Postselecting probabilistic finite state recognizers and verifiers

University of Latvia
Faculty of computing
PhD program student

Maksims Dimitrijevs,
Abuzer Yakaryılmaz

Our scope

Different bounded-error probabilistic models:
Error bound ε (0 ≤ ε < ½):

- if w ∈ L, w is accepted with probability 1-ε;
- if w ∉ L, w is rejected with probability 1-ε.

Deterministic Turing machines can recognize only countably many languages. How many resources is enough for probabilistic models to define uncountably many languages?

$$\aleph_1$$

Restricted 2-way input head

- 2-way model.
- Sweeping model.
- Restarting realtime model.

Postselection

Postselection is the ability to give a decision by assuming that the computation is terminated with pre-determined outcome(s) and discarding the rest of the outcomes. Final probabilities:

$$\frac{a(w)}{a(w)+r(w)} \text{ and } \frac{r(w)}{a(w)+r(w)}$$

Restarting realtime PFAs = Postselecting realtime PFAs

Realtime PostPFA

$$P = (\Sigma, S, \delta, s_I, s_{pa}, s_{pr})$$

- Σ - the input alphabet,
- S - the finite set of states,
- δ: S x Σ∪{▷,◁} x S ⟶[0,1] - the transition function,
- s_I ∈ S - the initial state,
- s_{pa} ∈ S and s_{pr} ∈ S are the postselecting accepting and rejecting states, respectively.

Recognition of a language

Language $L \subseteq \Sigma^*$ is said to be recognized by a PostPFA P with error bound ε if:

- any member is accepted by P with probability at least 1-ε,
- any non-member is rejected by P with probability at least 1-ε.

One-way private-coin IPS

- Interactive proof system - the prover and probabilistic verifier.
- Private-coin - the prover does not know the probabilistic outcomes of the verifier.
- One-way - the whole responses of the prover can be seen as an infinite string and this string is called as (membership) certificate. The automaton reads the provided certificate in one-way mode.

PostPFA verifier

$$V = (\Sigma, \Upsilon, S, \delta, s_I, s_{pa}, s_{pr})$$

- Σ - the input alphabet,
- Y - the certificate alphabet,
- S - the finite set of states,
- δ: $S \times \Sigma \cup \{\triangleright, \triangleleft\} \times Y \times S \times \{0,1\} \longrightarrow [0,1]$ - the transition function,
- $s_I \in S$ - the initial state,
- $s_{pa} \in S$ and $s_{pr} \in S$ are the postselecting accepting and rejecting states, respectively.

Verification of a language

Language $L \subseteq \Sigma^*$ is said to be verified by a PostPFA verifier V with error bound ε if:

- for any member $w \in L$, there exists a certificate, say c_w, such that V accepts w with probability at least 1-ε,
- for any non-member $w \notin L$ and for any certificate $c \in \Upsilon^\infty$, V always rejects w with probability at least 1-ε.

Additional memory

A PFA can be extended with:

- integer counter (PCA), ?=0, +{-1,0,1},
- work tape (PTM).

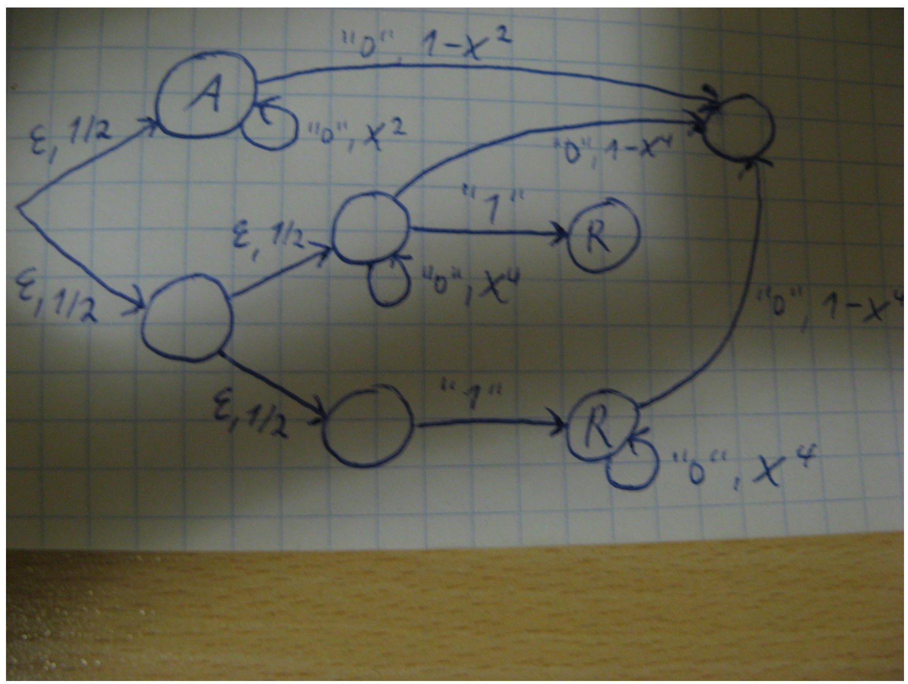
EQUAL

w=0^m10^n

$$\texttt{EQUAL} = \{0^m10^m \mid m > 0\}$$

$$Pr[A] = x^{2m+2n}$$

$$Pr[R] = \left(\frac{x^{4m} + x^{4n}}{2}\right)$$



EQUAL

$w = 0^m 1 0^n$

$$\texttt{EQUAL} = \{0^m 1 0^m \mid m > 0\}$$

$$\text{if } m = n, \text{ then } Pr[A] = Pr[R] = x^{4m}$$

else,

$$\frac{Pr[R]}{Pr[A]} = \frac{\frac{x^{4m}+x^{4n}}{2}}{x^{2m+2n}} = \frac{x^{2m-2n}}{2} + \frac{x^{2n-2m}}{2} > \frac{1}{2x^2}$$

Accept with pr. Pr[A], reject with pr. x∗Pr[R].

$$\frac{x^{-1}}{1+x^{-1}} = \frac{1}{x+1} \qquad \frac{(2x)^{-1}}{1+(2x)^{-1}} = \frac{1}{2x+1}$$

EQUAL-BLOCKS

$$\texttt{EQUAL-BLOCKS} = \{0^{m_1}10^{m_1}10^{m_2}10^{m_2}1\cdots10^{m_t}10^{m_t} \mid t > 0\}$$

$$w = 0^{m_1}10^{n_1}10^{m_2}10^{n_2}1\cdots10^{m_t}10^{n_t}$$

$$Pr[A] = \underbrace{\left(x^{2m_1+2n_1}\right)}_{a_1}\underbrace{\left(x^{2m_2+2n_2}\right)}_{a_2}\cdots\underbrace{\left(x^{2m_t+2n_t}\right)}_{a_t}$$

$$Pr[R] = \underbrace{\left(\frac{x^{4m_1}+x^{4n_1}}{2}\right)}_{r_1}\underbrace{\left(\frac{x^{4m_2}+x^{4n_2}}{2}\right)}_{r_2}\cdots\underbrace{\left(\frac{x^{4m_t}+x^{4n_t}}{2}\right)}_{r_t}$$

EQUAL-BLOCKS(f)

$$\texttt{EQUAL-BLOCKS}(\texttt{f}) = \{0^{m_1}10^{f(m_1)}10^{m_2}10^{f(m_2)}1\cdots 10^{m_t}10^{f(m_t)} \mid t > 0\}$$

f(m)=am+b, a≥0, b≥0

$$w = 0^{m_1}10^{n_1}10^{m_2}10^{n_2}1\cdots 10^{m_t}10^{n_t}$$

$$Pr[A] = \underbrace{\left(x^{2f(m_1)+2n_1}\right)}_{a_1}\underbrace{\left(x^{2f(m_2)+2n_2}\right)}_{a_2}\cdots\underbrace{\left(x^{2f(m_t)+2n_t}\right)}_{a_t}$$

$$Pr[R] = \underbrace{\left(\frac{x^{4f(m_1)}+x^{4n_1}}{2}\right)}_{r_1}\underbrace{\left(\frac{x^{4f(m_2)}+x^{4n_2}}{2}\right)}_{r_2}\cdots\underbrace{\left(\frac{x^{4f(m_t)}+x^{4n_t}}{2}\right)}_{r_t}$$

LOG

$$\texttt{LOG} = \{010^{2^1}10^{2^2}10^{2^3}\cdots 0^{2^{m-1}}10^{2^m} \mid m > 0\}$$

$$0^{2^0}10^{m_1}10^{m_2}1\ldots 10^{m_t}$$

$$Pr[A] = \underbrace{\left(x^{4m_1+2m_2}\right)}_{a_1}\underbrace{\left(x^{4m_2+2m_3}\right)}_{a_2}\cdots\underbrace{\left(x^{4m_{t-1}+2m_t}\right)}_{a_{t-1}}$$

$$Pr[R] = \underbrace{\left(\frac{x^{8m_1}+x^{4m_2}}{2}\right)}_{r_1}\underbrace{\left(\frac{x^{8m_2}+x^{4m_3}}{2}\right)}_{r_2}\cdots\underbrace{\left(\frac{x^{8m_{t-1}}+x^{4m_t}}{2}\right)}_{r_{t-1}}$$

LOG

Fact. If a binary language L is recognized by a bounded-error PTM in space s(n), then the binary language LOG(L) is recognized by a bounded-error PTM in space log(s(n)), where

$$\mathtt{LOG}(\mathrm{L}) = \{0(1w_1)0^{2^1}(1w_2)0^{2^2}(1w_3)0^{2^3}\cdots 0^{2^{m-1}}(1w_m)0^{2^m} \mid w = w_1\cdots w_m \in L\}$$

LOG

Corollary. If a binary language L is recognized by a bounded-error PostPTM in space s(n), then the binary language LOG(L) is recognized by a bounded-error PostPTM in space log(s(n)).

Corollary. If a binary language L is recognized by a bounded-error PostPCA in space s(n), then the binary language LOG(L) is recognized by a bounded-error PostPCA in space log(s(n)).

UPOWER

$$\texttt{UPOWER} = \{0^{2^m} \mid m > 0\}$$

The expected certificate for the member is:

$$\underbrace{0^{2^{m-1}-1}1}_{1st\ block}\ \underbrace{0^{2^{m-2}-1}1}_{2nd\ block} \cdots 1\ \underbrace{0001}_{\cdots}\ \underbrace{01}_{\cdots}\ \underbrace{1}_{m\text{-}th\ block}\ \$\$^*$$

Verification with perfect completeness.

UPOWERk

$$\mathtt{UPOWERk} = \{0^{2^{km}} \mid m > 0\}$$

Verification with perfect completeness.

USQUARE

$$\texttt{USQUARE} = \{0^{m^2} \mid m > 0\}$$

The expected certificate for the member is:

$$a^{m_1} b^{m_2} a^{m_3} \cdots d^{m_t} \$\$^*$$

checks:

$$m_1 = m_2 = \cdots = m_t = t + 1$$

$$|w| = m_1 + m_2 + \cdots + m_t + (t + 1)$$

Verification with perfect completeness.

Lemma for 64^k coin flips

- Let $x = x_1x_2x_3 \ldots$ be an infinite binary sequence. If a biased coin lands on head with probability $p = 0.x_101x_201x_301\ldots$, then the value x_k can be determined with probability $\frac{3}{4}$ after 64^k coin tosses.

Sweeping PCAs

Fact. Bounded-error linear-space sweeping PCAs can recognize uncountably many languages in subquadratic time.

$$\mathtt{LOG(L)} = \{0(1w_1)0^{2^1}(1w_2)0^{2^2}(1w_3)0^{2^3}\cdots 0^{2^{m-1}}(1w_m)0^{2^m} \mid w = w_1\cdots w_m \in L\}$$

Corollary. The cardinality of languages recognized by bounded-error sweeping PCAs with arbitrary small non-constant space bound is uncountably many.

DIMA3

$$\mathtt{DIMA3} = \{0^{2^0}10^{2^1}10^{2^2}1\cdots10^{2^{6k-2}}110^{2^{6k-1}}11^{2^{6k}}(0^{2^{3k}-1}1)^{2^{3k}} \mid k > 0\}$$

Recognition with bounded-error linear-space PostPCA.

DIMA3(I)

$$\mathtt{DIMA3} = \{0^{2^0}10^{2^1}10^{2^2}1\cdots10^{2^{6k-2}}110^{2^{6k-1}}11^{2^{6k}}(0^{2^{3k}-1}1)^{2^{3k}} \mid k>0\}$$

$$\mathcal{I} = \{I \mid I \subseteq \mathbb{Z}^+\}$$

Let w_k be the k-th shortest member of DIMA3 for k>0.

$$\mathtt{DIMA3}(I) = \{w_k \mid k>0 \text{ and } k \in I\}$$

Recognition with bounded-error linear-space PostPCA for any I.

Corollary

Bounded-error linear-space PostPCA can recognize DIMA3(l) for any l.

If a binary language L is recognized by a bounded-error PostPCA in space s(n), then the binary language LOG(L) is recognized by a bounded-error PostPCA in space log(s(n)).

Corollary. The cardinality of languages recognized by bounded-error PostPCAs with arbitrary small non-constant space bound is uncountably many.

UPOWER6(I)

$$\texttt{UPOWER6}(I) = \{0^n \mid n = 2^{6k}, k > 0 \text{ and } k \in I\}$$

$$\mathcal{I} = \{I \mid I \subseteq \mathbb{Z}^+\}$$

$$c_w = \begin{array}{|c|c|c|c|c|c}
\hline
c'_w[1] & c'_w[2] & c'_w[3] & \cdots & c'_w[j] & \cdots \\
\hline
c''_w[1] & c''_w[2] & c''_w[3] & \cdots & c''_w[j] & \cdots \\
\hline
\end{array}$$

- c’ used for UPOWER6,
- c’’ used for USQUARE.

Results

- If a binary language L is recognized by a bounded-error realtime PostPTM/PostPCA in space s(n), then the binary language LOG(L) is recognized by a bounded-error realtime PostPTM/PostPCA in space log(s(n)).
- Realtime PostPFAs verify UPOWERk, USQUARE with perfect completeness.

Results

- The cardinality of languages recognized by bounded-error realtime PostPCAs with arbitrary small non-constant space bound is uncountably many.
- Bounded-error unary realtime PostPFAs can verify uncountably many languages.

Open question

- Bounded-error 2PFAs can recognize non-context-free languages.
- Bounded-error realtime PostPFAs can define uncountably many languages with the help of a prover/arbitrarily small counter (with a prover even in unary case).

Thank you for your attention!
Ďakujem!