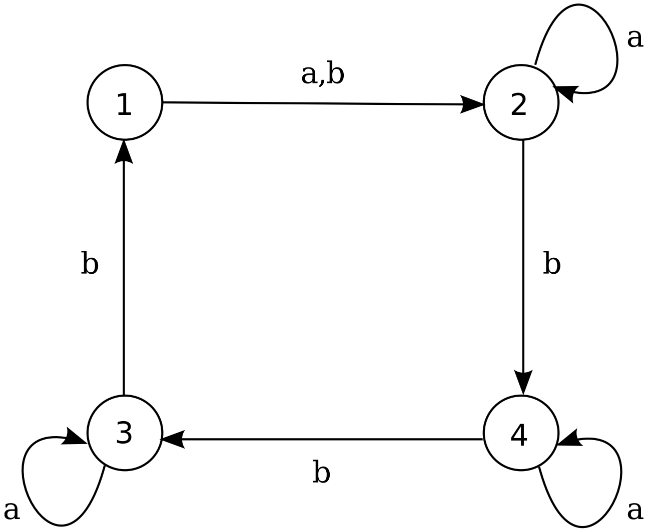
Černý's Conjecture

Narad Rampersad

Department of Mathematics and Statistics
University of Winnipeg

Finite Automata

Here is a finite automaton.



Formal Definition

- For the purposes of this talk a finite automaton is a directed multigraph where
  - every vertex has constant out-degree k, and
  - the outgoing arcs of each vertex are labeled by distinct elements of a fixed k-element set.
- We call the vertices states and denote the set of states by Q.
- We call the arcs transitions.
- Arcs are labeled by letters.
- A sequence of letters is called a word.

Formal Definition

- A transition from state p to state q labeled by the letter a is denoted by the transition function δ, where $\delta(p, a) = q$.
- If $w = w_1 w_2 \cdots w_n$ is a word we define

$$\delta(q, w) = \delta(\delta(q, w_1 w_2 \cdots w_{n-1}), w_n);$$

  i.e., $\delta(q, w)$ is the state reached by starting at q and following the sequence of arcs labeled $w_1, w_2, \ldots, w_n$.
- If $A \subseteq Q$ is a set of states we define

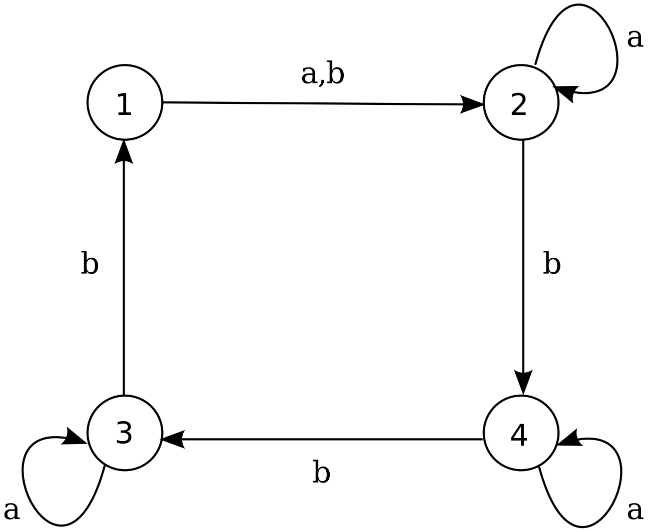
$$\delta(A, w) = \bigcup_{q \in A} \delta(q, w).$$

Synchronizing Automata

- An automaton is synchronizing if there exists a word w, called the reset word, such that $\delta(q, w) = \delta(q', w)$ for all pairs of states $q, q' \in Q$.
- Equivalently, there exists a state p and a word w such that $\delta(Q, w) = \{p\}$.
- Given an automaton, can we decide if it is synchronizing?
- If so, can we find the shortest reset word?

A Synchronizing Automaton

Reset word: *abbbabbba*.



Applications

- Moore's Gedanken-experiments (1950's):
- Imagine a satellite orbiting the moon: its behaviour while on the dark side of the moon cannot be observed. When control is reestablished, we wish to reset the system to a particular configuration.
- Robotics (Natarajan 1980's):
- Imagine parts arriving on an assembly line with arbitrary orientations. The parts must be manipulated into a fixed orientation before proceeding with assembly.
- Concept of a synchronizing automaton independently rediscovered many times.

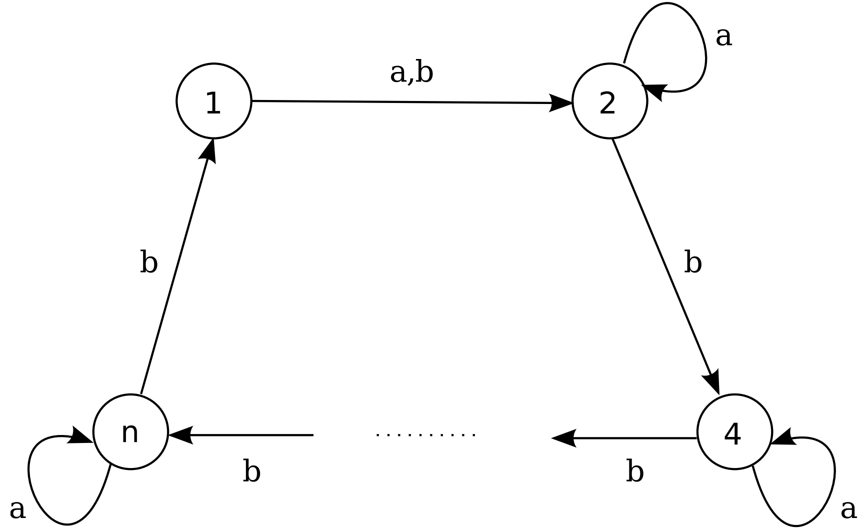
Černý's Conjecture

Conjecture (Černý 1964)

The shortest reset word of any synchronizing automaton with n states has length at most $(n-1)^2$.

Černý's Construction

Reset word: $(ab^{n-1})^{n-2}a$ (length $(n-1)^2$).



The Greedy Algorithm

- If M is a synchronizing automaton, there is a sequence of sets $Q = P_1, P_2, \ldots, P_t$, and a sequence of words $w_1, w_2, \ldots, w_{t-1}$, such that
  - $\delta(P_i, w_i) = P_{i+1}$, for $i = 1, \ldots, t-1$;
  - $|P_i| > |P_{i+1}|$, for $i = 1, \ldots, t-1$;
  - $|P_t| = 1$.
- Then $w = w_1 w_2 \cdots w_{t-1}$ is a reset word for M.

Algorithm to find reset word w

Set $P_1 = Q$ and $t = 1$.

While $|P_t| > 1$:

  Find a smallest word w_t such that $|\delta(P_t, w_t)| < |P_t|$.

  Set $P_{t+1} = \delta(P_t, w_t)$ and increment t.

Return $w = w_1 w_2 \cdots w_{t-1}$.

The Reset Word Found by the Greedy Algorithm

- What is the maximum length of w found by the greedy algorithm?
- In the worst case, $|P_i| - |P_{i+1}| = 1$, so that $t = n$.
- Consider a generic step k: i.e., P_k and w_k such that $|\delta(P_k, w_k)| < |P_k|$.
- What is the longest that w_k can be?
- Let $w_k = a_1 a_2 \cdots a_{m+1}$.
- Then we have a sequence of sets $P_k = A_1, A_2, \ldots, A_{m+2}$ such that
  - $\delta(A_i, a_1) = A_{i+1}$ for $i = 1, \ldots, m+1$;
  - $|A_i| = |A_{i+1}|$ for $i = 1, \ldots, m$;
  - $|A_{m+1}| > |A_{m+2}|$.

A Bound on the Length of the Reset Word

- Observe that for $i = 1, \ldots, m+1$,

$$|\delta(A_i, a_i \cdots a_{m+1})| < |A_i|.$$

- This implies that there exists $q_i, q_i' \in A_i$ such that

$$\delta(q_i, a_i \cdots a_{m+1}) = \delta(q_i', a_i \cdots a_{m+1}).$$

- To each A_i, associate the set $B_i = \{q_i, q_i'\}$, for $i = 1, \ldots, m$.
- Note that for $i = 1, \ldots, m$, $B_i \subseteq A_i$.
- Furthermore, for $i < j$, $B_j \not\subseteq A_i$; otherwise, we would have a shorter word $w_k' = a_1 \cdots a_{i-1} a_j \cdots a_{m+1}$ such that $|\delta(P_k, w_k')| < |P_k|$, contradicting the minimality of w_k.

A Bound on the Length of the Reset Word

- Let $\overline{A_i}$ denote the complement of A_i, i.e., the set $Q \setminus A_i$.
- We thus have
  - $B_i \cap \overline{A_i} = \emptyset$ for $i = 1, \ldots, m$;
  - $B_j \cap \overline{A_i} \neq \emptyset$ for $i < j$.
- What is the largest that m can be subject to these constraints?
- Let $|Q| = n$. Then $|\overline{A_i}| = n - k$ (since $|A_i| = k$) and $|B_i| = 2$ for $i = 1, \ldots, m$.
- We claim that $m \leq \binom{n-k+2}{2}$ (we shall prove this later).
- The total length of the reset word $w = w_1 w_2 \cdots w_{n-1}$ is then at most

$$\sum_{k=2}^{n} \binom{n-k+2}{2} = \frac{n^3 - n}{6}.$$

The Current Status of the Conjecture

- This bound of $(n^3 - n)/6$ is the best known upper bound on the length of a shortest reset word.
- Originally conjectured by Fischler and Tannenbaum in 1970 and (independently) by Pin in 1981.
- After hearing Pin's 1981 talk, Frankl proved the inequality $m \leq \binom{n-k+2}{2}$ mentioned earlier, thus establishing the result.
- Recall that Černý's conjecture is that the optimal upper bound is $(n-1)^2$.
- The conjecture has been established for certain special cases: e.g., in 2003 Kari verified the conjecture for synchronizing automata whose underlying digraphs are Eulerian.

A Result from Extremal Set Theory

Theorem (Frankl 1982)

Let $A_1, \ldots, A_m$ be sets of size r and let $B_1, \ldots, B_m$ be sets of size s such that

(a) $A_i \cap B_i = \emptyset$ *for* $i = 1, \ldots, m$;

(b) $A_i \cap B_j \neq \emptyset$ *if* $i < j$.

Then $m \leq \binom{r+s}{s}$.

- Set $X = \bigcup_{i=1}^{m} (A_i \cup B_i)$.
- Choose $V \subseteq \mathbb{R}^{r+1}$ so that $|V| = |X|$ and the vectors in V are in general position (i.e., any $r+1$ vectors from V are linearly independent).
- Associate to each element of X a corresponding element of V.
- From now on, consider the A_i's and B_i's to be subsets of V, rather than X.

The Proof of Frankl's Result

- Associate to each B_j a polynomial f_j in the variables $x = (x_1, \ldots, x_{r+1})$:
$$f_j(x) = \prod_{v \in B_j} \langle v, x \rangle.$$
- Since A_i consists of r linearly independent vectors, span A_i has dimension r.
- For each i, choose an element y_i in the 1-dimensional orthogonal space of span A_i.
- Then $\langle v, y_i \rangle = 0$ iff $v \in$ span A_i.
- We claim that $v \in$ span A_i iff $v \in A_i$.
- Suppose $v \in$ span A_i but $v \notin A_i$.
- Then span $(A_i \cup \{v\}) =$ span A_i has dimension r, contradicting the assumption that V consists of vectors in general position.
- Thus, $\langle v, y_i \rangle = 0$ iff $v \in A_i$.

The Proof of Frankl's Result

- Recall,

$$f_j(x) = \prod_{v \in B_j} \langle v, x \rangle.$$

- Thus, $f_j(y_i) = 0$ iff $\langle v, y_i \rangle = 0$ for some $v \in B_j$.
- Thus, $\langle v, y_i \rangle = 0$ for some $v \in B_j$ iff ($v \in B_j$ and $v \in A_i$) iff $A_i \cap B_j \neq \emptyset$.
- By assumption, $A_i \cap B_j \neq \emptyset$ for $i < j$, and $A_i \cap B_j = \emptyset$ for $i = j$.
- Thus, $f_j(y_i) = 0$ for $i < j$ and $f_j(y_i) \neq 0$ for $i = j$.
- We wish to show that the f_j's are linearly independent.
- Suppose not. Then there is a non-trivial linear relation

$$c_1 f_1 + \cdots + c_m f_m = 0.$$

The Proof of Frankl's Result

- Let k be the least index so that $c_k \neq 0$.
- Evaluate the f_j's at y_k to obtain

$$c_1 f_1(y_k) + \cdots + c_k f_k(y_k) + \cdots + c_m f_m(y_k) = 0.$$

- The first $k-1$ terms of this sum vanish by our choice of k.
- The last $m-k$ terms of this sum vanish since $f_j(y_i)$ vanishes whenever $i < j$.
- We thus have $c_k f_k(y_k) = 0$. But $f_k(y_k) \neq 0$, so $c_k = 0$, contrary to our choice of c_k.
- We conclude that the f_j's are linearly independent.

The Proof of Frankl's Result

- We now bound the dimension of the subspace containing the f_j's.
- The monomials of the f_j's all have degree s.
- The monomials of degree s thus form a basis for this subspace.
- How many such monomials are there?
- A monomial of degree s is of the form

$$x_1^{\ell_1} \cdots x_{r+1}^{\ell_{r+1}},$$

  where $\ell_1 + \cdots + \ell_{r+1} = s$.
- The number of solutions to this Diophantine equation in non-negative integers $\ell_1, \ldots, \ell_{r+1}$ is $\binom{r+s}{s}$.
- The f_j's thus consists of m linearly independent polynomials in a space of dimension at most $\binom{r+s}{s}$.
- It follows that $m \leq \binom{r+s}{s}$, and the proof is complete.

Applying the Combinatorial Result

- When analyzing the greedy algorithm, at step k we had sets $\overline{A_i}$ and B_i, where
  - $|\overline{A_i}| = n - k$ for $i = 1, \ldots, m$;
  - $|B_i| = 2$ for $i = 1, \ldots, m$;
  - $B_i \cap \overline{A_i} = \emptyset$ for $i = 1, \ldots, m$;
  - $B_j \cap \overline{A_i} \neq \emptyset$ for $i < j$.
- Frankl's result gives $m \leq \binom{n-k+2}{2}$.
- We then summed these lengths to obtain the upper bound

$$\sum_{k=2}^{n} \binom{n-k+2}{2} = \frac{n^3 - n}{6}$$

on the length of a reset word.

Summary

Conjecture (Černý 1964)

The shortest reset word of any synchronizing automaton with n states has length at most $(n-1)^2$.

- We have a matching lower bound of $(n-1)^2$.
- We have an upper bound of $(n^3-n)/6$.
- The conjecture has been proved for several particular classes of automata.

Thank you!