CS 330 Formal Methods and Models

Dana Richards, section 003, George Mason University, Fall 2017

Quiz Solutions

Quiz 1, Propositional Logic

Date: September 7

1. Prove $(p \wedge q) \leftrightarrow \neg(p \rightarrow \neg q)$,

   (a) (*5pts*) using truth tables.

p	q	$p \wedge q$	$\neg q$	$p \rightarrow \neg q$	$\neg(p \rightarrow \neg q)$	$(p \wedge q) \leftrightarrow \neg(p \rightarrow \neg q)$
T	T	T	F	F	T	T
T	F	F	T	T	F	T
F	T	F	F	T	F	T
F	F	F	T	T	F	T

   (b) (*5pts*) using algebra.

$$
\begin{array}{ll}
(p \wedge q) \leftrightarrow \neg(p \rightarrow \neg q) & \\
\quad \equiv (p \wedge q) \leftrightarrow \neg(\boldsymbol{\neg p \vee \neg q}) & \text{conditional law} \\
\quad \equiv (p \wedge q) \leftrightarrow (\boldsymbol{\neg\neg p \wedge \neg\neg q}) & \text{DeMorgan's law} \\
\quad \equiv (p \wedge q) \leftrightarrow (\neg\neg p \wedge \boldsymbol{q}) & \text{law of negation} \\
\quad \equiv (p \wedge q) \leftrightarrow (\boldsymbol{p} \wedge q) & \text{law of negation} \\
\quad \equiv \boldsymbol{((p \wedge q) \rightarrow (p \wedge q)) \wedge ((p \wedge q) \rightarrow (p \wedge q))} & \text{biconditional law} \\
\quad \equiv \boldsymbol{(p \wedge q) \rightarrow (p \wedge q)} & \text{idempotence} \\
\quad \equiv \boldsymbol{\neg(p \wedge q) \vee (p \wedge q)} & \text{conditional law} \\
\quad \equiv TRUE & \text{excluded middle}
\end{array}
$$

Quiz 2, Rules of Inference

Date: September 14

1. (*10pts*) Prove $(p \wedge q) \leftrightarrow \neg(p \rightarrow \neg q)$, using inference rules.

1	$[p \wedge q]$	Assumption
2	p	$\wedge$ elimination, 1
3	q	$\wedge$ elimination, 1
4	$[p \rightarrow \neg q]$	Assumption
5	$\neg q$	Modus ponens 4,2
6	$FALSE$	Contradiction 3,5
7	$\neg(p \rightarrow \neg q)$	Reduction to absurdity 4,6
8	$(p \wedge q) \rightarrow \neg(p \rightarrow \neg q)$	$\rightarrow$ introduction 1,7
9	$[\neg(p \rightarrow \neg q)]$	Assumption
10	$[\neg(p \wedge q)]$	Assumption
11	$[p]$	Assumption
12	$[q]$	Assumption
13	$p \wedge q$	$\wedge$ introduction 11,12
14	$FALSE$	contradiction 10,13
15	$\neg q$	Reduction to absurdity 12,14
16	$p \rightarrow \neg q$	$\rightarrow$ introduction 11,15
17	$FALSE$	Contradiction 9,16
18	$\neg\neg(p \wedge q)$	Reduction to absurdity 10,17
19	$(p \wedge q)$	$\neg\neg$ elimination 18
20	$\neg(p \rightarrow \neg q) \rightarrow (p \wedge q)$	$\rightarrow$ introduction 9,19
21	$(p \wedge q) \leftrightarrow \neg(p \rightarrow \neg q)$	$\leftrightarrow$ introduction 8,20

Quiz 3, Predicate Logic

Date: September 21

1. (*5pts*) Assert that an array $A[1, ..., n]$ increases and decreases once.

   "if j is to the left of i, then the series increases going to the right of j":
   $$(j < i) \rightarrow (A[j] < A[j+1])$$

   "if j is to the right of i, then the series decreases coming from the left of j":
   $$(i < j) \rightarrow (A[j-1] > A[j])$$

   "there is a point i such that the series is increasing everywhere to the left of i, and decreasing everywhere to the right of i":
   $$\begin{aligned}\exists i \in I_n :& (\forall j \in I_n : (j < i) \rightarrow (A[j] < A[j+1]) \\ & \wedge (\forall j \in I_n : (i < j) \rightarrow (A[j-1] > A[j]))\end{aligned}$$

   This assumes that either the first or second part can be a sequence of one element, i.e. the whole sequence can be just increasing or decreasing. Otherwise, insert "$i \neq 1 \wedge i \neq n$" after the first colon.

2. (*5pts*) Assert that a graph has 2 vertices such that every vertex is connected to one of the two. $G = V$ and $Edge(x, y)$.

   "a vertex z is connected to either vertex x or vertex y":
   $$Edge(z, x) \ \vee \ Edge(z, y)$$

   "every vertex z, if it isn't x or y itself, is connected to x or y":
   $$\forall z \in V : ((z \neq x) \wedge (z \neq y)) \rightarrow (Edge(z, x) \ \vee \ Edge(z, y))$$

   "there is a pair of vertices, x and y, such that every vertex is connected to one of the two":
   $$\exists x \in V : \exists y \in V : \forall z \in V : ((z \neq x) \wedge (z \neq y)) \rightarrow (Edge(z, x) \vee Edge(z, y))$$

Quiz 4, Mathematical Induction

Date: September 28

1. (*5pts*) Prove $2^{2n} - 1$ is divisible by 3, $n \geq 1$
   (i.e. $\exists m \in \mathcal{N} : 2^{2n} - 1 = 3m$)
   (Hint: $4 = 3 + 1$).

   When $n = 1$, $2^{2n} - 1 = 2^2 - 1 = 3$, which is divisible by 3, thus proving the base case.

   Assume that for some $k \geq 1$, $2^{2k} - 1$ is divisible by 3, so for some integer m_k,

   $$2^{2k} - 1 = 3m_k$$

   We would like to prove the $k + 1$ case,

   $$2^{2(k+1)} - 1 = 3m_{k+1} \qquad \text{(for some integer } m_{k+1}\text{)}$$

   To do this, we begin with the left hand side, and work until we can substitute the inductive hypothesis,

   $$\begin{aligned} 2^{2(k+1)} - 1 &= 2^{2k}2^2 - 1 \\ &= 4 \times 2^{2k} - 1 \\ &= 3 \times 2^{2k} + 2^{2k} - 1 && \text{(from the hint)} \\ &= 3 \times 2^{2k} + 3m_k && \text{(by the inductive hypothesis)} \\ &= 3(2^{2k} + m_k) \\ &= 3m_{k+1} && \text{(if we let } m_{k+1} = 2^{2k} + m_k\text{)} \end{aligned}$$

   This proves the inductive conclusion, thus by mathematical induction, the theorem is proved.

2. (*5pts*) Let $S_{n+1} = 2S_n + 1$, $n \geq 0$, $S_0 = 0$,
Prove $S_n = 2^n - 1$, $n \geq 0$.

When $n = 0$, we have

$$S_n = S_0 = 0 = 2^n - 1 = 2^0 - 1 = 1 - 1 = 0$$

Assume that for some $k \geq 0$,

$$S_k = 2^k - 1$$

We would like to prove the $k+1$ case,

$$S_{k+1} = 2^{k+1} - 1$$

To do this, we begin with the left hand side,

$$\begin{aligned} S_{k+1} &= 2S_k + 1 && \text{(from the recursive definition)} \\ &= 2(2^k - 1) + 1 && \text{(from the inductive hypothesis)} \\ &= 2 \times 2^k - 2 + 1 \\ &= 2^{k+1} - 1 \end{aligned}$$

This proves the inductive conclusion, thus by mathematical induction, the theorem is proved.

Quiz 5, Program Verification

Date: October 10

1. (*5pts*) State, prove, and use the loop invariant for the following code, assuming $n \geq 0$.

   $i \Leftarrow 0$
   $s \Leftarrow 1$
   while $i < n$ **do**
   $\quad s \Leftarrow \frac{5}{2} * s$
   $\quad i \Leftarrow i + 1$
   $\quad s \Leftarrow 6 * s$

   Solution:

   $i \Leftarrow 0$
   $s \Leftarrow 1$
   $// \quad (s = 15^i) \wedge (i \leq n)$
   while $i < n$ **do**
   $// \qquad (s = 15^i) \wedge (i \leq n) \wedge (i < n)$
   $\quad s \Leftarrow \frac{5}{2} * s$
   $// \qquad (s = \frac{5}{2} \times 15^i) \wedge (i \leq n) \wedge (i < n)$
   $\quad i \Leftarrow i + 1$
   $// \qquad (s = \frac{5}{2} \times 15^{i-1}) \wedge (i \leq n)$
   $\quad s \Leftarrow 6 * s$
   $// \qquad (s = 6 \times \frac{5}{2} \times 15^{i-1} = 15 \times 15^{i-1} = 15^i) \wedge (i \leq n)$
   $// \quad (s = 15^i) \wedge (i \leq n) \wedge \neg(i < n)$

   Note that $(i \leq n) \wedge \neg(i < n)$ implies $i = n$, so $s = 15^n$ at the end.

2. (*5pts*) State, prove, and use the loop invariant for the following code, assuming $n \geq 0$.

$m \Leftarrow n$
$y \Leftarrow 1$
$z \Leftarrow x$
while $m < 0$ **do**
  if $ODD(m)$ **then** $y \Leftarrow y * z$
  $z \Leftarrow z * z$
  $m \Leftarrow FLOOR(m/2)$

Solution:

$m \Leftarrow n$
$y \Leftarrow 1$
$z \Leftarrow x$
// $(yz^m = x^n) \wedge (m \geq 0)$
while $m < 0$ **do**
// $(yz^m = x^n) \wedge (m \geq 0) \wedge (m > 0)$
  if $ODD(m)$ **then** $y \Leftarrow y * z$
// $(yz^{2\lfloor \frac{m}{2} \rfloor} = x^n) \wedge (m \geq 0) \wedge (m > 0)$
  $z \Leftarrow z * z$
// $(yz^{\lfloor \frac{m}{2} \rfloor} = x^n) \wedge (m \geq 0) \wedge (m > 0)$
  $m \Leftarrow FLOOR(m/2)$
// $(yz^m = x^n) \wedge (m \geq 0)$
// $(yz^m = x^n) \wedge (m \geq 0) \wedge \neg(m > 0)$

Note that $(m \geq 0) \wedge \neg(m > 0)$ implies $m = 0$, so $y = x^n$ at the end.

Quiz 6, Mathematical Induction II

Date: October 24

1. (*5pts*) Prove $\sum_{i=0}^{n} a^i = \frac{a^{n+1}-1}{a-1}$, $a \neq 1$, $n \geq 0$.

   When $n = 0$, $\sum_{i=0}^{n} a^i = \sum_{i=0}^{0} a^i = a^0 = 1$, and $\frac{a^{n+1}-1}{a-1} = \frac{a^{0+1}-1}{a-1} = \frac{a-1}{a-1} = 1$, which proves the base case.

   Assume that for some $k \geq 0$, $\sum_{i=0}^{k} a^i = \frac{a^{k+1}-1}{a-1}$ with $a \neq 1$.

   We would like to prove the $k+1$ case, $\sum_{i=0}^{k+1} a^i = \frac{a^{(k+1)+1}-1}{a-1}$

   To do this, we begin with the left hand side, and work until we can substitute the inductive hypothesis,

$$\begin{aligned}\sum_{i=0}^{k+1} a^i &= a^{k+1} + \sum_{i=0}^{k} a^i \\ &= a^{k+1} + \frac{a^{k+1}-1}{a-1} && \text{(from the inductive hypothesis)} \\ &= \frac{a^{k+1}(a-1) + a^{k+1} - 1}{a-1} \\ &= \frac{a^{k+1+1}-1}{a-1}\end{aligned}$$

   This proves the inductive conclusion, thus by mathematical induction, the theorem is proved.

2. (*5pts*) Let $S_{n+1} = S_n + \left(\frac{1}{2}\right)^n$, $n \geq 0$, $S_0 = 0$.
Prove $S_n = 2 - \left(\frac{1}{2}\right)^{n-1}$, $n \geq 0$.

When $n = 0$, $2 - \left(\frac{1}{2}\right)^{n-1} = 2 - \left(\frac{1}{2}\right)^{0-1} = 2 - 2 = 0 = S_0 = S_n$, which proves the base case.

Assume that for some $k \geq 0$, $S_k = 2 - \left(\frac{1}{2}\right)^{k-1}$.

We would like to prove the $k+1$ case, $S_{k+1} = 2 - \left(\frac{1}{2}\right)^{(k+1)-1} = 2 - \left(\frac{1}{2}\right)^k$.

To do this, we begin with the left hand side, and work until we can substitute the inductive hypothesis,

$$
\begin{aligned}
S_{k+1} &= S_k + \left(\frac{1}{2}\right)^k && \text{(from the recursive definition)} \\
&= 2 - \left(\frac{1}{2}\right)^{k-1} + \left(\frac{1}{2}\right)^k && \text{(from the inductive hypothesis)} \\
&= 2 - 2 \times \left(\frac{1}{2}\right)^k + \left(\frac{1}{2}\right)^k \\
&= 2 - \left(\frac{1}{2}\right)^k
\end{aligned}
$$

This proves the inductive conclusion, thus by mathematical induction, the theorem is proved.

Quiz 7, Regular Expressions

Date: November 2

1. (*3pts*) Write all strings of length 6 in $\mathcal{L}(r)$, $r = ((a + ab)^*ba^*)$.

$$\begin{aligned}\mathcal{L}(r) = \{&baaaaa, abaaaa, abbaaa, aabaaa, ababaa,\\ &aabbaa, ababba, aaabaa, abaaba, aababa,\\ &ababab, aaabba, abaabb, aababb, aaaaba,\\ &abaaab, aabaab, aaabab, aaaabb, aaaaab\}\end{aligned}$$

2. (*3pts*) Simplify $(0 + 1)^*0(0 + 1)^* + (0 + 1)^*00(0 + 1)^*$.

   Note that $(0 + 1)^*00(0 + 1)^* \subseteq (0 + 1)^*0(0 + 1)^*$, which allows us to simplify the sum to $(0 + 1)^*0(0 + 1)^*$. Since the string must have a first zero, this expression can be further simplified to $1^*0(0 + 1)^*$.

3. (*4pts*) Give r, $\mathcal{L}(r) = \{x \mid x \text{ contains } aba \text{ but not } aa\}$.

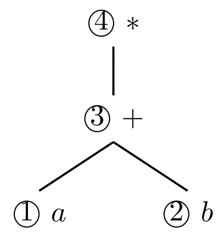
   The set of all strings of as and bs is given by $(a + b)^*$, so the set of strings without consecutive as which does not end on an a is given by $(ab + b)^*$. Similarly, the set of strings without consecutive as which does not begin with an a is given by $(ba + b)^*$. Combining with the required aba gives the solution:

   $r = (ab + b)^*aba(ba + b)^*$

Quiz 8, Regular Grammars

Date: November 7

1. (*6pts*) Convert $(a+b)^*$ into a regular grammar with unit productions.



$P_1 = \{S_1 \to aA_1, A_1 \to \Lambda\}$

$P_2 = \{S_2 \to bA_2, A_2 \to \Lambda\}$

$P_3 = \{S_3 \to S_1, S_3 \to S_2, S_1 \to aA_1, A_1 \to \Lambda, S_2 \to bA_2, A_2 \to \Lambda\}$

$P_4 = \{S_4 \to \Lambda, S_4 \to S_3, S_3 \to S_1, S_3 \to S_2,$
$S_1 \to aA_1, A_1 \to S_4, S_2 \to bA_2, A_2 \to S_4\}$

Using P_4 as the final answer, the start symbol is S_4.

2. (*4pts*) Convert into a regular grammar:
$\{S \to aA, S \to B, A \to aA, A \to bB, B \to \Lambda, B \to A\}$.

Solution:

$S \to aA$
$\cancel{S \to B}$

$A \to aA$
$A \to bB$

$B \to \Lambda$
$\cancel{B \to A}$

$\cancel{S \to A}$

$S \to \Lambda$
$S \to bB$

$B \to aA$
$B \to bB$

Quiz 9, Regular Grammar Conversion

Date: November 14

1. (*6pts*) Convert $\{S \to aS,\ S \to bB,\ A \to aB,\ A \to aS,\ B \to bA,\ B \to \Lambda\}$ into a regular expression.

   First add S', H, and missing loopbacks.

$S' \to S$	$S \to bB$	$A \to aB$	$B \to bA$	$H \to \Lambda$
	$S \to aS$	$A \to aS$	$B \to H$	
		$A \to A$	$B \to B$	

   To remove S then A then B, begin by removing S.

   $$S' \to S \ / \ S \to aS \ / \ S \to bB \quad : \quad S' \to a^*bB$$
   $$A \to aS \ / \ S \to aS \ / \ S \to bB \quad : \quad A \to aa^*bB$$

   After removing S the remaining productions are:

$S' \to a^*bB$	$A \to a + aa^*bB$	$B \to bA$	$H \to \Lambda$
	$A \to A$	$B \to H$	
		$B \to B$	

   Remove A

   $$B \to bA \ / \ A \to A \ / \ A \to a + aa^*bB \quad : \quad B \to b(a + aa^*b)B$$

   After removing A, the remaining productions are:

$S' \to a^*bB$	$B \to H$	$H \to \Lambda$
	$B \to \Lambda + b(a + aa^*b)B$	

   Remove B

   $$S' \to a^*bB \ / \ B \to \Lambda + b(a + aa^*b)B \ / \ B \to H \quad :$$

   Regular expression: $a^*b(b(a + aa^*b))^*$

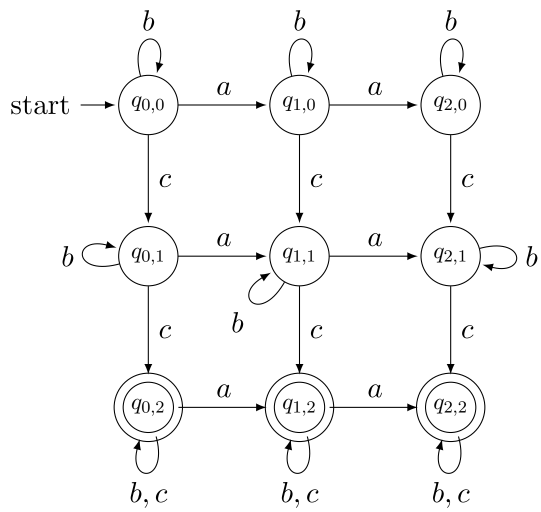
2. (*6pts*) Convert $\{S \to aS,\ S \to bB,\ A \to aB,\ A \to aS,\ B \to bA,\ B \to \Lambda\}$ into a deterministic regular grammar.

$$
\begin{array}{lll}
V_{\{S\}} \to aV_{\{S\}} & V_{\{A\}} \to aV_{\{S,B\}} & V_{\{B\}} \to aV_{\emptyset} \\
V_{\{S\}} \to bV_{\{B\}} & V_{\{A\}} \to bV_{\emptyset} & V_{\{B\}} \to bV_{\{A\}} \\
 & & \\
V_{\{S,B\}} \to aV_{\{S\}} & V_{\{A,B\}} \to aV_{\{S,B\}} & V_{\{B\}} \to \Lambda \\
V_{\{S,B\}} \to bV_{\{A,B\}} & V_{\{A,B\}} \to bV_{\{A\}} & V_{\{S,B\}} \to \Lambda \\
 & & V_{\{A,B\}} \to \Lambda
\end{array}
$$

Quiz 10, Finite Automata

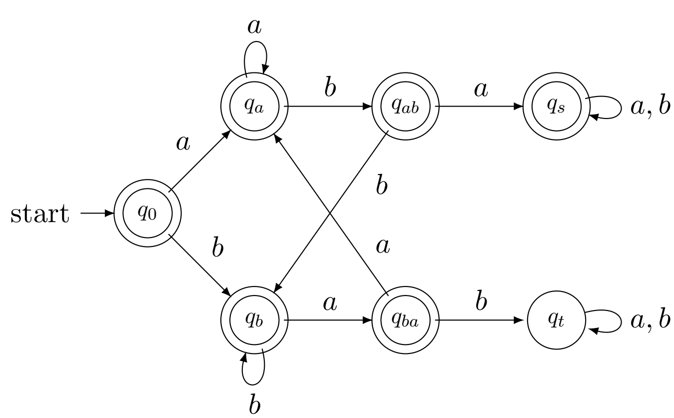
Date: November 21

1. (*5pts*) Build a DFA for $\Sigma = \{a, b, c\}$,
   $L = \{x \mid x$ contains at most 2 as and at least two cs$\}$.



2. (*5pts*) Build a DFA for $\Sigma = \{a, b\}$,
$L = \{x \mid x \text{ contains } aba \text{ before any } bab\}$.

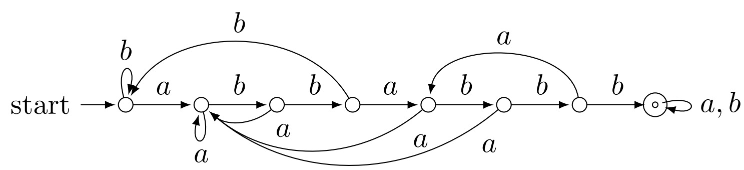
q_0 - no as or bs seen
q_a - last seen a (but not ba), no aba or bab yet
q_{ba} - last pair seen is ba, no aba or bab yet
q_b - last seen b (but not ab), no aba or bab yet
q_{ab} - last pair seen is ab, no aba or bab yet
q_s - aba seen first
q_t - bab seen first (trap state; does not need to be shown)



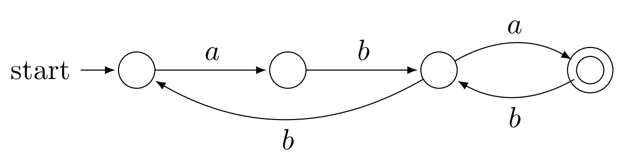
Quiz 11, Finite Automata II

Date: November 30

1. (*3pts*) Give a DFA for $\mathcal{L}(P)$, $P = abbabbbb$.



2. (*4pts*) Give a DFA for $\mathcal{L}(r)$, $r = (abb + ab)^*aba$.



3. (*3pts*) Prove $L = \{a^i b^j \mid i > j\}$ is not regular.

   Let S be the set $S = \{a^i \mid i \geq 0\}$. Pick any distinct pair $x = a^i$ and $y = a^j$ from S, and without loss of generality assume that $i > j$ (since x and y are different, then one of them has to be the longer one, so we'll call x the longer one).

   Let $z = b^j$, so z is the same length as y and shorter than x. It follows that $xz = a^i b^j \in L$ but $yz = a^j b^j \notin L$. This means that no matter which distinct pair of elements are picked from S, there is some string which can be appended to each of them which will allow them to be distinguished by a state machine.

   Since every string in S is distinguishable by a state machine, any state machine which recognizes the language must have an infinite number of states to accommodate for each of the strings in S. No finite automata can have an infinite number of states, therefore the language L is not regular.

Quiz 12, Context-Free Grammars

Date: December 7

1. (*5pts*) Give a CFG for $\{a^i b^j c^k \mid j = 2i + 3k\}$.

   Since $j = 2i + 3k$, the resulting string can be rewritten as
   $a^i b^{2i+3k} c^k = (a^i b^{2i})(b^{3k} c^k)$.

   Let A generate strings of the form $a^i b^{2i}$ and C generate strings of the form $b^{3k} c^k$. Then the following CFG will generate the language:

   $S \to AC$
   $A \to aAbb \mid \Lambda$
   $C \to bbbCc \mid \Lambda$

2. (*5pts*) Give a CFG for $\{a^i b^j c^k \mid i + j > k\}$.

   We note that since $i + j > k$, we can find some i' and j' such that $i' + j' = k$ and both $i \geq i'$ and $j \geq j'$. Thus, $i = i' + n$ and $j = j' + m$ for some non-negative n and m. Furthermore,
   $i + j = (i' + n) + (j' + m) = (i' + j') + (n + m) = k + (n + m)$,
   so $n + m$ must be greater than zero.

   The resulting string can be rewritten $a^{i'+n} b^{j'+m} c^{i'+j'} = a^{i'}(a^n b^m)(b^{j'} c^{j'}) c^{i'}$.
   Let A generate strings of the form a^n, B generate strings of the form b^m, X generate nonempty strings of the form $a^n b^m$, and C generate strings of the form $b^{j'} c^{j'}$. Then the following CFG will generate the language:

   $S \to aSc \mid XC$
   $A \to aA \mid \Lambda$
   $B \to bB \mid \Lambda$
   $X \to AaB \mid AbB$
   $C \to bCc \mid \Lambda$