From: Miller, Carl A. (Fed)
To: Knill, Emanuel H. (Fed)
Cc: (b) (6) [redacted]; Bierhorst, Peter L. (Assoc)
Subject: Re: berb review for the probability estimation paper
Date: Friday, August 18, 2017 3:53:37 PM

Hi all –

Update: I showed this problem to Honghao and he seemed to think he could make some progress with computer work. Will keep you all posted. (He's going to be away next week and then we'll pick up again in the new semester.)

-Carl

____
Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

On 8/15/17, 4:55 PM, "Miller, Carl A. (Fed)" <carl.miller@nist.gov> wrote:

Hi Manny –

Sounds good – we will focus on Renyi powers. (That's what I'm used to from previous work, actually, and it will be nice to return to it.)

What I have in mind is the following reasoning: suppose that we know the conditional probability distribution of the inputs and the outputs, and we additionally assume that the angle between Alice's measurements is \theta_1 and the angle between Bob's measurements is \theta_2. Then, we can deduce the density matrix like so: let Z_t denote the 2x2 Hermitian matrix which fixes the vector cos t |0> + sin t |1> and negates the vector sin t |0> - cos t |1>. Then, the nine operators

{ I, Z, Z_{\theta_1} } \otimes { I, Z, Z_{\theta_2} }

are all real 4x4 Hermitian operators. Assume that the density operator \rho is real. By assumption, we know the inner product of \rho with each of the nine operators above.

Now, at this point I wanted to conclude that we therefore know what \rho is. But now I'm realizing that's not quite true – the set of real 4x4 Hermitian operators is 10 dimensional, whereas we only know the inner product of \rho with 9 independent vectors in that space. So there still is an additional degree of freedom. (Maybe that's what you were referring to.)

Perhaps then there are just three additional parameters we need, and we need to minimize the Renyi power function over all states arising from choices of those parameters.

I look forward to seeing your notes whenever they're ready.

-Carl

____
Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

On 8/11/17, 2:07 PM, "Emanuel Knill" <emanuel.knill@nist.gov> wrote:

On Friday, August 11, 2017 11:02:56 AM Miller, Carl A. wrote:
> Hi Manny et al. –
>
> I talked about this stuff with Honghao, and it seems like it might be doable
> on computer. It seems that given a correlation \nu, all we need to do is
> to choose the relevant angles \theta_1 and \theta_2 and then the density
> matrix is automatically determined. (Or at least the real part of it is.)
> Then we can compute the conditional Renyi or von Neumann entropies from
> there.

> We could calculate the minimum average entropy that occurs for various
> correlations and then see if we can come up with a QEF from that data –
> does that sound like it's worth doing?

Sure, just watch out for Renyi entropies versus Renyi powers and which
you calculate when. I am fundamentally interested in the powers, not
the entropies, which matters when averaging. I'll send you the
mathematical context to clarify when I have it layed out better. How
did you eliminate the extra weights encoded in the state after
postselection by E? From my notes, the primary formulation of the problem
has the angles and a pure CP map defined by a positive semdefinite A
that E can use to prepare the desired non-maximally-entangled state at
the devices.

> (BTW, we're having a meeting at 11:30am MDT about the randomness beacon:
> https://hangouts.google.com/hangouts/_/umd.edu/beacon . Feel free to join,
> and also let me know if you'd like to join the newly created beacon mailing
> list, which is nistbeacon@nist.gov, for any future announcements.)

Got this a bit too late to join the hangout, but I suppose I ought
to be on the mailing list...

Manny

>   -Carl
>
> ——————
> Carl A. Miller
> Mathematician, Computer Security Division
> National Institute of Standards and Technology
> Gaithersburg, MD
>
>
>
> On 8/2/17, 2:44 PM, "Miller, Carl A. (Fed)" <carl.miller@nist.gov> wrote:
>
>   Hi Manny --
>
>
>   >   > Given a quantum correlation \nu, our goal is then to find an
>   >   > entropy

> > > estimator which exhibits the largest possible average on \nu.
> > > Right?
>
>
>
> > That's a reasonable goal from the point of view of entropy
> > accumulation, but likely doesn't lead to the best finite-data
> > certificates.
>
>
> Ok. If we measure “randomness” using (1 + \beta)-Renyi entropy, rather
> than von Neumann entropy, does that make it good for finite-date
> certificates? Or are there more subtleties?

> The minimization problem as Manny described it sounds nice & compact – I
> sent along the problem to my student Honghao to see if it’s something he
> might be interested in tackling by computer.

> So, sketching out the big picture a little further (and apologies if
> this repeats stuff that’s already known or obvious):

> For given input and output alphabets, we can look at the space of all
> quantum correlations over those alphabets. We can calculate, for each
> point x in this space, the minimum possible amount of randomness F(x) that
> a device that exhibits that correlation must achieve. Here we can measure
> randomness by either conditional von Neumann entropy or by (1+\beta)-Renyi
> entropy, as we like. Given a particular point \nu in the space of
> correlations, we want to find an affine-linear function G (x) which is a
> lower bound for F (x) such that G (\nu) is as large as possible. (?)

> A natural thing to do would be to let G (x) be the unique
> affine-linear function such that F (\nu) = G (\nu) and the gradient of
> F and G are the same at \nu. Is this something that’s been looked at?
> (Arnon-Friedman/Dupuis mention gradients but I don’t know if they mention
> them in this context.)

> -Carl
>
> ——————
> Carl A. Miller
> Mathematician, Computer Security Division
> National Institute of Standards and Technology
> Gaithersburg, MD
>
>
>
> On 7/31/17, 4:08 PM, "Emanuel Knill" <knill@boulder.nist.gov> wrote:
>
> On Thursday 27 July 2017 15:37:31 Miller, Carl A. (Fed) wrote:
>
> > Ok. I may offer this problem to my student Honghao, who is good
> > with
> >
> > computer work.
> >
> >
> >

> > Let me see if I can translate the problem a little more into my
> > own words
> > (and you can tell me if I'm right). For any nonlocal game G, an
> > entropy
> > estimator is a function F from input-output 4-tuples (a, b, x, y)
> > to the
> > real numbers, which constitutes a "guess" at how much randomness
> > has been
> > generated when a device has outputted (a, b, x, y). We don't
> > require that
> > the guess always be correct, but we require that it be correct
> > "on
> > average" – that is, for any quantum correlation, the average
> > value of F
> > over that correlation does not exceed the average amount of
> > randomness
> > generated by the correlation. (In our case, this randomness is
> > measured
> > against an adversary who holds a purifying state of the
> > devices.)
>
>
> That's a reasonable interpretation.
>
>
> > Given a quantum correlation \nu, our goal is then to find an
> > entropy
> > estimator which exhibits the largest possible average on \nu.
> > Right?
>
>
> That's a reasonable goal from the point of view of entropy
> accumulation, but likely doesn't lead to the best finite-data
> certificates.
>
>
> > One thing I just noticed is that in (2,2,4)-dimensional case
> > we're
> > discussing, the subnormalized states that appear on the
> > adversary's side
> > would all be rank-one. That also seems to simplify the problem
> > somewhat …
>
>
> Yes, and I believe they can also be assumed to be real. I think you
> meant the (2,2,2) configuration? (Not sure about your labeling.) But you
> can parametrize the relevant states that need to be checked by the relative
> angles θ_1 and θ_2 of the two (orthogonal, projective)
> measurements used by the two stations/parties/devices, and a semidefinite
> operator in four dimensions A, where you take the sixteen projectors
> π_{abxy} for the measurements on two qubits, and transform them to get
> $\sigma_{abxy} = A\pi_{abxy} A$ as the side-information state up to scale
> at uniform settings
> probabilities. The traced out (sum over ab) settings-conditional
> state
is A^2 up to normalization, so you may prefer writing
> $A=\sigma^{1/2}$. This should give you a sufficiently large set to

>   check convex properties on.
>
>   Manny
>
>
>   >
>   >
>   >   -Carl
>   >
>   >
>   >
>   > ___________
>   > Carl A. Miller
>   > Mathematician, Computer Security Division
>   > National Institute of Standards and Technology
>   > Gaithersburg, MD
>   >
>   >
>   >
>   >
>   >
>   > On 7/25/17, 1:28 PM, "Emanuel Knill" <knill@boulder.nist.gov>
>   > wrote:
>   >
>   >
>   >
>   >
>   >
>   >   I see you already thought through the relevant bits. It is
>   >   claimed in
>   >   one or both of the Arnon-Friedman papers with a reference, at
>   >   some
>   >   point I just did what you did and thought it through
>   >   directly. Chaining is handled at the level of QEFs, so each
>   >   trial can
>   >   be considered in isolation. But the fact that we can
>   >   restrict to
>   >   extremal (so pure) states is helpful, and also a general
>   >   property for
>   >   QEFs. The full argument is interesting in its own right of
>   >   course,
>   >   but either way, it suffices to consider the standard 2x2
>   >   dimensional
>   >   scenario.
>   >
>   >
>   >
>   >
>   >   > Now we have a finite dimensional problem. Suppose that
>   >   > we're given
>   >
>   > a > quantum correlation \nu, and we want to find a QEF that
>   > maximizes the
>   >
>   > > amount of randomness coming out of that distribution. We can
>   > > look at
>   >

> > the > set of all 2/2/4-dimensional quantum strategies that will
> > produce
> > that > quantum correlation \nu, look at the amount of randomness
> > coming
> > from > each, and construct a QEF from that data…?
> >
> >
> >
> > It's worth a try. Alternatively, it is a small dimensional
> > but
> > non-linear optimization problem, the trick is to make sure no
> > extrema
> > are missed.
> >
> >
> >
> > Manny
> >
> >
> >
> >
> > On Tuesday 25 July 2017 09:45:36 Miller, Carl A. (Fed)
> > wrote:
> >
> > > I thought about the (2,2,2) case a little more, and it
> > > seems
> >
> > doable: >
> >
> > > First, I think we can indeed assume that the systems in
> > > the devices
> >
> > are > just qubit states. (We can perform a measurement on both
> > devices
> > that > projects onto a 2-dimensional space, and this measurement
> > with
> > commute > with the later measurements used by the devices and
> > won't
> > affect the > outcome statistics. I'm not 100% sure of this, but
> > I think
> > it works.) >
> >
> > > Second, we can assume that the state shared by the devices
> > > & the
> > > environment is pure. (Mixed states can only increase the
> > > amount of
> > > randomness.)
> > >
> > >
> > >
> > > Third, since we have a pure entangled state between two
> > > qubit
> >
> > systems > (total dimension = 4) and the environment, we may
> > assume that
> > environment > has dimension 4.
> >

>　>　>
>　>　>
>　>　> Now we have a finite dimensional problem. Suppose that
>　>　> we're given
>　>
>　> a > quantum correlation \nu, and we want to find a QEF that
>　> maximizes the
>　>
>　> > amount of randomness coming out of that distribution. We can
>　> > look at
>　>
>　> the > set of all 2/2/4-dimensional quantum strategies that will
>　> produce
>　> that > quantum correlation \nu, look at the amount of randomness
>　> coming
>　> from > each, and construct a QEF from that data…?
>　>
>　>　>
>　>　>
>　>　>   -Carl
>　>　>
>　>　>
>　>　>
>　>　> ___________
>　>　> Carl A. Miller
>　>　> Mathematician, Computer Security Division
>　>　> National Institute of Standards and Technology
>　>　> Gaithersburg, MD
>　>　>
>　>　>
>　>　>
>　>　>
>　>　>
>　>　> On 7/24/17, 5:41 PM, "Miller, Carl A. (Fed)"
>　>　> <carl.miller@nist.gov>
>　>
>　> wrote: >
>　>
>　>　>   Hi Manny --
>　>　>
>　>　>
>　>　>
>　>　>   Ok, so here's a question that we can ask: Is the
>　>　>   (2,2,2) case
>　>
>　> (2 > inputs, 2 outputs, 2 players) fully reducible to
>　> 2-dimensions? We
>　> know > that in the (2,2,2) case, we can decompose the
>　> measurements into
>　>
>　> > two-dimensional blocks. However the states may not respect
>　> > that block
>　> > structure. A good first step might be to determine whether
>　> > states that
>　> > don't respect the block structure give us any less randomness
>　> > than
>　>

> > those > that do. Do you think that’s a good question, or is it
> > already
> > answered? > -Carl
> >
> > >
> > >
> > > ___________
> > > Carl A. Miller
> > > Mathematician, Computer Security Division
> > > National Institute of Standards and Technology
> > > Gaithersburg, MD
> > >
> > >
> > >
> > >
> > >
> > > On 7/20/17, 4:55 PM, "Emanuel Knill"
> > > <knill@boulder.nist.gov>
> >
> > wrote: >
> >
> > > Scott and Yi-Kai: If you would like to continue to
> > > be cc'ed
> >
> > for > this thread, let me know. Otherwise I'll narrow it
> > to Carl,
> > Yanbao > and Peter next time.
> >
> > >
> > >
> > > I'll skip to the relevant part: For rigidity you
> > > probably
> >
> > need \nu > extremal rather than just on the boundary. At
> > such a
> > \nu, the > side-information operators are all
> > proportional to
> > each other, so > the direct, classical-side-information
> > calculation for
> > available > randomness works, which is what you are referring
> > to? The
> > QEF must be a > linear constraint on the values of (v_{ij})=(Tr
> > [
> > \rho_{ij}^(1 +\beta)] / > Tr [\rho^(1+beta)]) over all
> > possible
> > (\rho_{ij}). That is QEF.v/4\leq > 1. The expectation of -log
> > QEF (over
> > settings and outcomes) at \nu > presumably can approach the
> > available
> > randomness, but usually only as the > power beta goes to zero.
> > (I tried
> > to put in the adjustment factor for > uniform settings choices
> > for your
> > convention, assuming settings are given > away, but may have
> > misplaced
> > it.) I am curious as to whether it really is > simpler to find
> > good QEFs

> > at finite beta for extremal rather than general > nu.
> >
> > >
> > >
> > > Manny
> >
> >
> >
> >
>
>
>
>
>