**HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY**

# GRADUATION THESIS

## Run length limited de Bruijn sequences for quantum communication

**NGUYEN TIEN LONG**
long.nt180129@sis.hust.edu.vn

**Major: Computer Science**

**Supervisor:** Dr. Vu Van Khu

Dr. Tran Vinh Duc _____

Signature

**Department:** Computer Science

**School:** School of Information and Communications Technology

**HANOI, 08/2022**

# ACKNOWLEDGMENT

First and foremost, I would like to express my sincere gratitude to the subject teachers at Hanoi University of Science and Technology for their continuous guidance throughout my study, especially ones from School of Information and Communication Technology. During the past three and a half years, I have learned from them needed knowledge for pursuing later stages in my Computer Science journey.

I thankfully acknowledge the support of Prof. Huynh Thi Thanh Binh, who accepted me into MSO Lab and guided me in the first steps of my research career. My appreciation also extends to my laboratory colleagues, I'm very happy to have had the opportunity to collaborate with all of you, especially M.Sc. Tran Ba Trung, who introduced and invited me to joint work with him on our very first theoretical topic. I would also like to send my sincerity to other members of MSO Lab, Dr. Nguyen Thi My Binh, M.Sc. Nguyen Hong Ngoc, Tran Cong Dao, Tran Huy Hung and Nguyen Dac Tam. Dr.Binh and M.Sc Ngoc supported me a lot when I first joint our lab. Brothers Dao, Hung, and Tam lent a hand to review my thesis.

I also cherish the moment of doing my thesis under the supervision of Dr. Tran Vinh Duc. Though time is short, but his style in research inspired me so much.

Taking my first step in doing theoretical research, I owe a great debt of gratitude to Dr. Ta Duy Hoang (ENS de Lyon) and Dr. Vu Van Khu (National University of Singapore) for training and mentoring me during the working on various problems including ones in this thesis. Without their support (both professionally and personally), it would not have been possible for this work to progress as far as it has.

I'm also grateful to FPT Young Talent's members, especially Do Hoang Khanh, Lai Ngoc Tan, and Thanh La. I'll always remember the late night we spent together sharing our stories and our plans. I had known the way to find my answer to "Who am I going to be? How do I want to live in the next 10 years? 20 years? . . . ?" since that night.

In Bach Khoa Street Workout, my gratitude goes to Xuan Nam, Duc Anh, and Thanh Hai. We've trained and shared our experiences in SW, life and work as brothers.

My student's life must be harder without the following idiots: Phan Viet Hoang, Phi Phuc , Khanh Doan, Ng Duc Long, Tran Anh, Ba Tan, and Hong Sang. They

are my best friends for the last four years.

I’m also very grateful to my aunt Hang and uncle Lich, who always look after me just like my mom and dad.

Last but not least, this thesis is dedicated to my parents for the two decades of your love and support. I would not have come this far without your loving weight behind me.

# ABSTRACT

Quantum key distribution (Quantum key distribution) is a secure communication enabling two parties to produce a shared random secret key known only to them. Current commercial deployed QKD systems have transmission range restricted to under $1000$ km because they rely on optical fiber. The alternative method, satellite QKD, is able to overcome this issue but faces a new challenge caused by noisy environments and swift relative motion between the transmitter and receiver.

Therefore, a classical channel, which actually is a timing and synchronization system, is used along with the quantum channel. In such systems, Peide Zhang .et.al proposed to transmit a positioning sequence (also known as a de Bruijn sequence). To consider the timing jitter performance, a long period of no-pulses should be forbidden. In Peide Zhang's method, two pulse slots are used to represent a single bit (on-on is $1$ and on-off is $0$) so that one can avoid two consecutive no-pulses. However, the above scheme, called Hybrid de Bruijn (Hybrid de Bruijn) code, requires $2n$ pulse slots to represent a de Bruijn sequence of length $n$ and it needs to receive a sub-sequence of $2 \log n$ pulse slots to locate its position.

Observe that it is possible to use less redundant pulse slots to achieve both goals: to synchronize accurately and to avoid a long period of no-pulses, in this thesis, Run length limited de Bruijn sequences are designed in which each binary bit is represented by only one pulse slot, $1$ is on and $0$ is off. The RdB sequences are shown to be more general and efficient than the previous work.

This thesis provides the first explicit formula for the maximal length of the run length limited de Bruijn sequences. Furthermore, using Lyndon words, an efficient construction of a run length limited de Bruijn sequence with the maximal length is presented. In addition, a sub-linear decoding algorithm that can locate the position of an arbitrary substring is also provided.

**TABLE OF CONTENTS**

## LIST OF FIGURES

## LIST OF TABLES

## LIST OF ABBREVIATIONS

| Abbreviation | Definition |
|---|---|
| dBTS | a timing and synchronization system using Hybrid de Bruijn code (de Bruijn based Timing and Synchronization system) |
| FKM | Algorithm of Fredricksen, Kessler and Maiorana to generate granddaddy sequence |
| HdB | de Bruijn sequences encoded with a beacon model, on-on is $1$ and on-off is $0$ (Hybrid de Bruijn sequence) |
| LFSR | an algorithm to generate a de Bruijn sequence using a linear function (Linear feedback shift register) |
| LHS | Left hand side of a specific equation (Left Hand Side) |
| QKD | a secure communication method involving components of quantum mechanics for exchanging encryption keys (Quantum key distribution) |
| RdB | a sequence that is the combination of positioning sequence and run length sequence (Run length limited de Bruijn sequence) |
| RHS | Right hand side of a specific equation (Right Hand Side) |
| RLL | a line coding technique that is used to send arbitrary data over a communications channel with bandwidth limits (Run length limited) |

## Notation Table

| Notation | Meaning |
|---|---|
| $\Sigma_q$ | alphabet of size $q$, $\Sigma_q = (0, 1, 2, \ldots, q-1)$ |
| $\boldsymbol{x} \in \Sigma^n$ | binary sequence $\boldsymbol{x}$ of length $n$ over alphabet $\Sigma$ |
| $0^i$ ($1^i$) | concatenation of $i$ symbols $0$ ($1$) |
| $W(n, s)$ | set of all sequences of length $n$ containing at most $s$ consecutive bits $0$ |
| $\text{Ł}_n$ | set of all Lyndon words of length $n$ |
| $\text{Ł}^{(n)}$ | set of all Lyndon words whose length are divisors of $n$ |
| $\langle \boldsymbol{x} \rangle$ | minimal rotation of sequence $\boldsymbol{x}$ |
| $G_k$ | de Bruijn graph of order $k$ |
| $G_{k,s} = (V^{k-1,s}, E^{k,s})$ | $(k, s)$-RdB graph with vertex set $V^{k-1,s}$, edges set $E^{k,s}$ |
| $V_{i,j}^{k-1,s}$ | set of all vertices in $G_{k,s}$ satisfying the first $i+1$ letters are $(0, 0, \ldots, 0, 1)$ and the last $j+1$ letters are $(1, 0, 0, \ldots, 0)$ |
| $\ell(G_{k,s})$ | length of the longest simple path in $G_{k,s}$ |
| $N(k, s)$ | length of the longest $(k, s)$-RdB sequence |
| $\mathbb{U}(k, s)$ | upper bound for the length of the longest simple path in $G_{k,s}$ |
| $\mathcal{U}(k, s)$ | upper bound for the length of the longest $(k, s)$-RdB sequence |