AFRL-RV-PS-
TR-2022-0030

AFRL-RV-PS-
TR-2022-0030

ALGORITHM DESIGN FOR OPTIMIZATION IN COMMUNICATION AND NAVIGATION

Yuyuan Ouyang

Clemson University
Division of Research
201 Sikes Hall
Clemson, SC 29634-0001

31 Jan 2022

Final Report

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

AIR FORCE RESEARCH LABORATORY
Space Vehicles Directorate
3550 Aberdeen Ave SE
AIR FORCE MATERIEL COMMAND
KIRTLAND AIR FORCE BASE, NM 87117-5776

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research which is exempt from public affairs security and policy review in accordance with AFI 61-201, paragraph 2.3.5.1. This report is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RV-PS-TR-2022-0030 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

//SIGNED//

THOMAS LOVELL
Program Manager

//SIGNED//

ANDREW SINCLAIR
Tech Advisor, Space Control Technologies Branch

//SIGNED//

JOHN BEAUCHEMIN
Chief Engineer, Spacecraft Technology Division
Space Vehicles Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

Approved for public release; distribution unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
31-01-2022	Final Report	14 Aug 2019 – 31 Jan 2022

4. TITLE AND SUBTITLE
Algorithm Design for Optimization in Communication and Navigation

5a. CONTRACT NUMBER
FA9453-19-1-0078

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)
Yuyuan Ouyang

5d. PROJECT NUMBER
3003

5e. TASK NUMBER

5f. WORK UNIT NUMBER
V1QF

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Clemson University
Division of Research
201 Sikes Hall
Clemson, SC 29634-0001

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory
Space Vehicles Directorate
3550 Aberdeen Avenue SE
Kirtland AFB, NM 87117-5776

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/RVSV

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-RV-PS-TR-2022-0030

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
Algorithm Design for Optimization in Communication and Navigation

14. ABSTRACT
This report was developed under grant FA9453-19-1-0078. Two research directions were successfully investigated during the duration of the grant that applies to communication and navigation. First, two numerical methods were proposed for solving nonlinear optimization problems arising from communication and navigation. Second, two results were discovered concerning solution quality and security of machine learning models.

15. SUBJECT TERMS
Nonlinear Optimization, Distributed optimization, Machine Learning, Security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Thomas Lovell
Unclassified	Unclassified	Unclassified	SAR	18	**19b. TELEPHONE NUMBER** *(include area code)*

--- This Page Intentionally Left Blank ---

TABLE OF CONTENTS

Page

1. SUMMARY 1

2. INTRODUCTION 2

3. METHODS, ASSUMPTIONS, AND PROCEDURES 4
3.1 Solving Linearly Constrained Optimization and Bilinear Saddle Point Problems 4
3.1.1 Designing an Alternating Direction Method of Multipliers 4
3.1.2 Designing an Accelerated Gradient Sliding Algorithm 5
3.2 Analyzing Solution Quality of Conditional Logistic Regression Models with Clusters .. 6
3.3 Designing Protocol for Secure Matrix Multiplication 7

4. RESULTS AND DISCUSSION 9
4.1 Training Opportunities 9
4.2 Publications 9

5. CONCLUSIONS 10

REFERENCES 11

(This Page Intentionally Left Blank)

1. SUMMARY

The goal of the research project is to develop efficient large-scale nonlinear optimization algorithms for solving data analysis problems in communication and navigation. These problems are well-recognized as being mathematically challenging and directly relevant to the interests of the Air Force.

Two research directions were successfully investigated during the duration of the grant. First, we designed optimal first-order methods for large-scale nonlinear optimization problems. In this direction, we proposed two first-order methods which could perform proximal gradient updates on decision variables. Both methods could solve nonlinear optimization problems arising from multi-agent optimization with decentralized communication. By reformulating the multi-agent optimization as constrained problems, our developed methods could solve the problem with optimal gradient/operator evaluation complexity. Our developed methods could also be used to solve image reconstruction problems.

Second, we analyzed solution quality and security issues in machine learning models. In this direction, we accomplished two research results. Our first result is concerning the properties of estimators computed from the conditional logistic regression model with binary outcomes under a multiple-cluster setting. We showed that the conditional maximum likelihood estimators from the model is approaching the maximum likelihood estimators asymptotically when each individual data point is replicated infinitely many times. Our second result is concerning the problem of secure matrix multiplication and we designed a method for performing distributed matrix multiplication accurately and securely. Our secure protocol can make sure that no information will be leaked during the communications for performing such matrix multiplication.

Two PhD students were supported as Graduate Research Assistants and received training during the performance period. The outcome of the proposed projects includes four academic journal papers. One paper has been published, another is under second-round review, and two others are in preparation and will be submitted for publication soon. [1-3]

2. INTRODUCTION

Three research problems were studied, and four research results were discovered during the performance period of this grant. The three research problems are: algorithm design for nonlinear optimization with linear constraints, conditional logistic regression estimator analysis, and distributed secure matrix multiplication.

In the research problem on algorithm design for linearly constrained nonlinear optimization, our problem of interest is

$$\min_{x\in X} f(x) \coloneqq \sum_{i=1}^{m} f_i(x) \text{ subject to } Kx = b \tag{1}$$

where x is a variable vector that can be decomposed to m vectors $x_1, \cdots, x_m$, functions f_i's are convex and differentiable, and K is a linear operator. Such a problem can be used to model multi-agent optimization that involves m agents. Here the agents will collaboratively minimize an objective function $f(x)$ that is the sum of their individual objectives f_i's, and they will communicate through a network whose topological structure is described by the constraint $Ax = b$. Such linearly constrained nonlinear optimization problem can be used to model any applications that involve collaboration between agents in a decentralized communication network.

Our second research problem is concerning the study of conditional logistic regression model with binary outcomes. Specifically, we analyze the solution quality of the estimator β that maximizes the following likelihood:

$$l_R^c(\beta) = \frac{1}{RN}\left[R\sum_{j=1}^{J}\sum_{k=1}^{k_j} Y_{j,k}X_{j,k}^T\beta - \sum_{j=1}^{J}\log g_{j,R,\sum_{k=1}^{K_j} Y_{j,k}}(\beta)\right], \tag{2}$$

where

$$g_{j,R,T}(\beta) \coloneqq \sum_{\substack{r_1,\cdots,r_{K_j}\in\{0,1,\cdots,R\} \\ \sum_{s=1}^{K} r_s = RT}} \binom{R}{r_1}\cdots\binom{R}{r_{K_j}} exp\left(\sum_{k=1}^{K_j} r_k X_{j,k}^T\beta\right). \tag{3}$$

Here we assume that there exists J clusters in the model, each with K_j individual data points that sum to N. Within each cluster, we assume the logistic regression model with data vector $X_{j,k}$, binary outcome $Y_{j,k}$, and bias b_j. Our goal is to recover estimator vector β for the model. The above research problem is closely related to machine learning for binary classification. Moreover, our study also considers the additional impact of multiple clusters in the model.

Our third research problem is secure matrix multiplication in which we would like to compute $C = AB^T$ in a distributed and secure manner. Such research is important since matrix multiplications is the fundamental operation in any communication and navigation models, and it is critical to make sure that the operation can be performed securely without leaking information to any other parties. Specifically, assuming that three parties and multiple workers are involved in the operation, with one party holding shares of matrix A, one party holding shares of matrix B, one party looking for the multiplication result C, and several workers working on performing the matrix multiplication, we designed a protocol of secure matrix multiplication using the Reed-Solomon codes.

3. METHODS, ASSUMPTIONS, AND PROCEDURES

The research discoveries of the three research projects studied during the performance period of the grant are stated below.

3.1 Solving Linearly Constrained Optimization and Bilinear Saddle Point Problems

We studied the constrained optimization problem described in the Introduction. For this research problem, we made two research discoveries.

3.1.1 Designing an Alternating Direction Method of Multipliers.

We consider a special case of the constrained optimization problem described as follows:

$$\min_{x\in X, y\in Y} \psi(x) := f(x) + J(y) \text{ subject to } y - Kx = b. \tag{4}$$

Here we assume that X and Y are closed convex sets, f and J are convex functions, and K is a linear map from X to Y. The above problem can be used to model either multi-agent optimization of image reconstruction or sensing models. Our goal is to compute an approximate solution x such that the objective function value is close to optimal, namely, $\psi(x) - \psi(x^*) \leq \varepsilon$, where x^* is an optimal solution and ε is the accuracy threshold. The PI has previously studied the problem and proposed a novel algorithm named accelerated alternating direction of multipliers that is able to compute an approximate solution with

$$O\left(\sqrt{\frac{L}{\varepsilon}} + \frac{\|K\|}{\varepsilon}\right) \tag{5}$$

gradient evaluations of ∇f and the same number of operator evaluations involving K and K^T (See [4]; see also related works in [5-7]). However, the previous method requires knowledge of the number of maximum iterations N. Such assumption is not suitable for practical computations: while one can decide N by the above theoretical bounds on the total number of gradient and operator evaluations required for compute an ε-approximate solution, such theoretical bound is usually conservative and will require unnecessary number of evaluations.

The PI and his research team developed a modification of the previous algorithm by introducing extra dual regularization terms in the subproblems. With the extra dual regularization terms, we can design algorithm parameters that do not require the knowledge of the maximum number of iterations. Consequently, we no longer need to run iterations that match the theoretical bound but can terminate early if the solution quality is satisfactory.

The discovery has been summarized to a technical report titled “Gradient Sliding Alternating Direction Method of Multipliers”. We are currently in the last stage of preparation and are expecting to submit the technical report for publication to an academic journal soon.

3.1.2 Designing an Accelerated Gradient Sliding Algorithm.

We derived the accelerated gradient sliding algorithm for minimizing the sum of two smooth convex functions:

$$\min_{x\in X} \psi(x) \coloneqq f(x) + h(x). \tag{6}$$

Here X is a closed convex set and f and h are two convex and differentiable functions. We assume that the gradients ∇f and ∇h are Lipchitz continuous with constants L and M respectively. Consequently, the Lipschitz constant of the gradient $\nabla\psi$ is $L + M$. Previously, it is known that the number of gradient evaluations of $\nabla\psi$ for computing an ε-approximate solution is in the order of (see [8])

$$O\left(\sqrt{\frac{L+M}{\varepsilon}}\right), \tag{7}$$

which depends on the Lipschitz constant $L + M$ of the gradient $\nabla\psi$ and the accuracy threshold ε. Consequently, the numbers of gradient evaluations of both ∇f and ∇h are in the above order. We derived a novel first-order algorithm to reduce the number of gradient evaluations to

$$O\left(\sqrt{\frac{L}{\varepsilon}}\right) \text{ and } O\left(\sqrt{\frac{L+M}{\varepsilon}}\right) \tag{8}$$

respectively. To the best of our knowledge, the above result has not yet been achieved in the literature. The benefit of the proposed algorithm is that it significantly reduces the time for computing gradient ∇f when the Lipschitz constants $L \ll M$.

The proposed accelerated gradient sliding algorithm can also be used to minimize the following sum of functions:

$$\min_{x\in X} \psi(x) \coloneqq f(x) + \max_{y\in Y}[< Kx, y > -J(y)]. \tag{9}$$

Here Y is a closed convex set, J is a convex function, and K is a linear operator from X to Y. The gradient ∇f is still assumed to be Lipschitz continuous with constant L. The above problem can be used to model image reconstruction and sensing problems. Moreover, a special case of it also covers multi-agent optimization with decentralization communication. Note that when $J(y) \coloneqq < b, y >$ and Y is a finite dimensional vector space, then the above problem is equivalent to constrained optimization

$$\min_{x\in X} f(x) \text{ subject to } Kx = b, \tag{10}$$

which can be used to model multi-agent optimization as described in the introduction. With a smooth technique, our proposed accelerated gradient sliding method can compute an approximate solution with

$$O\left(\sqrt{\frac{L}{\varepsilon}}\right) \text{ and } O\left(\sqrt{\frac{L}{\varepsilon}}+\frac{\|K\|}{\varepsilon}\right) \tag{11}$$

gradient evaluations of ∇f and operator evaluations involving K and K^T, respectively. To the best of our knowledge, the above result has also not yet been achieved in the literature. When applied to image reconstruction problems, we can skip computations of gradient evaluations of ∇f from time to time to compute an approximate solution more efficiently. When applied to multi-agent optimization under decentralized communication, we can make sure that the number gradient evaluations of ∇f is not impacted by the graph topology described in operator K.

Our proposed accelerated gradient sliding method has been summarized to a technical report titled "Accelerated Gradient Sliding for Structured Convex Optimization" and submitted to an academic journal, Computational Optimization and Applications. It has been accepted and is currently in press.

3.2 Analyzing Solution Quality of Conditional Logistic Regression Models with Clusters

We analyzed a cluster-specific logistic model with J clusters and K_j individual data points in each cluster, as described in the introduction. We use $\hat{\beta}^c(R)$ to describe the conditional logistic regression estimator with R data replications. Specifically, $\hat{\beta}^c(R)$ maximizes the following conditional maximum likelihood estimation function:

$$l_R^c(\beta)=\frac{1}{RN}\left[R\sum_{j=1}^{J}\sum_{k=1}^{k_j}Y_{j,k}X_{j,k}^T\beta-\sum_{j=1}^{J}\log g_{j,R,\sum_{k=1}^{K_j}Y_{j,k}}(\beta)\right] \tag{12}$$

where

$$g_{j,R,T}(\beta):=\sum_{\substack{r_1,\cdots,r_{K_j}\in\{0,1,\cdots,R\}\\ \sum_{s=1}^{K}r_s=RT}}\binom{R}{r_1}\cdots\binom{R}{r_{K_j}}exp\left(\sum_{k=1}^{K_j}r_kX_{j,k}^T\beta\right). \tag{13}$$

Previously, the relationship between the above conditional logistic regression parameter and the ordinary logistic regression parameter is not understood clearly. The ordinary logistic regression parameter $\hat{\beta}^o$ is the maximizer of the following ordinary logistic regression likelihood:

$$l^o(\beta,b):=\frac{1}{N}\sum_{j=1}^{J}\sum_{k=1}^{K_j}Y_{j,k}\left(X_{j,k}^T\beta+b_j\right)-log\left[1+\exp\left(X_{j,k}^T\beta+b_j\right)\right]. \tag{14}$$

The study of the relationship between conditional and ordinary logistic regression estimators will advance our knowledge on this fundamental machine learning models for binary classification with clusters.

Through theoretical derivations based on the observation that a term appearing in the conditional log-likelihood function is the coefficient of a polynomial, by transforming the analysis to the one over a complex integral by Cauchy's differentiation formula, we are able to perform asymptotic analysis that establishes the relationship between conditional and ordinary logistic regression estimators. Specifically, we obtained the following theorem:

Theorem 1. For the cluster-specific logistic model, under the assumptions of cluster independence and full column rank data matrices, for any fixed J and K_j's, if the estimators $\hat{\beta}^c(R)$ and $\hat{\beta}^o$ exist, then $\hat{\beta}^c(R)$ approaches $\hat{\beta}^o$ as R approaches infinity.

Based on the above discovery, we are now able to develop a new perspective in terms of the relationship between conditional and ordinary cluster-specific logistic regression models.

The research discovery has been summarized to a paper titled "An Asymptotic Result of Conditional Logistic Regression Estimator" and has been published on Communications in Statistic – Theory and Methods in 2021.

3.3 Designing Protocol for Secure Matrix Multiplication

We derived a strategy for performing secure matrix multiplication between multiple parties. Specifically, our goal is to design a secure protocol of computing $C = AB^T$. Here we use transpose operation in the notation B^T for convenience, so that the operations are directly derived from column spaces of both A and B. Specifically, we assume that there are three parties $P_1, P_2,$ and P_3. Matrix A is held by party P_1, matrix B is held by party P_2, and the third party P_3 would like to have the result $C = AB^T$. The computation is facilitated by a group of workers. When the three parties are the same, our setting is called delegated computing, in which we would like workers to perform matrix multiplications for us without leaking matrix information to the workers. When the three parties are different, our setting is known as federated learning. Both the delegated computing and federated learning settings are important in distributed communication applications and machine learning computations.

Our research discovery is a novel method that uses Reed-Solomon codes for securing the distributed matrix multiplication protocol. In particular, the parties P_1 and P_2 will distribute their respective shares of matrices A and B after adding random noise and perform discrete Fourier transforms. Due to the security of Reed-Solomon codes, we can prove that for each group of workers, if the union of their shares of portions of matrices A and B are smaller than a threshold

t, then working together such group of workers will not be able to recover any digit of entries in matrices A or B.

The research discovery has been summarized to a technical report titled “Secure Distributed Matrix Multiplication”. It is currently in the last stage of preparation and will be submitted to an academic journal soon.

4. RESULTS AND DISCUSSION

The four research discoveries on the three research problems have been described in the previous section. Moreover, during this performance period of the grant the PI was able to successfully train two PhD students.

4.1 Training Opportunities

Two PhD students conducted research relative to the proposed efforts and were supported by this grant as Graduate Research Assistants. One of the PhD students successfully defended the PhD dissertation.

PhD student Trevor Squires investigated the study on the gradient sliding alternating direction method multipliers stated in accomplishment 3. He defended his dissertation titled "Improved First-Order Techniques for Certain Classes of Convex Optimization" in March 2022.

PhD student Yu-Chung Liu investigated the study on the secure matrix multiplication strategy decision stated in accomplishment 4.

4.2 Publications

Two papers were completed as stated below.

- Z. He and Y. Ouyang, "An Asymptotic Result of Conditional Logistic Regression Estimator", *Communications in Statistic – Theory and Methods*, 2021. doi: 10.1080/03610926.2021.1999978
- G. Lan and Y. Ouyang, "Accelerated Gradient Sliding for Structured Convex Optimization", *Computational Optimization and Applications*, 2022 (in press).

Two papers are in preparation as stated below.

- Ouyang, Y., Squires, T., "Sliding Alternating Direction Method of Multipliers".
- Gao, S., Manganiello, F., McMahan, C., Liu, Y., Ouyang, Y. "Secure Distributed Matrix Multiplication".

5. CONCLUSIONS

During the performance period of this grant, the PI studied three research problems and discovered four research results. The research problems are concerning algorithm design for nonlinear optimization problems, machine learning models, and secure matrix multiplication protocols. Two PhD students were supported by the grant as Graduate Research Assistants and received training during their investigations on the research projects. One of the PhD students successfully defended the PhD dissertation in March 2022. Among the four research results, one has been published in an academic journal, one is under second-round review, and two are in preparation and will be submitted soon.

REFERENCES

[1] Z. He and Y. Ouyang, "An Asymptotic Result of Conditional Logistic Regression Estimator," *Communications in Statistic – Theory and Methods*, 2021.

[2] G. Lan and Y. Ouyang, "Accelerated Gradient Sliding for Structured Convex Optimization," *Computational Optimization and Applications*, 2022 (in press).

[3] T. Squires, "Improved First-Order Techniques for Certain Classes of Convex Optimization," PhD Dissertation, Clemson University, Clemson, South Carolina, 2022.

[4] Y. Ouyang, Y. Chen, G. Lan, and E. Pasiliao Jr., "An Accelerated Linearized Alternating Direction Method of Multipliers," *SIAM Journal on Imaging Sciences*, **Vol. 8**, 2015, pp. 644-681.

[5] Y. Ouyang and Y. Xu, "Lower Complexity Bounds of First-Order Methods for Convex-Concave Bilinear Saddle-Point Problems," *Mathematical Programming*, **Vol. 185**, 2021, pp. 1-35.

[6] Y. Chen, G. Lan, and Y. Ouyang, "Optimal primal-dual methods for a class of saddle point problems," *SIAM Journal on Optimization*, **Vol. 24**, 2014, pp. 1779-1814.

[7] Y. Chen, G. Lan, and Y. Ouyang, "Accelerated schemes for a class of variational inequalities," *Mathematical Programming*, **Vol. 165**, 2017, pp. 113-149.

[8] Y. Nesterov, *Lectures on convex optimization*, Springer International Publishing, 2018.

DISTRIBUTION LIST

DTIC/OCP
8725 John J. Kingman Rd, Suite
0944 Ft Belvoir, VA 22060-6218 1 cy

AFRL/RVIL
Kirtland AFB, NM 87117-5776 1 cy

Official Record Copy
AFRL/ RVS/Thomas Lovell 1 cy

Approved for public release; distribution unlimited.