Robust Interior Point Methods and FR for Key Rate Computation in Quantum Key Distribution

Henry Wolkowicz
Dept. Comb. and Opt., Univ. of Waterloo, Canada

(joint with: Hao Hu, Jiyoung (Haesol) Im, Jie Lin, Norbert Lütkenhaus)

Mon. April 5, 2021, 15:30 CEST
At: One World Optimization Seminar

Motivation/Outline

- find reliable, efficient numerical method for calculating key rates for quantum key distribution (QKD) protocols
- Currently: ill-posed models; i.e., we want to (minimize)

  find reliable provable lower bound

  for the convex relative entropy: $\operatorname{trace} \rho \log \rho - \sigma \log \rho$

  $\sigma, \rho \succeq 0$ (positive semidefinite matrices), even though singular (opt. currently on boundary of SDP cone)

regulariz. using FACIAL REDUCTION, FR; on both constraints and nonlinear objective

- (I) theoretically proven upper and lower bounds with possible approximate FR; high precision
- (II) (Gauss-Newton) interior point approach on regularized problem; (originally singularity degree ONE>0)
- avoid current perturbation approach to get $\rho \succ 0$ (pos. def.)

QKD Background (Details in References)

- Quantum key distribution, QKD: the art of distributing secret keys between two honest parties, traditionally known as Alice and Bob;
- secret key rate (number of bits of secret key obtained per exchange of quantum signal) calculation is at the core of a security proof for any QKD protocol;
- calculation is a convex minimization (lower bound) problem, s.t. constraints to detect presence of any third party (Eve eavesdropping); fundamentally: security comes from the Heisenberg uncertainty principle as eavesdropping means detectable disturbances so Alice and Bob can detect presence of Eve;
- even with a quantum computer, a secret key generated by QKD remains secure.

(asymptotic) Key Rate Calculation

Winick, Lütkenhaus, Coles [9]

$$\begin{array}{rll} p^* = & \min_\rho & D(\mathcal{G}(\rho)\|\mathcal{Z}(\mathcal{G}(\rho))) \\ & \text{s.t.} & \Gamma(\rho) = \gamma, \quad (\operatorname{trace}\rho = 1) \\ & & \rho \succeq 0 \qquad \text{(density matrices)} \end{array}$$

Here:

- $D(\delta\|\sigma) = f(\delta,\sigma) = \operatorname{trace}\delta[\log\delta - \log\sigma]$ is the quantum relative entropy;
- $\Gamma : \mathbb{H}^n \to \mathbb{R}^m$ lin. transf., $\quad \Gamma(\rho) = (\operatorname{trace}\Gamma_i\rho) = (\langle\Gamma_i, \rho\rangle)$;
- $\mathbb{H}^n$ linear space Hermitian matrices over $\mathbb{R}$; $\quad \gamma \in \mathbb{R}^m$
- $\mathcal{G}$ and $\mathcal{Z}$ are linear, completely positive maps, CP (here, sums of products $Z_i\rho Z_i^*$)

CP $\mathcal{G}, \mathcal{Z}$; e.g., $\mathcal{G} : \mathbb{H}^n \to \mathbb{H}^k$, $k > n$, $\mathcal{G}(\mathbb{H}^n_+) \subseteq \mathbb{H}^k_+$

e.g. $\mathcal{G}(\rho) = \sum_{j=1}^t K_j\rho K_j^*, \quad \sum_{j=1}^t K_j^* K_j \preceq I$.

Linear Maps $\mathcal{G}, \mathcal{Z}$

Definition ($\mathcal{G} : \mathbb{H}^n \to \mathbb{H}^k$ (Kraus repres.))

$$\mathcal{G}(\rho) := \sum_{j=1}^{\ell} K_j \rho K_j^*,$$

$K_j \in \mathbb{C}^{k \times n}$, $\sum_{j=1}^{\ell} K_j^* K_j \preceq I$; adjoint $\mathcal{G}^*(\delta) := \sum_{j=1}^{\ell} K_j^* \delta K_j$;
Generally $k = i * n > n, i = 2, 3, \ldots;$
and so typically $\mathcal{G}(\rho)$ rank deficient $\forall \rho \succ 0$ (positive definite)

Definition (self-adjoint (projection) $\mathcal{Z} : \mathbb{H}^k \to \mathbb{H}^k$)

$$\mathcal{Z}(\delta) := \sum_{j=1}^{N} Z_j \delta Z_j,$$

$Z_j = Z_j^2 = Z_j^* \in \mathbb{H}_+^k$ and $\sum_{j=1}^{N} Z_j = I_k$

Properties of QKD Problem

Lemma

The linear map $\mathcal{Z}$ *is an orthogonal projection on* $\mathbb{H}^k$ *and* $\text{trace}(\delta) \leq 1, \delta \succ 0$ *implies:*

$$\text{trace}\left(\delta \log \mathcal{Z}(\delta)\right) = \text{trace}\left(\mathcal{Z}(\delta) \log \mathcal{Z}(\delta)\right)$$

$\mathcal{G}$, $\mathcal{Z} \circ \mathcal{G}$ May not Preserve Positive Definiteness

$$\begin{array}{rll} p^* = & \min_\rho & D(\mathcal{G}(\rho) \| \mathcal{Z}(\mathcal{G}(\rho))) \\ & \text{s.t.} & \Gamma(\rho) = \gamma, \\ & & \rho \succeq 0 \qquad \text{(density matrices)} \end{array}$$

Known Properties

$$\min_{\rho,\sigma,\delta} \text{trace}(\delta(\log \delta)) - \text{trace}(\sigma(\log \sigma))$$

quantum relative entropy D is finite under range condition; jointly convex in both δ and σ

Equivalent Formulation

Ready for FR, Facial Reduction (Regularization)

$$
\begin{array}{rll}
p^* = & \min_{\rho,\sigma,\delta} & \operatorname{trace}(\delta(\log \delta)) - \operatorname{trace}(\sigma(\log \sigma)) \\
& \text{s.t.} & \Gamma(\rho) = \gamma \\
& & \sigma = \mathcal{Z}(\delta) \\
& & \delta = \mathcal{G}(\rho) \\
& & \rho, \sigma, \delta \succeq 0.
\end{array}
$$

Our Goal: Final Asymptotic Key Rate

obtained by getting a reliable lower bound of this problem (and then removing the cost of error correction, a constant).

Facial Reduction, FR, Borwein-W. [3], Preliminaries

Slater Constraint Qualification, Strict Feasibility, Stability

Slater: $\exists \hat{\rho} \succ 0 : \Gamma \hat{\rho} = \gamma$

Strong Duality, Stability

Slater is sufficient for strong duality;
equivalent to numerical stability under RHS perturbations;
Slater fails in surprisingly many applications

Advantages of FR

FR can be used to obtain strict feasibility and regularize the problem, and often simultaneously simplify the problem.

current applications: e.g.

hard discrete opt.; (distance geometry); EDM and low rank matrix completion etc ... (recent survey Drusvyatskiy-W. [5])

Facial Reduction, FR, Preliminaries cont...

convex cone: $K : \lambda K \subseteq K, \forall \lambda \geq 0,\ K + K \subset K$,
dual cone: $S^* = \{\phi \in \mathbb{H} : \langle \phi, s \rangle \geq 0,\ \forall s \in S\}$.
convex cone F is a face of a convex cone K, $F \trianglelefteq K$, if

$$x, y \in K, x + y \in F \implies x, y \in F.$$

Faces of the positive semidefinite cone are characterized by the range or nullspace of any element in the relative interior:

Lemma

Let F a convex subset of $\mathbb{H}^n_+$ with $X \in \operatorname{ri} F$ with orthogonal spectral decomposition $X = \begin{bmatrix} P & Q \end{bmatrix} \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} P & Q \end{bmatrix}^*$, with $D \in \mathbb{H}^r_{++}$. Then TFAE:

(i) $F \trianglelefteq \mathbb{H}^n_+$;

(ii) $F = \{Y \in \mathbb{H}^n_+ : \operatorname{range}(Y) \subset \operatorname{range}(X)\}$
$\quad = \{Y \in \mathbb{H}^n_+ : \operatorname{null}(Y) \supset \operatorname{null}(X)\}$;

(iii) $F = P\mathbb{H}^r_+ P^*$; *(iv)* $F = \mathbb{H}^n_+ \cap (QQ^*)^\perp$ *(exposing QQ^*)*

Facial Reduction via Theorem of Alternative

Lemma (theorem of the alternative)

For the feasible constraint system, exactly one of the following statements holds:

1. *there exists* $\rho \succ 0$ *such that* $\Gamma(\rho) = \gamma$ *(Slater);*
2. *there exists* y *(and exposing vector* Z*) such that*

$$0 \neq Z = \Gamma^*(y) \succeq 0 \ , \ \langle \gamma, y \rangle = 0.$$

The matrix $Z = \Gamma^* y$ above is an exposing vector for the feasible set.

Definition (minimal face)

K a closed convex cone; $S \subseteq K$ a convex set; then $\mathrm{face}(S) \unlhd K$ is the *minimal face*, the intersection of all faces of K that contain S.

First (Partial) FR Step on S_R (Analytical/Accurate)

affine manifold constraint is divided into two sets

observable, reduced density operator constraint sets, $S_O \cap S_R$; with Kronecker product, $\otimes$

$$S_O = \left\{ \rho \succeq 0 \,:\, \langle P_s^A \otimes P_t^B, \rho \rangle = p_{st}, \, \forall s, t \right\},$$

$$\begin{array}{rcll} S_R & = & \{ \rho \succeq 0 \,:\, \mathrm{trace}_B(\rho) = \rho_A \} & \text{(partial trace)} \\ & = & \left\{ \rho \succeq 0 \,:\, \langle \Theta_j \otimes \mathrm{I}_B, \rho \rangle = \theta_j, \, \forall j = 1, \ldots, m_R \right\}, & \end{array}$$

where

data $\theta_j = \langle \Theta_j, \rho_A \rangle$; and $\rho_A \in \mathbb{H}_+^{n_A}$ often singular
$\{\Theta_j\}$ orthonormal basis system A.

Let range $P = \mathrm{range}\, \rho_A \subsetneq \mathbb{H}^{n_A}$, $P^*P = \mathrm{I}_r$, and let $V = P \otimes \mathrm{I}_B$.
Then $\boxed{\mathrm{FR}: \; \rho \in S_R \implies \rho = VRV^*, \text{ for some } R \in \mathbb{H}_+^{r \cdot n_B}}$

FR on the Objective Function

Lemma (useful equivalent form for entropy function)

Let $Y = VRV^* \in \mathbb{H}_+$, $R \succ 0$ *be the compact spectral decomposition of* Y *with* $V^*V = I$. *Then*

$$\operatorname{trace}(Y \log Y) = \operatorname{trace}(R \log R).$$

Proof.

We obtain a unitary matrix $U = \begin{bmatrix} V & P \end{bmatrix}$ by completing the basis. Then $Y = UDU^*$, where $D = \operatorname{BlkDiag}(R, 0)$. We conclude, with $0 \cdot \log 0 = 0$, that

$\operatorname{trace} Y \log Y = \operatorname{trace} D \log D = \operatorname{trace} R \log R$. □

Exposing Vectors Analytically; Spectral Decomposition

We use the following simple result to obtain the exposing vectors of the minimal face in the problem analytically, i.e., we find the matrices V with orthonormal columns.

Lemma (analytic FR)

Let $\mathcal{C} \subseteq \mathbb{H}^n_+$ be a given closed convex set with nonempty interior. Let $Q_i \in \mathbb{H}^{k\times n}$, $i = 1, \ldots, t$, be given matrices. Define the linear map $\mathcal{A} : \mathbb{H}^n \to \mathbb{H}^k$ and matrix V by

$$\mathcal{A}(X) = \sum_i^t Q_i X Q_i^*, \quad \operatorname{range}(V) = \operatorname{range}\left(\sum_{i=1}^t Q_i Q_i^*\right).$$

Then the minimal face,

$$\operatorname{face}(\mathcal{A}(\mathcal{C})) = V\mathbb{H}^r_+ V^*.$$

Obtain the Minimal Faces, $V\mathbb{H}_+V^*$

$$
\begin{array}{rcl}
\rho & = & V_\rho R_\rho V_\rho^* \in \mathbb{H}_+^n, \quad R_\rho \in \mathbb{H}_+^{n_\rho} \\
\delta & = & V_\delta R_\delta V_\delta^* \in \mathbb{H}_+^k, \quad R_\delta \in \mathbb{H}_+^{k_\delta} \\
\sigma & = & V_\sigma R_\sigma V_\sigma^* \in \mathbb{H}_+^k, \quad R_\sigma \in \mathbb{H}_+^{k_\sigma}
\end{array}
$$

Define the linear maps

$$
\begin{array}{llcrcl}
\Gamma_V: & \mathbb{H}_+^{n_\rho} \to \mathbb{R}^m & \text{by} & \Gamma_V(R_\rho) & = & \Gamma(V_\rho R_\rho V_\rho^*), \\
\mathcal{G}_V: & \mathbb{H}_+^{n_\rho} \to \mathbb{H}_+^k & \text{by} & \mathcal{G}_V(R_\rho) & = & \mathcal{G}(V_\rho R_\rho V_\rho^*), \\
\mathcal{Z}_V: & \mathbb{H}_+^{k_\delta} \to \mathbb{H}_+^k & \text{by} & \mathcal{Z}_V(R_\delta) & = & \mathcal{Z}(V_\delta R_\delta V_\delta^*).
\end{array}
$$

Substitute with Linear Mapping $\mathcal{V}_\delta(\cdot) := V_\delta \cdot V_\delta^*$

Equivalent Formulation

$$
\begin{array}{ll}
\min & \operatorname{trace}(R_\delta \log(R_\delta)) - \operatorname{trace}\left(R_\sigma \log(R_\sigma)\right) \\
\text{subject to:} & \Gamma_V(R_\rho) = \gamma \\
& \mathcal{V}_\sigma(R_\sigma) - \mathcal{Z}_V(R_\delta) = 0 \\
& \mathcal{V}_\delta(R_\delta) - \mathcal{G}_V(R_\rho) = 0 \\
& R_\rho, R_\sigma, R_\delta \succeq 0.
\end{array}
$$

After Rotation and Substitution; final model (QKD)

$$
\begin{array}{rll}
p^* = & \min & f(\rho) = \operatorname{trace}\left(\widehat{\mathcal{G}}(\rho)(\log \widehat{\mathcal{G}}(\rho))\right) \\
& & \qquad - \operatorname{trace}\left(\widehat{\mathcal{Z}}(\rho) \log \widehat{\mathcal{Z}}(\rho)\right) \\
& \text{subject to:} & \Gamma_V(\rho) = \gamma_V \\
& & \rho \in \mathbb{H}_+^{n_\rho},
\end{array}
$$

Slater holds; smaller regularized problem;
positive definiteness preserved in obj. fn

Derivatives

Theorem (Derivatives of regularized objective)

Let $\rho \succ 0$*. The gradient of f is*

$$\nabla f(\rho) = \boxed{\widehat{\mathcal{G}}^*(\log[\widehat{\mathcal{G}}(\rho)]) + \widehat{\mathcal{G}}^*(I)} - \boxed{\widehat{\mathcal{Z}}^*(\log[\widehat{\mathcal{Z}}(\rho)]) + \widehat{\mathcal{Z}}^*(I)}.$$

The Hessian in direction $\Delta\rho$ *is (1st order info)*

$$\begin{aligned}\nabla^2 f(\rho)(\Delta\rho) &= \boxed{\widehat{\mathcal{G}}^*(\log'[\widehat{\mathcal{G}}(\rho)](\widehat{\mathcal{G}}(\Delta\rho))} - \\ &\quad \boxed{\widehat{\mathcal{Z}}^*(\log'[\widehat{\mathcal{Z}}(\rho)](\widehat{\mathcal{Z}}(\Delta\rho))}\end{aligned}$$

Theorem (subdifferential)

Let $\{\rho_i\}_i \subseteq \mathbb{S}^{n_\rho}_{++}$ *with* $\rho_i \to \bar{\rho}$*. If we have the convergence* $\lim_i \nabla f(\rho_i) = \phi$*, then*

$$\phi \in \partial f(\bar{\rho}).$$

Part II: Opt. Cond.; Bounds; GN Int. Pt. Method

- Duality, and primal-dual optimality conditions with null-space representation
- Derive a Gauss-Newton search direction for the nonlinear SDP (with exact primal and dual feasibility possible)
- derive provable lower and upper bounds
- Empirics

Facially Reduced (Regularized) Nonlinear SDP

$$\begin{array}{rccl} p^* = & \min & f(\rho) & \text{(regularized relative entropy)} \\ & \text{subject to:} & \Gamma_V(\rho) = \gamma_V & \text{(FR constraints)} \\ & & \rho \in \mathbb{H}_+^{n_\rho} & \text{(smaller SDP constr.)} \end{array}$$

Duality/Optimality

Theorem (Basic Duality/Opt)

1. *Lagrangian* $L(\rho, y) = f(\rho) + \langle y, \Gamma_V \rho - \gamma_V \rangle$, $y \in \mathbb{R}^{m_V}$.
2. *Strong Duality*

$$\begin{aligned} p^* &= \max_y \min_{\rho \succeq 0} L(\rho, y) \\ &= d^* = \max_{Z \succeq 0, y} \left(\min_\rho (L(\rho, y) - \langle Z, \rho \rangle) \right) \end{aligned}$$

and d^* *is attained for some* $(y, Z) \in \mathbb{R}^{m_V} \times \mathbb{H}_+^{n_\rho}$.

3. *p-d pair* $(\rho, (y, Z))$, *with* $\partial f(\rho) \neq \emptyset$, *is optimal iff*

$$\begin{array}{rcll} 0 & \in & \partial f(\rho) + \Gamma_V{}^* y - Z & \text{(dual feasibility)} \\ 0 & = & \Gamma_V \rho - \gamma_V & \text{(linear primal feasibility)} \\ 0 & = & \langle \rho, Z \rangle & \text{(complementary slackness)} \\ 0 & \preceq & \rho, Z & \text{(SDP primal feasibility).} \end{array}$$

Moreover, $\Gamma_V^* y \succeq 0$, $\langle y, \gamma_V \rangle < 0$, *for some* y, *implies infeas.*

Nullspace Representation/Residuals

Definition (nullspace representation)

$\hat{\rho} \in \mathbb{H}^{n_\rho}$ feasible point for $\Gamma_V(\cdot) = \gamma_V$.
$\mathcal{N}^* : \mathbb{R}^{n_\rho^2 - m_V} \to \mathbb{H}^{n_\rho}$ injective linear map in adjoint form so that we have the nullspace representation for the residual:

$$F_\mu^p = \Gamma_V \rho - \gamma_V \iff F_\mu^p = \mathcal{N}^*(v) + \hat{\rho} - \rho, \text{ for some } v.$$

Perturbed Optimality Conditions/Residuals

(i) dual feas.; (ii) primal feas.; (iii) perturbed compl. slack.

$$F_\mu(\rho, v, y, Z) = \begin{bmatrix} F_\mu^d \\ F_\mu^p \\ F_\mu^c \end{bmatrix} = \begin{bmatrix} \nabla_\rho f(\rho) + {\Gamma_V}^* y - Z \\ \mathcal{N}^* v + \hat{\rho} - \rho \\ Z\rho - \mu I \end{bmatrix} = 0, \quad \rho, Z \succ 0.$$

EXACT p-d feas if updated as: $\rho \leftarrow \Delta v$; $Z \leftarrow \Delta\rho, \Delta y$;
after a steplength $= 1$ is taken, exact p.f. is maintained.
exact dual feas. for Z is key for lower bound

Projected Gauss-Newton P-D I-P Method

Linearized System for GN Direction; OVERDETERMINED

$$F'_\mu d_{GN} = \begin{bmatrix} \nabla^2 f(\rho)\Delta\rho + \Gamma_V{}^*\Delta y - \Delta Z \\ \mathcal{N}^*(\Delta v) - \Delta\rho \\ Z\Delta\rho + \Delta Z\rho \end{bmatrix} \approx -F_\mu.$$

From First Block (for backsubstitution)

$$\begin{aligned} \Delta Z &= F_\mu^d + \nabla^2 f(\rho)\Delta\rho + \Gamma_V{}^*\Delta y \\ &= F_\mu^d + \nabla^2 f(\rho)(F_\mu^p + \mathcal{N}^*(\Delta v)) + \Gamma_V{}^*\Delta y. \end{aligned}$$

From Second Block (for backsubstitution)

$$\Delta\rho = F_\mu^p + \mathcal{N}^*(\Delta v).$$

Now substitute $\Delta Z, \Delta\rho$ into third block.

Projected GN direction

$d_{GN} = (\Delta v \quad \Delta y)$ (backsubst. for $\Delta\rho, \Delta Z$)

found from the least squares solution of (OVERDETERMINED)

$$\left[Z\mathcal{N}^*(\Delta v) + \nabla^2 f(\rho)\mathcal{N}^*(\Delta v)\rho\right] + [\Gamma_V{}^*\Delta y \rho] \\ = -F_\mu^c - ZF_\mu^p - \left(F_\mu^d + \nabla^2 f(\rho) F_\mu^p\right)\rho$$

(Uses Hessian acting on a vector: $\nabla^2 f(\rho) : \mathbb{H} \to \mathbb{H}$)

Initialize: $\hat{\rho} \succ 0$, $\mu \in \mathbb{R}_{++}$, $\eta \in (0,1)$
WHILE: stopping criteria is not met
solve for $(\Delta v, \Delta y)$
$\Delta\rho = F_\mu^p + \mathcal{N}^*(\Delta v)$
$\Delta Z = F_\mu^d + \nabla^2 f(\rho)(F_\mu^p + \mathcal{N}^*(\Delta v)) + \Gamma_V{}^*\Delta y$
choose steplength α
$(\rho, y, Z) \leftarrow (\rho, y, Z) + \alpha(\Delta\rho, \Delta y, \Delta Z)$
$\mu = \text{trace}(\rho Z)/n$; $\mu \leftarrow \eta\mu$
ENDWHILE

Implementation Details

Sparse Nullspace Representation

We use a matrix representation M for Γ and a row and column permutation to get a well-conditioned near triangular basis matrix B. nullspace representation:

$$\hat{r} = \text{Hvec}\,\hat{\rho};\ \Gamma_V\hat{\rho} = M\hat{r}(cp) = \gamma_V,\ M = \begin{bmatrix} B & E \end{bmatrix},\ N^* = \begin{bmatrix} B^{-1}E \\ -I \end{bmatrix};$$

Optimal Diagonal Preconditioning, [4]

$d_i = \|F_\mu^{c\prime}(e_i)\|$, for unit vectors e_i; column precondition using

$$F_\mu^{c\prime} \leftarrow F_\mu^{c\prime}\mathrm{Diag}\,(d)^{-1}$$

MATLAB: $d_{GN} = ((F_\mu^{c\prime}/\mathrm{Diag}\,(d))\backslash RHS)./d$
Performed exceptionally well; problems are VERY ill-conditioned.

Upper Bounds

Evaluate f at Feasible ρ; Iterative Refinement if Needed

if approximate linear feasibility $\Gamma_V \hat{\rho} \approx \gamma_V$, we apply iterative refinement by finding the projection Let $\hat{\rho} \succ 0$, $F^p_\mu = \Gamma_V \hat{\rho} - \gamma_V$. Then

$$\rho = \hat{\rho} - {\Gamma_V}^\dagger F^p_\mu = \operatorname{argmin}_\rho \left\{ \frac{1}{2} \|\rho - \hat{\rho}\|^2 \;:\; \Gamma_V \rho = \gamma_V \right\},$$

where we denote ${\Gamma_V}^\dagger$, generalized inverse. If $\rho \succeq 0$, then $p^* \leq f(\rho)$.

EXACT Primal Feasibility

In our tests we take a Newton step quite early, and maintain exact primal feasibility (no roundoff error buildup) for the further iterations.

Lower Bound from Weak Duality

$\rho \succ 0, Z \succ 0$ in Interior Point Algorithm

The gradients exist at $\rho \succ 0$; we can verify dual feasibility.

Corollary (Lower Bound for FR problem from EXACT Dual Feas.)

$\hat{\rho}, \hat{y}$ primal-dual iterate; $\hat{\rho} \succ 0$. Set $\boxed{\bar{Z} = \nabla f(\hat{\rho}) + \Gamma_V{}^* \hat{y}}$.
If $\bar{Z} \succeq 0$, then lower bound is:

$$p^* \geq f(\hat{\rho}) + \langle \hat{y}, \Gamma_V \hat{\rho} - \gamma_V \rangle - \langle \hat{\rho}, \bar{Z} \rangle.$$

Proof.

Consider the dual problem
$d^* = \max_{y, Z \succeq 0} \min_{\rho \in \mathbb{H}^{n_\rho}} L(\rho, y) - \langle Z, \rho \rangle$. Dual feasibility implies:

$$\bar{Z} \succeq 0,\ \nabla f(\hat{\rho}) + \Gamma_V{}^* \hat{y} - \bar{Z} = 0 \implies \hat{\rho} \in \operatorname{argmin}_\rho L(\rho, \hat{y}) - \langle \bar{Z}, \rho \rangle.$$

Result follows from weak duality. □

Numerics; GN vs FW with/without FR

Problem Data		Gauss-Newton		FW (FR)		FW (no FR)		cvxquad (FR)	
protocol	size	gap	time	gap	time	gap	time	gap	time
ebBB84	(4,16)	6.0e-13	0.4	1.0e-04	86.9	1.2e-04	93.9	5.5e-01	194
ebBB84	(4,16)	1.2e-12	0.3	1.7e-04	96.8	1.3e-04	110.5	5.4e-01	1938
ebBB84	(4,16)	1.1e-12	0.2	1.6e-04	86.5	2.2e-04	112.0	5.7e-01	1979
ebBB84	(4,16)	4.2e-13	0.2	2.2e-04	88.6	2.2e-04	111.9	6.3e-01	523
pmBB84	(8,32)	5.5e-13	0.2	3.1e-05	1.3	6.5e-04	1.6	5.3e-01	158
pmBB84	(8,32)	6.1e-13	0.2	1.6e-04	1.1	3.8e-04	93.0	5.2e-01	207
pmBB84	(8,32)	6.3e-13	0.2	5.5e-05	1.1	3.0e-04	112.3	5.6e-01	299
pmBB84	(8,32)	1.3e-12	0.2	2.6e-04	1.1	1.3e-03	87.0	5.9e-01	188
mdiBB84	(48,96)	7.9e-13	0.9	9.6e-05	1.6	5.4e-04	120.9	1.8e-01	570
mdiBB84	(48,96)	1.4e-12	0.7	5.5e-05	101.2	6.6e-04	119.7	2.4e-01	585
mdiBB84	(48,96)	5.7e-13	0.9	1.5e-04	101.9	1.7e-03	439.3	3.1e-01	584
mdiBB84	(48,96)	9.2e-13	0.8	1.8e-04	100.0	2.2e-03	441.3	3.7e-01	558

Table: Numerical Report: Gauss-Newton, Frank-Wolfe (FW), cvxquad

- GN performs significantly better for both accuracy and running time
- only three protocols (each with four different parameter settings);
  that is all that cvxquad could handle;
- FW is significantly improved by using our new FR

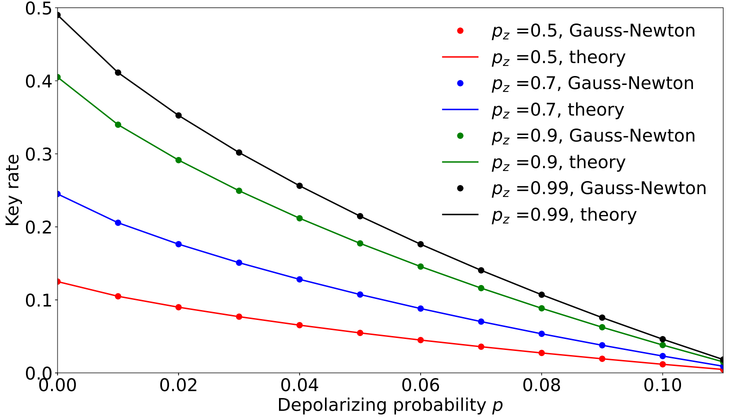
Larger Numerics; cvxquad Failed

Problem Data		Gauss-Newton		FW (FR)		FW (no FR)	
protocol	**size**	**gap**	**time**	**gap**	**time**	**gap**	**time**
TFQKD	(12,24)	5.9e-13	1.1	2.6e-09	1.9	1.6e-03	364.1
TFQKD	(12,24)	1.2e-12	0.8	3.8e-09	1.5	5.6e-04	369.1
TFQKD	(12,24)	3.2e-13	0.8	4.0e-09	1.3	1.7e-04	4.1
DMCV	(44,176)	2.7e-09	1326.1	2.4e-06	2808.4	3.4e-06	4933.9
DMCV	(44,176)	2.7e-09	1377.4	1.3e-06	974.2	2.5e-06	1281.2
DMCV	(48,192)	3.1e-09	1807.1	2.7e-06	3167.4	5.1e-06	5407.5
DMCV	(48,192)	3.2e-09	2110.6	2.6e-06	979.8	2.0e-06	1756.3
dprBB84	(12,48)	4.9e-13	1.3	3.8e-06	88.0	9.4e-05	123.0
dprBB84	(24,96)	1.0e-12	12.1	6.2e-06	15.9	3.6e-06	31.1
dprBB84	(36,144)	5.0e-13	69.3	6.5e-04	8.8	2.1e-02	30.1
dprBB84	(48,192)	1.1e-12	325.5	4.4e-05	17.1	9.8e-04	181.9

Table: Numerical Report: Gauss-Newton, Frank-Wolfe (FW)

- GN performs significantly better again
- FW does significantly better with our new FR again

GN is Exactly Analytical (Protocol mdiBB84)



The • are the lower bounds from GN; they coincide exactly with the analytical values on the curves.
This meets with the empirical evidence of gaps $\approx 10^{-12}$

Conclusion

- regularized the key rate calculation using FACIAL REDUCTION on both constraints and nonlinear (relative entropy) objective function over the Hermitians (complex);
- provided theoretically proven upper and lower bounds with high precision
- derived robust (Gauss-Newton) interior point approach on regularized problem
  - avoids current perturbation approach to get $\rho \succ 0$;
  - avoids roundoff error from backsubstitution steps;
  - attains exact primal feasibility during iterations
  - uses exact dual feasibility steps to improve on lower bounds

References I

BORWEIN, J., AND WOLKOWICZ, H.
Characterization of optimality for the abstract convex program with finite-dimensional range.
J. Austral. Math. Soc. Ser. A 30, 4 (1980/81), 390–411.

BORWEIN, J., AND WOLKOWICZ, H.
Facial reduction for a cone-convex programming problem.
J. Austral. Math. Soc. Ser. A 30, 3 (1980/81), 369–380.

BORWEIN, J., AND WOLKOWICZ, H.
Regularizing the abstract convex program.
J. Math. Anal. Appl. 83, 2 (1981), 495–530.

DENNIS JR., J., AND WOLKOWICZ, H.
Sizing and least-change secant methods.
SIAM J. Numer. Anal. 30, 5 (1993), 1291–1314.

DRUSVYATSKIY, D., AND WOLKOWICZ, H.
The many faces of degeneracy in conic optimization.
Foundations and Trends® in Optimization 3, 2 (2017), 77–170.

FAYBUSOVICH, L., AND ZHOU, C.
Long-step path-following algorithm in quantum information theory: Some numerical aspects and applications, 2020.

References II

GEORGE, I., LIN, J., AND LÜTKENHAUS, N.
Numerical calculations of the finite key rate for general quantum key distribution protocols.
Physical Review Research 3 (2021), 013274.

LIN, J., UPADHYAYA, T., AND LÜTKENHAUS, N.
Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution.
Phys. Rev. X 9 (2019), 041064.

WINICK, A., LÜTKENHAUS, N., AND COLES, P.
Reliable numerical key rates for quantum key distribution.
Quantum 2 (Jul 2018), 77.

Thanks for your attention!

Robust Interior Point Methods and FR for Key Rate Computation in Quantum Key Distribution

Henry Wolkowicz
Dept. Comb. and Opt., Univ. of Waterloo, Canada

(joint with: Hao Hu, Jiyoung (Haesol) Im, Jie Lin, Norbert Lütkenhaus)

Mon. April 5, 2021, 15:30 CEST
At: One World Optimization Seminar