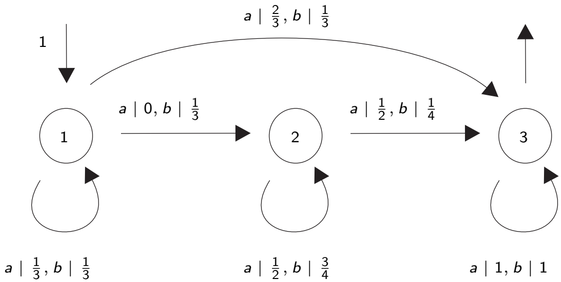
From Quantum Automata to Quaternions and Rational Pairing Functions

Paul Bell (p.c.bell@keele.ac.uk) [1]
Mika Hirvensalo (mikhirve@utu.fi) [2]

[1]School of Mathematics and Computer Science, Keele University
[2]Department of Mathematics and Statistics, University of Turku

WORReLL'23
Paderborn

Probabilistic automata (Rabin 1963)



$$M_a = \begin{pmatrix} \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ \frac{2}{3} & \frac{1}{2} & 1 \end{pmatrix}, M_b = \begin{pmatrix} \frac{1}{3} & 0 & 0 \\ \frac{1}{3} & \frac{3}{4} & 0 \\ \frac{1}{3} & \frac{1}{4} & 1 \end{pmatrix}$$

Probabilistic automata

Definition

An n-state probabilistic automaton over Σ is a triplet

$$P = (\boldsymbol{y}, \{M_a \mid a \in \Sigma\}, \boldsymbol{x}),$$

where

- $\boldsymbol{x}$ is an initial stochastic (column) vector,
- $\boldsymbol{y} \in \{0, 1\}^n$ is the final (row) vector,
- each $M_a \in \mathbb{R}^{n \times n}$ is a stochastic matrix

Definition

The probability P associates to $w = a_1 \dots a_n \in \Sigma^*$ is given by

$$\mathbb{P}_P(w) = \boldsymbol{y} M_{a_n} \dots M_{a_1} \boldsymbol{x}.$$

Cut-point languages

Definition

For a stochastic automaton P and $\lambda \in [0,1]$ let

$$L_{\geq}(P,\lambda) = \{w \in \Sigma^* \mid \mathbb{P}_P(w) \geq \lambda\}$$

be a cut-point language and

$$L_{>}(P,\lambda) = \{w \in \Sigma^* \mid \mathbb{P}_P(w) > \lambda\}$$

a *strict* cut-point language.

Cut-point languages

Known properties

- Can define any regular language.
- Not necessary regular: $\{a^n b^n \mid n \in \mathbb{N}\}$ is a (strict) cut-point language (Turakainen 1969)
- If cutpoint is *isolated*, meaning that $(\exists \epsilon > 0)(\forall w)(\mathbb{P}_P(w) \notin (\lambda - \epsilon, \lambda + \epsilon))$ then regular (Rabin 1963)
- In the isolated case, at most exponential advantage over DFA size (Rabin 1963)

Measure-Once Quantum Automata (1997)

Definition

An n-state MO-QFA, aka Moore-Crutchfield QFA over Σ is a triplet

$$\mathcal{Q} = (P, \{U_a \mid a \in \Sigma\}, \boldsymbol{x}),$$

- Where $\boldsymbol{x} \in \mathbb{C}^n$ is the *initial vector* with the property $||\boldsymbol{x}|| = 1$,
- $P : \mathbb{C}^n \to \mathbb{C}^n$ is a projection,
- each $U_a \in \mathbb{C}^{n \times n}$ is a unitary matrix. $(U^*U = UU^* = I)$

Definition

The probability $\mathcal{Q}$ associates to $w = a_1 \dots a_n \in \Sigma^*$ is given by

$$\mathbb{P}_{\mathcal{Q}}(w) = ||PU_{a_n} \dots U_{a_1}\boldsymbol{x}||^2,$$

where $||\boldsymbol{x}||$ is the usual L_2-norm of $\boldsymbol{x}$.

Cut-point languages (MO-QFA)

Known properties

- For non-isolated cutpoint, simple examples of non-regular languages such as $\{w \mid |w|_a = |w|_b\}$.
- If cutpoint is isolated, then regular (Ablayev & al. 2000)
- But then only group languages can be recognized (Brodsky & Pippenger 2002)
- Example: Cannot recognize $\{a, b\}^* a$.

Decidability questions

Classical vs. Quantum

	$L_{\geq}(A, \lambda) = \emptyset$	$L_{>}(A, \lambda) = \emptyset$
PFA	Undecidable	Undecidable
QFA	Undecidable	Decidable

(Blondel & al. (binary alphabet, 47 states) 2003, Hirvensalo (25 & 21 states) 2007. Decidability assumes matrix entries from $\mathbb{Q}[i]$)

Injectivity problem for MO-QFA

Definition

Given a MO-QFA $\mathcal{Q}$, if the acceptance function of $\mathcal{Q}$ is injective, then we call $\mathcal{Q}$ injective.

Main Theorem (The injectivity problem)

Given a MO-QFA $\mathcal{Q}$, it is undecidable whether $\mathcal{Q}$ is injective.

Post Correspondence Problem

PCP

Given a collection of word pairs $(u_1, v_1), \ldots, (u_n, v_n)$ over an alphabet Δ, decide if there exists a nonempty index sequence $i_1 \ldots i_k$ so that

$$u_{i_1} u_{i_2} \ldots u_{i_k} = v_{i_1} v_{i_2} \ldots v_{i_k}?$$

Alternative formulation

Denote $w = i_1 i_2 \ldots i_k \in \Sigma^*$, where $\Sigma = \{1, 2, \ldots, n\}$ and define morphisms $h, g : \Sigma^* \to \Delta^*$ by $h(i_j) = u_{i_j}$, and $g(i_j) = v_{i_j}$. Does there exist a $w \in \Sigma^+$ so that

$$h(w) = g(w)?$$

https://webdocs.cs.ualberta.ca/~games/PCP/list.htm

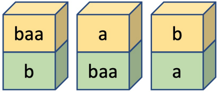


Figure: An easy case? (3 pairs)

Mixed Post Correspondence Problem

Mixed PCP

Given two morphisms $h, g : \Sigma^* \to \Delta^*$, decide if there exists a word $w = w_1 \dots w_n \in \Delta^+$ so that

$$h_1(w_1) \dots h_n(w_n) = g_1(w_1) \dots g_n(w_n),$$

where $h_i, g_i \in \{h, g\}$ and at least one $h_j \neq g_j$.

Theorem: Mixed PCP is undecidable

Injectivity problem for MO-QFA

Unitary embedding

- Let U_a and U_b be unitary matrices generating a free group. Then there is an embedding $w \to U_w$ from alphabet $\{a, b\}$ into the group $\langle U_a, U_b \rangle$.
- Let $h, g : \Sigma \to \{a, b\}^*$ be morphisms of a mixed PCP instance. Let also $e : \Sigma \to \{a, b\}^*$ be an embedding.
- For each $\sigma \in \Sigma$ define two unitary matrices $X_\sigma^h = U_{e(\sigma)} \oplus U_{h(\sigma)}$ and $X_\sigma^g = U_{e(\sigma)} \oplus U_{g(\sigma)}$, and let X be the union of those matrices.
- Define a QFA with matrices X and input alphabet $\Sigma \times \{g, h\}$.
- For an input word $w = (\sigma_1, f_1) \ldots (\sigma_n, f_n) = (u, v)$ we have $X_w = (U_{e(\sigma_1)} \oplus U_{f_1(\sigma_1)}) \ldots (U_{e(\sigma_n)} \oplus U_{f_n(\sigma_n)}) = U_{e(u)} \oplus U_{f_v(u)}$, where $f_v(u) = f_1(\sigma_1) \ldots f_n(\sigma_n)$. Hence
- $X_{w_1} = X_{w_2} \iff U_{e(u_1)} \oplus U_{f_{v_1}(u_1)} = U_{e(u_2)} \oplus U_{f_{v_2}(u_2)} \iff u_1 = u_2 = u$ and $f_{v_1}(u) = f_{v_2}(u)$.

Injectivity problem for MO-QFA

Notice that:

- Mixed PCP has a solution iff there are words $w_1 \neq w_2$ so that $X_{w_1} = X_{w_2}$
- The construction requires unitary embedding $w \to U_w$, $X_\sigma^f = U_{e(\sigma)} \oplus U_{f(\sigma)}$
- However, the mapping $X_w \to ||PX_w\mathbf{x}||^2$ may not be injective, meaning that the acceptance probability does not uniquely determine X_w.

Embedding to Binary Alphabet

Embedding of γ_1

Let $\Sigma_n = \{a_1, \ldots, a_n\}$ and $\Sigma_2 = \{a, b\}$. Then $\gamma_1 : \Sigma_n \to \Sigma_2^*$ is an embedding where $\gamma_1(a_k) = a^k b$

Extension

- Can be extended to $\gamma_1 : \Sigma_n^* \to \Sigma_2^*$ by $\gamma_1(w_1 w_2 \cdots w_k) = \gamma_1(w_1)\gamma_1(w_2 \cdots w_k)$.

Embedding to Quaternions

Embedding of γ_2

Let $\Sigma_2 = \{a, b\}$ and define $\gamma_2 : \Sigma_2 \to \mathbb{H}(\mathbb{Q})$ by $\gamma_2(a) = (\frac{3}{5}, \frac{4}{5}\mathbf{i}, 0, 0)$ and $\gamma_2(b) = (\frac{3}{5}, 0, \frac{4}{5}\mathbf{j}, 0)$ with $\gamma_2(\varepsilon) = I_4$. Note that $\{\gamma_2(a), \gamma_2(b)\}$ represent rotations about perpendicular axes by a rational angle

Theorem (Swierczkowski)

- If $\cos(\theta) \in \mathbb{Q}$ then the subgroup of $SO_3(\mathbb{R})$ generated by rotations of angle θ about two perpendicular axes is free iff $\cos(\theta) \neq 0, \pm\frac{1}{2}, \pm 1$.

Proposition

Thus $\langle \gamma_2(a), \gamma_2(b) \rangle$ is freely generated and γ_2 is an injective homomorphism

Embedding to Unitary Matrices

Embedding of $\gamma_3 : \mathbb{H}(\mathbb{Q}) \to \mathbb{Q}^{4\times 4}$

$$\gamma_3(\gamma_2(a)) = U_a = \frac{1}{5}\begin{pmatrix} 3 & 4 & 0 & 0 \\ -4 & 3 & 0 & 0 \\ 0 & 0 & 3 & 4 \\ 0 & 0 & -4 & 3 \end{pmatrix}, \quad \gamma_3(\gamma_2(b)) = U_b = \frac{1}{5}\begin{pmatrix} 3 & 0 & 4 & 0 \\ 0 & 3 & 0 & -4 \\ -4 & 0 & 3 & 0 \\ 0 & 4 & 0 & 3 \end{pmatrix}$$

Denote $U_w = U_{w_1} \dots U_{w_n}$ and $R_1(U_w) = (\left|(U_w)_{11}\right|, \left|(U_w)_{12}\right|, \left|(U_w)_{13}\right|)$.

Theorem

- U_a and U_b generate a free group.
- If $R_1(U_u) = R_1(U_v)$, then $u = v$.
- Requires analysis of quaternion structure for $\gamma_2(a)$ and $\gamma_2(b)$.

Our injective homomorhism γ

Final embedding

By the previous observations $\gamma : \Sigma_k^* \to \mathbb{Q}^{4\times 4}$ is an injective homomorphism, where $\gamma(w) = \gamma_3(\gamma_2(\gamma_1(w)))$

Injectivity problem for MO-QFA

Observation

- Matrix $X_u^{f_v} = U_{e(u)} \oplus U_{f_v(u)}$ is fully determined by $R_1(U_{e(u)})$ and $R_1(U_{f(u)})$.
- Mixed PCP has a solution iff there is $(u_1, v_1) = w_1 \neq w_2 = (u_2, v_2)$ so that $R_1(U_{e(u_1)}) = R_1(U_{e(u_2)})$ (which implies $u_1 = u_2 = u$) and $R_1(U_{f_{v_1}(u)}) = R_1(U_{f_{v_2}(u)})$
- Mixed PCP has a solution iff there is $(u_1, v_1) = w_1 \neq w_2 = (u_2, v_2)$ so that

$$\begin{aligned} & (|X_{w_1}|_{11}, |X_{w_1}|_{12}, |X_{w_1}|_{13}, |X_{w_1}|_{55}, |X_{w_1}|_{56}, |X_{w_1}|_{57}) \\ = \; & (|X_{w_2}|_{11}, |X_{w_2}|_{12}, |X_{w_2}|_{13}, |X_{w_2}|_{55}, |X_{w_2}|_{56}, |X_{w_2}|_{57}) \end{aligned}$$

Tools

Lemma

a) There exist MO-QFA Q_0 and Q_1 so that $\mathbb{P}_{Q_0}(w) = 0$ and $\mathbb{P}_{Q_1}(w) = 1$ for each $w \in \Sigma^*$.

b) Given two MO-QFA's Q_1 and Q_2, complex numbers α and β so that $|\alpha|^2 + |\beta|^2 = 1$, there exists

  b.1) A MO-QFA Q so that $\mathbb{P}_Q(w) = \mathbb{P}_{Q_1}(w)\mathbb{P}_{Q_2}(w)$

  b.2) A MO-QFA Q so that $\mathbb{P}_Q(w) = |\alpha|^2 \mathbb{P}_{Q_1}(w) + |\beta|^2 \mathbb{P}_{Q_2}(w)$

Proof

a) Trivial b.1) Tensor product construction b.2) Direct sum construction

Observation

If $P = \text{diag}(0, \ldots, 1, \ldots, 0)$ (jth position) and $\boldsymbol{x} = (0, \ldots, 1, \ldots, 0)$ (ith position), then

$$||PU\boldsymbol{x}||^2 = |U_{ij}|^2 .$$

Reduction to Mixed PCP

- According to a previous observation, there is a MO-QFA which, on input $w = (u, v)$, produces output (acceptance probability) $|(X_w)_{ij}|^2 = \left|(U_{e(u)} \oplus U_{f_v(u)})_{ij}\right|^2$
- From the construction tools, it follows that there exists a MO-QFA producing output (acceptance probability)

$$|\lambda_1|^2 |(X_w)_{11}|^2 + |\lambda_2|^2 |(X_w)_{12}|^2 + |\lambda_3|^2 |(X_w)_{13}|^2 + |\kappa_1|^2 |(X_w)_{55}|^2 + |\kappa_2|^2 |(X_w)_{56}|^2 + |\kappa_3|^2 |(X_w)_{57}|^2 , \quad (1)$$

  where $\lambda_1, \lambda_2, \lambda_3, \kappa_1, \kappa_2, \kappa_3$ are complex numbers satisfying $|\lambda_1|^2 + |\lambda_2|^2 + |\lambda_3|^2 + |\kappa_1|^2 + |\kappa_2|^2 + |\kappa_3|^2 = 1$
- Mixed PCP has a solution if and only if the same acceptance probability (1) can be obtained for at least two words $w_1 \neq w_2$ (Meaning that the automaton is ambiguous or not injective)

Undecidability

Conclusion

- For the final conclusion, we have to be sure that mapping

$$
\begin{aligned}
& (|X_{11}|, |X_{12}|, |X_{13}|, |X_{55}|, |X_{56}|, |X_{57}|) \\
\rightarrow \quad & |\lambda_1|^2 |X_{11}|^2 + |\lambda_2|^2 |X_{12}|^2 + |\lambda_3|^2 |X_{13}|^2 \\
+ \quad & |\kappa_1|^2 |X_{55}|^2 + |\kappa_2|^2 |X_{56}|^2 + |\kappa_3|^2 |X_{57}|^2
\end{aligned}
$$

  is injective.
- If now $|\lambda_1|^2, \ldots, |\kappa_1|^2, \ldots,$ (can be introduced in the initial vector by construction) are linearly independent over $\mathbb{Q}$, we can conclude that the matrix elements $|X_{11}|^2, \ldots$ uniquely determines the probability.

Undecidability

Forcing linear independence

- Theorem: If n_i are coprime integers, then $\sqrt{n_i}$ are linearly independent over $\mathbb{Q}$.
- We can then choose $\lambda_1 = \sqrt[4]{n_1}, \ldots$ and a renormalizaton factor to introduce linear independence and the case is closed. QED
- Is this an elegant solution for linear independence? Depends on the judge / no
- Any better? Only using rational numbers?

Solution using only rationals?

Observation

- Given a multivariate polynomial $f \in \mathbb{N}_0[x_1, \ldots, x_6]$, the construction tools and some other tricks give a $\lambda \in \mathbb{Q}_+$ and a QFA Q so that

$$\mathbb{P}_Q(w) = \lambda f(|X_{11}|^2, |X_{12}|^2, |X_{13}|^2, |X_{55}|^2, |X_{56}|^2, |X_{57}|^2).$$

- Does there exist a multivariate polynomial $f \in \mathbb{N}_0[x_1, \ldots, x_6]$ which is injective on rational numbers?

Finding injections

Problems

- Does there exist a multivariate polynomial $f \in \mathbb{N}_0[x_1, \ldots, x_n]$ so that $f : \mathbb{Q}^n \to \mathbb{Q}$ is an injection?
- Does there exist a multivariate polynomial $f \in \mathbb{N}_0[x_1, \ldots, x_n]$ so that $f : \mathbb{Q}^n_{\geq 0} \to \mathbb{Q}_{\geq 0}$ is an injection?
- Does there exist a bivariate polynomial $f_2 \in \mathbb{N}_0[x, y]$ so that $f_2 : \mathbb{Q}_{\geq 0} \times \mathbb{Q}_{\geq 0} \to \mathbb{Q}_{\geq 0}$ is an injection?
  - If we have an injection f_2 for $n = 2$ then it can be extended:

$$f_3(x, y, z) = f_2(x, f_2(y, z)), \quad f_4(x, y, z, w) = f_2(x, f_2(y, f_2(z, w))), \quad \text{etc.}$$

- Does there exist a bivariate polynomial $f \in \mathbb{N}_0[x, y]$ so that $f : \Lambda \times \Lambda \to \Lambda$ is an injection? Here $\Lambda = \{\frac{a}{5^k} \mid k \in \mathbb{N}, a \in \mathbb{N}_0, 0 \leq a \leq 5^k\}$.

Finding injections

Theorem (Cantor pairing)

$$C : \mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0, C(x, y) = \frac{1}{2}(x + y + 1)(x + y) + x$$

is a bijection. $C(0, 0) = 0$, $C(0, 1) = 1$, $C(1, 0) = 2$, $C(0, 2) = 3$, $C(1, 1) = 4$, $\ldots$.

Remark

- No degree 2 polynomial bijections exist other than $C(x, y)$ and $C(y, x)$ (Fueter & Pólya, 1923; Vsemirnov, 2001)
- No degree > 2 polynomial bijection $\mathbb{N}_0 \times \mathbb{N}_0 \to \mathbb{N}_0$ exists (P.W. Adriaans 2018)

Finding injections

Observation

$$C\left(\frac{2}{25}, \frac{11}{25}\right) = \frac{297}{625} = C\left(\frac{3}{25}, \frac{9}{25}\right).$$

More genererally, if $2a + b = 2c + d$ and $e = a + b + c + d$, then

$$C\left(\frac{a}{e}, \frac{b}{e}\right) = C\left(\frac{c}{e}, \frac{d}{e}\right).$$

Finding injections

G. Cornelissen 1999:

- Question (Harvey Friedman): Does there exist a polynomial injection $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$?
- Reply (Don Zagier): Sure, almost all complex enough polynomials will do, for example $x^7 + 3y^7$ is most likely a desired injection.

Finding injections

Theorem (Poonen 2010)

Assume that there is a homogenous polynomial $F(x, y)$ over rationals so that the rational points in the projective surface X defined as $F(x, y) = F(z, w)$ are not Zariski dense in X. Then there exists a polynomial injection $f : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$.

Conjecture (Bombieri-Lang)

If X is a smooth projective irreducible algebraic surface over rationals of general type. Then the set of rational points of X is not Zariski dense in X.

Remark

"General type" in the above definition refers to the Kodaira dimension. It suffices that $F(x, y)$ is separable, homogenous, and of degree at least 5 (Poonen 2010)

Remark (Cornelissen 1999)

From the (generalized) *abc*-conjecture it follows that $f(x, y) = x^n + 3y^n$ defines an injection $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ if (odd) n is large enough.

Rational Pairing Function

Theorem

Let $\Lambda = \left\{ \frac{a}{5^k} | a, k \in \mathbb{N}_0, a < 5^k \right\}$. Then $f : \Lambda \times \Lambda \to 25\Lambda$ is an injection, where:

$$f(x, y) = (x^4 + y^4)^3 + x^4$$

Note

- We can estimate the value $f(x, y)$ as

$$|(x^4 + y^4)^3 + x^4| \leq (1 + 1)^3) + 1 = 9 < 25$$

  thus $f(x, y) \in 25\Lambda$ thus an injection $f' : \Lambda \times \Lambda \to \Lambda$ can be found be introducing.a normalization factor $\frac{1}{25}$
- Injectivity follows from elementary number theory / Fermat's little theorem

QFA without radicals

Unique matrix products

As before we can use our monomorphism $\gamma : \Sigma^* \to \mathbb{Q}^{4\times 4}$ so that it is undecidable to determine if there exists a matrix in the following semigroup with two different factorizations:

$$\Gamma = \langle \{\gamma(x_j) \oplus \gamma(h(x_j)), \gamma(x_j) \oplus \gamma(g(x_j)) | 1 \leq j \leq |\Sigma|\} \rangle \subseteq \mathbb{Q}^{8\times 8}$$

Unique encoding of matrix

As before, each element of Γ is uniquely determined by six elements:

$$|X_{1,1}|, |X_{1,2}|, |X_{1,3}|, |X_{5,5}|, |X_{5,6}|, |X_{5,7}|$$

and thus by

$$\mathbf{x} = (X_{1,1}^2, X_{1,2}^2, X_{1,3}^2, X_{5,5}^2, X_{5,6}^2, X_{5,7}^2)$$

Embedding to QFA without radicals

Encoding the polynomial

As before, let $f_2(x,y) = (x^4+y^4)^3 + x^4$ and then define:

$$f_6(x_1,\dots,x_6) = f_2(x_1, f_2(x_2, f_2(x_3, f_2(x_4, f_2(x_5, x_6)))))$$

of degree $d = 12^5$

Proof Idea

Thus, $f_6(\mathbf{x}) = f_6(X_{1,1}^2, X_{1,2}^2, X_{1,3}^2, X_{5,5}^2, X_{5,6}^2, X_{5,7}^2)$ uniquely determines X

Embedding to QFA without radicals

Encoding to matrices

$$f_6(\mathbf{x}) = \sum_{i=1}^{d} T_i(\mathbf{x}) = \sum_{i=1}^{d}\sum_{j=1}^{t(i)} T_{i,j}(\mathbf{x}) = \sum_{i=1}^{d}\sum_{j=1}^{t(i)} c_{i,j} R_{i,j}(\mathbf{x}) \quad c_{i,j} \in \mathbb{N}$$

$$= \sum_{i=1}^{d}\sum_{j=1}^{t(i)} c_{i,j} \prod_{m=1}^{i} a_{i,j,m} \quad a_{i,j,m} \in \{|X_{1,1}|, |X_{1,2}|, |X_{1,3}|, |X_{5,5}|, |X_{5,6}|, |X_{5,7}|\}$$

$$= \sum_{i=1}^{d}\sum_{j=1}^{t(i)} \sum_{k=1}^{4} d_{i,j,k}^2 \prod_{m=1}^{i} a_{i,j,m} \quad \text{Lagrange's Theorem}$$

Embedding to Matrices

Embedding

Let us consider a particular term $c_{i,j}R_{i,j}$, of degree $i \leq \deg(f_6) = 12^5$. Note that there exists $1 \leq s, r \leq 8^i$ such that $X^{\otimes i}_{s,r} = R_{i,j}(\mathbf{x})$

Theorem

- Define $u'_{i,j,k} = d_{i,j,k} \cdot e_r \in \mathbb{Q}^{8^i}$ and $P'_{i,j} = e_s e_s^T \in \mathbb{Q}^{8^i \times 8^i}$ and then:

$$P'_{i,j} X^{\otimes i} u'_{i,j,k} = d_{i,j,k} R_{i,j}(\mathbf{x})$$

Encoding the rational pairing function

Embedding

Finally then define $P_{i,j} = \oplus_{k=1}^{4} P'_{i,j}$, $u_{i,j} = \oplus_{k=1}^{4} u'_{i,j,k}$ and $\zeta_{i,j} = \oplus_{k=1}^{4} X^{\otimes i}$

Valuation

$$\begin{aligned}
||P_{i,j}\zeta_{i,j}(X)u||^2 &= \left|\left|\bigoplus_{k=1}^{4} P'_{i,j}\zeta'_{i,j}(X)d_{i,j,k}u'\right|\right|^2 \\
&= \left(\sqrt{\sum_{k=1}^{4} d_{i,j,k}^2 R_{i,j}(\mathbf{x})^2}\right)^2 = \sum_{k=1}^{4} d_{i,j,k}^2 R_{i,j}(\mathbf{x})^2 = c_{i,j}R_{i,j}(\mathbf{x^2})
\end{aligned}$$

Final thoughts

Final embedding

With some more work we can embed the entire polynomial using tensor products and direct sums

Theorem

The injectivity problem for measure-once quantum finite automata is undecidable for $< 4 * 8^{12^5+5}$ states.

Final thoughts

Open problem

Is the knapsack variant of injectivity undecidable for MO-QFA?

Example

Given $\mathcal{Q} = (P, \{U_1, \dots U_\ell\}, \boldsymbol{x})$, does there exist distinct $k_1, \dots, k_\ell, k'_1, \dots, k'_\ell \geq 0$ such that:

$$||PU_1^{k_1} \cdots U_\ell^{k_\ell} \boldsymbol{x}||^2 = ||PU_1^{k'_1} \cdots U_\ell^{k'_\ell} \boldsymbol{x}||^2$$

Temporary page!

LaTeX was unable to guess the total number of pages correctly. As there was some unprocessed data that should have been added to the final page this extra page has been added to receive it.

If you rerun the document (without altering it) this surplus page will go away, becau

LaTeX now knows how many pages to expect for this document.