Fall 2020 QIC 890 / CO 781 Assignment 2

Due Friday Oct 30, 2020, 10pm, on Crowdmark.

Method of types, strong typicality, entanglement concentraton and dilution

You will derive and analyse methods for entanglement concentration and dilution, using the method of types and strong typicality, which you will also learn a little through this assignment. This question is self-contained. Additional references include quant-ph/9902045 and 0204092, and the textbooks by Cover and Thomas and by Csiszar and Körner (warning: be cautious about notation switches between references). Relevant pages in the textbooks will be shared on Slack.

Question 1. Method of types (3/22 marks)

This part elaborates what we discussed briefly in class.

Consider the set $\Omega = \{1, 2, \cdots, m\}$. Fix n and consider Ω^n, the set of all possible n-tuples $x^n = x_1 x_2 \cdots x_n$ such that each symbol x_i comes from Ω.

For example, $m = 3$, $n = 10$, $x^n = 2213123112$.

For each $a \in \Omega$, define $t_a(x^n)$ to be the number of times a appears in x^n. The *type* of x^n, denoted $t(x^n)$, is the m-tuple, $t(x^n) = (t_1(x^n), t_2(x^n), \cdots, t_m(x^n))$. Each x^n defines an empirical distribution q_{x^n} on Ω such that $q_{x^n}(a) = \frac{1}{n} t_a(x^n)$.

For example, $t_1(2213123112) = 4$, $t_2(2213123112) = 4$, $t_3(2213123112) = 2$. The *type* of 2213123112 is given by $t(2213123112) = (4, 4, 2)$. The probabilities of 1,2,3 in the empirical distribution $q_{2213123112}$ are 0.4, 0.4, 0.2 respectively.

(a)[1 mark] Given a quick explanation why there are at most $(n+1)^m$ types.

Note that many n-tuples have the same type.

For example, $t(1111222233)$ is also $(4, 4, 2)$.

For each type τ, the type class Λ_τ consists of all possible n-tuples of type τ. In other words,

$$\Lambda_\tau = \{x^n : t(x^n) = \tau\}.$$

Note that two n-tuples are in the same type class iff one can be obtained by permuting the entries of the other. The set of all possible type classes is a partition of Ω^n.

For example, in the binary case ($m = 2$), there are $n+1$ types: $(n, 0)$, $(n-1, 1)$, $\cdots$, $(1, n-1)$, $(0, n)$. The type of x^n is specified by the number of 1's in the n-tuple, and it belongs to exactly one type class. The type class $(n-k, k)$ has $\binom{n}{k}$ elements.

In general, the size of each type class $|\Lambda_\tau|$ is hard to enumerate. The method of types gives a straightforward proof for

$$\frac{1}{(n+1)^m} 2^{nH(\tau)} \le |\Lambda_\tau| \le 2^{nH(\tau)}$$

where $H(\tau)$ is the entropy of the distribution q_{x^n} for any $x^n \in \Lambda_\tau$. The alternative proofs may require a detailed counting argument and/or the Stirling approximation, which we will not use in this assignment.

(b)[2 marks] Prove that $|\Lambda_\tau| \le 2^{nH(\tau)}$.

Hint: what is the probability of each n-tuple $x^n \in \Lambda_\tau$ under the distribution of n iid draws of q_{x^n}? (See also our discussion for AEP in class.) Note that the probability is only used as an intermediate tool in the proof of a cardinality bound.

The proof for the lower bound is more involved and will be left as a reading exercise. The answer is detailed in Cover and Thomas p282-284. You can use both bounds for the rest of the assignment.

Question 2. Strong typicality (5/22 marks)

We continue to use previously defined concepts and symbol. For the rest of the assignment, $\Omega = \{1, 2, \cdots, m\}$ is the sample space of some random variable X with distribution $p(a)$. WLOG, $p(a) > 0$ for all a (by trimming the sample space if need to).

We say that x^n is η-strongly typical if, $\forall_{a \in \Omega} |q_{x^n}(a) - p(a)| \leq \eta$. (Note that this definition and many other concepts about strong typicality do not assume any distribution on Ω^n.)

Continuing on our earlier example with $m = 3, n = 10$, let $p(1) = 0.3$, $p(2) = 0.45$, $p(3) = 0.25$. The string 2213123112 is 0.1-strongly typical, and so are strings obtained by permuting those n symbols. Permutations of 1112222333 are 0.05-strongly typical, and so are permutations of 1112222233.

Let Σ_η denote the set of all η-strongly typical sequences (shorthand η-strongly-typical-set). Σ_η depends on p and n but as they are fixed so far, we omit them from the notation. If need to vary n, we write $\Sigma_{n,\eta}$.

(c)[1 mark] Show that if x^n is η-strongly-typical (with respective to p), then, for very small η, $|H(q_{x^n}) - H(p)| \leq cm\eta$ where $c = \max_a |\log p(a) + \frac{1}{\ln 2}|$.

Finally, consider n iid draws of p. The probability of an event E under this distribution is denoted $p^{\otimes n}(E)$. Caution: x^n defines an empirical distribution q_{x^n} but here the distribution is n iid draws of p.

Recall the notion of typicality covered in the lecture; that is sometimes called weakly-typical, or entropy-typical. Part (c) says that η-strongly-typical sequences are $cm\eta$-weakly-typical; this justifies the two names – it is a stronger requirement to be strongly typical.

We now relate the type classes to strong typicality. For each type τ, we say τ is η-strongly-typical (with respect to the underlying distribution p) if elements of Λ_τ are η-strongly-typical. The η-strongly-typical-set is in fact the union of all type classes with η-strongly-typical types,

$$\Sigma_\eta = \bigcup_{\tau \text{ is } \eta-\text{strongly}-\text{typical}} \Lambda_\tau$$

.

Back to the $m = 3, n = 10, (p(1), p(2), p(3)) = (0.3, 0.45, 0.25)$ example, $\Sigma_{0.05} = \Lambda_{(3,4,3)} \bigcup \Lambda_{(3,5,2)}$. Incidentally, for $n = 10$, Σ_η is empty for $\eta < 0.05$.

You will now show that under the distribution p, draw iid n times, the result is most likely strongly-typical.

(d)[4 marks] Prove that $p^{\otimes n}(\Sigma_\eta) \geq 1 - \frac{m}{4n\eta^2}$.

Hint: fix one a. Let $X_1 X_2 \cdots X_n$ be drawn iid according to p. What is the probability $X_i = a$ for each i? The total number of times with $X_i = a$ is an induced random variable with well defined expectation and variance. We can apply Chebyshev's inequality to this random variable to upper bound the probability that it is too far from the expectation (similar to the proof for the AEP in class). Then, taken the union bound over a.

Question 3. Entanglement concentration (8/22 marks)

In this and the next questions, we take n large enough so that our desirable results hold.

Let $\Delta > 0$ be a large but fixed integer.

Note that we can choose $\eta = \frac{\Delta}{\sqrt{n}}$ in our earlier analysis (since no dependence between n and η was assumed).

(e)[4 marks] With this choice of η, show that for large enough n, there are constants K, L such that
(i) $|\Sigma_\eta| \leq 2^{nH(p)+Km\Delta\sqrt{n}}$ and
(ii) for any η-strongly typical type τ, $2^{nH(p)-Lm\Delta\sqrt{n}} \leq |\Lambda_\tau| \leq 2^{nH(p)+Lm\Delta\sqrt{n}}$.

Let $|\psi\rangle = \sum_{a=1}^{m} \sqrt{p(a)}\ |a\rangle|a\rangle$.

Consider entanglement concentration. Suppose Alice and Bob share $|\psi\rangle^{\otimes n}$; the i-th copy of $|\psi\rangle$ lives on A_iB_i and Alice has A_i, Bob has B_i. The joint state can be written as $|\psi\rangle^{\otimes n} = \sum_{x^n \in \Omega^n} \sqrt{p(x^n)}|x^n\rangle_{A_1\cdots A_n}|x^n\rangle_{B_1\cdots B_n}$. They can each measure the type on their system (locally) and from the above expression, their outcomes are always the same (due to the entanglement between their systems). Conditioned on each outcome τ, Alice and Bob have a state with equal nonzero Schmidt coefficients (since all n-tuples within the same type class are equiprobability under n iid draws of p).

(f)[1 mark] Use part (d) to show that the probability of getting a type τ that is η-strongly-typical with respect to p is at least $1 - \frac{m}{4\Delta^2}$.

(g)[3 marks] Use (f) and (e)(ii) to show that for any $\epsilon > 0$, for large enough n, with probability at least $1-\epsilon$, at least $\approx nH(p) - 2Lm\Delta\sqrt{n}$ ebits can be obtained for $\Delta \geq \sqrt{\frac{m}{2\epsilon}}$.

Hint: conditioned on getting the outcome τ, we can have a maximally entangled state over $|\Lambda_\tau|$ local dimensions. For many purposes they are as useful as ebits. If one really wants ebits and $\log|\Lambda_\tau|$ is not an integer, one has to choose an l and divide $|\Lambda_\tau|$ into $\lfloor\frac{|\Lambda_\tau|}{2^l}\rfloor$ blocks each of 2^l terms, and give up the remainders. There is a tradeoff between a large enough l and a small enough probability getting the remainders. See bottom of left column of p6 of 0204092 for details.

Question 4. Entanglement dilution (6/22 marks)

Consider the reverse problem of entanglement dilution, that Alice and Bob want to create an approximation of $|\psi\rangle^{\otimes n}$ using ebits and classical communication.

Note that $|\psi\rangle^{\otimes n} = \sum_{x^n\in\Sigma_\eta} \sqrt{p(x^n)}|x^n\rangle_{A_1\cdots A_n}|x^n\rangle_{B_1\cdots B_n} + \sum_{x^n\in\Omega^n\setminus\Sigma_\eta} \sqrt{p(x^n)}|x^n\rangle_{A_1\cdots A_n}|x^n\rangle_{B_1\cdots B_n}$.

(h)[3 marks] Show that the first term can be transformed by some local unitaries $U_{A_1\cdots A_n} \otimes V_{B_1\cdots B_n}$ into a subnormalized state $\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right)^l \otimes |\mu_1\rangle + |\mu_2\rangle$ where $l = \lfloor\log\frac{|\Lambda_\tau|}{2^{Lm\Delta\sqrt{n}}}\rfloor \gtrapprox nH(p) - 2Lm\Delta\sqrt{n}$, each of Alice and Bob holds one qubit of each $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\mu_1\rangle$ is a subnormalized state shared by Alice and Bob with Schmidt rank upper bounded by $2^{(K-2L)m\Delta\sqrt{n}}$, and for any $\epsilon > 0$, $\langle\mu_2|\mu_2\rangle + p^{\otimes n} \leq \epsilon$.

(Hint: use (d), (e), and the proof for (g).)

(i)[3 marks] Use (h) (and the proof of (g) to construct a dilution protocol with the following properties. For any $\epsilon > 0$, the output has at least $\sqrt{1-\epsilon}$ fidelity with $|\psi\rangle^{\otimes n}$. The protocol uses $nH(p) + Km\Delta\sqrt{n}$ ebits and $2(K + 2L)m\Delta\sqrt{n}$ cbits.