Robust Interior Point Method for Quantum Key Distribution Rate Computation

Hao Hu [1] Haesol Im [2] Jie Lin [2] Norbert Lütkenhaus [2] Henry Wolkowicz [2]

[1]Clemson University [2]University of Waterloo

Introduction

Motivation: Why do we compute key rate for QKD ?

Quantum Key Distribution (QKD)

A secure, quantum-resistant communication mechanism used for **sharing secrets** over a public channel between two parties

Example

- 10 (qu)bits used in QKD
  5 (qu)bits are used to form the secret → key rate $\frac{5}{10} = \frac{1}{2}$
  Under the presence of Eve who disrupts the communication → key rate goes down to $\frac{1}{10}$

Question

Q. How many (qu)bits need to be used get n bits of secret key under Eve's attack?

A. Model using a convex optimization problem [Ref 2]

Optimization Problem: Objective & Constraint

$$(\text{QKD}) \qquad p^* := \min_{\rho}\{f(\rho) \ : \ \Gamma(\rho) = \gamma, \ \rho \succeq 0\}$$

1. **Objective Function** : composite of quantum relative entropy function and two linear maps
   After simplification,
   $$f(\rho) \ = \ \operatorname{trace}(\mathcal{A}(\rho)\log\mathcal{A}(\rho) - \mathcal{B}(\rho)\log\mathcal{B}(\rho)),$$
   where $\mathcal{A}(\rho) = \sum_j A_j\rho A_j^*$, and $\mathcal{B}(\rho) = \sum_j B_j\rho B_j^*$.
2. **Constraint**: spectrahedron
   $$\{\rho \in \mathbb{H}^n_+ \ : \ \Gamma(\rho) = \gamma\},$$
   where $(\Gamma(\rho))_i = \operatorname{trace}(\Gamma_i\rho) = \gamma_i, \forall i = 1,\ldots,m,$ with $\Gamma_i \in \mathbb{H}^n$ and $\gamma_i \in \mathbb{R}$.

Difficulties with the Model: Failure of Regularity

1. Constraint: $\{\rho \in \mathbb{H}^n_+ \ : \ \Gamma(\rho) = \gamma\}$
   There is no positive definite ρ → Slater condition fails
   - Strong duality may not hold
   - Small noise could yield large error

   Remedy → facial reduction
2. Objective: $\operatorname{trace}(\mathcal{A}(\rho)\log\mathcal{A}(\rho) - \mathcal{B}(\rho)\log\mathcal{B}(\rho))$
   There are no positive definite $\mathcal{A}(\rho), \mathcal{B}(\rho)$ → Cannot differentiate $f(\rho)$

   ex) $\rho = \begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix} \succ 0, \quad \mathcal{A}(\rho) = \sum_j A_j\rho A_j^* = \begin{bmatrix} 1/2 & 0 & 0 \\ 0 & 1/2 & 0 \\ 0 & 0 & 0 \end{bmatrix} \succeq 0$

   Remedy → facial reduction

Our Approach

1. Strong Reformulation: *Two types* of facial reduction
   - Facial reduction on the constraint set
   - Facial reduction on the objective (new!)
2. Good Choice of Algorithm: Solve the reformulated model using a *stable* interior point method

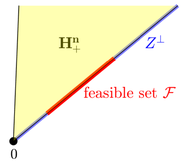
Reformulation

Facial Reduction Towards Slater: Constraint $\{\rho \in \mathbb{H}^n_+ \ : \ \Gamma(\rho) = \gamma\}$

Every face F of $\mathbb{H}^n_+$ is exposed, i.e., $\exists Z \in \mathbb{H}^n_+, V \in \mathbb{C}^{n\times r}, r \le n$, such that

$$F = \mathbb{H}^n_+ \cap Z^\perp = V\mathbb{H}^r_+V^*$$

Geometric view: restriction on a slice $(V\mathbb{H}^r_+V^*)$ of $\mathbb{H}^n_+$



Find a matrix V with orthonormal columns, feasible point $\rho = VRV^* \in V\mathbb{H}^r_+V^*$,

$$\gamma_i = \operatorname{trace}(\Gamma_i\rho) = \operatorname{trace}(\Gamma_i VRV^*) = \operatorname{trace}(V^*\Gamma_i VR)$$

Important: there exists a positive *definite* R satisfying the equality system → Slater condition holds!

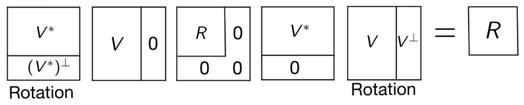
Facial Reduction Towards Differentiability: Objective $f(\rho)$

First term $\operatorname{trace}(\mathcal{A}(\rho)\log\mathcal{A}(\rho))$

$$\text{By facial reduction,} \qquad \mathcal{A}(\rho) = V_AR_AV_A^*, \ R_A \succ 0$$

$$\operatorname{trace}\mathcal{A}(\rho)\log\mathcal{A}(\rho) = \operatorname{trace}\left(V_AR_AV_A^*\right)\log\left(V_AR_AV_A^*\right) = \operatorname{trace}R_A\log R_A$$

Interpretation: Rotation



Second term $\operatorname{trace}(\mathcal{B}(\rho)\log\mathcal{B}(\rho))$

$$\text{Similarly via facial reduction, } \mathcal{B}(\rho) = V_BR_BV_B^*, \ R_B \succ 0 \implies \operatorname{trace}R_B\log R_B$$

Reduced Objective

$$\begin{aligned} f(\rho) \ &= \ \operatorname{trace}(\mathcal{A}(\rho)\log\mathcal{A}(\rho) - \mathcal{B}(\rho)\log\mathcal{B}(\rho)) \\ &\quad \downarrow V_AR_AV_A^* = \mathcal{A}(\rho) \implies R_A = V_A^*\mathcal{A}(\rho)V_A =: \widehat{\mathcal{A}}(\rho) \\ &\quad \downarrow V_BR_BV_B^* = \mathcal{B}(\rho) \implies R_B = V_B^*\mathcal{B}(\rho)V_B =: \widehat{\mathcal{B}}(\rho) \\ \widehat{f}(\rho) \ &= \ \operatorname{trace}(\widehat{\mathcal{A}}(\rho)\log\widehat{\mathcal{A}}(\rho)) - \operatorname{trace}(\widehat{\mathcal{B}}(\rho)\log\widehat{\mathcal{B}}(\rho)) \end{aligned}$$

Facially Reduced Model: Reduction = Redefining Problem Data!

$$\begin{aligned} &(\text{QKD}) \qquad p^* := \min_{\rho}\{f(\rho) \ : \ \Gamma(\rho) = \gamma, \ \rho \succeq 0\} \\ &\Downarrow \qquad \text{substitute } \rho \leftarrow V_\rho R_\rho V_\rho^*, \ \mathcal{A}(\rho) \leftarrow V_AR_AV_A^*, \ \mathcal{B}(\rho) \leftarrow V_BR_BV_B^* \\ &(\text{QKD}) \qquad p^* := \min_{R_\rho}\{\widehat{f}(R_\rho) \ : \ \widehat{\Gamma}(R_\rho) = \gamma, \ R_\rho \succeq 0\} \\ &\Downarrow \qquad \text{replace } \rho \leftarrow R_\rho, \ \ f(\rho) \leftarrow \widehat{f}(\rho) \\ &(\text{QKD}) \qquad p^* := \min_{\rho}\{f(\rho) \ : \ \Gamma(\rho) = \gamma, \ \rho \succeq 0\} \end{aligned}$$

Algorithm

Algorithm: Gauss-Newton Method

Optimality Conditions

$$\begin{aligned} &\text{dual feasibility} && : F_\mu^d = \nabla_\rho f(\rho) + \Gamma^*(y) - Z = 0 \\ &\text{primal feasibility} && : F_\mu^p = \Gamma(\rho) - \gamma = 0 \\ &\text{perturbed complementarity} && : F_\mu^c = Z\rho - \mu I = 0, \ Z, \rho \succ 0. \end{aligned}$$

Using the optimality conditions, form

$$\|F_\mu(\rho,y,Z)\|^2 = \|F_\mu^d(\rho,y,Z)\|_F^2 + \|F_\mu^p(\rho)\|_2^2 + \|F_\mu^c(\rho,Z)\|_F^2.$$

Solve the nonlinear least squares problem

$$\min_{\rho,Z\succ 0,y} \ \frac{1}{2}\|F_\mu(\rho,y,Z)\|^2$$

If we find (ρ,y,Z) satisfying $\|F_0(\rho,y,Z)\|^2 = 0 \implies$ Optimality
Note: nonlinear overdetermined least squares problem!

Gauss-Newton direction, d_{GN} = least squares solution of the linearization

$$F_\mu' d_{GN} \approx -F_\mu \ \text{ i.e., } \begin{bmatrix} \nabla^2 f(\rho)\Delta\rho + \Gamma^*(\Delta y) - \Delta Z \\ \mathcal{N}(\Delta v) - \Delta\rho \\ Z\Delta\rho + \Delta Z\rho \end{bmatrix} = - \begin{bmatrix} F_\mu^d \\ F_\mu^p \\ F_\mu^c \end{bmatrix}.$$

We use *projected* Gauss-Newton direction for computational efficiency (e.g., ΔZ is eliminated)

Bounding: Our Approach

The main goal of (QKD): Obtain a provable, tight lower bound to the optimal value p^*

The dual problem

$$d^* = \max_{y,Z\succeq 0}\min_{\rho\in\mathbb{H}^n} L(\rho,y) - \langle Z,\rho\rangle.$$

We can always find a dual feasible point that minimizes the dual functional

$$\bar{Z} = \nabla f(\hat{\rho}) + \Gamma^*(\hat{y}) \succeq 0.$$

Lower Bound via Lagarangian dual

$$\begin{aligned} p^* \ &= \ d^* && \text{(strong duality)} \\ &\ge \ \min_\rho L(\rho,y) - \langle\bar{Z},\rho\rangle && (\bar{Z} = \nabla f(\hat{\rho}) + \Gamma^*(\hat{y}) \succeq 0) \\ &= \ f(\hat{\rho}) + \langle\hat{y},\Gamma(\hat{\rho}) - \gamma\rangle - \langle\hat{\rho},\bar{Z}\rangle && (\hat{\rho} = \operatorname{argmin}_\rho L(\rho,\hat{y}) - \langle\bar{Z},\rho\rangle) \end{aligned}$$

Upper Bound via Projection

$$\bar{\rho} = \operatorname{argmin}_\rho\left\{\frac{1}{2}\|\rho - \hat{\rho}\|^2 \ : \ \Gamma(\rho) = \gamma\right\}, \quad \bar{\rho} \succeq 0 \implies p^* \le f(\bar{\rho}).$$

References

- Ref 1. Hao Hu, Haesol Im, Jie Lin, Nobert Lütkenhaus, and Henry Wolkowicz.
  Robust Interior Point Method for Quantum Key Distribution Rate Computation (Quantum 6, Vol 6, 2022)
- Ref 2. Adam Winick, Norbert Lütkenhaus, and Patrick J. Coles.
  Reliable numerical key rates for quantum key distribution (Quantum vol 2, p.77, 2018)