Quantum Bit Strings and Prefix-Free Subspaces

Markus Müller* & Caroline Rogers†

*Max Planck Institute for Mathematics in the Sciences, Leipzig
†Department of Computer Science, University of Warwick, UK

Las Vegas, July 16, 2008

A set of code words is prefix-free, if no code word is the prefix of another code word.

A set of code words is prefix-free, if no code word is the prefix of another code word.

- Code word=binary string out of $\{0,1\}^* = \{\lambda, 0, 1, 00, \ldots\}$,

A set of code words is prefix-free, if no code word is the prefix of another code word.

- Code word=binary string out of $\{0,1\}^* = \{\lambda, 0, 1, 00, \ldots\}$,
- e.g. 10 is a prefix of 100, 0 is *not* a prefix of 10.

A set of code words is prefix-free, if no code word is the prefix of another code word.

- Code word=binary string out of $\{0,1\}^* = \{\lambda, 0, 1, 00, \ldots\}$,
- e.g. 10 is a prefix of 100, 0 is *not* a prefix of 10.

Prefix-free sets like $\{0, 10, 110, 111\}$ can be concatenated and then uniquely decoded:

$$\text{QUELLE} \quad \xrightarrow{\text{Coding}} \quad 111 \circ 110 \circ 0 \circ 10 \circ 10 \circ 0$$

A set of code words is prefix-free, if no code word is the prefix of another code word.

- Code word=binary string out of $\{0,1\}^* = \{\lambda, 0, 1, 00, \ldots\}$,
- e.g. 10 is a prefix of 100, 0 is *not* a prefix of 10.

Prefix-free sets like $\{0, 10, 110, 111\}$ can be concatenated and then uniquely decoded:

$$\text{QUELLE} \xrightarrow{\text{Coding}} 111 \circ 110 \circ 0 \circ 10 \circ 10 \circ 0$$
$$= 111110010100$$

A set of code words is prefix-free, if no code word is the prefix of another code word.

- Code word=binary string out of $\{0,1\}^* = \{\lambda, 0, 1, 00, \ldots\}$,
- e.g. 10 is a prefix of 100, 0 is *not* a prefix of 10.

Prefix-free sets like $\{0, 10, 110, 111\}$ can be concatenated and then uniquely decoded:

$$\text{QUELLE} \xrightarrow{\text{Coding}} 111 \circ 110 \circ 0 \circ 10 \circ 10 \circ 0$$

$$= 111110010100$$

$$\downarrow$$

$$111, 110, 0, 10, 10, 0$$

A set of code words is prefix-free, if no code word is the prefix of another code word.

- Code word=binary string out of $\{0,1\}^* = \{\lambda, 0, 1, 00, \ldots\}$,
- e.g. 10 is a prefix of 100, 0 is *not* a prefix of 10.

Prefix-free sets like $\{0, 10, 110, 111\}$ can be concatenated and then uniquely decoded:

$$\mathrm{QUELLE} \xrightarrow{\text{Coding}} 111 \circ 110 \circ 0 \circ 10 \circ 10 \circ 0 = 111110010100$$

$$\downarrow$$

$$\mathrm{QUELLE} \xleftarrow{\text{Decoding}} 111, 110, 0, 10, 10, 0$$

A set of code words is prefix-free, if no code word is the prefix of another code word.

- Code word=binary string out of $\{0,1\}^* = \{\lambda, 0, 1, 00, \ldots\}$,
- e.g. 10 is a prefix of 100, 0 is *not* a prefix of 10.

Prefix-free sets like $\{0, 10, 110, 111\}$ can be concatenated and then uniquely decoded:

$$\text{QUELLE} \xrightarrow{\text{Coding}} 111 \circ 110 \circ 0 \circ 10 \circ 10 \circ 0$$
$$= 111110010100$$
$$\downarrow$$
$$\text{QUELLE} \xleftarrow{\text{Decoding}} 111, 110, 0, 10, 10, 0$$

Not prefix-free sets like $\{0, 00\}$: $0 \circ 00 \xleftarrow{?} 000 \xrightarrow{?} 00 \circ 0$

Theorem (Kraft Inequality)

There exists a prefix code $\{c_1, \ldots, c_n\}$ *with code word lengths* $\{l_1, \ldots, l_n\} = \{\ell(c_1), \ldots, \ell(c_n)\} \subset \mathbb{N}_0$, *if and only if*

$$\sum_{i=1}^{n} 2^{-l_i} \leq 1.$$

Theorem (Kraft Inequality)

There exists a prefix code $\{c_1, \ldots, c_n\}$ *with code word lengths* $\{l_1, \ldots, l_n\} = \{\ell(c_1), \ldots, \ell(c_n)\} \subset \mathbb{N}_0$, *if and only if*

$$\sum_{i=1}^{n} 2^{-l_i} \leq 1.$$

- Extremely useful for deciding if certain codes exist.

Theorem (Kraft Inequality)

There exists a prefix code $\{c_1, \ldots, c_n\}$ *with code word lengths* $\{l_1, \ldots, l_n\} = \{\ell(c_1), \ldots, \ell(c_n)\} \subset \mathbb{N}_0$, *if and only if*

$$\sum_{i=1}^{n} 2^{-l_i} \leq 1.$$

- Extremely useful for deciding if certain codes exist.

Theorem (Kraft Inequality)

There exists a prefix code $\{c_1, \ldots, c_n\}$ *with code word lengths* $\{l_1, \ldots, l_n\} = \{\ell(c_1), \ldots, \ell(c_n)\} \subset \mathbb{N}_0$, *if and only if*

$$\sum_{i=1}^{n} 2^{-l_i} \leq 1.$$

- Extremely useful for deciding if certain codes exist.

Algorithmic Probability: If $U : \{0,1\}^* \to \{0,1\}^*$ is a universal prefix computer, then

$$P_U(s) := \sum_{x \in \{0,1\}^* : U(x) = s} 2^{-\ell(x)}$$

Theorem (Kraft Inequality)

There exists a prefix code $\{c_1, \ldots, c_n\}$ *with code word lengths* $\{l_1, \ldots, l_n\} = \{\ell(c_1), \ldots, \ell(c_n)\} \subset \mathbb{N}_0$, *if and only if*

$$\sum_{i=1}^{n} 2^{-l_i} \leq 1.$$

- Extremely useful for deciding if certain codes exist.

Algorithmic Probability: If $U : \{0,1\}^* \to \{0,1\}^*$ is a universal prefix computer, then

$$\begin{aligned} P_U(s) &:= \sum_{x \in \{0,1\}^* : U(x) = s} 2^{-\ell(x)} \\ \Omega_U &:= \sum_{s \in \{0,1\}^*} P_U(s) \leq 1. \end{aligned}$$

Quantum Bit Strings

Aim: Explain the notions of prefix und concatenation for qubit strings like $|\psi\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |111\rangle)$.

Quantum Bit Strings

Aim: Explain the notions of prefix und concatenation for qubit strings like $|\psi\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |111\rangle)$.

- Qubit Strings live on string space $\mathcal{H}_{\{0,1\}^*} := \bigoplus_{n=0}^{\infty} \left(\mathbb{C}^2\right)^{\otimes n}$.

Quantum Bit Strings

Aim: Explain the notions of prefix und concatenation for qubit strings like $|\psi\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle + |111\rangle\right)$.

- Qubit Strings live on string space $\mathcal{H}_{\{0,1\}^*} := \bigoplus_{n=0}^{\infty}\left(\mathbb{C}^2\right)^{\otimes n}$.
- Two notions of "length" for qubit strings $\rho = |\psi\rangle\langle\psi|$:

Quantum Bit Strings

Aim: Explain the notions of prefix und concatenation for qubit strings like $|\psi\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |111\rangle)$.

- Qubit Strings live on string space $\mathcal{H}_{\{0,1\}^*} := \bigoplus_{n=0}^{\infty} \left(\mathbb{C}^2\right)^{\otimes n}$.
- Two notions of "length" for qubit strings $\rho = |\psi\rangle\langle\psi|$:
  - Base Length: $\ell(\rho) := \max\{\ell(s) \mid \langle s|\rho|s\rangle > 0, \;\; s \in \{0,1\}^*\}$.

Quantum Bit Strings

Aim: Explain the notions of prefix und concatenation for qubit strings like $|\psi\rangle := \frac{1}{\sqrt{2}}\left(|0\rangle + |111\rangle\right)$.

- Qubit Strings live on string space $\mathcal{H}_{\{0,1\}^*} := \bigoplus_{n=0}^{\infty} \left(\mathbb{C}^2\right)^{\otimes n}$.
- Two notions of “length” for qubit strings $\rho = |\psi\rangle\langle\psi|$:
  - Base Length: $\underline{\ell}(\rho) := \max\{\ell(s) \mid \langle s|\rho|s\rangle > 0, \ \ s \in \{0,1\}^*\}$.
  - Average Length: $\overline{\ell}(\rho) := \mathrm{Tr}\left(\Lambda\rho\right)$, where Λ is the length operator: $\Lambda|s\rangle := \ell(s)|s\rangle$ for every $s \in \{0,1\}^*$.

Quantum Bit Strings

Aim: Explain the notions of prefix und concatenation for qubit strings like $|\psi\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |111\rangle)$.

- Qubit Strings live on string space $\mathcal{H}_{\{0,1\}^*} := \bigoplus_{n=0}^{\infty} \left(\mathbb{C}^2\right)^{\otimes n}$.
- Two notions of "length" for qubit strings $\rho = |\psi\rangle\langle\psi|$:
  - Base Length: $\ell(\rho) := \max\{\ell(s) \mid \langle s|\rho|s\rangle > 0, \ \ s \in \{0,1\}^*\}$.
  - Average Length: $\bar{\ell}(\rho) := \mathrm{Tr}(\Lambda\rho)$, where Λ is the length operator: $\Lambda|s\rangle := \ell(s)|s\rangle$ for every $s \in \{0,1\}^*$.

In this case e.g. $\ell(|\psi\rangle) = 3$ and $\bar{\ell}(|\psi\rangle) = 2$.

Quantum Bit Strings

Aim: Explain the notions of prefix und concatenation for qubit strings like $|\psi\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |111\rangle)$.

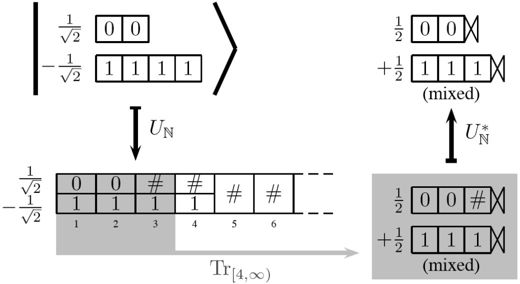
- Qubit Strings live on string space $\mathcal{H}_{\{0,1\}^*} := \bigoplus_{n=0}^{\infty} \left(\mathbb{C}^2\right)^{\otimes n}$.
- Two notions of "length" for qubit strings $\rho = |\psi\rangle\langle\psi|$:
  - Base Length: $\ell(\rho) := \max\{\ell(s) \mid \langle s|\rho|s\rangle > 0, \;\; s \in \{0,1\}^*\}$.
  - Average Length: $\bar{\ell}(\rho) := \mathrm{Tr}\,(\Lambda\rho)$, where Λ is the length operator: $\Lambda|s\rangle := \ell(s)|s\rangle$ for every $s \in \{0,1\}^*$.

  In this case e.g. $\ell(|\psi\rangle) = 3$ and $\bar{\ell}(|\psi\rangle) = 2$.
- Restrictions or prefixes ψ_1^2 (:=the first two qubits of $|\psi\rangle$) should be given by partial trace:

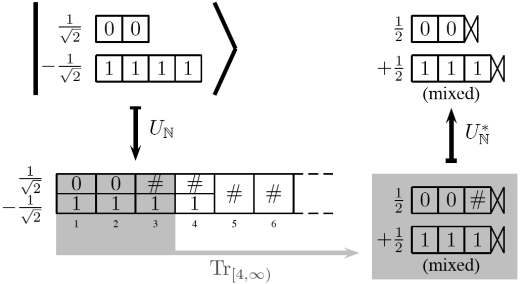
$$\psi_1^2 = \mathrm{Tr}_{[3,\infty)}|\psi\rangle\langle\psi| \qquad \text{Tensor product structure??}$$

Solution: Embed the qubit strings ρ into the Hilbert space of the tape of a quantum Turing machine:

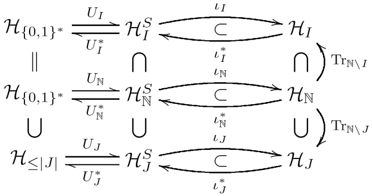
Solution: Embed the qubit strings ρ into the Hilbert space of the tape of a quantum Turing machine:



Solution: Embed the qubit strings ρ into the Hilbert space of the tape of a quantum Turing machine:

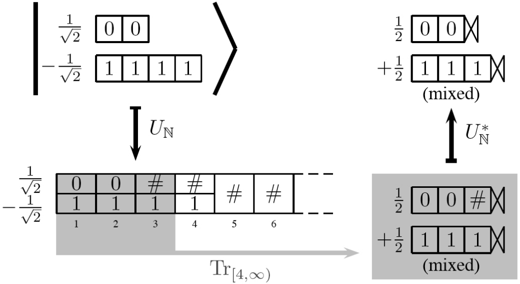


Draft of the formal definition:

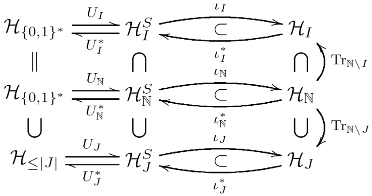


($J \subset \mathbb{N}$ finite, $I \subset \mathbb{N}$ infinite)

Solution: Embed the qubit strings ρ into the Hilbert space of the tape of a quantum Turing machine:



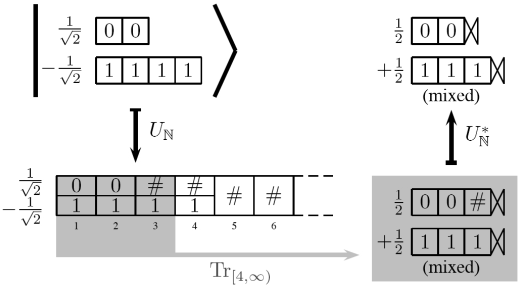
Draft of the formal definition:



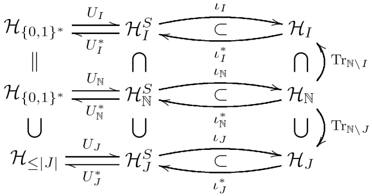
($J \subset \mathbb{N}$ finite, $I \subset \mathbb{N}$ infinite)

- $\rho_I :=$ Restriction of ρ to the qubits indexed by $i \in I$.

Solution: Embed the qubit strings ρ into the Hilbert space of the tape of a quantum Turing machine:



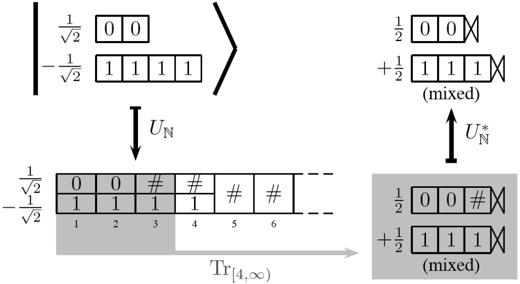
Draft of the formal definition:



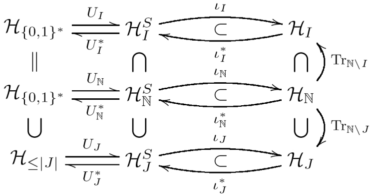
($J \subset \mathbb{N}$ finite, $I \subset \mathbb{N}$ infinite)

- ρ_I :=Restriction of ρ to the qubits indexed by $i \in I$.
- Formal definition: $\rho_I := U_I^* \iota_I^* \mathrm{Tr}_{\mathbb{N}\setminus I}\left(\iota_{\mathbb{N}} U_{\mathbb{N}} \rho U_{\mathbb{N}}^* \iota_{\mathbb{N}}^*\right) \iota_I U_I$.

Solution: Embed the qubit strings ρ into the Hilbert space of the tape of a quantum Turing machine:



Draft of the formal definition:



($J \subset \mathbb{N}$ finite, $I \subset \mathbb{N}$ infinite)

- ρ_I :=Restriction of ρ to the qubits indexed by $i \in I$.
- Formal definition: $\rho_I := U_I^* \iota_I^* \mathrm{Tr}_{\mathbb{N}\setminus I} \left(\iota_{\mathbb{N}} U_{\mathbb{N}} \rho U_{\mathbb{N}}^* \iota_{\mathbb{N}}^* \right) \iota_I U_I$.
- Prefix $\rho_1^n := \rho_{[1,n]}$ is in general a mixed state!

Rule of Thumb: Fill up everything with blanks $\#$.

Rule of Thumb: Fill up everything with blanks #.

Example: $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle + |110\rangle\right)$, two-qubit-prefix $\psi_1^2 = \psi_{[1,2]}$ is

Rule of Thumb: Fill up everything with blanks $\#$.

Example: $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle + |110\rangle\right)$, two-qubit-prefix $\psi_1^2 = \psi_{[1,2]}$ is

$$\psi_1^2 \equiv |\psi\rangle\langle\psi|_1^2 = \frac{1}{2}\Big(|1\#\#\rangle\langle 1\#\#| + |1\#\#\rangle\langle 110| + |110\rangle\langle 1\#\#| + |110\rangle\langle 110|\Big)_1^2$$

Rule of Thumb: Fill up everything with blanks #.

Example: $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle + |110\rangle\right)$, two-qubit-prefix $\psi_1^2 = \psi_{[1,2]}$ is

$$
\begin{aligned}
\psi_1^2 &\equiv |\psi\rangle\langle\psi|_1^2 = \frac{1}{2}\big(|1\#\#\rangle\langle 1\#\#| + |1\#\#\rangle\langle 110| + \\
&\qquad\qquad |110\rangle\langle 1\#\#| + |110\rangle\langle 110|\big)_1^2 \\
&= \frac{1}{2}|1\#\rangle\langle 1\#|\langle\#|\#\rangle + \frac{1}{2}|1\#\rangle\langle 11|\langle 0|\#\rangle + \frac{1}{2}|11\rangle\langle 1\#|\langle\#|0\rangle \\
&\quad + \frac{1}{2}|11\rangle\langle 11|\langle 0|0\rangle
\end{aligned}
$$

Rule of Thumb: Fill up everything with blanks #.

Example: $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle + |110\rangle\right)$, two-qubit-prefix $\psi_1^2 = \psi_{[1,2]}$ is

$$\begin{aligned}
\psi_1^2 &\equiv |\psi\rangle\langle\psi|_1^2 = \frac{1}{2}\Big(|1\#\#\rangle\langle 1\#\#| + |1\#\#\rangle\langle 110| + \\
&\qquad\qquad |110\rangle\langle 1\#\#| + |110\rangle\langle 110|\Big)_1^2 \\
&= \frac{1}{2}|1\#\rangle\langle 1\#|\langle\#|\#\rangle + \frac{1}{2}|1\#\rangle\langle 11|\langle 0|\#\rangle + \frac{1}{2}|11\rangle\langle 1\#|\langle\#|0\rangle \\
&\quad + \frac{1}{2}|11\rangle\langle 11|\langle 0|0\rangle \\
&= \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|11\rangle\langle 11|.
\end{aligned}$$

Rule of Thumb: Fill up everything with blanks $\#$.
Example: $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle + |110\rangle\right)$, two-qubit-prefix $\psi_1^2 = \psi_{[1,2]}$ is

$$\begin{aligned}
\psi_1^2 &\equiv |\psi\rangle\langle\psi|_1^2 = \frac{1}{2}\big(|1\#\#\rangle\langle 1\#\#| + |1\#\#\rangle\langle 110| + \\
&\qquad\qquad |110\rangle\langle 1\#\#| + |110\rangle\langle 110|\big)_1^2 \\
&= \frac{1}{2}|1\#\rangle\langle 1\#|\langle\#|\#\rangle + \frac{1}{2}|1\#\rangle\langle 11|\langle 0|\#\rangle + \frac{1}{2}|11\rangle\langle 1\#|\langle\#|0\rangle \\
&\quad + \frac{1}{2}|11\rangle\langle 11|\langle 0|0\rangle \\
&= \frac{1}{2}|1\rangle\langle 1| + \frac{1}{2}|11\rangle\langle 11|.
\end{aligned}$$

This definition of restriction is consistent with a natural tensor product in $\mathcal{H}_{\{0,1\}^*}$.

Define the concatenation of qubit strings by linear extension of the classical concatenation:

Define the concatenation of qubit strings by linear extension of the classical concatenation:
$|\psi\rangle = \sum_{s\in\{0,1\}^*} \alpha_s |s\rangle$ and $|\varphi\rangle = \sum_{t\in\{0,1\}^*} \beta_t |t\rangle$, then

$$|\psi \circ \varphi\rangle := |\psi\rangle \circ |\varphi\rangle = \sum_{s,t\in\{0,1\}^*} \alpha_s \beta_t |s \circ t\rangle.$$

Define the concatenation of qubit strings by linear extension of the classical concatenation:
$|\psi\rangle = \sum_{s\in\{0,1\}^*} \alpha_s |s\rangle$ and $|\varphi\rangle = \sum_{t\in\{0,1\}^*} \beta_t |t\rangle$, then

$$|\psi \circ \varphi\rangle := |\psi\rangle \circ |\varphi\rangle = \sum_{s,t\in\{0,1\}^*} \alpha_s \beta_t |s \circ t\rangle.$$

- Convergence is not always clear.

Define the concatenation of qubit strings by linear extension of the classical concatenation:
$|\psi\rangle = \sum_{s\in\{0,1\}^*} \alpha_s|s\rangle$ and $|\varphi\rangle = \sum_{t\in\{0,1\}^*} \beta_t|t\rangle$, then

$$|\psi\circ\varphi\rangle := |\psi\rangle \circ |\varphi\rangle = \sum_{s,t\in\{0,1\}^*} \alpha_s\beta_t|s\circ t\rangle.$$

- Convergence is not always clear.
- If $|\psi\rangle$ is a length eigenvector, then $|\psi\circ\varphi\rangle = |\psi\rangle \otimes |\varphi\rangle$.

Define the concatenation of qubit strings by linear extension of the classical concatenation:
$|\psi\rangle = \sum_{s\in\{0,1\}^*} \alpha_s |s\rangle$ and $|\varphi\rangle = \sum_{t\in\{0,1\}^*} \beta_t |t\rangle$, then

$$|\psi \circ \varphi\rangle := |\psi\rangle \circ |\varphi\rangle = \sum_{s,t\in\{0,1\}^*} \alpha_s \beta_t |s \circ t\rangle.$$

- Convergence is not always clear.
- If $|\psi\rangle$ is a length eigenvector, then $|\psi \circ \varphi\rangle = |\psi\rangle \otimes |\varphi\rangle$.
- The concatenation is in general not isometric: If $|\psi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |00\rangle\right)$, then

$$|\psi \circ \psi\rangle = \frac{1}{2}|00\rangle + |000\rangle + \frac{1}{2}|0000\rangle.$$

Definition (Quantum Prefix Freedom)

A subset $M \subset \mathcal{H}_{\{0,1\}^*}$ of the qubit strings is called prefix-free, if one of the following four equivalent conditions is satisfied:

Definition (Quantum Prefix Freedom)

A subset $M \subset \mathcal{H}_{\{0,1\}^*}$ of the qubit strings is called prefix-free, if one of the following four equivalent conditions is satisfied:

- For all $|\varphi\rangle, |\psi\rangle \in M$ and $s \in \{0,1\}^* \setminus \{\lambda\}$ it holds $\langle\varphi|\psi \circ s\rangle = 0$.

Definition (Quantum Prefix Freedom)

A subset $M \subset \mathcal{H}_{\{0,1\}^*}$ of the qubit strings is called prefix-free, if one of the following four equivalent conditions is satisfied:

- For all $|\varphi\rangle, |\psi\rangle \in M$ and $s \in \{0,1\}^* \setminus \{\lambda\}$ it holds $\langle\varphi|\psi \circ s\rangle = 0$.
- For all $|\varphi\rangle, |\psi\rangle \in M$ and qubit strings $|\chi\rangle \perp |\lambda\rangle$ it holds $\langle\varphi|\psi \circ \chi\rangle = 0$.

Definition (Quantum Prefix Freedom)

A subset $M \subset \mathcal{H}_{\{0,1\}^*}$ of the qubit strings is called prefix-free, if one of the following four equivalent conditions is satisfied:

- For all $|\varphi\rangle, |\psi\rangle \in M$ and $s \in \{0,1\}^* \setminus \{\lambda\}$ it holds $\langle\varphi|\psi \circ s\rangle = 0$.
- For all $|\varphi\rangle, |\psi\rangle \in M$ and qubit strings $|\chi\rangle \perp |\lambda\rangle$ it holds $\langle\varphi|\psi \circ \chi\rangle = 0$.
- For all $|\varphi\rangle, |\psi\rangle \in M$ and $s, t \in \{0,1\}^*$ with $s \neq t$ it holds $\langle\varphi \circ t|\psi \circ s\rangle = 0$.

Definition (Quantum Prefix Freedom)

A subset $M \subset \mathcal{H}_{\{0,1\}^*}$ of the qubit strings is called prefix-free, if one of the following four equivalent conditions is satisfied:

- For all $|\varphi\rangle, |\psi\rangle \in M$ and $s \in \{0,1\}^* \setminus \{\lambda\}$ it holds $\langle\varphi|\psi \circ s\rangle = 0$.
- For all $|\varphi\rangle, |\psi\rangle \in M$ and qubit strings $|\chi\rangle \perp |\lambda\rangle$ it holds $\langle\varphi|\psi \circ \chi\rangle = 0$.
- For all $|\varphi\rangle, |\psi\rangle \in M$ and $s, t \in \{0,1\}^*$ with $s \neq t$ it holds $\langle\varphi \circ t|\psi \circ s\rangle = 0$.
- For all $|\varphi\rangle, |\psi\rangle \in M$ and qubit strings $|\chi\rangle, |\tau\rangle \in \mathcal{H}_{\{0,1\}^*}$ with $|\chi\rangle \perp |\tau\rangle$ it holds $\langle\varphi \circ \tau|\psi \circ \chi\rangle = 0$.

Definition (Quantum Prefix Freedom)

A subset $M \subset \mathcal{H}_{\{0,1\}^*}$ of the qubit strings is called prefix-free, if one of the following four equivalent conditions is satisfied:

- For all $|\varphi\rangle, |\psi\rangle \in M$ and $s \in \{0,1\}^* \setminus \{\lambda\}$ it holds $\langle\varphi|\psi \circ s\rangle = 0$.
- For all $|\varphi\rangle, |\psi\rangle \in M$ and qubit strings $|\chi\rangle \perp |\lambda\rangle$ it holds $\langle\varphi|\psi \circ \chi\rangle = 0$.
- For all $|\varphi\rangle, |\psi\rangle \in M$ and $s, t \in \{0,1\}^*$ with $s \neq t$ it holds $\langle\varphi \circ t|\psi \circ s\rangle = 0$.
- For all $|\varphi\rangle, |\psi\rangle \in M$ and qubit strings $|\chi\rangle, |\tau\rangle \in \mathcal{H}_{\{0,1\}^*}$ with $|\chi\rangle \perp |\tau\rangle$ it holds $\langle\varphi \circ \tau|\psi \circ \chi\rangle = 0$.

Theorem: A closed subspace $\mathcal{H} \subset \mathcal{H}_{\{0,1\}^*}$ is prefix-free if and only if one (and thus every) orthonormal basis of $\mathcal{H}$ is prefix-free.

- In contrast to classical strings, qubit strings can be proper prefixes of themselves: E.g. for $|\varphi\rangle := \frac{3}{5}|1\rangle + \frac{4}{5}|10\rangle$ it holds

$$\langle\varphi|\varphi\circ 0\rangle = \frac{3\cdot 3}{5\cdot 5}\underbrace{\langle 1|10\rangle}_{0} + \frac{3\cdot 4}{5\cdot 5}\underbrace{\langle 1|100\rangle}_{0} + \frac{4\cdot 3}{5\cdot 5}\underbrace{\langle 10|10\rangle}_{1} + \frac{4\cdot 4}{5\cdot 5}\underbrace{\langle 10|100\rangle}_{0} \neq 0,$$

so the singleton $\{|\varphi\rangle\}$ is not prefix-free.

- In contrast to classical strings, qubit strings can be proper prefixes of themselves: E.g. for $|\varphi\rangle := \frac{3}{5}|1\rangle + \frac{4}{5}|10\rangle$ it holds

$$\langle\varphi|\varphi\circ 0\rangle = \frac{3\cdot 3}{5\cdot 5}\underbrace{\langle 1|10\rangle}_{0} + \frac{3\cdot 4}{5\cdot 5}\underbrace{\langle 1|100\rangle}_{0} + \frac{4\cdot 3}{5\cdot 5}\underbrace{\langle 10|10\rangle}_{1} + \frac{4\cdot 4}{5\cdot 5}\underbrace{\langle 10|100\rangle}_{0} \neq 0,$$

  so the singleton $\{|\varphi\rangle\}$ is not prefix-free.
- Attention: $|\psi\rangle := \frac{1}{2}|1\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|0\rangle - \frac{1}{2}|00\rangle$ is e.g. not a prefix of itself!

- In contrast to classical strings, qubit strings can be proper prefixes of themselves: E.g. for $|\varphi\rangle := \frac{3}{5}|1\rangle + \frac{4}{5}|10\rangle$ it holds

$$\langle\varphi|\varphi\circ 0\rangle = \frac{3\cdot 3}{5\cdot 5}\underbrace{\langle 1|10\rangle}_{0} + \frac{3\cdot 4}{5\cdot 5}\underbrace{\langle 1|100\rangle}_{0} + \frac{4\cdot 3}{5\cdot 5}\underbrace{\langle 10|10\rangle}_{1} + \frac{4\cdot 4}{5\cdot 5}\underbrace{\langle 10|100\rangle}_{0} \neq 0,$$

  so the singleton $\{|\varphi\rangle\}$ is not prefix-free.
- Attention: $|\psi\rangle := \frac{1}{2}|1\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|0\rangle - \frac{1}{2}|00\rangle$ is e.g. not a prefix of itself!

Theorem (Perfect Distinguishability by means of Prefixes)

An orthonormal system $M \subset \mathcal{H}_{\{0,1\}^*}$ of length eigenvectors is prefix-free if and only if for all $|\varphi\rangle \neq |\psi\rangle \in M$ it holds

$$\langle\psi|\varphi_1^{\ell(\psi)}|\psi\rangle = 0. \qquad (1)$$

- In contrast to classical strings, qubit strings can be proper prefixes of themselves: E.g. for $|\varphi\rangle := \frac{3}{5}|1\rangle + \frac{4}{5}|10\rangle$ it holds

$$\langle\varphi|\varphi\circ 0\rangle = \frac{3\cdot 3}{5\cdot 5}\underbrace{\langle 1|10\rangle}_{0} + \frac{3\cdot 4}{5\cdot 5}\underbrace{\langle 1|100\rangle}_{0} + \frac{4\cdot 3}{5\cdot 5}\underbrace{\langle 10|10\rangle}_{1} + \frac{4\cdot 4}{5\cdot 5}\underbrace{\langle 10|100\rangle}_{0} \neq 0,$$

  so the singleton $\{|\varphi\rangle\}$ is not prefix-free.
- Attention: $|\psi\rangle := \frac{1}{2}|1\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|0\rangle - \frac{1}{2}|00\rangle$ is e.g. not a prefix of itself!

Theorem (Perfect Distinguishability by means of Prefixes)

An orthonormal system $M \subset \mathcal{H}_{\{0,1\}^*}$ of length eigenvectors is prefix-free if and only if for all $|\varphi\rangle \neq |\psi\rangle \in M$ it holds

$$\langle\psi|\varphi_1^{\ell(\psi)}|\psi\rangle = 0. \tag{1}$$

Schumacher+Westmoreland (2001) use (1) as a definition of prefix freedom $\longrightarrow$ restriction to M and $\mathcal{H} \subset \mathcal{H}_{\{0,1\}^*}$!

Example for a "skew" prefix-free Hilbert space: $\mathcal{H} := \mathrm{span}\, M$ with

$$M := \left\{ \underbrace{\frac{1}{\sqrt{2}}\left(|1\rangle + |01\rangle\right)}_{=:|\psi\rangle}, \underbrace{\frac{1}{\sqrt{2}}\left(|10\rangle - |010\rangle\right)}_{=:|\varphi\rangle} \right\}.$$

Example for a "skew" prefix-free Hilbert space: $\mathcal{H} := \mathrm{span}\, M$ with

$$M := \left\{ \underbrace{\frac{1}{\sqrt{2}}\left(|1\rangle + |01\rangle\right)}_{=:|\psi\rangle}, \underbrace{\frac{1}{\sqrt{2}}\left(|10\rangle - |010\rangle\right)}_{=:|\varphi\rangle} \right\}.$$

- M ist prefix-free (in particular $\langle\varphi|\psi \circ 0\rangle = 0$), thus so is $\mathcal{H}$.

Example for a "skew" prefix-free Hilbert space: $\mathcal{H} := \mathrm{span}\, M$ with

$$M := \left\{ \underbrace{\frac{1}{\sqrt{2}}\left(|1\rangle + |01\rangle\right)}_{=:|\psi\rangle}, \underbrace{\frac{1}{\sqrt{2}}\left(|10\rangle - |010\rangle\right)}_{=:|\varphi\rangle} \right\}.$$

- M ist prefix-free (in particular $\langle\varphi|\psi \circ 0\rangle = 0$), thus so is $\mathcal{H}$.
- $\mathcal{H}$ has no basis of length eigenvectors.

Example for a "skew" prefix-free Hilbert space: $\mathcal{H} := \operatorname{span} M$ with

$$M := \left\{ \underbrace{\frac{1}{\sqrt{2}}\left(|1\rangle + |01\rangle\right)}_{=:|\psi\rangle}, \underbrace{\frac{1}{\sqrt{2}}\left(|10\rangle - |010\rangle\right)}_{=:|\varphi\rangle} \right\}.$$

- M ist prefix-free (in particular $\langle\varphi|\psi \circ 0\rangle = 0$), thus so is $\mathcal{H}$.
- $\mathcal{H}$ has no basis of length eigenvectors.
- But $|\varphi\rangle$ and $|\psi\rangle$ can not be distinguished by means of the first two qubits: $\langle\psi|\varphi_1^2|\psi\rangle = \frac{1}{4} \neq 0$.

Theorem (Quantum Kraft Inequality, MM & CR 2008)

Let $\mathcal{H} \subset \mathcal{H}_{\{0,1\}^*}$ be a prefix-free Hilbert space, spanned by an orthonormal system $\{|e_i\rangle\}_{i \in I} \subset \mathcal{H}_{\{0,1\}^*}$. Then it holds

$$\sum_{i \in I} 2^{-\ell(e_i)} \leq \sum_{i \in I} 2^{-\bar{\ell}(e_i)} \leq \mathrm{Tr}\left(2^{-\Lambda}\mathbb{P}(\mathcal{H})\right) \leq 1.$$

Inequality in the first two "$\leq$" holds if and only of each $|e_i\rangle$ is a length eigenvector.

Theorem (Quantum Kraft Inequality, MM & CR 2008)

Let $\mathcal{H} \subset \mathcal{H}_{\{0,1\}^*}$ be a prefix-free Hilbert space, spanned by an orthonormal system $\{|e_i\rangle\}_{i\in I} \subset \mathcal{H}_{\{0,1\}^*}$. Then it holds

$$\sum_{i\in I} 2^{-\ell(e_i)} \leq \sum_{i\in I} 2^{-\bar{\ell}(e_i)} \leq \mathrm{Tr}\left(2^{-\Lambda}\mathbb{P}(\mathcal{H})\right) \leq 1.$$

Inequality in the first two "$\leq$" holds if and only of each $|e_i\rangle$ is a length eigenvector.

Conjecture (Quantum Kraft Inequality and its Converse)

For a closed subspace $\mathcal{H} \subset \mathcal{H}_{\{0,1\}^*}$, there exists a length-preserving unitary $U : \mathcal{H}_{\{0,1\}^*} \to \mathcal{H}_{\{0,1\}^*}$ such that $U\mathcal{H}$ is prefix-free if and only if $\mathrm{Tr}\left(2^{-\Lambda}\mathbb{P}(\mathcal{H})\right) \leq 1$.

On prefix-free subspaces, the concatenation is an isometry and can thus be realized physically:

On prefix-free subspaces, the concatenation is an isometry and can thus be realized physically:

Lemma (Concatenation as Isometry)

Let $\mathcal{H} \subset \mathcal{H}_{\{0,1\}^*}$ be a prefix-free subspace, and let $|\varphi_1\rangle, |\varphi_2\rangle \in \mathcal{H}$. Then

$$\langle \varphi_1 \circ \psi_1 | \varphi_2 \circ \psi_2 \rangle = \langle \varphi_1 | \varphi_2 \rangle \langle \psi_1 | \psi_2 \rangle \qquad \forall |\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}_{\{0,1\}^*}.$$

On prefix-free subspaces, the concatenation is an isometry and can thus be realized physically:

Lemma (Concatenation as Isometry)

Let $\mathcal{H} \subset \mathcal{H}_{\{0,1\}^*}$ be a prefix-free subspace, and let $|\varphi_1\rangle, |\varphi_2\rangle \in \mathcal{H}$. Then

$$\langle \varphi_1 \circ \psi_1 | \varphi_2 \circ \psi_2 \rangle = \langle \varphi_1 | \varphi_2 \rangle \langle \psi_1 | \psi_2 \rangle \qquad \forall |\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}_{\{0,1\}^*}.$$

Hence there is a unique isometry $U : \mathcal{H} \otimes \mathcal{H}_{\{0,1\}^*} \to \mathcal{H}_{\{0,1\}^*}$ with $U|\varphi\rangle \otimes |\psi\rangle = |\varphi \circ \psi\rangle$ for all $|\varphi\rangle \in \mathcal{H}$ and $|\psi\rangle \in \mathcal{H}_{\{0,1\}^*}$.

On prefix-free subspaces, the concatenation is an isometry and can thus be realized physically:

Lemma (Concatenation as Isometry)

Let $\mathcal{H} \subset \mathcal{H}_{\{0,1\}^*}$ *be a prefix-free subspace, and let* $|\varphi_1\rangle, |\varphi_2\rangle \in \mathcal{H}$*. Then*

$$\langle \varphi_1 \circ \psi_1 | \varphi_2 \circ \psi_2 \rangle = \langle \varphi_1 | \varphi_2 \rangle \langle \psi_1 | \psi_2 \rangle \qquad \forall |\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}_{\{0,1\}^*}.$$

Hence there is a unique isometry $U : \mathcal{H} \otimes \mathcal{H}_{\{0,1\}^*} \to \mathcal{H}_{\{0,1\}^*}$ *with* $U|\varphi\rangle \otimes |\psi\rangle = |\varphi \circ \psi\rangle$ *for all* $|\varphi\rangle \in \mathcal{H}$ *and* $|\psi\rangle \in \mathcal{H}_{\{0,1\}^*}$.

- Schumacher+Westmoreland: Restriction to $\mathcal{H}$ that are spanned by Λ-eigenvectors: Concatenation="Condensation"

On prefix-free subspaces, the concatenation is an isometry and can thus be realized physically:

Lemma (Concatenation as Isometry)

Let $\mathcal{H} \subset \mathcal{H}_{\{0,1\}^*}$ be a prefix-free subspace, and let $|\varphi_1\rangle, |\varphi_2\rangle \in \mathcal{H}$. Then

$$\langle \varphi_1 \circ \psi_1 | \varphi_2 \circ \psi_2 \rangle = \langle \varphi_1 | \varphi_2 \rangle \langle \psi_1 | \psi_2 \rangle \qquad \forall |\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}_{\{0,1\}^*}.$$

Hence there is a unique isometry $U : \mathcal{H} \otimes \mathcal{H}_{\{0,1\}^*} \to \mathcal{H}_{\{0,1\}^*}$ with $U|\varphi\rangle \otimes |\psi\rangle = |\varphi \circ \psi\rangle$ for all $|\varphi\rangle \in \mathcal{H}$ and $|\psi\rangle \in \mathcal{H}_{\{0,1\}^*}$.

- Schumacher+Westmoreland: Restriction to $\mathcal{H}$ that are spanned by Λ-eigenvectors: Concatenation="Condensation"
- Asymptotic compression of a source ρ with rate $S(\rho)$.

- If ρ is a density operator on some $\mathcal{H}$, then

$$S(\rho) \leq \min_U \bar{\ell}(U\rho U^*) \leq S(\rho) + 1. \tag{2}$$

(Min. over all isometries $U : \mathcal{H} \to \mathcal{H}_{\{0,1\}^*}$ such that $U\mathcal{H}$ is prefix-free.)

- If ρ is a density operator on some $\mathcal{H}$, then

$$S(\rho) \leq \min_U \bar{\ell}(U\rho U^*) \leq S(\rho) + 1. \qquad (2)$$

(Min. over all isometries $U : \mathcal{H} \to \mathcal{H}_{\{0,1\}^*}$ such that $U\mathcal{H}$ is prefix-free.)

- Lossless Quantum Block Coding: ψ q-information source, ψ_I:=restriction of ψ to local algebra at $I \subset \mathbb{Z}$.

$$|\underbrace{- - - - -}_{\psi_{[1,n_1]}=:\rho_1}|\underbrace{- - - - - - - -}_{\psi_{[n_1+1,n_2]}=:\rho_2}|\underbrace{- - - - - - - - - - - - - -}_{\psi_{[n_2+1,n_3]}=:\rho_3}|\cdots$$

- If ρ is a density operator on some $\mathcal{H}$, then

$$S(\rho) \leq \min_U \bar{\ell}(U\rho U^*) \leq S(\rho) + 1. \tag{2}$$

(Min. over all isometries $U : \mathcal{H} \to \mathcal{H}_{\{0,1\}^*}$ such that $U\mathcal{H}$ is prefix-free.)

- Lossless Quantum Block Coding: ψ q-information source, ψ_I:=restriction of ψ to local algebra at $I \subset \mathbb{Z}$.

$$|\underbrace{-\,-\,-\,-}_{\psi_{[1,n_1]}=:\rho_1}|\underbrace{-\,-\,-\,-\,-\,-}_{\psi_{[n_1+1,n_2]}=:\rho_2}|\underbrace{-\,-\,-\,-\,-\,-\,-\,-\,-\,-\,-\,-\,-}_{\psi_{[n_2+1,n_3]}=:\rho_3}|\cdots$$

Let U_i be the corresponding minimizer for $\rho = \rho_i$ in (2).

Concatenation: $U_\circ^{(N)} |\varphi_1\rangle \otimes \ldots \otimes |\varphi_N\rangle := |\varphi_1 \circ \ldots \circ \varphi_N\rangle$.

$\longrightarrow$ Compression map for N blocks: $U_\circ^{(N)} (U_1 \otimes \ldots \otimes U_N)$.

- If ρ is a density operator on some $\mathcal{H}$, then

$$S(\rho) \leq \min_U \bar{\ell}(U\rho U^*) \leq S(\rho) + 1. \qquad (2)$$

(Min. over all isometries $U : \mathcal{H} \to \mathcal{H}_{\{0,1\}^*}$ such that $U\mathcal{H}$ is prefix-free.)

- Lossless Quantum Block Coding: ψ q-information source, ψ_I:=restriction of ψ to local algebra at $I \subset \mathbb{Z}$.

$$|\underbrace{-\,-\,-\,-}_{\psi_{[1,n_1]}=:\rho_1}|\underbrace{-\,-\,-\,-\,-\,-}_{\psi_{[n_1+1,n_2]}=:\rho_2}|\underbrace{-\,-\,-\,-\,-\,-\,-\,-\,-\,-\,-\,-\,-}_{\psi_{[n_2+1,n_3]}=:\rho_3}|\cdots$$

Let U_i be the corresponding minimizer for $\rho = \rho_i$ in (2).
Concatenation: $U_\circ^{(N)}|\varphi_1\rangle \otimes \ldots \otimes |\varphi_N\rangle := |\varphi_1 \circ \ldots \circ \varphi_N\rangle$.
$\longrightarrow$ Compression map for N blocks: $U_\circ^{(N)}(U_1 \otimes \ldots \otimes U_N)$.

- This way, $\bar{\ell}$ is minimized losslessly. (But the base length ℓ remains large, and yields some loss if the output is "cut down" to some fixed length e.g. before transmission.)

Conclusions

Conclusions

- We have defined concatenation, prefixes, restrictions, and tensor products for indeterminate-length quantum bit strings.

Conclusions

- We have defined concatenation, prefixes, restrictions, and tensor products for indeterminate-length quantum bit strings.
- There is a natural definition of prefix-free qubit strings with interesting properties:

Conclusions

- We have defined concatenation, prefixes, restrictions, and tensor products for indeterminate-length quantum bit strings.
- There is a natural definition of prefix-free qubit strings with interesting properties:
  - A subspace is prefix-free if and only if one (and thus every) orthonormal basis is prefix-free.

Conclusions

- We have defined concatenation, prefixes, restrictions, and tensor products for indeterminate-length quantum bit strings.
- There is a natural definition of prefix-free qubit strings with interesting properties:
  - A subspace is prefix-free if and only if one (and thus every) orthonormal basis is prefix-free.
  - Qubit strings can be proper prefixes of themselves.

Conclusions

- We have defined concatenation, prefixes, restrictions, and tensor products for indeterminate-length quantum bit strings.
- There is a natural definition of prefix-free qubit strings with interesting properties:
  - A subspace is prefix-free if and only if one (and thus every) orthonormal basis is prefix-free.
  - Qubit strings can be proper prefixes of themselves.
  - Orthonormal systems of length eigenvectors are prefix-free iff they can be distinguished perfectly by means of their prefixes.

Conclusions

- We have defined concatenation, prefixes, restrictions, and tensor products for indeterminate-length quantum bit strings.
- There is a natural definition of prefix-free qubit strings with interesting properties:
  - A subspace is prefix-free if and only if one (and thus every) orthonormal basis is prefix-free.
  - Qubit strings can be proper prefixes of themselves.
  - Orthonormal systems of length eigenvectors are prefix-free iff they can be distinguished perfectly by means of their prefixes.
  - There are "skew" prefix-free subspaces.

Conclusions

- We have defined concatenation, prefixes, restrictions, and tensor products for indeterminate-length quantum bit strings.
- There is a natural definition of prefix-free qubit strings with interesting properties:
  - A subspace is prefix-free if and only if one (and thus every) orthonormal basis is prefix-free.
  - Qubit strings can be proper prefixes of themselves.
  - Orthonormal systems of length eigenvectors are prefix-free iff they can be distinguished perfectly by means of their prefixes.
  - There are "skew" prefix-free subspaces.
- We have proved a general quantum Kraft inequality.

Conclusions

- We have defined concatenation, prefixes, restrictions, and tensor products for indeterminate-length quantum bit strings.
- There is a natural definition of prefix-free qubit strings with interesting properties:
  - A subspace is prefix-free if and only if one (and thus every) orthonormal basis is prefix-free.
  - Qubit strings can be proper prefixes of themselves.
  - Orthonormal systems of length eigenvectors are prefix-free iff they can be distinguished perfectly by means of their prefixes.
  - There are "skew" prefix-free subspaces.
- We have proved a general quantum Kraft inequality.
- Concatenation is physically realizable on prefix-free subspaces, and can be used for lossless quantum block compression.

Conclusions

- We have defined concatenation, prefixes, restrictions, and tensor products for indeterminate-length quantum bit strings.
- There is a natural definition of prefix-free qubit strings with interesting properties:
  - A subspace is prefix-free if and only if one (and thus every) orthonormal basis is prefix-free.
  - Qubit strings can be proper prefixes of themselves.
  - Orthonormal systems of length eigenvectors are prefix-free iff they can be distinguished perfectly by means of their prefixes.
  - There are "skew" prefix-free subspaces.
- We have proved a general quantum Kraft inequality.
- Concatenation is physically realizable on prefix-free subspaces, and can be used for lossless quantum block compression.
- **ArXiv:0804.0022**