mixed states. If ρ is pure, then $\rho^2 = \rho$, so $Tr(\rho^2) = Tr(\rho) = 1$ by Definition A.2.5, and $Tr(\rho)$ attains the upper bound. If $\rho = \frac{1}{q^n} I$ is the maximally mixed state, then $Tr(\rho^2) = Tr(\frac{1}{q^{2n}} I) = \frac{1}{q^n}$ and the lower bound is met.

□

Lemma 3.4.8. *Fix a pure state ρ on $\mathbb{C}^{\mathbb{Z}_q}$. Let $\mathcal{B} = \{B_i\}_{i=1}^{q+1}$ be the $q+1$ measurements of Example 3.4.5. Then*

$$\sum_{i=1}^{q+1} \sum_{b \in out(B_i)} (p(b|B_i))^2 = 2,$$

where $p(b|B_i) \coloneqq Tr(\rho b)$.

Proof. Proposition 3.3.13 gives that for each $i \in \{1, 2, \ldots, q+1\}$, we have $p(b|B_i) = \sum_{x \in P_{b,B_i}} W_\rho(x)$, where $P_{b,B_i} \in Line(\mathbb{Z}_q^2)$ is defined in Definition 3.3.14. It follows that for each i, $p(b|B_i)^2 = \sum_{x,y \in P_{b,B_i}} W_\rho(x) W_\rho(y)$.

We have the following calculation.

$$\sum_{i=1}^{q+1} \sum_{b \in out(B_i)} p(b|B_i)^2 = \sum_{i=1}^{q+1} \sum_{b \in out(B_i)} \sum_{x,y \in P_{b,B_i}} W_\rho(x) W_\rho(y) \qquad \text{Part 1 of Theorem 3.3.5}$$

(3.9)

$$= \sum_{l \in Line(\mathbb{Z}_q^2)} \sum_{x,y \in l} W_\rho(x) W_\rho(y) \qquad \text{Striations partition } Line(\mathbb{Z}_q^2)$$

(3.10)

$$= \sum_{x \neq y \in \mathbb{Z}_q^2} W_\rho(x) W_\rho(y) + (q+1) \sum_{x \in \mathbb{Z}_q^2} W_\rho(x)^2 \qquad \text{Proposition 3.4.4}$$

(3.11)

$$= (\sum_{x \in \mathbb{Z}_q^2} W_\rho(x))^2 + q \sum_{x \in \mathbb{Z}_q^2} W_\rho(x)^2 \qquad \text{Factoring the first summand}$$

(3.12)

$$\leq 2 \qquad \text{Lemma 3.4.7}$$

(3.13)

The inequality in the last step is saturated iff ρ is a pure state. □

Theorem 3.4.9. *([112]) Let q be an odd prime, and let $\mathcal{B} = \{B_i\}_{i=1}^{q+1}$ be the collection of $q+1$ mutually unbiased bases of $\mathbb{C}^{\mathbb{Z}_q}$ in Example 3.4.5. For any quantum state ρ on $\mathbb{C}^{\mathbb{Z}_q}$, $\mathbb{E}_{B_i \in \mathcal{B}}[H_2(B_i)] \geq \log_2(q+1) - 1$, where $H_2(B_i)$ is the 2-Rényi entropy of the probability distribution of the set of outcomes $out(B_i)$ when measured on ρ.*

The expected value is calculated relative to the uniform distribution on $\mathcal{B}$.

Proof. We use the concavity of log and Lemma 3.4.8.

$$\begin{aligned}
\mathbb{E}_{B_i \in \mathcal{B}}[H_2(B_i)] &= \frac{1}{q+1} \sum_{i=1}^{q+1} (-\log_2(\sum_{b \in out(B_i)} p(b|B_i)^2)) && \text{Definition 3.4.1} \\
&\geq -\log_2(\frac{1}{q+1} \sum_{b \in out(B_i), i=1}^{i=q} p(b|B_i)^2) && \text{Proposition C.4.16} \\
&\geq \log_2(q+1) - 1 && \text{Lemma 3.4.8}
\end{aligned}$$

□

The more general result of [112] applies to every collection of $q+1$ mutually unbiased bases in $\mathbb{C}^q$ for $q \in \mathbb{N}$ not necessarily prime. We will generalize Theorem 3.4.9 in another direction by allowing $n \geq 1$ and by allowing partial measurements.

Definition 3.4.10 (Grouped)**.** *Let $n \in \mathbb{N}$, and let R be a striation of $\mathbb{Z}_q^{2n}$. Then two points $x, y \in \mathbb{Z}_q^{2n}$ are said to be* grouped *by R if they appear in the same part of the striation. We denote this by $x \sim_R y$.*

Since there is a bijection between ${}^q\mathcal{L}^n$ and striations of $\mathbb{Z}_q^{2n}$, we also allow writing $x \sim_T y$ if x and y are grouped by the striation in direction T, for $T \in {}^q\mathcal{L}^n$.

The following lemma is the analog of the fact, "Every two distinct points have a unique line containing them."

Lemma 3.4.11. *Let $n, k \in \mathbb{N}$ with $n \geq k$. Let $x \neq y \in \mathbb{Z}_q^{2n}$. Then*

$$|\{T \in {}^q\mathcal{L}_k^n \mid x \sim_T y\}| = \frac{q^{2n-k} - 1}{q^k - 1} \prod_{i=1}^{k-1} \frac{q^{2n-i} - q^i}{q^k - q^i}.$$

Proof. Apply an affine transformation so that x is the origin and y is some non-origin point. This will permute the striations, but will not affect the count by Proposition 3.3.10.

Our counting problem simplifies to finding $N \coloneqq |\{T \in {}^q\mathcal{L}_k^n \mid y \in T\}|$.

Since $Sp(2n, \mathbb{Z}_q)$ acts transitively on non-origin points of $\mathbb{Z}_q^{2n}$[4], N is independent of y.

We will use a counting argument based on the equation $N(q^{2n}-1) = SR$, where N is the number of times each non-origin point is covered, $S = \prod_{i=0}^{k-1} \frac{q^{2n-i}-q^i}{q^k-q^i}$ is the number of k-dimensional isotropic spaces (See Proposition 2.1.8.), and $R = q^{2n-k}-1$ is the number of points (other than the origin) in $T^\perp$ for $T \in {}^q\mathcal{L}_k^n$.

Thus,

$$N = \frac{q^{2n-k}-1}{q^{2n}-1} \prod_{i=0}^{k-1} \frac{q^{2n-i}-q^i}{q^k-q^i} = \frac{q^{2n-k}-1}{q^k-1} \prod_{i=1}^{k-1} \frac{q^{2n-i}-q^i}{q^k-q^i}.$$

□

The following lemma is the analog of Lemma 3.4.8

Lemma 3.4.12. *Let $n \in \mathbb{N}$, and let ρ be a state on $\mathbb{C}^{\mathbb{Z}_q^n}$. Then*

$$\sum_{B \in {}^q\mathcal{L}_k^n} \sum_{b \in out(B)} p(b \mid B)^2 = C\left(\frac{q^{2n} + q^{3n-k} - q^n - q^{2n-k}}{(q^k-1)q^n}\right),$$

where $p(b|B) = Tr(\rho b)$ for $B \in {}^q\mathcal{L}_k^n$, $b \in out(B)$ and $C = \prod_{i=1}^{m-1} \frac{q^{2n-i}-q^i}{q^k-q^i}$.

Proof. As with the proof of Lemma 3.4.9, we count the sum of squared probabilities of outcomes.

Lemma 3.4.11 asserts that every pair of distinct points of $\mathbb{Z}_q^{2n}$ are grouped together in $\frac{q^{2n-k}-1}{q^k-1}C$ striations, and every point is in $\frac{q^{2n}-1}{q^k-1}C = |{}^q\mathcal{L}_k^n|$ striations.

[4] See Corollary A.3.50.

$$\sum_{B\in {}^q\mathcal{L}_k^n}\sum_{b\in out(B)} p(b|B)^2 = \sum_{B\in {}^q\mathcal{L}_k^n}\sum_{b\in out(B)}(\sum_{x\in P_{b,B}} W_\rho(x))^2 \qquad \text{Proposition 3.3.13}$$

$$= \sum_{B\in {}^q\mathcal{L}_k^n}\sum_{b\in out(B)}\sum_{x,y\in P_{b,B}} W_\rho(x)W_\rho(y) \qquad \text{Distributivity}$$

$$= \frac{q^{2n-k}-1}{q^k-1}C\sum_{x\neq y} W_\rho(x)W_\rho(y) + \frac{q^{2n}-1}{q^k-1}C\sum_{x\in\mathbb{Z}_q^{2n}} W_\rho(x)^2 \qquad \text{Lemma 3.4.11}$$

$$= \frac{q^{2n-k}-1}{q^k-1}C(\sum_{x\in\mathbb{Z}_q^{2n}} W_\rho(x))^2 + (\frac{q^{2n}-1}{q^k-1} - \frac{q^{2n-k}-1}{q^k-1})C\sum_{x\in\mathbb{Z}_q^{2n}} W_\rho(x)^2 \qquad \text{Analog of 3.11}$$

$$\leq \frac{q^{2n-k}-1}{q^k-1}C + \frac{q^{2n}-1-(q^{2n-k}-1)}{(q^k-1)q^n}C \qquad \text{Equation 3.8}$$

$$= C(\frac{q^{2n}+q^{3n-k}-q^n-q^{2n-k}}{(q^k-1)q^n}) \qquad \text{Combining terms}$$

□

Theorem 3.4.13. *Let $n, k \in \mathbb{N}$, $k \leq n$. For each fixed state on $\mathbb{C}^{\mathbb{Z}_q^n}$, the following inequality holds.*

$$\mathbb{E}_{S\in {}^q\mathcal{L}_k^n}[H_2(S)] \geq \log_2\left(\frac{q^n(q^{2n}-1)}{q^{2n}+q^{n+k}-q^n-q^k}\right),$$

where $H_2(S)$ is the Rényi 2-entropy of the distribution of outcomes that results from applying the measurement S to ρ according to Dogma A.2.12. The expected value is calculated relative to the uniform distribution on ${}^q\mathcal{L}_k^n$.

Proof. Again, we use the concavity of information:

$$\begin{aligned}
\mathbb{E}_{S\in {}^q\mathcal{L}_k^n}[H_2(S)] &= \frac{1}{\frac{q^{2n}-1}{q^k-1}C}\sum_{B\in {}^q\mathcal{L}_k^n} -\log_2\Big(\sum_{b\in out(B)} p(b|B)^2\Big) && \text{Definition 3.4.1}\\
&\geq -\log_2\Big(\frac{1}{\frac{q^{2n}-1}{q^k-1}C}\sum_{b,B} p(b|B)^2\Big) && \text{Propositions C.4.15 and C.4.16}\\
&\geq -\log_2\left(\frac{q^{2n}+q^{3n-k}-q^n-q^{2n-k}}{q^n(q^{2n}-1)}\right) && \text{Lemma 3.4.12}\\
&= \log_2\left(\frac{q^{2n}-1}{q^{2n-k}+q^n-q^{n-k}-1}\right). && \text{Using } -\log_2(x)=\log_2(\frac{1}{x})
\end{aligned}$$

□

When $k = n$, we recover the same bound as for mutually unbiased bases, Theorem 3.4.9.

Example 3.4.14. *Suppose that $q = 3$ and $n = 2$. Choose $k = 1$ to bound the expected Rényi entropy of Pauli operators ${}^q\mathcal{L}_k^n$. Theorem 3.4.13 gives $\mathbb{E}_{B\in {}^q\mathcal{L}_k^n}[H_2(B)] \geq 1.32$. This seems stronger than every bound that can be obtained by using Theorem 3.4.9. Even supposing that each Pauli measurement of ${}^q\mathcal{L}_k^n$ could be put into a mutually unbiased basis, this would only give us a lower bound of 1, on the average.*

3.5 Contextuality and the Wigner function

In this section, we see how our observations about the Wigner function can be used to investigate the contextuality of the Pauli measurements when q is odd.

Let $x \in \mathbb{Z}_q^{2n}$ be a point of phase space for some $n \in \mathbb{N}$. Let $M \in {}^q\mathcal{L}^n$ be a Pauli measurement. Then M corresponds to a striation of $\mathbb{Z}_q^{2n}$. Let p be the part of this striation containing x. Let us say that the outcome p occurs when $x \in p$. Note that this is the outcome that is predicted by applying Dogma A.2.12 to M with the phase-point operator $A(x)$ as the state, ignoring that $A(x)$ is not positive and so cannot be a state.