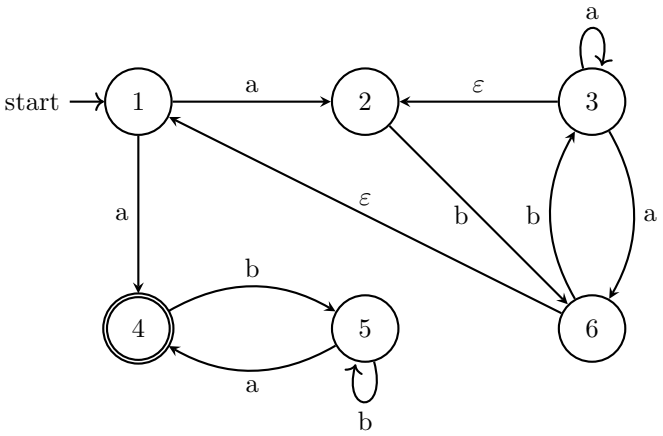
Practice Proof Writing

Rebecca J Young

Questions

Induction with NFAs

Prove, by induction on n, that for all positive integers n, the string $(abba)^n$ is accepted by this NFA.



Contradiction

Let a language be called *huggy* if and only if for every pair of distinct words, x and y, in the language, the words xyx and yxy are also in the language.

Prove by contradiction that every *huggy* language that contains at least two words is infinite.

Induction with NFAs

Let $P(n)$ be the predicate 'the string $(abba)^n$ is accepted by this NFA'.
We will prove that $P(n)$ is true for all $n \geq 1$.

Base Case: We show that P(1) is true.
There exists a path from the start state (1) to the accept state (4) that reads in the string $(abba)^1 = abba$.
The path is: $1 \to 4 \to 5 \to 5 \to 4$. Thus $(abba)^1$ is accepted by this NFA. $P(1)$ is true.

Inductive Hypothesis:
Let $k \geq 1$. Assume that $P(k)$ is true.
Let $k \geq 1$. Assume that the string $(abba)^k$ is accepted by this NFA.

Inductive Step: We will show that $P(k+1)$ is true.
We will show that the string $(abba)^{k+1}$ is accepted by this NFA.
There exists a path from the start state (1) to the start state (1) that reads in the string $abba$. The path is: $1 \to 2 \to 6 \to 3 \to 6 \to 1$. Call this path P.
We know, by our inductive hypothesis, that there exists a path from the start state (1) to the accept state (4) that reads in the string $(abba)^k$. Call this path Q.
If we concatenate the paths P and Q to get the path PQ, this will be a path from the start state (1) to the accept state (4) that reads in the string $abba(abba)^k = (abba)^{k+1}$.
Thus there exists a path from the start state (1) to the accept state (4) that reads in the string $(abba)^{k+1}$.
We have proven that the string $(abba)^{k+1}$ is accepted by this NFA. $P(k+1)$ is true.

Conclusion: By the Principle of Mathematical Induction, $P(n)$ is true for all $n \geq 1$.
By the Principle of Mathematical Induction, the string $(abba)^n$ is accepted by this NFA for all $n \geq 1$.

Proof by Induction with NFAs: Commentary

Let $P(n)$ be the predicate 'the string $(abba)^n$ is accepted by this NFA'.

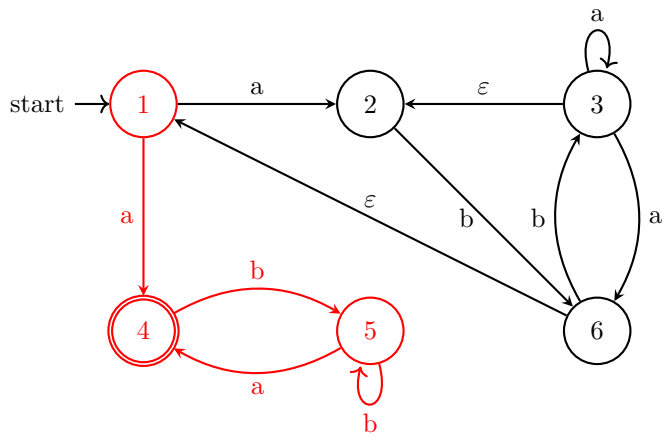
We will prove that $P(n)$ is true for all $n \geq 1$.

It is not necessary to define and use a predicate to write a good inductive proof.
Compare lines that use the predicate to equivalent lines that do not.

Base Case: We show that P(1) is true.

There exists a path from the start state (1) to the accept state (4)
that reads in the string $(abba)^1 = abba$. The path is: $1 \to 4 \to 5 \to 5 \to 4$.
Thus $(abba)^1$ is accepted by this NFA.
Thus $P(1)$ is true.

If we claim something *exists* then we must provide *evidence*.
Wrap up the Base Case by explaining what has been proven.



Inductive Hypothesis:

Let $k \geq 1$. Assume that $P(k)$ is true.

Let $k \geq 1$. Assume that the string $(abba)^k$ is accepted by this NFA.

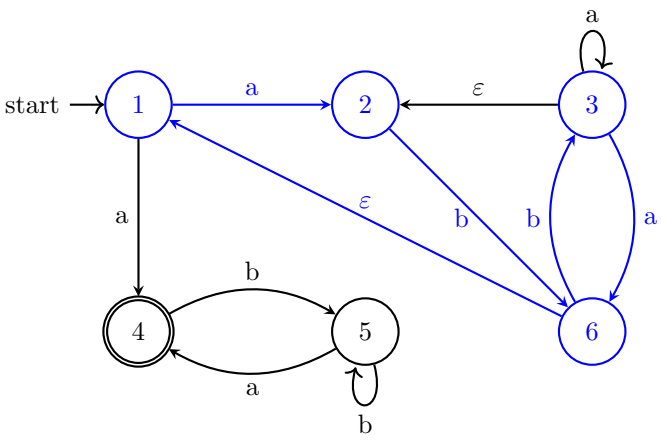
The IH must include the words 'assume' or 'suppose'.

Inductive Step: We will show that $P(k+1)$ is true.

We will show that the string $(abba)^{k+1}$ is accepted by this NFA.
There exists a path from the start state (1) to the start state (1)
that reads in the string $abba$.
The path is: $1 \to 2 \to 6 \to 3 \to 6 \to 1$. Call this path P.
We know, by our inductive hypothesis, that there exists a path from the start state (1) to the accept state (4) that reads in the string $(abba)^k$. Call this path Q.
If we concatenate the paths P and Q to get the path PQ, this will be a path from the start state (1) to the accept state (4) that reads in the string $abba(abba)^k = (abba)^{k+1}$.
Thus there exists a path from the start state (1) to the accept state (4) that reads in the string $(abba)^{k+1}$.
We have proven that the string $(abba)^{k+1}$ is accepted by this NFA.
Thus $P(k+1)$ is true.

Naming things is not necessary, but it is useful.
The IS *must* include a reference to the IH. Without this, it is not an inductive proof.

Show the reader how the IH combines with the IS reasoning.
Wrap up the IS by explaining what has been proven.



Conclusion:

The conclusion must mention induction and the range of n.

By the Principle of Mathematical Induction, $P(n)$ is true for all $n \geq 1$.

By the Principle of Mathematical Induction, the string $(abba)^n$ is accepted by this NFA for all $n \geq 1$.

Alternative approach*: It is possible to instead construct an inductive proof for the statement:
'For all non-negative integers n there exists a path for the string $(abba)^n$ from state 1 to state 1'.

Once the above proof is complete, it can be combined with the observation:
'As we have now proven there exists a path for the string $(abba)^n$ for all non-negative integers n from state 1 to state 1; and there exists a path for the string $abba$ from state 1 to state 4 ($1 \to 4 \to 5 \to 5 \to 4$); we may conclude that there exists a path from state 1 to state 4 for the string $(abba)^n$ for all positive integers n. That is, we may conclude that for all positive integers n, the string $(abba)^n$ is accepted by this NFA.'

*Thanks to the several FIT2014 students who presented this proof.

Contradiction

Assumption: We assume, for the purpose of contradiction, that it is not the case that every huggy language that contains at least two words is infinite.
That is, we assume that there exists a huggy language that contains at least two words that is finite.

Discussion:
Let L be any huggy language that contains at least two words and is finite.
As L is finite, by assumption, we know it must contain a longest word. Call this word w.
As L has at least two words, by assumption, L must contain at least one other word. Call this word u.
We know that $w \neq u$. Thus it is only possible for at most one of w or u to be ε. As w is the longest word, $w \neq \varepsilon$.
As u and w are words in L, and L is huggy, uwu and wuw must also be words in L.
As $w \neq \varepsilon$ the length of wuw is at least double the length of w.

Contradiction: Thus there exists a word in L (wuw) that is longer than the longest word in L (w).
This is a contradiction. We must conclude that it is not true that there exists a huggy language that contains at least two words that is finite.

Conclusion: We have proven using contradiction that every huggy language that contains at least two words is infinite.

Proof by Contradiction: Commentary

Assumption: We assume, for the purpose of contradiction, that it is not the case that every huggy language that contains at least two words is infinite.
That is, we assume that there exists a huggy language that contains at least two words that is finite.

The Assumption must include the words 'assume' or 'suppose'.

Use this structure if you are worried about how to construct your assumption.

Be careful to avoid making your assumption too strong: $\neg\forall = \exists\neg$

Discussion:
Let L be any huggy language that contains at least two words and is finite.
As L is finite, by assumption, we know it must contain a longest word.
Call this word w.
As L has at least two words, by assumption, L must contain at least one other word. Call this word u.
We know that $w \neq u$. Thus it is only possible for at most one of w or u to be ε. As w is the longest word, $w \neq \varepsilon$.
As u and w are words in L, and L is huggy, uwu and wuw must also be words in L.
As $w \neq \varepsilon$ the length of wuw is at least double the length of w.

Naming things is not necessary, but it is useful.

Ensure every claim is justified.

We must show that at least one word is non-empty.

Contradiction: Thus there exists a word in L (wuw) that is longer than the longest word in L (w).
This is a contradiction. We must conclude that it is not true that there exists a huggy language that contains at least two words that is finite.

We need to get to the point where we say 'Thus A and $\neg A$'. E.g.: there is a longer word than the longest word.

Use this structure to summarise the contradiction.

Conclusion: We have proven using contradiction that every huggy language that contains at least two words is infinite.

Conclude the proof.

Alternative approach*: Instead of generating the contradiction that there exists a word that is longer than the longest word, we can generate the contradiction that L, being a finite language, has n words (where n is some unknown, but locked-in number). We can then generate a word that was not included in the count of n, and thus show that the language has $n + 1$ words.

Note that this approach does not save us work, as we still need to reason that there is a longest word, and then show that this new word was not counted because it is longer than the longest word. However, this approach is sound.

*Thanks to the several FIT2014 students who presented this proof.