Chained Typical Subspaces - a Quantum Version of Breiman's Theorem

Igor Bjelaković[1], Tyll Krüger[1,2], Rainer Siegmund-Schultze[1], Arleta Szkoła[1]

[1] Technische Universität Berlin *, e-mail: {igor, tkrueger, siegmund, szkola}@math.tu-berlin.de
[2] Universität Bielefeld **

The date of receipt and acceptance will be inserted by the editor

Abstract. We give an equivalent finitary reformulation of the classical Shannon-McMillan-Breiman theorem which has an immediate translation to the case of ergodic quantum lattice systems. This version of a quantum Breiman theorem can be derived from the proof of the quantum Shannon-McMillan theorem presented in [2].

1. Introduction

In classical probability and information theories the Shannon-McMillan theorem was proved by Breiman in an almost sure version, saying that with probability one along a trajectory (message string) the individual probability decreases exponentially at a rate given by the entropy rate h of the ergodic stochastic process (over a finite alphabet). From the point of view of data compression and coding this means that the message string will not only belong to a typical set of approximate size e^{nh} at a given time n with overwhelming probability, as is guaranteed by the original Shannon-McMillan theorem, but it will eventually be captured in the sequence of typical sets almost surely. So sequential coding at entropy rate should be possible (and in fact, the Lempel-Ziv algorithm is such a sequential coding scheme).

* Fakultät II - Mathematik und Naturwissenschaften
Institut für Mathematik MA 7-2
Straße des 17. Juni 136
10623 Berlin, Germany
** Fakultät für Mathematik
Universitätsstr. 25
33619 Bielefeld, Germany

It is natural to ask for a corresponding result in the quantum context. In the quantum situation the notion of an individual trajectory is at least problematic. So it is not at all obvious what could be an analogue of Breiman's result. The approach chosen here is to give an equivalent reformulation of the classical Breiman result which allows an immediate translation into the quantum setting. In fact, the typical subsets according to Breiman's theorem are not isolated objects, one for each n, but comprise bundles of trajectories and hence can be chosen being chained in the sense that the predecessor subset consists exactly of the same sequences, only shortened for one letter. This simple observation leads to a finitary, simple and equivalent statement of Breiman's theorem avoiding the notion of a trajectory. Substituting typical subsets by typical subspaces of Hilbert spaces, the property of them to be chained can be expressed easily in terms of partial traces. It turns out that the proof of the quantum Shannon-McMillan theorem presented in [2], which is based to a substantial part on the earlier work of Hiai and Petz [3], yields the necessary tools to prove that typical subspaces can be chained.

2. A finitary reformulation of the Shannon-McMillan-Breiman theorem

Consider an arbitrary (not necessarily stationary) stochastic process P with a finite set A as state space. So P is a probability measure on $[A^{\mathbb{Z}}, \mathfrak{A}^{\mathbb{Z}}]$ where $\mathfrak{A}^{\mathbb{Z}}$ is the σ-field generated by cylinder sets. Let h be a non-negative real number. We say that P satisfies the condition (B) (with respect to h) if for P-a.e. sequence $(\xi_n)_{n\in\mathbb{Z}}$ the limit $-\frac{1}{n}\log P^{(n)}((\xi_i)_{i=1}^n)$ exists and equals h. Here $P^{(n)}$ is the marginal of P on the cartesian product $A^{(n)} := \prod_{i=1}^n A$.

The Shannon-McMillan-Breiman theorem asserts that ergodic P satisfy (B) with h being the entropy rate of the process.

Let $\mathbf{x} = (x_i)_{i=1}^n$ be a finite sequence from $A^* = \bigcup_{k\in\mathbb{N}} A^{(k)}$. We denote by $\mathbf{x}_\flat$ the sequence $(x_i)_{i=1}^{n-1}$ obtained from $\mathbf{x}$ by omitting the last symbol.

Definition 2.1. *We say that P satisfies condition (B*) with respect to h if for each ε there exists a sequence $\{C_\varepsilon^{(n)}\}_{n\in\mathbb{N}}$ of subsets of $A^{(n)}$, respectively, and a number $N(\varepsilon)$ such that*

1. $C_\varepsilon^{(n)} = (C_\varepsilon^{(n+1)})_\flat$ *for* $n \geq 1$
   (sets are chained)
2. $\#C_\varepsilon^{(n)} \in (e^{n(h-\varepsilon)}, e^{n(h+\varepsilon)})$ *for* $n \geq N(\varepsilon)$
   (exponential growth rate)
3. $P^{(n)}(\mathbf{x}) < e^{-n(h-\varepsilon)}$ *for* $n \geq N(\varepsilon)$ *and any* $\mathbf{x} \in C_\varepsilon^{(n)}$
   (upper semi-AEP)
4. $P^{(n)}(C_\varepsilon^{(n)}) > 1 - \varepsilon$
   (typical sets).

Except for the concatenation condition (1) these are known properties of the typical sets for the case of a stationary ergodic P. Condition (3) is a weakened version of the well-known Asymptotic Equipartition Property (AEP), particularly it ensures that h is an asymptotic entropy rate in the general (possibly non-stationary) situation.
We obtain the equivalence assertion

Lemma 2.1. *A probability measure P on $[A^{\mathbb{Z}}, \mathfrak{A}^{\mathbb{Z}}]$ satisfies (B) iff it satisfies (B*).*

The proof is entirely elementary. Observe that (1) describes a tree graph of one-sided infinite trajectories.

Proof of Lemma 2.1:
1. Assume that (B) is fulfilled. Let

$$A_{(M,\varepsilon)} := \{\mathbf{x} \in A^{\mathbb{Z}} |\ P^{(n)}((x_i)_{i=1}^n) \in (e^{-n(h+\varepsilon/2)}, e^{-n(h-\varepsilon/2)}), \quad \forall n \geq M\}.$$

Obviously (B) implies $P(A_{(M,\varepsilon)}) \underset{M\to\infty}{\longrightarrow} 1$ for fixed ε. So there is some $M(\varepsilon)$ with $P(A_{(M(\varepsilon),\varepsilon)}) > 1-\varepsilon$. Define

$$C_\varepsilon^{(n)} := \{\mathbf{y} \in A^{(n)} |\ \exists \mathbf{x} \in A_{(M(\varepsilon),\varepsilon)} :\ (y_i)_{i=1}^n = (x_i)_{i=1}^n\},$$

let $k(\varepsilon) = \min\{k \in \mathbb{N} | (1-\varepsilon)e^{k(h-\varepsilon/2)} > e^{k(h-\varepsilon)}\}$ and set $N(\varepsilon) = \max\{k(\varepsilon), M(\varepsilon)\}$. Then (1)-(4) are easily derived, taking into account that bounds on probabilities imply bounds on cardinality. So (B*) is a consequence of (B).

2. Assume (B*) to be satisfied. Then it is easy to see that we find a chained sequence $\{\overline{C}_\varepsilon^{(n)}\}$ and some $\overline{N}(\varepsilon)$ which fulfil (1)-(4) and even the full AEP condition

$$P^{(n)}(\mathbf{x}) \in (e^{-n(h+\varepsilon)}, e^{-n(h-\varepsilon)}), \quad \forall n \geq \overline{N}(\varepsilon),\ \forall \mathbf{x} \in \overline{C}_\varepsilon^{(n)}.$$

In fact, define

$$A_\varepsilon(n) := \{\mathbf{x} \in A^{\mathbb{Z}} |\ (x_i)_{i=1}^n \in C_\varepsilon^{(n)}\}$$

and observe that $A_\varepsilon(n) \underset{n\to\infty}{\searrow} A_\varepsilon$, where A_ε is the tree of trajectories associated with $\{C_\varepsilon^{(n)}\}$. Condition (4) implies $P(A_\varepsilon) \geq 1-\varepsilon$. Now let

$$\widetilde{A}_\varepsilon(n) := \{\mathbf{x} \in A_\varepsilon(n) |\ P^{(n)}((x_i)_{i=1}^n) \leq e^{-n(h+2\varepsilon)}\}.$$

By (2) it follows that $P(\widetilde{A}_\varepsilon(n)) \leq \#C_\varepsilon^{(n)} \cdot e^{-n(h+2\varepsilon)} < e^{-n\varepsilon}$. The Borel-Cantelli lemma implies now that $P(\bigcup_{n\geq m} \widetilde{A}_\varepsilon(n)) \underset{m\to\infty}{\searrow} 0$, so there is some $m(\varepsilon)$ with $P(\bigcup_{n\geq m(\varepsilon)} \widetilde{A}_\varepsilon(n)) < \varepsilon$. Let $\overline{N}(\varepsilon) := \max\{N(\varepsilon/2), m(\varepsilon/2), k(\varepsilon)\}$ (where $k(\varepsilon)$ was defined above) and

$$\overline{C}_\varepsilon^{(n)} := \{(x_i)_{i=1}^n \in C_{\varepsilon/2}^{(n)} | \ \exists \mathbf{w} \in A_{\varepsilon/2} : \ (w_i)_{i=1}^n = (x_i)_{i=1}^n, \\ P^{(k)}((w_i)_{i=1}^k) > e^{-k(h+\varepsilon)}, \ \forall k \geq N(\varepsilon)\}.$$

We have, denoting by $\overline{A}_\varepsilon$ the trajectory tree associated with $\{\overline{C}_\varepsilon^{(n)}\}$,

$$P^{(n)}(\overline{C}_\varepsilon^{(n)}) \geq P(\overline{A}_\varepsilon) = P(A_{\varepsilon/2} \setminus \bigcup_{n\geq \overline{N}(\varepsilon)} \widetilde{A}_{\varepsilon/2}(n)) \\ > 1 - \varepsilon/2 - \varepsilon/2 = 1 - \varepsilon.$$

Thus (4) is established. (1) and the ε-AEP are clearly fulfilled, and (2) follows from the AEP as in step 1. Now (B) follows immediately. □

3. A quantum Shannon-McMillan-Breiman theorem

We are now in a position to formulate and prove a quantum version of Breiman's theorem. With this paper being a continuation of [2] we adopt all settings from there, for simplicity only considering the one-dimensional case. That means that $\mathcal{A}^\infty$ is a quasilocal C^*-algebra over $\mathbb{Z}$ constructed from a finite dimensional C^*-algebra $\mathcal{A}$. For $m, n \in \mathbb{Z}$ with $m \leq n$ we denote by $\mathcal{A}_{[m,n]}$ the local algebra over the discrete interval $[m, n] \subset \mathbb{Z}$ and use the abbreviation $\mathcal{A}^{(n)}$ for $\mathcal{A}_{[1,n]}$, $n \in \mathbb{N}$. Instead of $\mathcal{A}_{[n,n]}$ we write $\mathcal{A}_{[n]}$. Recall that for a stationary, i.e. shift-invariant state Ψ on $\mathcal{A}^\infty$ the mean entropy s is defined as

$$s := \lim_{n\to\infty} \frac{1}{n} S(\Psi^{(n)}),$$

where $S(\Psi^{(n)}) := -\text{tr}D^{(n)} \log D^{(n)}$ is the von Neumann entropy of $\Psi^{(n)}$, the restriction of the state Ψ to the local algebra $\mathcal{A}^{(n)}$, and $D^{(n)}$ is the density operator from $\mathcal{A}^{(n)}$ corresponding to the state $\Psi^{(n)}$.
Let A be a self-adjoint element of a local algebra $\mathcal{A}_{[m,n]}$. Then $R(A)$ denotes its range projector and $\text{tr}_{[k,l]}(A)$ is the partial trace of A over the local algebra $\mathcal{A}_{[k,l]} \subset \mathcal{A}_{[m,n]}$.

Observe that for the case that the underlying algebra is abelian the following theorem reduces to the classical (reformulated) Breiman assertion. So it can be considered as a quantum analogue of the SMB theorem.

Theorem 3.1. *Let Ψ be an ergodic state on the quasilocal C*-algebra $\mathcal{A}^\infty$ with mean entropy s. Then to each $\varepsilon > 0$ there is a sequence of orthogonal projectors $\{p_\varepsilon^{(n)}\}_{n=1}^\infty$ in $\mathcal{A}^{(n)}$, respectively, and some $N(\varepsilon)$, such that*

(q1) $p_\varepsilon^{(n)} = R(\text{tr}_{n+1}\,(p_\varepsilon^{(n+1)}))$,

(q2) tr $(p_\varepsilon^{(n)}) \in (e^{n(s-\varepsilon)}, e^{n(s+\varepsilon)})$ *for* $n \geq N(\varepsilon)$,

(q3) there exist minimal projectors $p_i \in \mathcal{A}^{(n)}$ *fulfilling* $p_\varepsilon^{(n)} = \sum_{i=1}^{\mathrm{tr}\,(p_\varepsilon^{(n)})} p_i$ *and* $\Psi^{(n)}(p_i) < e^{-n(s-\varepsilon)}$ *if* $n \geq N(\varepsilon)$,

(q4) $\Psi^{(n)}(p_\varepsilon^{(n)}) > 1 - \varepsilon$.

Remark: It is a well known fact that each finite dimensional unital $*$- algebra $\mathcal{A}$ is isomorphic to $\bigoplus_{i=1}^{s} \mathcal{B}(\mathcal{H}_i)$, where $\mathcal{H}_i$ are finite dimensional Hilbert spaces. According to this representation, we may associate to each chained projector $p_\varepsilon^{(n)}$ in the theorem above a typical subspace of $\mathcal{H}^{\otimes n}$ with $\mathcal{H} := \bigoplus_{i=1}^{s} \mathcal{H}_i$.

Proof of Theorem 3.1

1. Let $\varepsilon > 0$ be given. Choose an integer $l > 0$ sufficiently large such that the entropy of $\Psi^{(l)}$ satisfies $s \leq \frac{1}{l} S(\Psi^{(l)}) < s + \varepsilon^2$. Take a complete set V_l of mutually orthogonal spectral projectors for $\Psi^{(l)}$. Let $\mathcal{B}$ denote the abelian subalgebra of $\mathcal{A}^{(l)}$ generated by these projectors. The completeness of V_l implies that $\mathcal{B}$ is maximal abelian. Furthermore the entropy of $\Psi^{(l)} \upharpoonright_{\mathcal{B}}$, the restriction of $\Psi^{(l)}$ to the subalgebra $\mathcal{B}$, is identical to $S(\Psi^{(l)})$. Generally we have the relation

$$S(\Psi^{(n)}) = \min\{S(\Psi^{(n)} \upharpoonright_{\mathcal{C}}) |\, \mathcal{C} \subset \mathcal{A}^{(n)} \text{ max. abelian subalgebra}\}. \quad (3.1)$$

The quasilocal algebra $\mathcal{B}^\infty$ constructed from $\mathcal{B}$ is an abelian subalgebra of $\mathcal{A}^\infty$ and Ψ acts on this algebra as a stochastic process P_l with alphabet V_l. The Shannon mean entropy h_l of this process can be estimated by $s \leq \frac{1}{l} h_l \leq \frac{1}{l} S(\Psi^{(l)} \upharpoonright_{\mathcal{B}}) < s + \varepsilon^2$. The first inequality is a consequence of (3.1). P_l is a stationary, but not necessarily ergodic process. We apply the corresponding version of the classical Shannon-McMillan-Breiman theorem (cf. [4], [1]) to this process and obtain that there is a set of trajectories $V_l^* \subset V_l^{\mathbb{Z}}$ of measure one such that for each $(v_i)_{i\in\mathbb{Z}} \in V_l^*$ the limit (individual mean entropy) $h((v_i)_{i\in\mathbb{Z}}) := \lim_{n\to\infty} -\frac{1}{n} \log P_l^{(n)}((v_i)_{i=1}^n)$ exists, and we have $\mathbb{E} h((v_i)_{i\in\mathbb{Z}}) = h_l$.

2. Let $V_l^{\varepsilon,-} \subset V_l^*$ be the subset of those trajectories, for which the relation $\frac{1}{l} h((v_i)_{i\in\mathbb{Z}}) < s - \varepsilon^2$ holds. We have $P_l(V_l^{\varepsilon,-}) = 0$. In fact, consider the sets $W_l^{(n),-} := \{(w_i)_{i=1}^n \in V_l^{(n)} | P_l^{(n)}((w_i)_{i=1}^n) > e^{-nl(s-\varepsilon^2)}\}$ obviously containing the sets $V_l^{(n),-} := \{(v_i)_{i=1}^n |\, \exists (w_i)_{i\in\mathbb{Z}} \in V_l^{\varepsilon,-} \text{ with } (w_i)_{i=1}^n = (v_i)_{i=1}^n \text{ and } P_l^{(m)}((v_i)_{i=1}^m) > e^{-ml(s-\varepsilon^2)} \text{ for all } m \geq n\}$, respectively. This means that $P_l^{(n)}(W_l^{(n),-}) \geq P_l^{(n)}(V_l^{(n),-})$. The cardinality of each $W_l^{(n),-}$ is bounded from above by $e^{nl(s-\varepsilon^2)}$. Now suppose $P_l(V_l^{\varepsilon,-}) > 0$. Then for n sufficiently large we would have $P_l^{(n)}(V_l^{(n),-}) > c$ for some $c > 0$ implying $P_l^{(n)}(W_l^{(n),-}) > c$. For the quantum state this would have the consequence that for large n there are

projectors $p^{(nl)} := \sum_{(w_i)_{i=1}^n \in W_l^{(n),-}} \otimes_{i=1}^n w_i$ with tr $(p^{(nl)}) < e^{nl(s-\varepsilon^2)}$ and $\Psi^{(nl)}(p^{(nl)}) > c$. This contradicts Proposition 2.1 in [2], saying that no sequence of projectors in $\mathcal{A}^{(nl)}$, respectively, of significant expectation can have asymptotically a smaller trace than $e^{nl(s-\varepsilon^2)}$.

3. Let $V_l^{\varepsilon,+} \subset V_l^*$ be the subset of those trajectories, for which the relation $\frac{1}{l}h((v_i)_{i\in\mathbb{Z}}) > s+\varepsilon$ holds. By 2. and by the relation $\mathbb{E}h((v_i)_{i\in\mathbb{Z}}) = h_l$ we obtain

$$h_l > l(s-\varepsilon^2)(1-P_l(V_l^{\varepsilon,+})) + l(s+\varepsilon)P_l(V_l^{\varepsilon,+})$$

resulting in $P_l(V_l^{\varepsilon,+}) < 2\varepsilon$.

4. Combining the preceeding results we can easily derive for each $\varepsilon > 0$ the existence of an l and of some $N(\varepsilon)$ such that there is a subset $\widetilde{V}_l^* \subset V_l^*$ with the properties

(a) $P_l(\widetilde{V}_l^*) > 1-\varepsilon$,
(b) $e^{-nl(s+\varepsilon)} < P_l^{(n)}((v_i)_{i=1}^n) < e^{-nl(s-\varepsilon)}$ for each $(v_i)_{i\in\mathbb{Z}} \in \widetilde{V}_l^*$ and $n > N(\varepsilon)$.

Indeed, assume $\varepsilon < 1$ (otherwise we would obtain the result above with ε^2 instead of ε) and set $A_{l,\varepsilon} := V_l^* \setminus (V_l^{\frac{\varepsilon}{2},-} \cup V_l^{\frac{\varepsilon}{2},+})$. We have $P_l(A_{l,\varepsilon}) > 1-\varepsilon$ and $A_{l,\varepsilon} \subseteq \bigcup_{n\geq 0} \bigcap_{k\geq n} A_{l,\varepsilon}^{(k)}$, where

$$A_{l,\varepsilon}^{(k)} := \left\{ (v_i)_{i\in\mathbb{N}} | \; -\frac{1}{k} \log P_l^{(k)}((v_i)_{i=1}^k) \in (l(s-\varepsilon), l(s+\varepsilon)) \right\}.$$

Then there exists $N(\varepsilon) \in \mathbb{N}$ such that $P_l(\bigcap_{k\geq N(\varepsilon)} A_{l,\varepsilon}^{(k)}) > 1-\varepsilon$. The set $\widetilde{V}_l^* := \bigcap_{k\geq N(\varepsilon)} A_{l,\varepsilon}^{(k)}$ fulfills both conditions above.

Obviously $\widetilde{V}_l^*$ generates a sequence of chained sets $\{C_\varepsilon^{(n)}\}_{n=1}^\infty$ fulfilling 1-4 given in section 2. In the given situation, we may reformulate these properties as follows:

(a) $C_\varepsilon^{(n)} = (C_\varepsilon^{(n+1)})_\flat$ for $n \geq 1$
(b) $\#C_\varepsilon^{(n)} \in (e^{nl(s-\varepsilon)}, e^{nl(s+\varepsilon)})$ for $n \geq N(\varepsilon)$
(c) $\Psi^{(nl)}(p) < e^{-nl(s-\varepsilon)}$ for $n \geq N(\varepsilon)$ and any $p = \otimes_{k=1}^n v_k$, where $(v_k)_{k=1}^n \in C_\varepsilon^{(n)}$
(d) $\Psi^{(nl)}(\sum_{(v_k)_{k=1}^n \in C_\varepsilon^{(n)}} \otimes_{k=1}^n v_k) > 1-\varepsilon$.

Now it is easy to define chained projectors, first for multiples of l:

$$p_\varepsilon^{(nl)} := \sum_{(v_k)_{k=1}^n \in C_\varepsilon^{(n)}} \otimes_{k=1}^n v_k,$$

and then for general $n = ml + r, r < l$ by the set-up

$$p_\varepsilon^{(n)} := R\left(\mathrm{tr}_{[ml+r+1,(m+1)l]}\left(p_\varepsilon^{((m+1)l)}\right)\right).$$

Observe that both definitions are compatible. Obviously, by definition the property (q1) is fulfilled by the defined system of projectors. Next, we have with $n = ml + r, r < l$

$$\begin{aligned} e^{n(s-2\varepsilon)} < \#C_\varepsilon^{(m)} \leq \mathrm{tr}(p_\varepsilon^{(n)}) \leq \#C_\varepsilon^{(m)}\mathrm{tr}(\mathbf{1}_{\mathcal{A}^{(l)}}) \\ < \mathrm{tr}(\mathbf{1}_{\mathcal{A}^{(l)}})e^{n(s+\varepsilon)} < e^{n(s+2\varepsilon)} \quad (3.2) \end{aligned}$$

for n sufficiently large. In fact, the first inequality in this chain is obvious. By definition we have

$$p_\varepsilon^{(ml)} = \sum_{i=1}^{\mathrm{tr}(p_\varepsilon^{(ml)})} q_i^{(m)}$$

for certain minimal projectors $q_i^{(m)}$ from $(\mathcal{B}_{(l)})^{(m)}$, and

$$p_\varepsilon^{((m+1)l)} = \sum_{i=1}^{\mathrm{tr}\,(p_\varepsilon^{(ml)})} \sum_{j=1}^{k_i} q_i^{(m)} \otimes q_{i,j}$$

for some minimal projectors $q_{i,j}$ from $\mathcal{B}_{[m+1]}$. In order to simplify our notation let

$$I(m,r) := [ml + r + 1, (m+1)l].$$

We obtain

$$\begin{aligned} \mathrm{tr}(p_\varepsilon^{(ml+r)}) &= \mathrm{tr}\left(R\left(\sum_{i=1}^{\mathrm{tr}(p_\varepsilon^{(ml)})} \sum_{j=1}^{k_i} q_i^{(m)} \otimes \mathrm{tr}_{I(m,r)} q_{i,j}\right)\right) \\ &= \mathrm{tr}\left(\sum_{i=1}^{\mathrm{tr}(p_\varepsilon^{(ml)})} R\left(q_i^{(m)} \otimes \sum_{j=1}^{k_i} \mathrm{tr}_{I(m,r)} q_{i,j}\right)\right) \\ &= \sum_{i=1}^{\mathrm{tr}(p_\varepsilon^{(ml)})} \mathrm{tr}\left(q_i^{(m)} \otimes R\left(\sum_{j=1}^{k_i} \mathrm{tr}_{I(m,r)} q_{i,j}\right)\right) \\ &= \sum_{i=1}^{\mathrm{tr}(p_\varepsilon^{(ml)})} \mathrm{tr}\left(R\left(\sum_{j=1}^{k_i} \mathrm{tr}_{I(m,r)} q_{i,j}\right)\right) \\ &\geq \mathrm{tr}(p_\varepsilon^{(ml)}) = \#C_\varepsilon^{(m)}. \end{aligned}$$

Here in the second step we made use of the mutual orthogonality of the $q_i^{(m)}$. This proves the second inequality in (3.2). The third inequality also immediately follows from the formula

$$\mathrm{tr}(p_\varepsilon^{(ml+r)}) = \sum_{i=1}^{\mathrm{tr}(p_\varepsilon^{(ml)})} \mathrm{tr}\left(R\left(\sum_{j=1}^{k_i} \mathrm{tr}_{I(m,r)}(q_{i,j}) \right) \right).$$

So (q2) is fulfilled, too (with 2ε instead of ε).

By (c) we see that (q3) is fulfilled if n is a multiple of l. In the general case $n = ml + r$ observe that in the representation

$$p_\varepsilon^{(ml+r)} = \sum_{i=1}^{\mathrm{tr}(p_\varepsilon^{(ml)})} q_i^{(m)} \otimes R\left(\sum_{j=1}^{k_i} \mathrm{tr}_{I(m,r)}(q_{i,j}) \right)$$

we sum over mutually orthogonal projectors each of them fulfilling

$$\begin{aligned}
&\Psi^{(ml+r)}\left(q_i^{(m)} \otimes R\left(\sum_{j=1}^{k_i} \mathrm{tr}_{I(m,r)}(q_{i,j}) \right) \right) \\
&\leq \Psi^{(ml+r)}\left(q_i^{(m)} \otimes \mathbf{1}_{I(m,r)} \right) \\
&= \Psi^{(ml)}(q_i^{(m)}) < e^{-ml(s-\varepsilon)} < e^{-n(s-2\varepsilon)}
\end{aligned}$$

if n is sufficiently large. Now (q3) follows easily, again with 2ε instead of ε.

Finally, we have

$$\begin{aligned}
&\Psi^{(ml+r)}(p_\varepsilon^{(ml+r)}) \\
&= \sum_{i=1}^{tr\,(p_\varepsilon^{(ml)})} \Psi^{(ml+r)}\left(q_i^{(m)} \otimes R\left(\sum_{j=1}^{k_i} \mathrm{tr}_{I(m,r)}(q_{i,j}) \right) \right) \\
&= \sum_{i=1}^{tr\,(p_\varepsilon^{(ml)})} \Psi^{((m+1)l)}\left(q_i^{(m)} \otimes R\left(\sum_{j=1}^{k_i} \mathrm{tr}_{I(m,r)}(q_{i,j}) \right) \otimes \mathbf{1}_{\mathcal{A}_{I(m,r)}} \right) \\
&\geq \sum_{i=1}^{tr\,(p_\varepsilon^{(ml)})} \Psi^{((m+1)l)}\left(q_i^{(m)} \otimes \sum_{j=1}^{k_i} q_{i,j} \right) = \Psi^{((m+1)l)}(p_\varepsilon^{((m+1)l)}) > 1-\varepsilon,
\end{aligned}$$

where we used the Schmidt representation and (d) to obtain the last line. This proves (q4). $\square$

Acknowledgements. We are deeply grateful to Ruedi Seiler for his continuous support of our work on a quantum version of the Shannon-McMillan-Breiman Theorem and for many helpful discussions.
This work was supported by the DFG via the SFB 288 "Differentialgeometrie und Quantenphysik" at the TU Berlin and the Forschergruppe "Stochastische Analysis und große Abweichungen" at University of Bielefeld.

References

1. P. Billingsley, Ergodic Theory and Information, John Wiley & Sons (1965)
2. I. Bjelaković, T. Krüger, Ra. Siegmund-Schultze, A. Szkoła, The Shannon-McMillan Theorem for Ergodic Quantum Lattice Systems, arxiv-math.DS/0207121
3. F. Hiai, D. Petz, The Proper Formula for Relative Entropy and its Asymptotics in Quantum Probability, Commun. Math. Phys. 143, 99-114 (1991)
4. G. Keller, Equilibrium States in Ergodic Theory, London Mathematical Society Student Texts 42, Cambridge (1998)