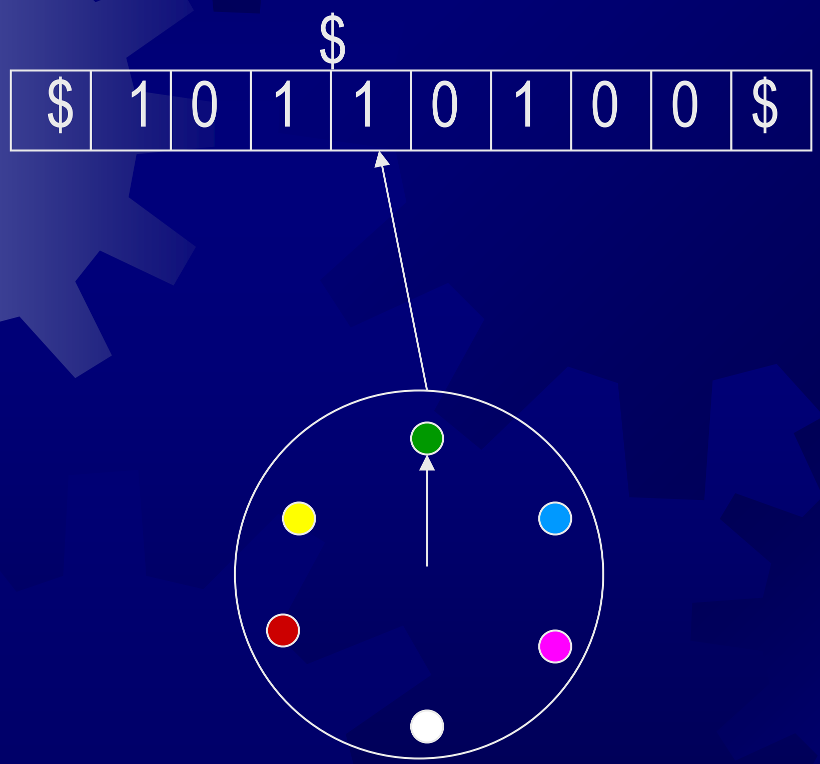
对星号运算的封闭性

- 定理2.24: 正则语言对星号封闭.
- 证明思路



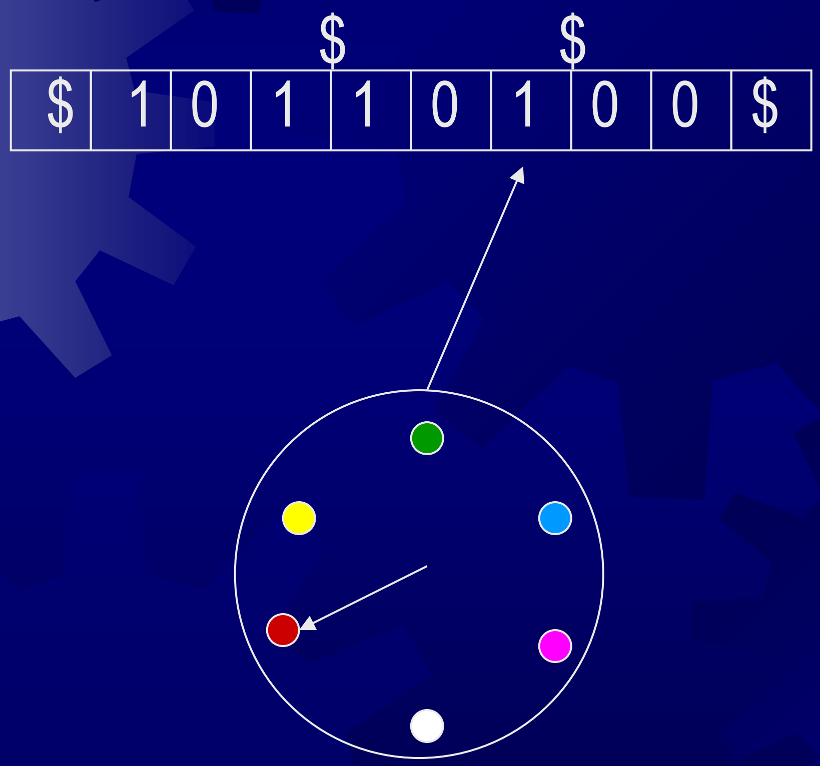
对星号运算的封闭性

- 定理2.24: 正则语言对星号封闭.
- 证明思路



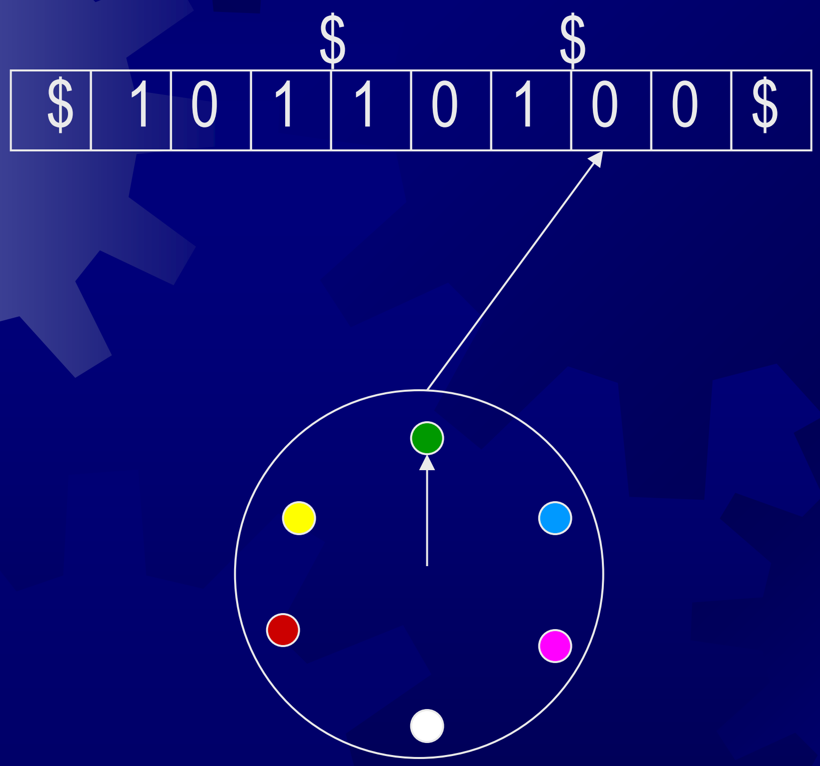
对星号运算的封闭性

- 定理2.24: 正则语言对星号封闭.
- 证明思路



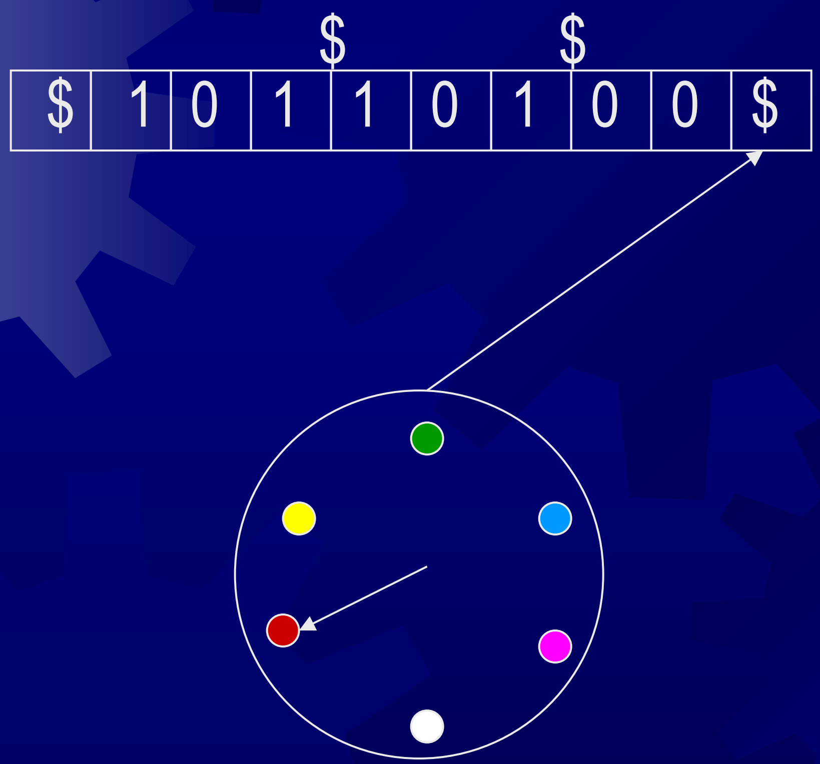
对星号运算的封闭性

- 定理2.24: 正则语言对星号封闭.
- 证明思路



对星号运算的封闭性

- 定理2.24: 正则语言对星号封闭.
- 证明思路



对星号运算的封闭性

- 定理2.24: 正则语言对星号封闭.
- 证明: ?

非确定性

作业

- 1.4 1.5 1.6 所有的单数题目