

TOWARDS NAVIGATION BASED ON 120 SATELLITES:  
ANALYZING THE NEW SIGNALS

A DISSERTATION  
SUBMITTED TO THE DEPARTMENT OF ELECTRICAL  
ENGINEERING  
AND THE COMMITTEE ON GRADUATE STUDIES  
OF STANFORD UNIVERSITY  
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS  
FOR THE DEGREE OF  
DOCTOR OF PHILOSOPHY

Grace Xingxin Gao  
September 2008

© Copyright by Grace Xingxin Gao 2009  
All Rights Reserved

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.



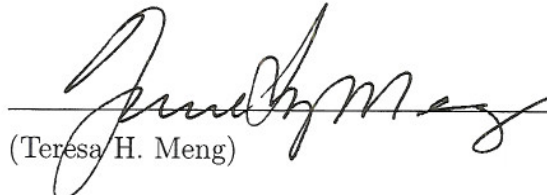
(Per K. Enge) Principal Adviser

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.



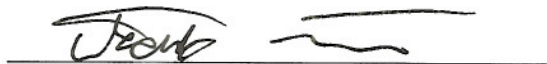
(Benjamin Van Roy)

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.



(Teresa H. Meng)

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.



(Todd Walter)

Approved for the University Committee on Graduate Studies.



# Abstract

Global Navigation Satellite Systems (GNSS) are experiencing a new era. The US Global Positioning System (GPS) now serves over 300 million users in a bewildering breadth of applications. The Russian GLONASS is enjoying a startling renaissance based on the recovery of the Russian economy. In addition, the European Union is developing the Galileo system that promises to place 30 more satellite in medium Earth orbit. If that is not enough, China has started their Compass system project that promises a rich combination of satellites in medium and geostationary earth orbit.

All of these satellites will broadcast at least three civil signals in a multiplicity of frequency bands. If all of these new satellites are launched, we will have 120 satellites and over 300 signals in space for global navigation by 2020.

So far, two test satellites of the European Galileo and one satellite from the Chinese Compass have been launched. The new satellites and new signals create a great opportunity for GNSS receivers to gain more redundancy and accuracy. On the other hand, the new GNSS signals could interfere with each other since their frequency bands overlap. Moreover, when the satellites were put into orbit, the signal specifications were not available to the public. This mystery made it impossible for GNSS receivers to acquire and track the new satellites. It was also impossible to analyze the interference among GNSS satellites. Thus, there was an urgent and great need for discovering the unknown signal characteristics.

The contribution of this work is to design algorithms for deciphering all the new test satellite signals from the Galileo and Compass satellite programs. We reveal the spread spectrum codes for all the signals on the prototype satellites listed above.

In addition, we derive the underlying code generators based on a modification of the Berlekamp-Massey algorithm for solving systems of equations over finite fields. Several receiver companies, such as Trimble, Septentrio, Javad, etc., have already developed their Galileo/Compass receivers based on our decoding results. As a final contribution, we use the codes to establish the multiple access capacity of GNSS. We are happy to note that this great family of satellite signals can coexist.

# Acknowledgments

The work in this dissertation would be impossible without the kind, patient and generous help from many people with whom I have been lucky to spend my Ph.D. years.

I feel deeply indebted to my principal advisor, Prof. Per Enge, an exceptional researcher and mentor with a wonderful sense of humor too. Every meeting with him brightens my whole day. His encouragement and guidance let me set and achieve goals beyond what I imagined. Per's gift for inspiration influences not just my research, but also my outlook on life.

I would also like to acknowledge the WAAS lab lead, Dr. Todd Walter. As my direct supervisor, he brings out the best in me by allowing me the freedom to define my research, yet always being available for impromptu discussions. Todd's knowledge about GPS and WAAS and his love of research are unparalleled.

I also thank Prof. James Spilker, Jr., for sharing with me his great passion and deep understanding of signal processing, satellite communications and navigation. I am particularly inspired by his drive and energy.

Professors Benjamin Van Roy and Teresa Meng graciously agreed to be the second and third readers for this dissertation and, together with Prof. Mark Kasevich, to serve on my oral defense committee. I thank them for their thoughtful questions and helpful comments.

Special thanks are due to Doug Archdeacon, Dana Parga, Sherann Ellsworth and Ralph Levine for their quick and professional assistance in systems, financial, logistical and academic administration. Without them, my Ph.D. studies would not have proceeded so smoothly.

I am also grateful for my collaborations and friendships with the members and alumni of the GPS lab at Stanford: Dennis Akos, Juan Blanch, Lee Boyce, Alan Chen, Tsung-Yu Chiou, Seebany Datta-Barua, Dave De Lorenzo, Juyong Do, Gabriel Elkaim, Alex Ene, Hiroshi Ito, Euiho Kim, Michael Koenig, Hiroyuki Konno, Jiyun Lee, Sherman Lo, Ming Luo, Paul Montgomery, Guttorm Opshaug, Youngshin Park, Prof. Brad Parkinson, Eric Phelts, Prof. David Powell, Sam Pullen, Di Qiu, Shankar Ramakrishnan, Jason Rife, Jiwon Seo, Godwin Zhang and Alan Zorn. Beyond Stanford, I have the pleasure of working with Glen Gibbons, Chris Hegarty, Gary Lennen, Prof. Jade Morton, Elizabeth Rooney, Stuart Riley, Qinfang Sun and many others. I thank them all.

The work reported in this dissertation is supported by a research grant from the Federal Aviation Administration (FAA). I would like to acknowledge the FAA for their generous financial support.

I feel very fortunate to have so many friends at Stanford and in the Bay Area that it is simply not possible to name them all. Yuan Zhang, Minqian Kang, Shanbin Zhao, Jia Feng and my family friend Amanda Gong are especially close to me and I thank them for their supportiveness. I also thank the Weins, Anne and Larry and the kids, and the Rewicks, Joy and Bob, for helping me adjust to my new life in America.

To my fiancé David Varodayan, thank you for loving me. I am grateful for your understanding, patience and encouragement. It is so wonderful to share my Ph.D. journey with you. Happiness doubles and sadness halves. Thank you also for proof-reading this dissertation and setting a high standard for me.

Finally and most importantly, to my mother Zongying Yang and father Delin Gao, no words can express my thanks for your absolutely unconditional and everlasting love. You selflessly support and encourage me, your only child, to travel to the other side of the world to pursue my dreams. You want the best for me, yet expect nothing in return. This work is humbly dedicated to you.



# Contents

<b>Abstract</b>	<b>v</b>
<b>Acknowledgments</b>	<b>vii</b>
<b>1 Introduction</b>	<b>1</b>
1.1 A New Era for GNSS . . . . .	1
1.2 Current Operational GNSS . . . . .	2
1.2.1 GPS . . . . .	2
1.2.2 GLONASS . . . . .	4
1.3 GNSS Under Development . . . . .	5
1.3.1 Galileo . . . . .	5
1.3.2 Compass . . . . .	7
1.4 Problem Statement . . . . .	9
1.5 Related Work . . . . .	11
1.6 Summary of Contributions . . . . .	13
1.7 Dissertation Outline . . . . .	15
<b>2 Capturing Satellite Transmission</b>	<b>17</b>
2.1 Stanford SRI 45.7 m Dish . . . . .	17
2.2 Stanford GNSS Monitor System 1.8 m Dish Antenna . . . . .	20
2.3 Summary . . . . .	29
<b>3 Signal Modeling and Decoding Overview</b>	<b>31</b>
3.1 GNSS Signal Modeling . . . . .	31

3.2	Decoding Overview . . . . .	35
3.3	Summary . . . . .	36
<b>4</b>	<b>Decoding Compass-M1</b>	<b>39</b>
4.1	E6 Code . . . . .	39
4.1.1	Carrier Wipeoff . . . . .	39
4.1.2	Correlation of Whole Data with a Small Slice of Itself . . . . .	40
4.1.3	Determination of Code Period . . . . .	44
4.1.4	Wipeoff of Doppler Frequency up to Half of the Code Repetition Rate . . . . .	44
4.1.5	Wipeoff of Secondary Code up to Overall Polarity . . . . .	46
4.1.6	Stacking Multiple Periods of the Whole Data . . . . .	49
4.1.7	Wipeoff of Doppler Ambiguity . . . . .	49
4.1.8	Zeroing Initial Phase . . . . .	52
4.1.9	Start of the Code and Shifting the Whole Data Set . . . . .	55
4.1.10	Code Chips up to Overall Polarity . . . . .	55
4.2	E6 Code Generator . . . . .	57
4.3	E2 and E5b Codes and Generators . . . . .	61
4.4	Summary . . . . .	62
<b>5</b>	<b>Decoding Galileo GIOVE-A and GIOVE-B</b>	<b>65</b>
5.1	Galileo Preliminaries . . . . .	65
5.2	GIOVE-A E5b Codes . . . . .	69
5.2.1	Interference Mitigation . . . . .	69
5.2.2	Code Period . . . . .	72
5.2.3	Wipeoff of Doppler Frequency up to Half of the Code Repetition Rate . . . . .	73
5.2.4	Wipeoff of Secondary Codes up to Overall Polarity . . . . .	73
5.2.5	Wipeoff of Doppler Ambiguity . . . . .	77
5.2.6	Zeroing the Initial Phase . . . . .	79
5.2.7	Start of the Code and Shifting the Whole Data Set . . . . .	79
5.2.8	Code Chips up to Overall Polarity . . . . .	80

5.3	GIOVE-A E5b Codes and Code Generators . . . . .	81
5.4	GIOVE-A E5a Codes and Code Generators . . . . .	83
5.5	GIOVE-A L1 Codes and Code Generators . . . . .	83
5.6	GIOVE-A E6 Codes and Generators . . . . .	87
5.7	GIOVE-B Codes and Generators . . . . .	88
5.8	Summary . . . . .	90
<b>6</b>	<b>How Many Satellites Are Too Many?</b>	<b>91</b>
6.1	Correlation Properties of Random Sequences . . . . .	91
6.1.1	Auto-correlation of BPSK random sequence . . . . .	92
6.1.2	Cross-correlation of BPSK random sequences . . . . .	93
6.1.3	Cross-correlation of BOC(1,1) and BPSK random sequences . . . . .	94
6.1.4	Cross-correlation of BOC(1,1) random sequences . . . . .	97
6.2	Auto- and Cross-correlation within a System . . . . .	98
6.3	Cross-correlation between Systems . . . . .	102
6.4	Multiple Access Capacity of GNSS . . . . .	104
6.5	Summary . . . . .	108
<b>7</b>	<b>Satellite Acquisition and Tracking Results</b>	<b>109</b>
7.1	Frequency Bands without DME/TACAN . . . . .	109
7.2	Frequency Bands with DME/TACAN . . . . .	112
7.3	DME/TACAN Interference Mitigation . . . . .	113
7.3.1	Pulse Blanking in Time Domain . . . . .	113
7.3.2	Notch Filtering In Frequency Domain . . . . .	115
7.3.3	Hybrid Blanking in Time-Frequency Domain . . . . .	117
7.4	DME/TACAN Mitigation at Stanford . . . . .	120
7.5	Summary . . . . .	124
<b>8</b>	<b>Conclusions</b>	<b>125</b>
8.1	Results and Contributions . . . . .	125
8.2	Directions for Future Work . . . . .	128

<b>A Acronyms</b>	<b>131</b>
<b>Bibliography</b>	<b>133</b>

# List of Tables

1.1	GNSS past, present and future . . . . .	2
1.2	Galileo frequencies . . . . .	6
1.3	Galileo signals compared to the GPS L1 civil signal . . . . .	7
1.4	Compass frequencies . . . . .	8
2.1	Link budget of GPS L1 signal at different elevations captured by 1.8 m dish . . . . .	20
4.1	Code generator polynomials and initial states for generating the first 8190 bits of the Compass E6 I-channel code . . . . .	60
4.2	Code generator polynomials and initial states for generating bits 8191-10230 (last 2040 bits) of the Compass E6 I-channel code . . . . .	60
4.3	Code generator polynomials and initial states for generating the Compass E2 I-channel code . . . . .	61
4.4	Summary of Compass-M1 broadcast code results (civil signal only) . .	63
5.1	Secondary code reading of E5b-I and E5b-Q based on Figure 5.14 . .	75
5.2	Code generator polynomials and initial states for GIOVE-A E5b-I PRN code . . . . .	82
5.3	Code generator polynomials and initial states for GIOVE-A E5b-Q PRN code . . . . .	82
5.4	Code generator polynomials and initial states for GIOVE-A E5a-I PRN code . . . . .	83

5.5	Code generator polynomials and initial states for GIOVE-A E5a-Q PRN code . . . . .	83
5.6	Code generator polynomials and initial states for GIOVE-A L1-B PRN code . . . . .	85
5.7	Code generator polynomials and initial states for GIOVE-A L1-C PRN code . . . . .	85
5.8	Code generator polynomials and initial states for GIOVE-A E6-B PRN code . . . . .	88
5.9	Code generator polynomials and initial states for GIOVE-A E6-C PRN code . . . . .	88
5.10	Code generator polynomials and initial states for GIOVE-B L1-B PRN code . . . . .	88
5.11	Code generator polynomials and initial states for GIOVE-B L1-C PRN code . . . . .	89
5.12	Code generator polynomials and initial states for GIOVE-B E5a-I PRN code . . . . .	89
5.13	Code generator polynomials and initial states for GIOVE-B E5a-Q PRN code . . . . .	89
5.14	Code generator polynomials and initial states for GIOVE-B E5b-I PRN code . . . . .	89
5.15	Code generator polynomials and initial states for GIOVE-B E5b-Q PRN code . . . . .	89
5.16	Summary of GIOVE-A and GIOVE-B broadcast codes . . . . .	90
6.1	Maximum side lobes of GIOVE-A auto-correlation . . . . .	98
6.2	Maximum side lobes of cross-correlation . . . . .	99
6.3	Maximum side lobes of Compass-M1 auto-correlation . . . . .	99
7.1	Acquisition results of the E5a, raw data . . . . .	121
7.2	Acquisition results of the E5a, pulse blanking . . . . .	121
7.3	Acquisition results of the E5a, notch filtering . . . . .	122
7.4	Acquisition results of the E5a, hybrid blanking . . . . .	124

# List of Figures

1.1	The orbits of GPS satellites are inclined to the Earth's equator by about $55^\circ$ . The system is designed to ensure that at least four satellites are visible at least $15^\circ$ above the horizon at any given time anywhere in the world. [1]	3
1.2	An unlaunched GPS satellite on display at the San Diego Aerospace museum. Photo credit: Scott Ehardt.	3
1.3	How positioning works.	4
1.4	Launch of the GIOVE-B satellite on April 27, 2008. Photo credit: ESA [2].	7
1.5	Frequency occupation of GPS, Galileo and Compass, adapted from [3]	9
2.1	Stanford SRI dish antenna, 45.7 m in diameter, 52 dB gain and $0.25^\circ$ beamwidth. Photo credit: Max Klein	18
2.2	The GIOVE-A L1 band spectrum observed by the Stanford SRI dish. The signals are down converted to baseband. The antenna gain is high enough to boost the signal above the noise. The two small lobes in the center correspond to the BOC(1,1) modulation of the L1 open service signal, and the two wider lobes located 15 MHz from the center frequency represent BOC(15, 2.5) modulation of the Galileo Public Regulated Service signal.	19
2.3	The GIOVE-A E6 band spectrum observed by the Stanford SRI dish. The main lobe in the center is a commercial access signal with BPSK(5) modulation, and the two side lobes represent a PRS signal with BOC(10,5) modulation.	19

2.4	Stanford GNSS Monitor System, 1.8m dish . . . . .	21
2.5	Stanford GNSS Monitor System. The 1.8 m dish antenna is controlled by Nova for Windows software, which drives the antenna azimuth and elevation motors to track satellites. The signal from the L band feed of the antenna passes through a band pass filter, low noise amplifiers (LNAs) and is collected by an Agilent 89600 Vector Signal Analyzer (VSA). . . . .	22
2.6	The GIOVE-A L1 band spectrum observed by the SGMS dish. The BOC(1,1) spectrum is slightly visible at the center of the plot. . . . .	23
2.7	The GIOVE-A E5a band spectrum observed by the SGMS dish. The BPSK(10) modulation for E5a is not visible since the signals are buried in noise. Moreover, we see strong narrow-band tones attributed to DME/TACAN, one obvious in the E5a band. Each tone represents the airborne interrogators and the beacon DME signal from a nearby airport. . . . .	24
2.8	The GIOVE-A E5b band spectrum observed by the SGMS dish. There are three strong narrow-band tones attributed to DME/TACAN. . . . .	25
2.9	The time-domain GIOVE-A E5a signal observed by the SGMS dish . . . . .	25
2.10	The time-domain GIOVE-A E5b signal observed by the SGMS dish. The DME/TACAN pulses in time domain are 5 to 100 times greater in amplitude than the noise, while the E5 signals are even weaker than noise. . . . .	26
2.11	The time-domain GIOVE-A E5b signal observed by the SGMS dish, zoomed in. . . . .	26
2.12	The time-domain GIOVE-A E5b signal observed by the SGMS dish, zoomed in further . . . . .	27
2.13	The Compass-M1 E2 band spectrum observed by the SGMS dish. The main lobe and the adjacent side lobes of the 2 MHz chipped E2 signal are visible without averaging. An L1 signal from a nearby GPS satellite can also be seen in this plot as well as some interference in the lower part of the bandwidth. . . . .	28



2.14	The Compass-M1 E5b band spectrum observed by the SGMS dish. The main lobe of the BPSK(2) civil signal is visible, and the main lobe of the BPSK(10) military signal can also be made out. As expected in this frequency band, we also see strong narrow-band DME/TACAN interference. . . . .	28
2.15	The Compass-M1 E6 band spectrum observed by the SGMS dish. The main feature is the main lobe of the QPSK(10) signal. Also visible is an as-yet-unidentified 1 MHz-wide transmission centered around 11 MHz below the E6 carrier frequency. . . . .	29
3.1	Example of relationship between the PRN code signal, the secondary code, and the carrier. The secondary code duration is the same as the PRN code period. . . . .	33
3.2	The relationship of $T_c$ , $T_d$ and $\tau_d$ with the recorded data. $T_c$ is the PRN code chip duration. $N_c$ is the number of bits per PRN code period. The PRN code period is the same as the secondary code bit duration, $T_d = N_c T_c$ . $\tau_d$ is the code phase offset arising from the lack of synchronization between the recorded data and the start of the PRN code. In other words, $\tau_d$ represents the start of the first complete period of the PRN code. . . . .	34
3.3	Decoding block diagram . . . . .	37
4.1	Correlation of the received code with time-shifted replicas. Correlation peaks occur whenever the time-shifted slice aligns with similar versions of itself or flipped versions. The $i$ th correlation peak polarity is determined by the secondary code bit of the small slice, $d_0$ , and the secondary code bit of the corresponding segment, $d_i$ . The triangular correlation peak width is twice the PRN code chip duration. . . . .	42
4.2	Correlation of whole data with a small slice of itself, inphase channel	43
4.3	Correlation of whole data with a small slice of itself, quadrature channel	43
4.4	Correlation after wiping off estimated Doppler offset, inphase channel	45
4.5	Correlation after wiping off estimated Doppler offset, quadrature channel	45

4.6	Secondary code wipeoff. Because the recording time is not synchronized with the start of a complete PRN code period, only the secondary code of the signal segments in the shaded area is wiped off. The transition point reveals the start of the PRN code period, $\tau_d$ . . .	47
4.7	Correlation after wiping off estimated Doppler offset and secondary code, inphase channel . . . . .	48
4.8	Multiple periods of signal stacked, inphase channel . . . . .	50
4.9	Multiple periods of signal stacked, quadrature channel . . . . .	50
4.10	Stacked signal with no Doppler ambiguity, inphase channel . . . . .	51
4.11	Stacked signal with no Doppler ambiguity, quadrature channel . . . . .	52
4.12	The I-Q plot of the stacked signal before phase adjustment . . . . .	53
4.13	The I-Q plot of the stacked signal after phase adjustment . . . . .	53
4.14	Stacked signal with initial phase adjusted, inphase channel . . . . .	54
4.15	Stacked signal with initial phase adjusted, quadrature channel . . . . .	54
4.16	Stacked signal with initial phase adjusted, zoom in . . . . .	55
4.17	Stacked signal with code start determined, zoom in . . . . .	56
4.18	First 50 bits of E6 I-channel PRN code . . . . .	56
4.19	Linear feedback shift register (LFSR) . . . . .	58
4.20	Search algorithm for linear code representation . . . . .	58
4.21	Code generator schematic of the Compass E2 I-channel signal . . . . .	61
5.1	PRN code chip with BPSK and BOC(1,1) modulation, respectively .	66
5.2	The spectrum of BPSK and BOC(1,1) modulation . . . . .	67
5.3	Correlation functions of BPSK and BOC(1,1) modulation, respectively	67
5.4	Overlap of DME/TACAN band and E5 band . . . . .	68
5.5	A DME/TACAN pulse pair . . . . .	68
5.6	The GIOVE-A E5b band spectrum observed by the SGMS dish. There are three strong narrow-band tones attributed to DME/TACAN. (Same as Figure 2.8) . . . . .	69

5.7	The time-domain GIOVE-A E5b signal observed by the SGMS dish. The DME/TACAN pulses in time domain are 5 to 100 times greater in amplitude than the noise, while the E5 signals are even weaker than noise. (Same as Figure 2.10) . . . . .	70
5.8	Signal spectrum after notch filtering . . . . .	71
5.9	Time-domain signal after notch filtering . . . . .	71
5.10	Correlation of the whole code sequence with a small slice of itself, inphase. The intervals between pairs of peaks are used to compute the code length. As the peaks occur at multiples of 1 ms, the PRN codes have period of 1 ms. . . . .	72
5.11	Correlation of the whole code sequence with a small slice of itself, quadrature . . . . .	73
5.12	Correlation of the whole code sequence with a small slice of itself, inphase, after Doppler offset removal. The correlation peaks have more uniform heights in the inphase channel. There are positive and negative peaks at multiples of 1 ms. Null peaks are deduced where no positive or negative peaks exist. The null peaks indicate that there are two signals superposed. . . . .	74
5.13	Correlation of the whole code sequence with a small slice of itself, quadrature, after Doppler removal. No correlation peaks appear in the quadrature channel. . . . .	74
5.14	Extracting secondary code bits according to correlation peaks. For the solid blue curve, the positive and negative peaks reveal the secondary code bits at the peak locations, while the secondary code bits corresponding to the null peaks are unknown. The ambiguity of null peaks are solved by correlating another slice of data that corresponds to a null peak as shown by the dashed red curve. All the original nulls are filled with dashed peaks. . . . .	76

5.15	Multiple periods of signal stacked, inphase channel. The first 0.84 ms appears to have a sinusoidal envelope and the rest looks like noise. The sinusoidal envelope is due to the Doppler residual of an integer multiple of 500 Hz. The transition between the sinusoidal part and the noise-like part is the boundary between PRN code periods. . . . .	77
5.16	Multiple periods of signal stacked, quadrature channel . . . . .	78
5.17	Stacked signal with no Doppler ambiguity, inphase channel. The signal now has a constant envelope instead of a sinusoidal one. . . . .	78
5.18	Stacked signal with no Doppler ambiguity, quadrature channel . . . .	79
5.19	The I-Q plot of the stacked signal . . . . .	80
5.20	The first 100 chips of the E5b-I code . . . . .	81
5.21	The E5b code generator . . . . .	82
5.22	A skyplot of GIOVE-A and GPS NAVSTAR satellites, in which GPS NAVSTAR 36 and 32 fall in the antenna main lobe of GIOVE-A. . .	84
5.23	Extracting secondary code bits according to correlation peaks. Since the GIOVE-A L1 band overlaps with the GPS L1 band, the GPS L1 signal is received as well, which is indicated by the small triangular correlation peaks (top). The correlation peaks of the GIOVE-A L1 signal have shapes consistent with typical BOC modulation. The double-in-height peaks (bottom left) and single-in-height peaks (bottom right) indicate two PRN codes are superimposed. One PRN code is twice as long as the other. . . . .	86
5.24	BOC modulation wipeoff. We align the BOC(1, 1) carrier with the stacked signal, and then multiply them together. . . . .	87
6.1	Auto-correlation mean of a random sequence of length $N$ with BPSK modulation. . . . .	92
6.2	Auto-correlation variance of a random sequence of length $N$ with BPSK modulation. . . . .	93
6.3	Cross-correlation variance of random sequences of length $N$ , both modulated by BPSK. . . . .	94

6.4	Illustration of a BOC modulated random sequence $X_{BOC}(t)$ and a BPSK modulated random sequence $Y(t)$ . . . . .	95
6.5	Variation of cross-correlation of random sequences of length $N$ , BOC(1,1) vs. BPSK . . . . .	96
6.6	The spectra of BPSK and BOC(1,1) modulation, same as Figure 5.2.	97
6.7	cross-correlation variance of random sequences of length $N$ , both modulated by BOC(1,1). . . . .	97
6.8	Maximum correlation side lobes of GIOVE-A L1 code auto-correlation	100
6.9	Maximum correlation side lobes of GIOVE-A E6 code auto-correlation	100
6.10	Max correlation side lobes of GIOVE-A E5a code auto-correlation . .	101
6.11	Maximum correlation side lobes of GIOVE-A E5b code auto-correlation	101
6.12	Maximum correlation side lobes of Compass E2/E5b and E6 code auto-correlation . . . . .	102
6.13	Maximum side lobes of cross-correlation between GIOVE-A L1 codes and GPS codes . . . . .	103
6.14	Maximum side lobes of cross-correlation between GIOVE-A E5b codes and Compass E5b code . . . . .	103
6.15	Received C/A code signal power available from an isotropic antenna as a function of elevation angle for a user on the surface of the earth [4].	105
6.16	Commercial L1 antenna gain pattern. Predicted pattern for a standard patch antenna mounted on a four-wavelength-diameter circular ground plane (Courtesy of Frank Bauregger, Novariant, Inc.) . . . . .	105
6.17	Received C/A code signal power subject to the gain of a patch antenna	106
6.18	Average-case multiple satellite self-interference, L1 band . . . . .	107
6.19	Average-case multiple satellite self-interference, L5 band . . . . .	108
7.1	Acquisition plot of Compass-M1 E2 I-channel . . . . .	110
7.2	Tracking results of Compass-M1 E2 I-channel . . . . .	111
7.3	Acquisition plot of Galileo GIOVE-A E5a Q-channel . . . . .	112
7.4	Tracking results of Galileo GIOVE-A E5a Q-channel . . . . .	113
7.5	Pulse blanking . . . . .	114

7.6	Time domain E5a signal before pulse blanking . . . . .	114
7.7	Time domain E5a signal after pulse blanking . . . . .	114
7.8	E5a power spectral density estimate, after pulse blanking . . . . .	115
7.9	E5a power spectral density estimate after notch filtering . . . . .	116
7.10	Time domain E5a signal, after notch filtering . . . . .	116
7.11	Hybrid blanking schematic . . . . .	118
7.12	Selectivity of pulse blanking, notch filtering and hybrid blanking . . .	118
7.13	E5a power spectral density estimate, after hybrid blanking . . . . .	119
7.14	Time domain E5a signal, after hybrid blanking . . . . .	119
7.15	Acquisition plot of the Galileo E5a signal, raw data without DME/TACAN interference mitigation . . . . .	120
7.16	Acquisition plot of the Galileo E5a signal, with pulse blanking. . . . .	121
7.17	Tracking results of GIOVE-A E5a Q-channel, after pulse blanking . .	122
7.18	Acquisition plot of the Galileo E5a signal, with notch filtering . . . .	123
7.19	Acquisition plot of the Galileo E5a signal, with hybrid blanking . . .	123

# Chapter 1

## Introduction

### 1.1 A New Era for GNSS

Global Navigation Satellite Systems (GNSS) are experiencing a new era. Until now, there have been only two operational systems, the United States' Global Positioning System (GPS) [4] and Russia's GLONASS [5]. The original satellites of both systems each transmitted just a single civil signal in one frequency band.

In recent years, the significance and value of global satellite navigation has been recognized by more countries. In particular, the European Union is developing their Galileo system [6]. The first two test satellite of the Galileo system, Galileo In-Orbit Validation Elements, GIOVE-A and GIOVE-B, were launched on December 28, 2005 [7, 8], and April 27, 2008 [2], respectively.

China was involved in the initial stages of Galileo [9], but later began development of its own system, Compass [10]. The first, and so far, only Medium Earth Orbit (MEO) satellite of the Compass system, Compass-M1 was launched on April 14, 2007 [3].

At full development, the Galileo and Compass systems are intended to have about 27 and 35 satellites, respectively. As shown in Table 1.1, the whole family of GNSS is projected to consist of about 120 satellites by 2020. Moreover, the new satellites are capable of transmitting multiple signals in multiple frequency bands. Altogether there will be more than 300 GNSS signals broadcast in the future. The GNSS world is

growing from a couple of dominant players to four complete systems, from 32 satellites to about 120 satellites, and from simple signals to an array of complicated signals.

Nation	System	2002	2008	2020
USA	GPS	24 satellites	31 satellites	$\sim 31$ satellites
EU	Galileo	-	2 satellites	$\sim 27$ satellites
China	Compass	-	1 satellite	$\sim 35$ satellites
Russia	GLONASS	8 satellites	16 satellites	$\sim 24$ satellites
	Total	32 satellites	50 satellites	$\sim 120$ satellites

Table 1.1: GNSS past, present and future

## 1.2 Current Operational GNSS

### 1.2.1 GPS

The Global Positioning System (GPS) is the first fully functional GNSS, developed by the United States Department of Defense for military applications in the 1970s. The federal government made the system available for civilian use in 1983, and GPS has served millions of users since. It not only provides three-dimensional location information for navigation applications, but also precise timing for communications and commerce [4].

As of August 2008, GPS comprises a constellation of 31 MEO satellites at an altitude of 20183 km [4]. The satellites orbit on six planes at approximately  $55^\circ$  inclination with respect to the equator, and are separated by  $60^\circ$  right ascension. The orbits are arranged so that at least six satellites are within line of sight from almost everywhere on Earth's surface, and at least four satellites are visible at least  $15^\circ$  above the horizon. Figure 1.1 shows the orbital planes and the constellation, and Figure 1.2 shows a GPS satellite on display at the San Diego Aerospace museum.

GPS is a Code Division Multiple Access (CDMA) communication system. Each satellite transmits a distinct spread spectrum code, or Pseudo Random Noise (PRN) code. A receiver on Earth knows all the PRN codes, calculates its distance from multiple visible GPS satellites, and determines its position by trilateration.



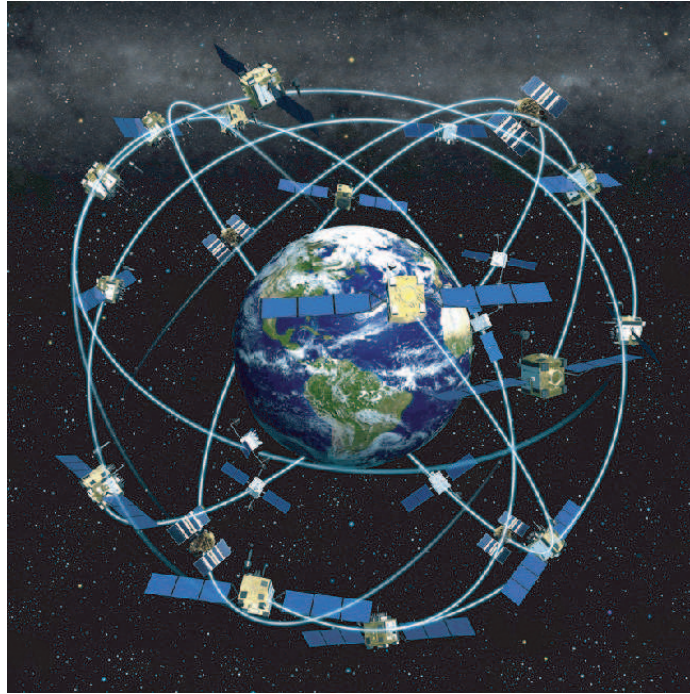


Figure 1.1: The orbits of GPS satellites are inclined to the Earth's equator by about  $55^\circ$ . The system is designed to ensure that at least four satellites are visible at least  $15^\circ$  above the horizon at any given time anywhere in the world. [1]

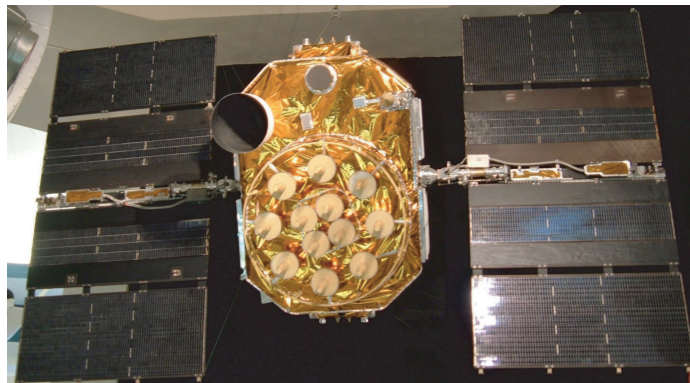


Figure 1.2: An unlaunched GPS satellite on display at the San Diego Aerospace museum. Photo credit: Scott Ehardt.

Figure 1.3 illustrates how a receiver calculates its distance from a certain satellite. The satellite broadcasts its distinct periodic PRN code to Earth. When the receiver picks up the signal, it generates a series of local PRN code replicas, each replica corresponding to a different GPS satellite. The receiver then correlates the received satellite signal with each local replica. If the local replica under consideration matches the satellite PRN code (the blue replica in Figure 1.3), a sharp correlation peak occurs when the code and replica are aligned in time. There are also small noise-like correlation side peaks. If the local replica does not match the satellite PRN code (the yellow replica in Figure 1.3), there is no main correlation peak. By searching for the main correlation peak, the receiver can both identify the satellite and determine the time of travel of the satellite signal. The receiver then computes its distance from the satellite by multiplying the travel time by the speed of light. By repeating this, the receiver can calculate its position by trilateration.

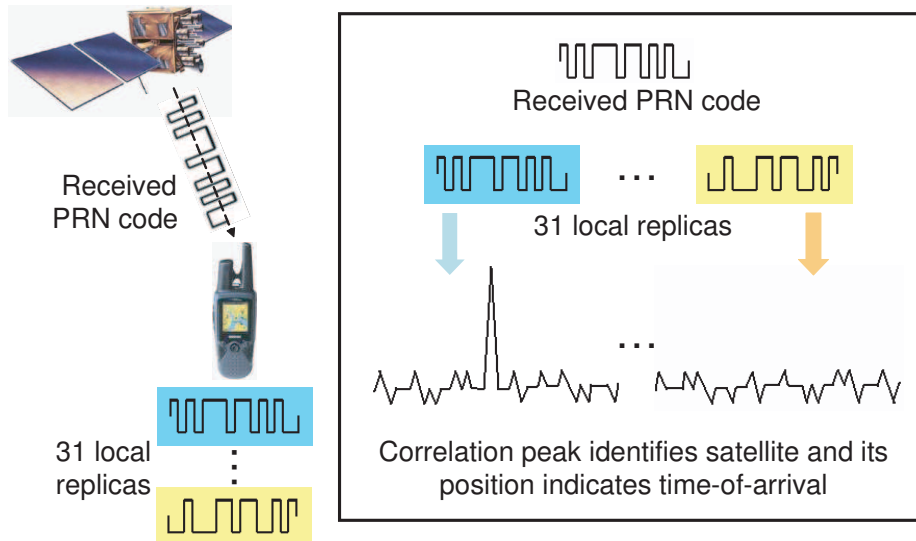


Figure 1.3: How positioning works.

## 1.2.2 GLONASS

GLONASS (pronounced as Gluh'naas in Russian, an acronym for GLObal'naya NAVigatsionnaya Sputnikovaya Sistema, translated as Global Navigation Satellite System)

was developed by the former Soviet Union starting in 1976. GLONASS is now operated for the Russian government by the Russian Space Forces [11]. Like GPS, GLONASS was originally designed for military use only, but in the late 1980s, some GLONASS signals were open for civilian use [12]. When the constellation was completed in the mid-1990s, civil users were excited about accessing two systems, both GPS and GLONASS [13, 14]. Unfortunately, GLONASS rapidly fell into disrepair with the change of the Russian political and economic environment [15]. Beginning in 2001, the Russian government has shown interest in restoring the system [16].

The GLONASS constellation contains 16 MEO satellites as of August 2008. They orbit at an altitude of 19100 km and at an inclination angle of  $64.8^\circ$  [4]. GLONASS availability (the fraction of time when a position can be calculated) in Russia is 66.2% and average availability for the whole Earth is at 56.0% [17].

In contrast to GPS, GLONASS is a Frequency Division Multiple Access (FDMA) system. There are two types of signals, a standard precision (SP) signal in L1 band and an obfuscated high precision (HP) signal in L2 band. The whole L1 band from 1602.5625 MHz to 1615.5 MHz is divided into 25 subbands, each 0.5625 MHz wide, while the L2 band spans from 1240 MHz to 1260 MHz, with each subband 0.4375 MHz wide. All satellites transmit the same Standard Precision code, but in different frequency subbands [18].

## 1.3 GNSS Under Development

### 1.3.1 Galileo

The Galileo system, named after the Italian astronomer Galileo Galilei, is the planned European (GNSS). The project is a joint initiative of the European Commission (EC) and the European Space Agency (ESA). It is an alternative and complementary counterpart to GPS and GLONASS. The Galileo system aims to provide a highly accurate, guaranteed global positioning service under civilian control [19]. When fully deployed, the Galileo system will have 30 MEO satellites at an altitude of 23222 km. There will be three orbital planes inclined at an angle of  $56^\circ$  to the equator. Ten

Frequency band	Center frequency (MHz)
L1	1575.42
E5a	1176.45
E5b	1207.14
E6	1278.75

Table 1.2: Galileo frequencies

satellites will occupy each orbital plane. Nine of them will be operational satellites with one spare for redundancy [20].

The first test satellite of the Galileo system, GIOVE-A, was launched on December 28, 2005. It secures the Galileo frequencies allocated by the International Telecommunication Union (ITU) and also tests certain Galileo satellite components [8]. GIOVE-A is capable of transmitting on two frequencies at once from an available set of L1 (1575.42 MHz), E5 (1191.80 MHz) and E6 (1278.75 MHz) bands as shown in Table 1.2. The E5 band has two sub-bands, E5a (1176.45 MHz) and E5b (1207.14 MHz) band. GIOVE-A started to broadcast Galileo signals on January 12, 2006, first on L1 and E6 bands. Based on our observation, it switched to L1 and E5 bands in August 2006 for a few weeks and switched back to L1 and E6 frequencies in September 2006. Since October 25, 2006, it has been again transmitting on L1 and E5 bands.

As a further step towards the development of Galileo, the second test satellite, GIOVE-B, was launched on April 27, 2008, as shown in Figure 1.4 [2]. GIOVE-B started to transmit signals on May 7, 2008 [21].

Galileo is similar to the United States GPS in both concept and design. They are both CDMA systems [22]. Multiple satellites transmit signals in the same bands but with different spread spectrum codes to differentiate themselves. Compared with the widely used GPS civil signal in the L1 band, Galileo signals are different in three respects: Galileo L1 signals use a new type of modulation scheme, Binary Offset Carrier (BOC); Galileo E5a and E5b signals suffer from pulsed interference from existing aeronautical systems, mainly Distance Measuring Equipment (DME) and Tactical Air Navigation (TACAN) systems; the Galileo E6, E5a and E5b codes have 5 to 10 times higher chip rate than that of the GPS L1 civil codes. These differences



Figure 1.4: Launch of the GIOVE-B satellite on April 27, 2008. Photo credit: ESA [2].

are summarized in Table 1.3. The DME/TACAN interference and higher chip rate will also appear in the future GPS L5 signal.

Galileo frequency band	Differences compared to GPS L1
L1	BOC modulation
E6	Fast code chip rate of 5.115 MHz
E5a	DME/TACAN interference Fast code chip rate of 10.230 MHz
E5b	DME/TACAN interference Fast code chip rate of 10.230 MHz

Table 1.3: Galileo signals compared to the GPS L1 civil signal

### 1.3.2 Compass

The Compass navigation satellite system (CNSS), which is also known as BeidouII, is China's entry into the realm of GNSS. The current design plans for 30 MEO

satellites and 5 geostationary orbit (GEO) satellites. The MEO satellites will operate in six orbital planes to provide global navigation coverage [10]. Compass will share many features in common with GPS and Galileo, providing the potential for low cost integration of these signals into combined GPS/Galileo/Compass receivers. These commonalities include multiple frequencies, signal structure, and services.

Statements from Chinese sources indicate that the system will provide at least two services: an open civilian service and a higher precision military/authorized user service [10]. According to International Telecommunication Union (ITU) filings by China, Compass will broadcast in four frequency bands known as E1, E2, E6 and E5b [3]. Table 1.4 provides center frequencies of the signal transmission bands. Figure 1.5, adapted from [3], shows the overlap in frequency of the Compass signals with those of GPS and Galileo. Like GPS and Galileo, the Compass navigation signals are CDMA signals. They use binary or quadrature phase shift keying (BPSK, QPSK, respectively) [4].

Frequency band	Center frequency (MHz)
E1	1589.74
E2	1561.10
E6	1268.52
E5b	1207.14

Table 1.4: Compass frequencies

The Compass-M1 satellite, launched on April 14, 2007, represents the first of the next generation of Chinese navigation satellites and differs significantly from China's previous Beidou navigation satellites. Those earlier satellites were considered experimental, and were developed for two-dimensional positioning using the radio determination satellite service (RDSS) concept pioneered by Geostar [23]. Compass-M1 is also China's first MEO navigation satellite. Geostar was based on two-way ranging, whereas Compass-M1 is based on one-way pseudo-ranging. Previous Beidou satellites were geostationary and only provided coverage over China. The global implications of this satellite and the new GNSS it represents make the satellite of great interest to navigation experts.

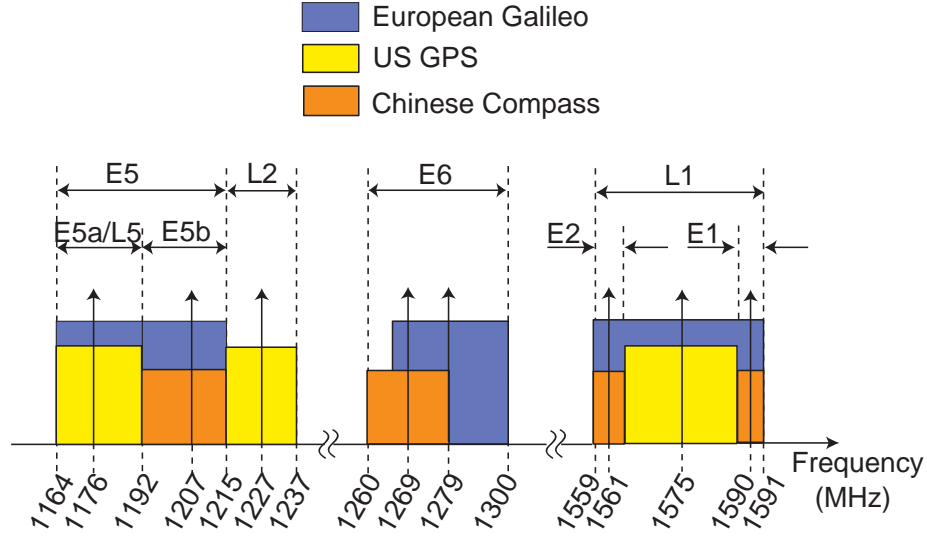


Figure 1.5: Frequency occupation of GPS, Galileo and Compass, adapted from [3]

## 1.4 Problem Statement

The similarity in frequency, signal structure, and services with GPS makes Galileo and Compass a tantalizing prospect for GNSS users. These similarities could allow for the addition of Compass and Galileo to an integrated GNSS receiver without additional expensive hardware or processing. As such, great motivation exists for understanding Compass and Galileo. Conversely, the signals of Galileo or Compass may pose a source of interference and degrade the performance of other GNSS, because the frequency bands overlap, as shown in Figure 1.5. Hence, understanding Compass and Galileo signal design and modulation is important to determine their potential for interoperability and interference. Finally, we study Galileo and Compass for engineering insight. GPS developers are considering designs for new signals for GPS and terrestrial ranging sources that could augment GPS. Thus, we are eager to gain a deep understanding of the recent efforts of our European and Chinese colleagues.

To summarize, the recently launched satellites provide tremendous opportunities to

- study the benefit of redundancy on positioning accuracy and integrity;

- study the extent of interference among GNSS satellites;
- learn from the signal design of our international colleagues.

The first step towards these goals is to determine the Compass and Galileo codes. However, little information was published on the broadcast PRN codes of the Compass-M1 or GIOVE satellites.

The goal of the research presented in this dissertation is to decipher the unknown signal structure broadcast by the Galileo GIOVE-A and GIOVE-B satellites and the Compass-M1 satellite; in particular, the PRN code sequences and code generation schemes. Since little information was released publicly about the test satellites, we aimed to characterize the signal definition by observation alone.

We now describe the main challenges in deciphering the PRN codes and their generation structures.

### **Very weak signal**

Received Compass and Galileo signals suffer from extremely low signal to noise ratio (SNR) due to path loss. Their signals travel 21550 km and 23222 km, respectively, to reach Earth. With an omnidirectional antenna, the received signal power is on the order of  $10^{-16}$  W, assuming a transmit power of 30 W. Even with a 1.8 m dish antenna and high-quality low noise amplifiers (LNA), the received SNR is still roughly 65 to 70 dBHz and the SNR in the signal noise equivalent bandwidth is about  $-5$  to 10 dB. The PRN code chips are buried in noise and not directly visible in the time domain.

### **Complicated unknown signal structure**

Another challenge is that the signal structure associated with the PRN codes is not only unknown, but also can be very complicated. The code periods and clock rate are unknown. There can be code overlays or composite codes. For example, there can be navigation data or secondary codes modulated on top of the primary PRN codes. Separate codes may be used on inphase and quadrature channels. The primary PRN codes can be truncated or concatenated.



### Unsynchronized data collection apparatus

The data collection apparatus is not synchronized with the transmission. There is an unknown Doppler shift associated with each satellite orbit. Furthermore, the receiver clock has limited precision. This together with satellite clock drift causes offsets in carrier frequency, carrier phase and code phase.

### Severe pulsed aeronautical interference

Finally, the Galileo and Compass E5 band suffers from strong pulsed DME/TACAN interference. Based on our observation at Stanford using our 1.8 m dish antenna, the DME/TACAN pulses are 10 to 100 times higher in amplitude than the noise floor, while the GNSS signals are even below the noise floor. These aeronautical pulses also occur as frequently as 10% to 14% of the time. The aeronautical interference degrades the already very low SNR and makes the PRN codes even more difficult to reveal.

## 1.5 Related Work

### Decoding GLONASS

Daly *et al.* from University of Leeds characterized and decoded the PRN codes of the Russian GLONASS satellites in the late 1980s [24, 25]. Although GLONASS codes are also linear, the GLONASS system is an FDMA system, which is very different from the CDMA systems of Galileo and Compass.

### Simulated study of aeronautical interference to GNSS

In November 1999, the Interagency GPS Executive Board (IGEB) endorsed a set of recommendations on implementing the third frequency L5 for civil GPS [26]. One of the recommendations was to ensure that L5 can coexist with aeronautical systems operating at the same or nearby frequencies. Hegarty *et al.* conducted pioneering research on the impact of pulsed interference on GPS user equipment [27]. The

following year, Grabowski *et al.* characterized the L5 receiver performance using digital pulse blanking [28], and Bastide *et al.* assessed the L5 performance in the presence of DME/TACAN interference with a realistic receiver simulator [29]. The research on coexistence of GPS and DME/TACAN was continued [30–32]. In 2004, the Radio Technical Commission for Aeronautics (RTCA) under the Federal Aviation Administration (FAA) presented a thorough report on the radio frequency interference in the GPS L5 band [33].

Aeronautical interference is also an issue for Galileo. Researchers in Europe have been analyzing the European L5/E5 band interference environment and assessing interference mitigation techniques [34, 35].

So far, all the research regarding DME/TACAN interference has been based on simulation or bench tests. We are the first to analyze such interference using real broadcast signals.

## **GIOVE-A and GIOVE-B**

We now briefly relate the history of the design, decoding and release of the GIOVE-A and GIOVE-B PRN codes. Hein *et al.* from the Galileo Signal Task Force of the European Commission first described a tentative Galileo frequency and signal design in 2001 [22], which became the baseline for the development of Galileo. Hein *et al.* updated the signal design, including the characteristics of the PRN codes such as the code rates, one year later [36, 37]. After the GIOVE-A launch in December 2005, we decoded the GIOVE-A PRN codes in the L1 and E6 bands, made them public on our lab website in April 2006 and presented the results at the ION GNSS conference in September 2006 [38]. Rooney *et al.* who were responsible for launching GIOVE-A provided GIOVE-A in orbit testing results [39, 40]. In the meantime, researchers from other universities and research institutes also studied the L1 PRN codes [41–43]. However, they only studied the PRN sequences, not the generating structures. Also, they limited their research to the L1 band, while our research went much further. Later that year, the GIOVE-A transmission switched to L1-E5 mode. We then also decoded the broadcast E5a and E5b PRN codes [44]. The first official appearance of PRN code sequences was in Galileo Open Service Signal In Space Interface Control

Document (OS SIS ICD) on May 23, 2006 [45]. However, the published codes differed from codes we decoded. The European Space Agency and Galileo Joint Undertaking released the GIOVE-A PRN codes in GIOVE-A Navigation SIS ICD in February 2007 [46]. This time, the released codes matched our decoding results. As for GIOVE-B, we observed its signals in L1, E5a and E5b bands on the same day of its first transmission on May 7, 2008. Within a couple of weeks, we decoded all PRN codes for civilian use in all GIOVE-B bands, and published our results in the May/June 2008 issue of the *Inside GNSS* magazine [47].

### **Compass-M1**

The global implications of the Compass-M1 satellite and the new GNSS it represents made the satellite of great interest to navigation experts. The rapid manner in which researchers trained their instruments onto the satellite proves this point. For example, Grelier *et al.* from Centre National d'Etudes Spatiales (CNES, the French space agency) published an informative overview of their initial observations of the Compass-M1 signals a month after its launch [3, 48]. We deciphered all Compass-M1 PRN codes and the code generators, and published our results in the July/August 2007 issue of the *Inside GNSS* magazine [49].

## **1.6 Summary of Contributions**

The main contribution of this work is to decipher the new test satellite signals from the Galileo and Compass satellite programs, where the signal definition had not been published, and to examine the properties and interaction of these CDMA multiple access codes.

### **Designed algorithms for deciphering unknown PRN codes chips**

The first step in analyzing the signals is to reveal the unknown PRN code chips. The concept is to raise the SNR level by synchronously combining multiple periods of the received signal. Due to the challenges mentioned in Section 1.4, the decoding

process includes signal conditioning, PRN code period determination, Doppler offset wipeoff, secondary code or navigation data removal, initial carrier phase adjustment, determination of the code start, and more.

### **Modified the Berlekamp-Massey algorithm in an error-tolerant manner**

Once the SNR is improved and the code chips are estimated, the code generators must be defined and analyzed. This step requires a substantial modification of the well-known Berlekamp-Massey algorithm [50], to be robust against a high probability of code chip error.

### **Characterized Galileo and Compass test satellite signals**

We apply the algorithms of our design to the current test satellites of the Galileo and Compass systems, to decipher all civil PRN codes in all frequency bands. We not only discover the PRN code sequences, but also derive the code generation schemes. All broadcast PRN codes of the GIOVE and Compass satellites are proved to be truncated or concatenated Gold Codes [38, 44, 47, 49], and can be generated by linear feedback shift registers (LFSR). The generator polynomials and initial states are calculated.

The deciphering results are already implemented in our software receiver to acquire and track the satellites. The deciphered PRN codes were also implemented in commercial receivers by various companies, such as Trimble Navigation, Ltd., Javad GNSS Inc., and Septentrio, Inc [51].

### **Established multiple access capacity of GNSS**

We assess the self-interference within GNSS, and hence establish their multiple access capacity, by examining the code interactions between satellites. This analysis requires considering cross-correlation properties of the codes at all possible Doppler frequency offsets between satellites.

### Analyzed pulsed interference mitigation

We analyze the pulsed DME/TACAN interference environment at Stanford, CA using real broadcast GNSS signals. A hybrid blanking technique for mitigating the interference is proposed and compared with existing techniques.

## 1.7 Dissertation Outline

Chapter 2 describes the equipment used to capture broadcast GIOVE and Compass signals. Two facilities are introduced: the 45.7 m Stanford SRI dish and the Stanford GNSS Monitor System (SGMS) with a 1.8 m dish antenna. Spectrum plots of all GIOVE and Compass transmission bands are presented. Time-domain signals in E5a and E5b bands show strong DME/TACAN interference pulses.

Chapter 3 is an overview of the GIOVE and Compass PRN code deciphering. A mathematical model for GNSS signals is developed based on our understanding of the GPS signals and a decoding flow chart based on this model is presented.

Chapter 4 describes the deciphering of the broadcast Compass-M1 codes. The Compass E6 decoding is described in detail. We not only reveal the code chips, but also demonstrate that the code sequences are linear, truncated Gold Codes. The generators (code polynomials and initial states) are also derived. We also tabulate the decoding results in other frequency bands, namely E2 and E5b bands.

Chapter 5 describes deciphering the Galileo GIOVE-A and GIOVE-B broadcast codes and deriving their code generators. The GIOVE codes are more complicated to decode than their Compass counterparts. First, there are two codes with different code periods superimposed in each channel. Thus, there is an additional challenge in separating the two codes. Second, the Galileo civil signals in E5 band suffer from more DME/TACAN interference, because the bandwidth covers more DME/TACAN frequencies. Third, the Galileo L1 band overlaps with GPS L1, so the GPS signals behave as additional noise when decoding Galileo GIOVE codes.

Chapter 6 analyzes the properties of the decoded codes, such as balancing and auto- and cross-correlation at different frequency offsets. The code properties are

then used to assess the self-interference among GNSS, and to establish the multiple access capacity of GNSS.

In Chapter 7, we modify a software receiver to acquire and track the GIOVE and Compass satellites. Using this platform, we then analyze the performance of the Galileo/Compass receivers in the presence of DME/TACAN interference in the Stanford environment. To mitigate interference, a time and frequency domain hybrid blanking technique is proposed and compared with the time domain or frequency domain only techniques. We show that mitigation of pulsed interference is beneficial to receiver performance.

## Chapter 2

# Capturing Satellite Transmission

The first step towards analyzing new satellite signals is to capture their transmissions. We use two facilities at Stanford University for this task.

### 2.1 Stanford SRI 45.7 m Dish

The 45.7 m dish in the Stanford hills operated by Stanford SRI International is shown in Figure 2.1. The SRI dish is a high gain parabolic antenna designed for L-band signals with central frequency 1420 MHz. Its attainable gain can be as high as 52 dB with  $0.25^\circ$  beamwidth and 35% efficiency. The total structure weighs 1,400,000 kg. The surface of the SRI dish is made of soft aluminum hex pattern mesh with 1.6 cm spacing [52]. A Vector Signal Analyzer (VSA) is used to collect the satellite transmission received through the Stanford SRI dish.

Figures 2.2 and 2.3 show the spectra of the GIOVE-A L1 and E6 signals, respectively, collected using the Stanford SRI dish on April 20, 2006. The signals are down converted to baseband. The antenna gain is high enough to boost the received Galileo signal above the noise floor. The shape of the spectra match the modulation of the L1 and E6 signals. In Figure 2.2, the two lobes in the center correspond to the BOC(1,1) modulation of the L1 open service signal, and the two wider lobes located 15 MHz from the center frequency represent BOC(15, 2.5) modulation of the Galileo Public Regulated Service (PRS) signal. In Figure 2.3, the main lobe in the center is



Figure 2.1: Stanford SRI dish antenna, 45.7 m in diameter, 52 dB gain and  $0.25^\circ$  beamwidth. Photo credit: Max Klein

a commercial access signal with BPSK(5) modulation. The two side lobes represent a PRS signal with BOC(10,5) modulation.

The strength of the Stanford SRI dish is high antenna gain, which makes it easier to subsequently decode the Galileo code sequences. However, the disadvantage is that it takes weeks and great expense to reserve usage. Therefore, we prefer to use another data collection facility with easier accessibility.



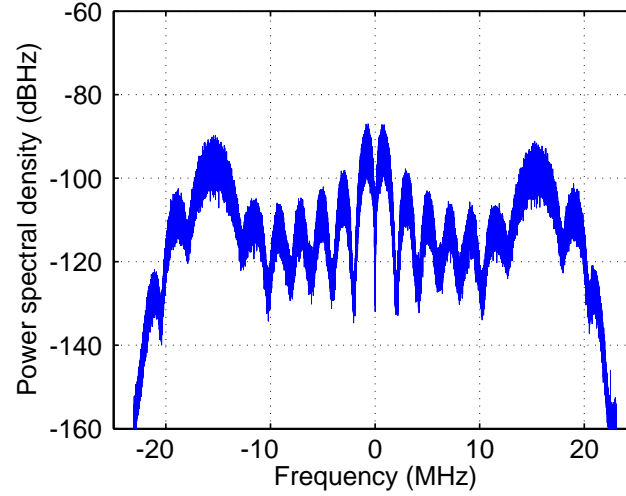


Figure 2.2: The GIOVE-A L1 band spectrum observed by the Stanford SRI dish. The signals are down converted to baseband. The antenna gain is high enough to boost the signal above the noise. The two small lobes in the center correspond to the BOC(1,1) modulation of the L1 open service signal, and the two wider lobes located 15 MHz from the center frequency represent BOC(15, 2.5) modulation of the Galileo Public Regulated Service signal.

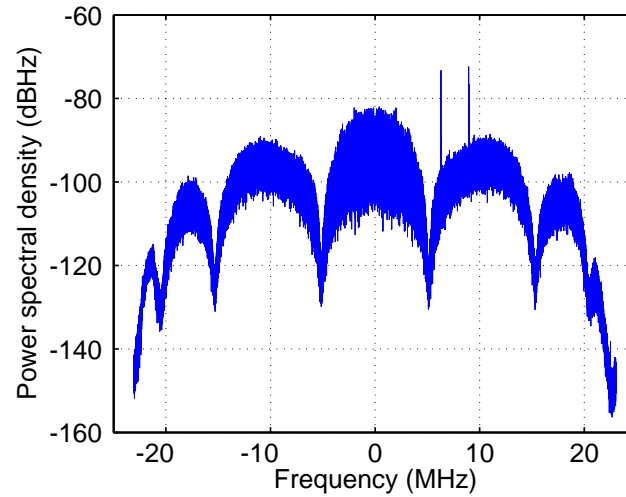


Figure 2.3: The GIOVE-A E6 band spectrum observed by the Stanford SRI dish. The main lobe in the center is a commercial access signal with BPSK(5) modulation, and the two side lobes represent a PRS signal with BOC(10,5) modulation.

## 2.2 Stanford GNSS Monitor System 1.8 m Dish Antenna

Our lab's Stanford GNSS Monitor System (SGMS) provides another method for collecting satellite transmissions. SGMS includes a 1.8 m steerable parabolic dish antenna, mounted on the roof of the Durand building, as shown in Figure 2.4. The 1.8 m dish, connected to an L band feed, has approximately  $7^\circ$  beamwidth and provides about 25 dB of gain over conventional patch antennas [53]. The antenna is controlled by satellite tracking software, Nova for Windows [54], which reports the satellite observation times and paths over our location. The software also drives the antenna azimuth and elevation motors, so that the main lobe of the antenna gain pattern always points to the satellite. The signal from the feed of the antenna passes through a band pass filter and LNAs and is collected by an Agilent 89600 VSA. The VSA can down convert the RF signal to baseband and save the I and Q channel data as complex samples in a computer-readable format. The entire SGMS is illustrated in Figure 2.5. Table 2.1 illustrates the link budget for the received GPS L1 C/A signal. The received SNR over 2 MHz bandwidth ranges 4 to 7 dB. For general GNSS signals, the received SNR in the signal noise equivalent bandwidth is about -5 to 10 dB.

	Units	Low El	Moderate El	Zenith
Frequency	GHz	1.57542	1.57542	1.57542
Wavelength	m	0.19	0.19	0.19
Transmitter Power	W	27	27	27
Antenna Diameter	m	1.8	1.8	1.8
Antenna Efficiency		0.5	0.5	0.5
Antenna Beamwidth	deg	7.41	7.41	7.41
Antenna Gain	dBi	26.39	26.39	26.39
Received Power	dBW	-133.63	-131.64	-133.59
Noise Density	dBW/Hz	-201	-201	-201
SNR (Over 2 MHz Band)	dB	4.36	6.35	4.4

Table 2.1: Link budget of GPS L1 signal at different elevations captured by 1.8 m dish



Figure 2.4: Stanford GNSS Monitor System, 1.8m dish

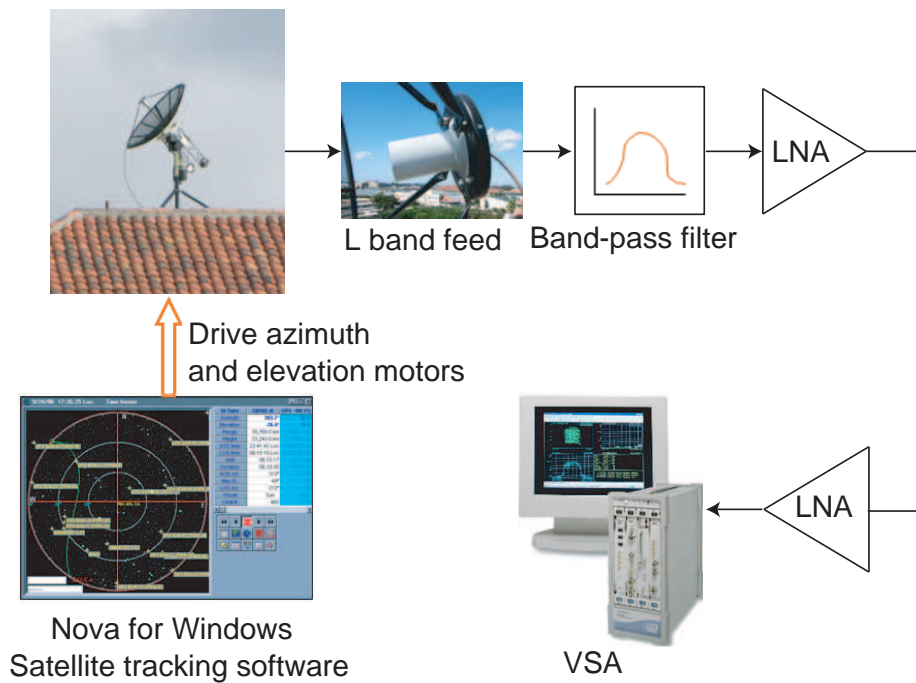


Figure 2.5: Stanford GNSS Monitor System. The 1.8 m dish antenna is controlled by Nova for Windows software, which drives the antenna azimuth and elevation motors to track satellites. The signal from the L band feed of the antenna passes through a band pass filter, low noise amplifiers (LNAs) and is collected by an Agilent 89600 Vector Signal Analyzer (VSA).

Figure 2.6 shows the baseband GIOVE-A L1 signal spectrum observed from the SGMS dish. The flat part is the noise floor filtered by a bandpass filter. Compared to the L1 spectrum observed by the Stanford SRI dish in Figure 2.2, the SGMS antenna gain is much lower. We can barely see the main lobes of the BOC(1,1) and BOC(15, 2.5) modulation. Most of the spectrum is buried in noise. So, the trade off for on-demand data collection and easy accessibility is low antenna gain. Chapters 3 to 5 will demonstrate how to use sophisticated signal processing to boost the signal above the noise.

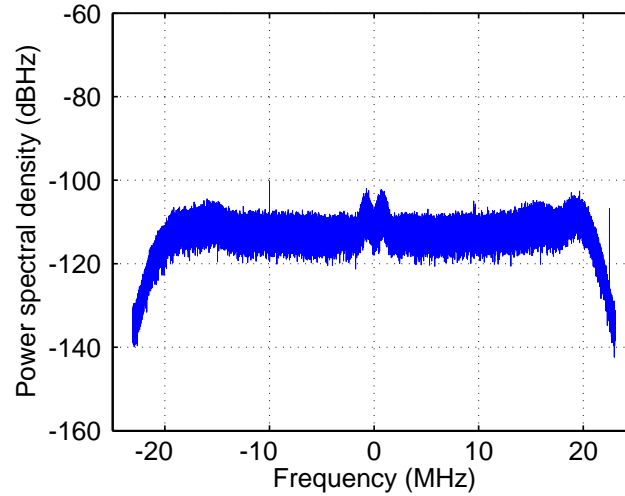


Figure 2.6: The GIOVE-A L1 band spectrum observed by the SGMS dish. The BOC(1,1) spectrum is slightly visible at the center of the plot.

Figures 2.7 and 2.8 show the frequency spectra of the GIOVE-A E5a and E5b signals in baseband. The BPSK(10) modulation for both E5a and E5b is not visible since the signals are buried in noise. Moreover, we see strong narrow band tones attributed to DME/TACAN, one obvious in the E5a band and three obvious in the E5b band. Each tone represents the airborne interrogators and the beacon DME signal from a nearby airport. The power spectral density of the DME interference exceeds the noise floor of -110 dB by 50 dB for E5a and by 32 dB for E5b. More troubling, even if these observed DME signals are not in the primary beamwidth of the antenna, their high power levels nevertheless make them apparent in the data.

The E5 signals are even weaker than the noise floor and are completely buried in noise, even though the antenna gain is as high as 25 dB. All that is apparent in the spectral density plots is the VSA filter shape and the DME interference.

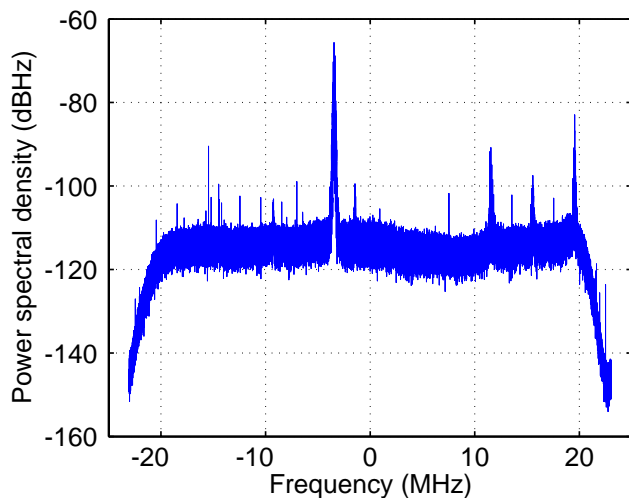


Figure 2.7: The GIOVE-A E5a band spectrum observed by the SGMS dish. The BPSK(10) modulation for E5a is not visible since the signals are buried in noise. Moreover, we see strong narrow-band tones attributed to DME/TACAN, one obvious in the E5a band. Each tone represents the airborne interrogators and the beacon DME signal from a nearby airport.

Time-domain observations of the E5a and E5b signals in Figures 2.9 and 2.10, respectively, show that strong DME/TACAN pulses are frequent. Figure 2.11 zooms in to the E5b signal and Figure 2.12 zooms in even further, showing a Gaussian pulse pair. The DME/TACAN pulses are 5 to 100 times greater in amplitude than the noise, while the E5 signals are even weaker than noise. Thus, DME interference poses a further challenge in decoding the signal.

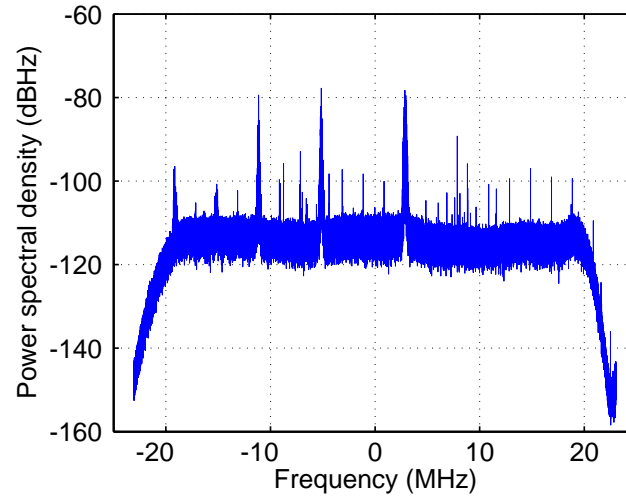


Figure 2.8: The GIOVE-A E5b band spectrum observed by the SGMS dish. There are three strong narrow-band tones attributed to DME/TACAN.

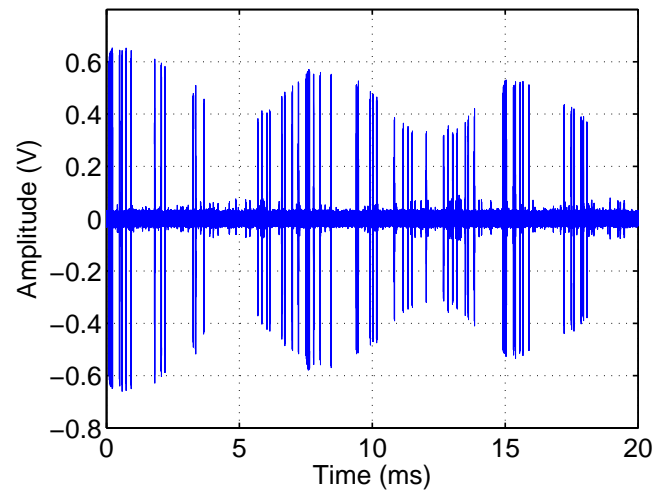


Figure 2.9: The time-domain GIOVE-A E5a signal observed by the SGMS dish

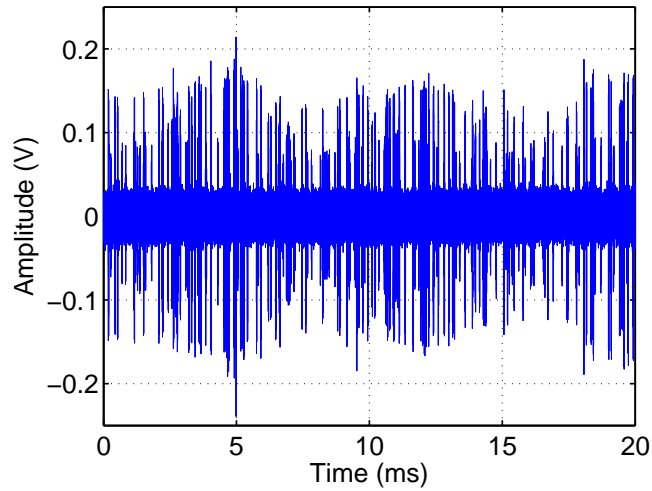


Figure 2.10: The time-domain GIOVE-A E5b signal observed by the SGMS dish. The DME/TACAN pulses in time domain are 5 to 100 times greater in amplitude than the noise, while the E5 signals are even weaker than noise.

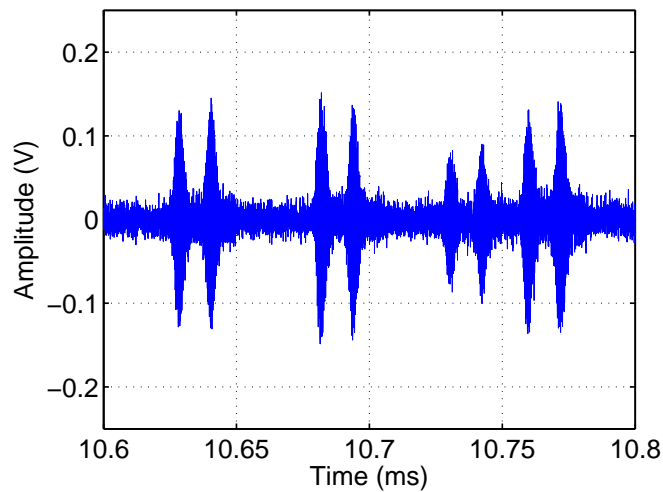


Figure 2.11: The time-domain GIOVE-A E5b signal observed by the SGMS dish, zoomed in.



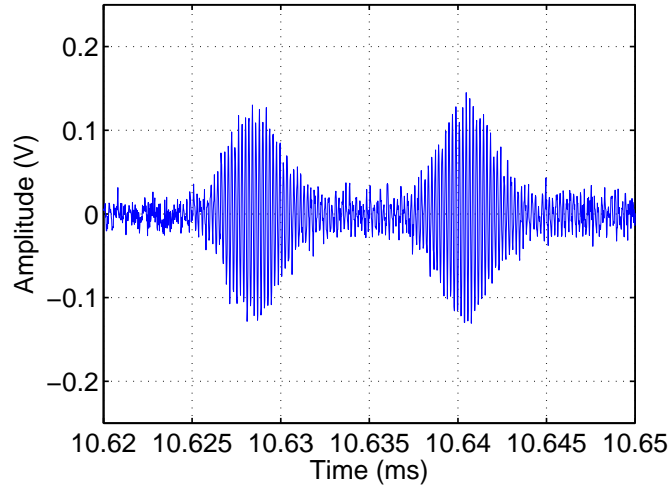


Figure 2.12: The time-domain GIOVE-A E5b signal observed by the SGMS dish, zoomed in further

Figures 2.13, 2.14 and 2.15 show the spectra of Compass-M1 signals in E2, E5b and E6 bands respectively. In Figure 2.13, the main lobe and the adjacent side lobes of the 2 MHz chipped E2 signal are visible without averaging. An L1 signal from a nearby GPS satellite can also be seen in this plot as well as some interference in the lower part of the bandwidth. In the E5b spectrum in Figure 2.14, the main lobe of the BPSK(2) civil signal is visible, and the main lobe of the BPSK(10) military signal can also be made out. As expected in this frequency band, we also see strong narrow-band DME/TACAN interference. Figure 2.15 shows the unaveraged E6 signal spectrum with the main feature being the main lobe of the QPSK(10) signal. Also visible is an as-yet-unidentified 1 MHz-wide transmission centered around 11 MHz below the E6 carrier frequency.

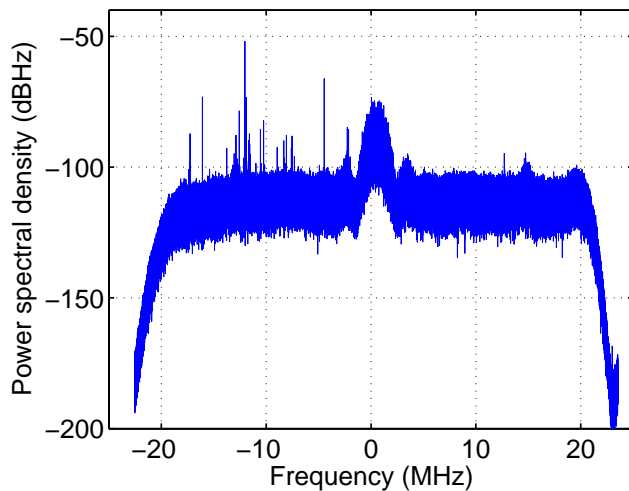


Figure 2.13: The Compass-M1 E2 band spectrum observed by the SGMS dish. The main lobe and the adjacent side lobes of the 2 MHz chipped E2 signal are visible without averaging. An L1 signal from a nearby GPS satellite can also be seen in this plot as well as some interference in the lower part of the bandwidth.

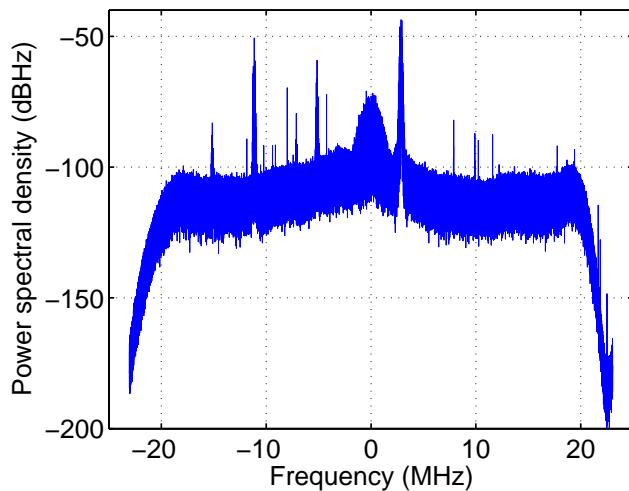


Figure 2.14: The Compass-M1 E5b band spectrum observed by the SGMS dish. The main lobe of the BPSK(2) civil signal is visible, and the main lobe of the BPSK(10) military signal can also be made out. As expected in this frequency band, we also see strong narrow-band DME/TACAN interference.

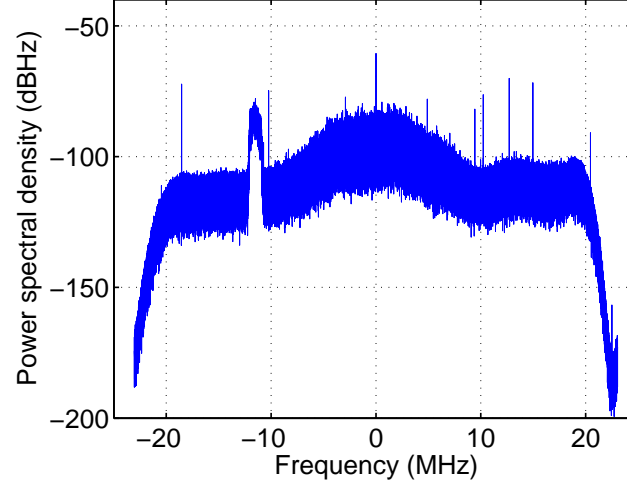


Figure 2.15: The Compass-M1 E6 band spectrum observed by the SGMS dish. The main feature is the main lobe of the QPSK(10) signal. Also visible is an as-yet-unidentified 1 MHz-wide transmission centered around 11 MHz below the E6 carrier frequency.

## 2.3 Summary

This chapter described the equipment for capturing broadcast GNSS signals. We used two facilities, the 45.7 m Stanford SRI dish and the 1.8 m SGMS dish antenna. The Stanford SRI dish has higher gain, while the SGMS dish is easier to access. Due to the convenient accessibility, we mainly used the 1.8 m SGMS dish to collect data, and only used the 45.7 m dish to verify the decoding results. Spectrum plots of all GIOVE and Compass transmission bands were presented. Time and frequency domain plots of GNSS signals in E5a and E5b bands showed strong DME/TACAN interference pulses, which make the deciphering process more challenging.



# Chapter 3

## Signal Modeling and Decoding Overview

In this chapter, we build a mathematical model for received Galileo and Compass signals. The model represents the components and the parameters of the received signals. We then outline a process of revealing the PRN codes by stripping off all the other components.

### 3.1 GNSS Signal Modeling

Since both Compass and Galileo are code division spread spectrum systems, a signal received from one of their satellites contains a spread PRN code, which is a binary  $\pm 1$  vector denoted as  $\mathbf{c} = (c_0, c_1, c_2, \dots, c_{N_c-1})$ . The PRN code is the spreading code that identifies each satellite and is the object of our decoding.

Each chip in the PRN code  $\mathbf{c}$  has a rectangular shape.

$$W_c(t) = \begin{cases} 1, & 0 < t \leq T_c \\ 0, & \text{otherwise,} \end{cases} \quad (3.1)$$

where  $T_c$  is the duration of a PRN code chip. As an exception, the PRN code chips of Galileo L1 signals are modulated with Binary Offset Carrier (BOC), which will be described in detail in Chapter 5.

The PRN code signal  $C(t)$  is therefore the periodic BPSK version of  $\mathbf{c}$ .  $C(t)$  is periodic with the code period,  $T_d = N_c T_c$ . In other words,

$$C(t) = C(t - lT_d), \quad (3.2)$$

for all integers  $l$ .

One period of  $C(t)$  is

$$C(t) = \sum_{i=0}^{N_c-1} c_i W_c(t - iT_c), \quad (3.3)$$

where  $N_c$  is the number of chips in the PRN code sequence.

The PRN code is modulated with either navigation data or a secondary code or both. The secondary code is a low-rate code modulated on top of the carrier and PRN code. Secondary codes increase the signal repetition time, moving individual spectral lines closer, and thus reducing the line spectrum in the frequency domain. Since receivers are expected to know the secondary codes beforehand, they can integrate for long periods of time for acquisition, and therefore obtain a high processing gain. In either case, we denote the binary  $\pm 1$  sequence as the vector  $\mathbf{d} = (d_0, d_1, d_2, \dots)$ , and refer to it as the secondary code, for simplicity. The secondary code bit duration is same as the PRN code period  $T_d$ . Then we express the square wave of the navigation signal as

$$D(t) = \sum_{i=0}^{\infty} d_i W_d(t - iT_d), \quad (3.4)$$

where  $W_d(t)$  is a rectangular window function with width  $T_d$ ,

$$W_d(t) = \begin{cases} 1, & 0 < t \leq T_d \\ 0, & \text{otherwise.} \end{cases} \quad (3.5)$$

The modulated signal,  $D(t)C(t)$ , is carried with a nominal carrier frequency  $f_c$ . Since the satellite is moving, the carrier is affected by a Doppler frequency offset  $f_D$  and an initial phase  $\theta$ . The relationship between the PRN code signal, the secondary code and the carrier is shown in Figure 3.1.

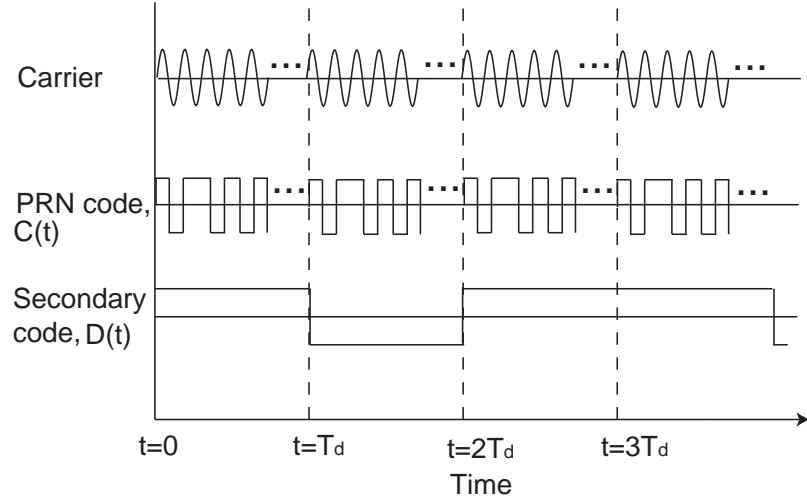


Figure 3.1: Example of relationship between the PRN code signal, the secondary code, and the carrier. The secondary code duration is the same as the PRN code period.

The received signal is written as

$$\sqrt{P}D(t - \tau_d)C(t - \tau_d) \exp j(2\pi(f_c + f_D)t + \theta) + n(t), \quad (3.6)$$

where  $\tau_d$  is the code phase offset arising from the lack of synchronization between the recorded data and the start of the PRN code. The signal power is  $P$ , and  $n(t)$  captures noise and interference. For decoding, the SNR matters, not the absolute signal power. Hence, we normalize by the signal power, and the noise becomes  $n_0(t) = n(t)/\sqrt{P}$ .

So, the received signal  $s(t)$  is written as

$$D(t - \tau_d)C(t - \tau_d) \exp j(2\pi(f_c + f_D)t + \theta) + n_0(t). \quad (3.7)$$

We now define the code phase  $\tau_d$  in (3.6) and (3.7) formally. First we set  $t = 0$  to represent the start of the recording. Then  $\tau_d$  is the start of the first complete period of the PRN code. Clearly,  $\tau_d$  is less than the secondary code bit duration; that is  $0 \leq \tau_d < T_d$ .

The relationship of  $T_c$ ,  $T_d$  and  $\tau_d$  with the recorded data is illustrated in Figure 3.2. For simplicity, the carrier, Doppler offset and noise are not shown in the figure.

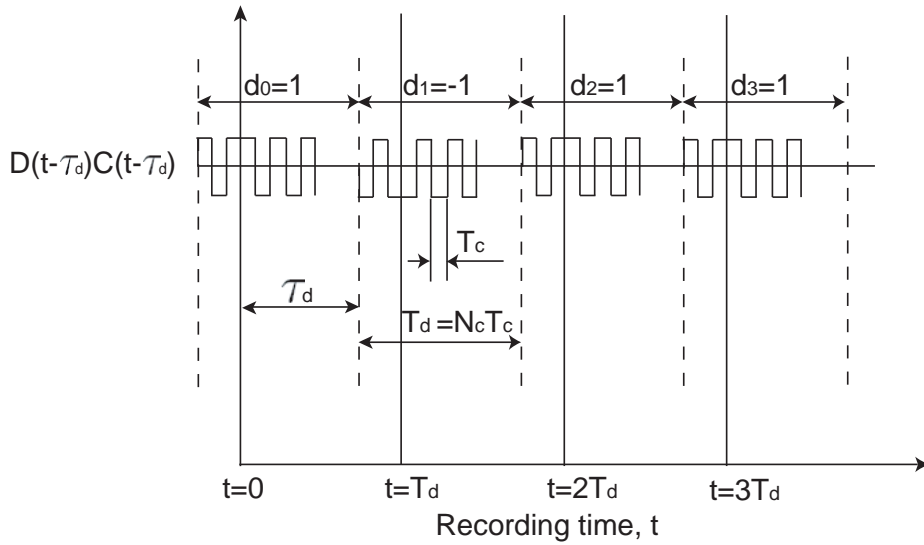


Figure 3.2: The relationship of  $T_c$ ,  $T_d$  and  $\tau_d$  with the recorded data.  $T_c$  is the PRN code chip duration.  $N_c$  is the number of bits per PRN code period. The PRN code period is the same as the secondary code bit duration,  $T_d = N_c T_c$ .  $\tau_d$  is the code phase offset arising from the lack of synchronization between the recorded data and the start of the PRN code. In other words,  $\tau_d$  represents the start of the first complete period of the PRN code.



Although (3.7) represents a basic mathematical model for received Compass or Galileo signals, the following additional details are specific to each system.

The Compass system always employs two signals in each frequency band, inphase and quadrature signals. The inphase signal contains a short PRN code for civilian use, while the quadrature signal contains a long PRN code for military use. Since we are only interested in the short civilian code, the signal model only shows the inphase code. We take the quadrature signal as interference and include it in  $n_0(t)$ .

The Galileo civil signals always use two codes superimposed in all frequency bands. So the signal model for E6, E5a and E5b signals is

$$\sum_{w=1}^2 D_w(t - \tau_d) C_w(t - \tau_d) \cdot \exp j(2\pi(f_c + f_D)t + \theta) + n_0(t), \quad (3.8)$$

where  $C_1$  and  $D_1$  are one pair of primary and secondary codes, and  $C_2$  and  $D_2$  are the other pair. For E5a and E5b signals,  $n_0(t)$  includes the DME/TACAN interference in the band.

The Galileo L1 signals not only have two code superimposed like their E6 and E5 counterparts, but also are further modulated with BOC. So the L1 signals are modeled as

$$\sum_{w=1}^2 D_w(t - \tau_d) C_w(t - \tau_d) \cdot BOC(t - \tau_d) \exp j(2\pi(f_c + f_D)t + \theta) + n_0(t), \quad (3.9)$$

where  $BOC(t)$  represents BOC modulation, which will be defined in Figure 5.1.

## 3.2 Decoding Overview

In order to decode the PRN code sequences, we need to process the data to boost the signal above the noise floor. The main idea is to accumulate the signal to suppress the noise. Our approach is to stack multiple periods of the PRN sequence. Discovering secondary code or navigation bit information is required for this method. The signal processing gain is proportional to the length of the data to be stacked. For data collected from the SGMS dish, a few hundred milliseconds to a few seconds of the

satellite transmission have to be recorded. The actual required data length depends on the code chip rate, code duration and the interference level. This method is also suitable for data received by a low cost patch antenna with only 0 to 3 dB antenna gain, but longer data sets need to be recorded in this case.

To reveal the PRN code from the received signal, we need to first condition the received signal if contaminated by DME/TACAN interference, then strip off the secondary code  $D(t)$ , wipe off Doppler offset  $f_D$ , zero the initial phase shift  $\theta$  and adjust the code phase offset  $\tau_d$ . If necessary, we also have to demodulate the BOC modulation as the last step.

The decoding diagram is shown in Figure 3.3. The processing flow follows the numbered arrows. The next two chapters explain the process of Figure 3.3 in detail for Compass and Galileo codes.

### 3.3 Summary

This chapter is an overview of the GIOVE and Compass PRN code deciphering. We first built a signal processing model for received Galileo and Compass signals. The signal model represents the components and the parameters of the received signals. The process of revealing Galileo and Compass codes is to strip off all other components from the received signals, leaving only the PRN codes behind. Therefore, the signal model is the base for the whole decoding process.

The chapter then addressed the challenges of decoding, and presented an overview of the decoding process including a flow chart. The following two chapters will follow the flow chart in detail and describe how to decode Compass and Galileo broadcast codes.

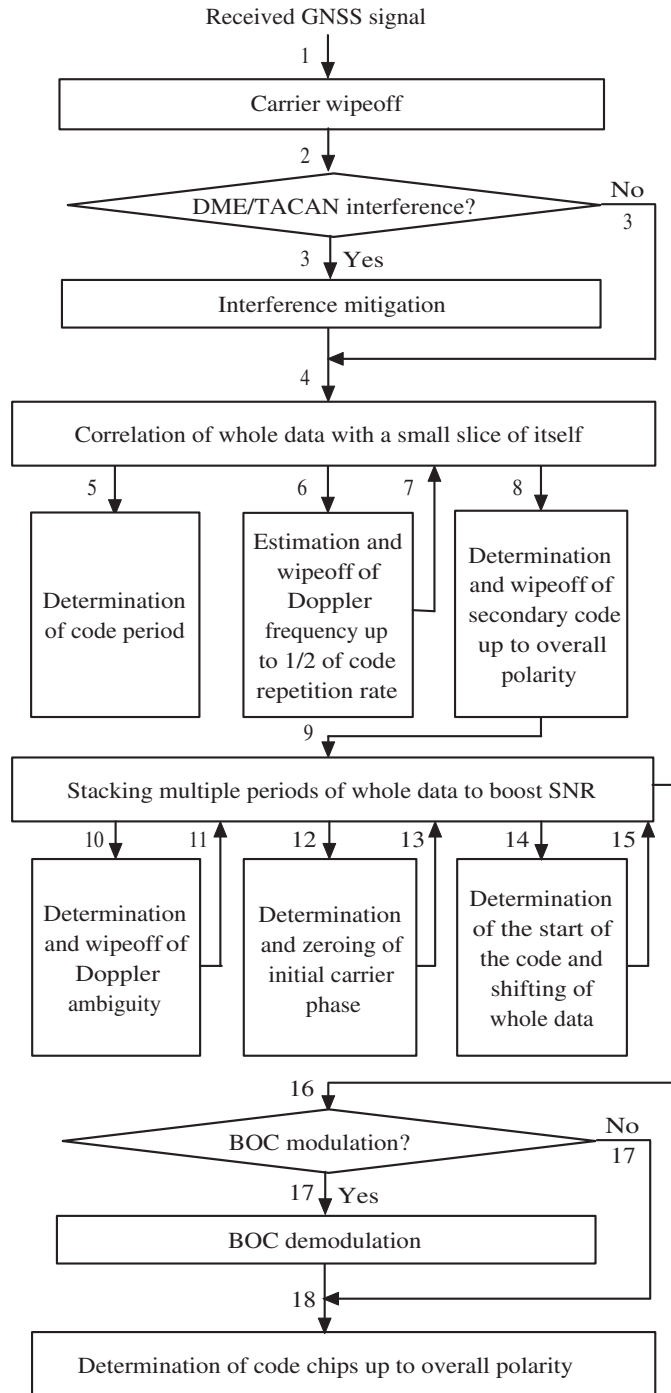


Figure 3.3: Decoding block diagram



# Chapter 4

## Decoding Compass-M1

This chapter discusses in detail how we determine the Compass-M1 E2, E5b and E6 inphase channel codes. The data are collected through the 1.8 m SGMS dish antenna with a sampling rate of 46.08 MHz. The decoding process follows the flow chart in Figure 3.3. We only show the derivation of E6 code, because the decoding process for E2 and E5b codes is similar. Moreover, E6 code is the most difficult to decode due to its high chip rate of 10 MHz. In comparison, the chip rates of the E2 and E5b codes are only 2 MHz.

### 4.1 E6 Code

#### 4.1.1 Carrier Wipeoff

The first step is carrier wipeoff. In our setup described in Chapter 2, the VSA down converts the incoming signal to the baseband. The baseband signal is written as

$$s_b(t) = D(t - \tau_d)C(t - \tau_d) \exp j(2\pi f_D t + \theta) + n_b(t), \quad (4.1)$$

where  $n_b(t)$  is the baseband noise.

Any error between the VSA frequency and the true carrier is treated as part of the Doppler offset and will be wiped off at a later stage.

### 4.1.2 Correlation of Whole Data with a Small Slice of Itself

Although the Compass signal is buried in noise, some of its characteristics can be obtained by correlation, namely code period, Doppler offset and navigation bits. We first correlate the whole data with a small slice of itself.

The small slice of the baseband data is denoted as

$$\tilde{s}_b(t) = \begin{cases} s_b(t), & 0 < t \leq t_0 \\ 0, & t > t_0, \end{cases} \quad (4.2)$$

where  $t_0$  is the duration of the slice of data. It is important that this slice of data does not contain a secondary code bit transition. That is, we need to guess  $t_0 < \tau_d$ . On the other hand, the slice should be large enough to make the correlation peaks discoverable. It may be necessary to adjust the time origin  $t = 0$  to satisfy these constraints.

The correlation function is

$$\begin{aligned} & \int_{-\infty}^{\infty} s_b(t + \tau) \tilde{s}_b^*(\tau) d\tau \\ &= \int_{-\infty}^{\infty} s_b(\tau) \tilde{s}_b^*(\tau - t) d\tau \\ &= \int_t^{t+t_0} s_b(\tau) s_b^*(\tau - t) d\tau \end{aligned} \quad (4.3)$$

Assuming no noise ( $n_b(t) \simeq 0$ ), we substitute (4.1) into (4.3) to express the correlation as

$$\begin{aligned} & \int_t^{t+t_0} [D(\tau - \tau_d) C(\tau - \tau_d) \exp j(2\pi f_D \tau + \theta)] \\ & \cdot [D(\tau - t - \tau_d) C(\tau - t - \tau_d) \exp -j(2\pi f_D(\tau - t) + \theta)] d\tau \\ &= \exp j2\pi f_D t \int_t^{t+t_0} [D(\tau - \tau_d) C(\tau - \tau_d) \cdot D(\tau - t - \tau_d) C(\tau - t - \tau_d)] d\tau \end{aligned} \quad (4.4)$$

The beauty of this correlation result is that the Doppler offset and initial phase cancel out. The expression has two parts, a sinusoidal envelope and an integral. The integral

$$\int_t^{t+t_0} [D(\tau - \tau_d)C(\tau - \tau_d)D(\tau - t - \tau_d)C(\tau - t - \tau_d)]d\tau \quad (4.5)$$

is the correlation between  $s_b'(t) = D(t - \tau_d)C(t - \tau_d)$  and its small slice,  $\tilde{s}_b'(t)$ ,

$$\tilde{s}_b'(t) = \begin{cases} s_b(t), & 0 < t \leq t_0 \\ 0, & t > t_0. \end{cases} \quad (4.6)$$

With respect to (4.1),  $s_b'(t)$  is the noiseless version of  $s_b(t)$  with no Doppler offset or initial phase. The evaluation of (4.5) is illustrated in Figure 4.1. Positive correlation peaks occur whenever the time-shifted slice  $\tilde{s}_b'(\tau - t)$  aligns with similar versions of itself in  $s_b'(t)$ , and negative ones whenever it aligns with flipped versions of itself. These alignments happen at multiples of the PRN code period. In other words, peaks of height  $d_0 d_i$  occur at  $t = iT_d$ ,  $i = 0, 1, 2, \dots$

Therefore, the correlation peak heights in (4.4) are

$$d_0 d_i \exp j2\pi f_D t, \quad (4.7)$$

at  $t = iT_d$ ,  $i = 0, 1, 2, \dots$ . The inphase and quadrature channels of the correlation results are shown in Figures 4.2 and 4.3. The inphase plot shows a large peak at time 0, which is due to the alignment of both the signal and the noise. The other peaks are spaced at 1 ms intervals, because the signal PRN code repeats every 1 ms. The peaks are positive or negative, because each PRN code period is modulated by the polarity of the secondary code. These peaks are smaller than the peak at time 0, because only the signal is coherent, not the noise. Finally, the Doppler effect causes phase drift. Thus, some of the inphase energy moves to the quadrature channel over time in a sinusoidal envelope. This result agrees with the expression in (4.7).

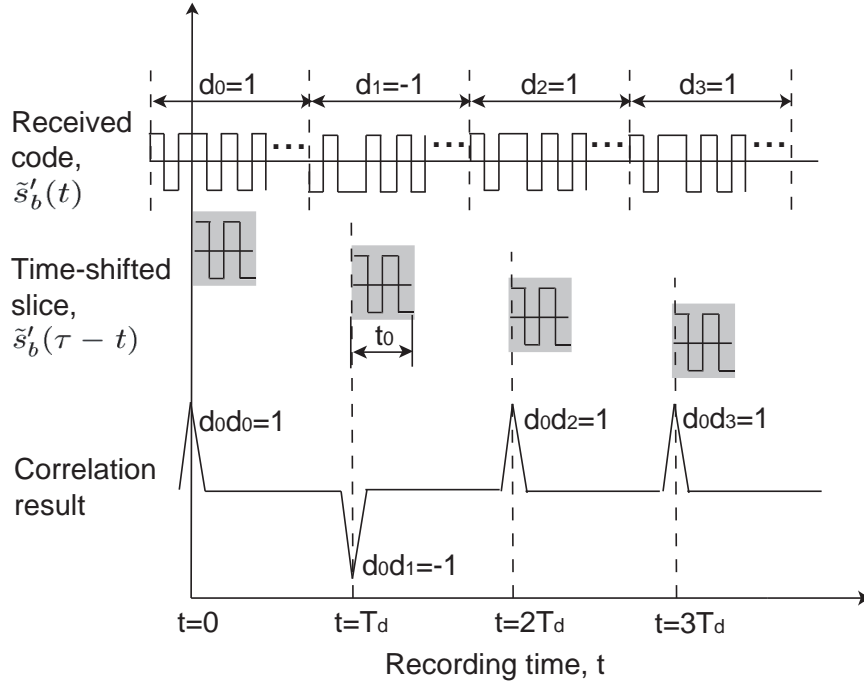


Figure 4.1: Correlation of the received code with time-shifted replicas. Correlation peaks occur whenever the time-shifted slice aligns with similar versions of itself or flipped versions. The  $i$ th correlation peak polarity is determined by the secondary code bit of the small slice,  $d_0$ , and the secondary code bit of the corresponding segment,  $d_i$ . The triangular correlation peak width is twice the PRN code chip duration.



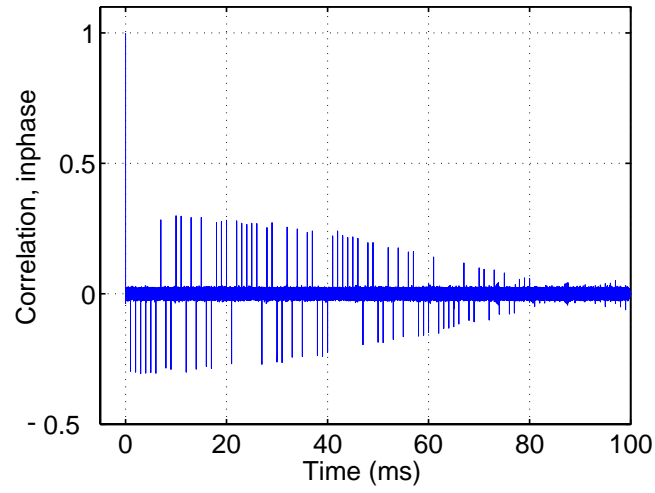


Figure 4.2: Correlation of whole data with a small slice of itself, inphase channel

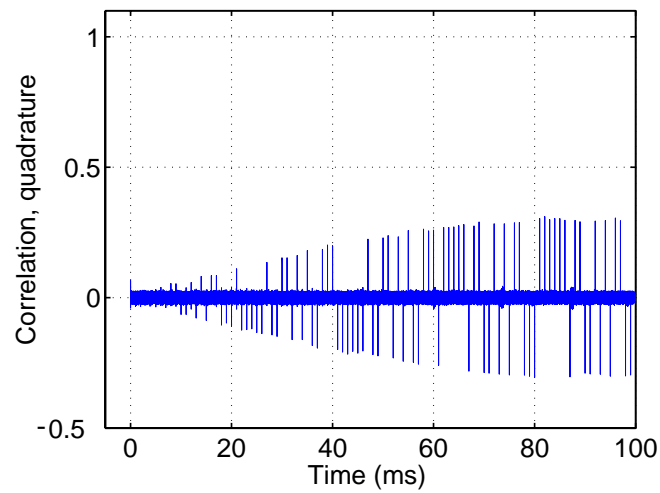


Figure 4.3: Correlation of whole data with a small slice of itself, quadrature channel

### 4.1.3 Determination of Code Period

Since we aim to stack multiple periods of the signal to boost SNR, we now determine the code period. According to Figure 4.1, the correlation peaks occur at multiples of the code period. Measuring the average inter-peak interval in Figure 4.2 and 4.3 yields the code period to be  $T_d = 1$  ms.

### 4.1.4 Wipeoff of Doppler Frequency up to Half of the Code Repetition Rate

In Figures 4.2 and 4.3, the height of the peaks varies due to the Doppler envelope, which is  $\exp j2\pi f_D t$  in (4.7). The next step is to estimate the Doppler offset  $f_D$  and wipe it off from the received baseband signal. Note that the Doppler estimation is based on the correlation peaks,  $T_d = 1$  ms apart. This is equivalent to estimating a signal with  $\frac{1}{T_d} = 1$  kHz sampling rate. Furthermore, we are unsure of the true polarity of the Doppler envelope. According to the Nyquist-Shannon sampling theorem, the estimated Doppler  $\hat{f}_D$  has an ambiguity equal to half of the sampling rate,  $\frac{1}{2T_d} = 500$  Hz. In other words,  $f_D = \hat{f}_D + k\frac{1}{2T_d}$ , for some  $k = 0, \pm 1, \pm 2, \dots$ . Therefore, we can only estimate Doppler offset up to half of the code repetition rate. One way of avoiding the Doppler ambiguity is to calculate the satellite speed using the satellite almanac. We will resolve the  $k\frac{1}{2T_d}$  Doppler ambiguity using signal processing methods described in Section 4.1.7 once multiple periods of data are stacked.

After compensating  $\hat{f}_D$ , the received baseband signal becomes

$$\begin{aligned} & s_b(t) \exp(-j2\pi \hat{f}_D t) \\ = & s_b(t) \exp(-j2\pi (f_D - k\frac{1}{2T_d})t). \end{aligned} \quad (4.8)$$

We substitute (4.1) into (4.8). The noiseless part of (4.8) then becomes

$$D(t - \tau_d)C(t - \tau_d) \exp j(\pi k \frac{1}{T_d} t + \theta). \quad (4.9)$$

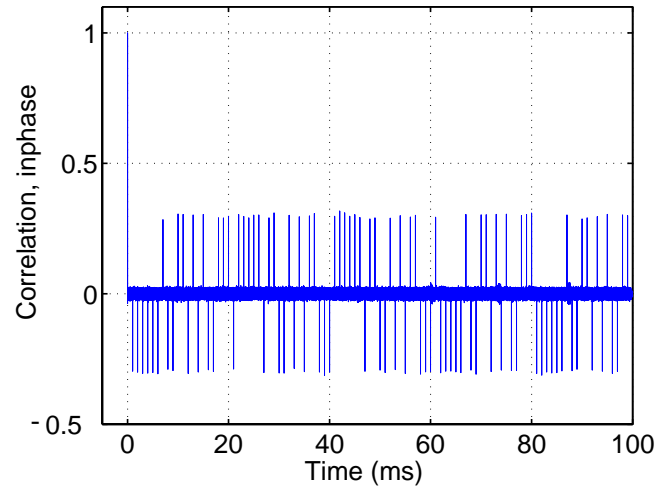


Figure 4.4: Correlation after wiping off estimated Doppler offset, inphase channel

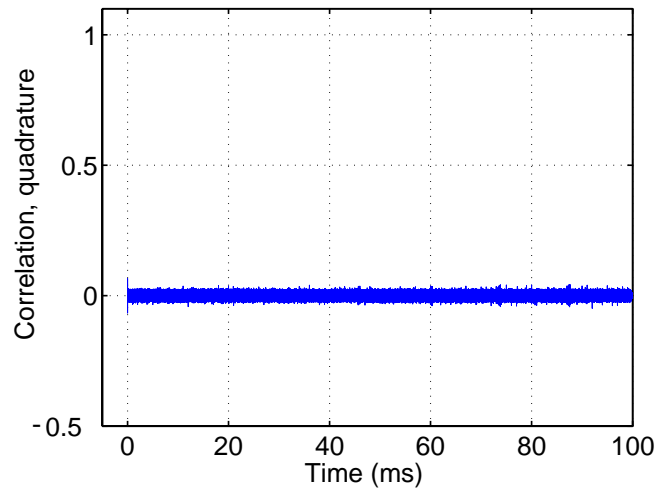


Figure 4.5: Correlation after wiping off estimated Doppler offset, quadrature channel

Figures 4.4 and 4.5 show the correlation results in inphase and quadrature channels after compensating for the estimated Doppler frequency offset. As expected, the removal of the Doppler offset corrects the phase drift, so all the energy stays in the inphase channel. There are no peaks in the quadrature channel. The peaks in the inphase channel (except the one at time 0) now have uniform heights, although varying polarities.

#### 4.1.5 Wipeoff of Secondary Code up to Overall Polarity

After the estimated Doppler offset is wiped off, the correlation peak heights from (4.7) become

$$d_0 d_i, \quad (4.10)$$

at  $t = iT_d$ ,  $i = 0, 1, 2, \dots$ .

This reflects the polarities of the positive and negative correlation peaks in Figure 4.4. If we assume  $d_0 = 1$ , the peak signs reveal the secondary code  $\mathbf{d}$  to be  $[1, -1, -1, -1, -1, -1, 1, -1, -1, 1, 1, -1, 1, -1, \dots]$ . Assuming  $d_0 = -1$  instead, flips the sign of all the data, including the primary PRN code  $\mathbf{c}$ . The sign flipping problem will be solved after the code generator polynomial is derived in Section 4.2. So far, we have determined the secondary code up to overall polarity.

We use this polarity information to wipe off the secondary code. We write the secondary code with overall polarity ambiguity in time domain as

$$d_0 D(t) = d_0 \sum_{i=0}^{\infty} d_i W_d(t - iT_d). \quad (4.11)$$

We then wipe off the secondary code in the Doppler compensated baseband signal in (4.9) by multiplying by (4.11). Since the start of the PRN code period,  $\tau_d$ , is as yet unknown, the local secondary code replica  $d_0 D(t)$  is not aligned with the secondary code of the received signal, as shown in Figure 4.6. For simplicity, Figure 4.6 does not show the Doppler residual.

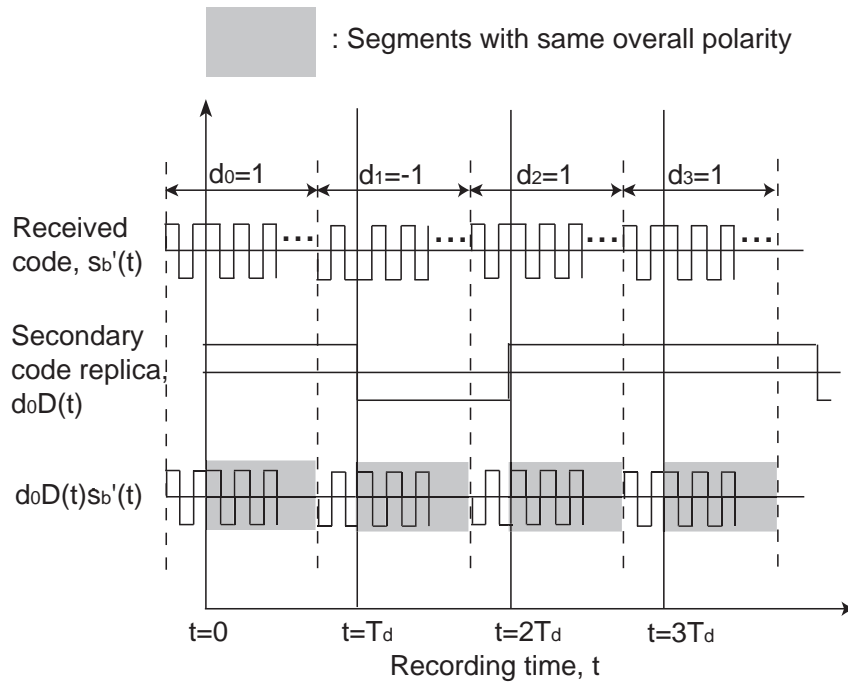


Figure 4.6: Secondary code wipeoff. Because the recording time is not synchronized with the start of a complete PRN code period, only the secondary code of the signal segments in the shaded area is wiped off. The transition point reveals the start of the PRN code period,  $\tau_d$ .

Now in each period of the received signal, the segment before the actual secondary code bit transition has the same overall polarity, while the segment after does not. Since  $d_i^2 = 1$ , the result after secondary code demodulation is

$$\begin{cases} d_0 C(t - \tau_d) \exp j(\pi k \frac{1}{T_d} t + \theta), & \text{for } iT_d \leq t < iT_d + \tau_d, \\ d_0 d_i d_{i+1} C(t - \tau_d) \exp j(\pi k \frac{1}{T_d} t + \theta), & \text{for } iT_d + \tau_d \leq t < (i+1)T_d, \end{cases} \quad (4.12)$$

where  $i=0, 1, 2, \dots$

In each period, the first  $\tau_d$  duration of data no longer contains secondary code except for the overall polarity  $d_0$ . So for these segments of data, the secondary code is wiped off. To verify, we correlate (4.12) with a small slice of itself. The correlation peaks become all positive as shown in Figure 4.7.

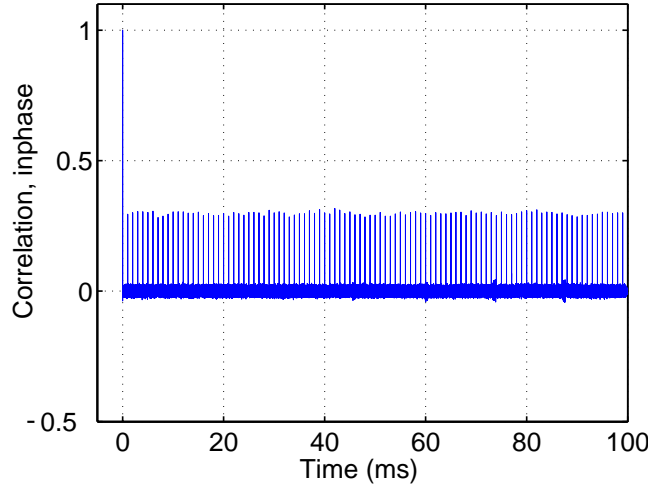


Figure 4.7: Correlation after wiping off estimated Doppler offset and secondary code, inphase channel

### 4.1.6 Stacking Multiple Periods of the Whole Data

In (4.12),  $d_0$  is a constant and  $C(t - \tau_d)$  repeats for each code period  $T_d$ . If  $k$  (associated with Doppler ambiguity) is an even number, then  $\exp j(\pi k \frac{1}{T_d} t + \theta)$  also repeats every time duration  $T_d$ . This means that the first  $\tau_d$  duration of each period of the signal is the same. This motivates us to stack  $N$  periods of the signal together. If we assume additive white noise, then the signal to noise power ratio is increased  $N$  times. The signal after stacking becomes

$$Nd_0C(t - \tau_d) \exp j(\frac{\pi k}{T_d} t + \theta), \quad \text{for } 0 \leq t < \tau_d, \quad (4.13)$$

and

$$d_0C(t - \tau_d) \exp j(\frac{\pi k}{T_d} t + \theta) \sum_{i=0}^{N-1} d_i d_{i+1}, \quad \text{for } \tau_d \leq t < T_d. \quad (4.14)$$

Recall that  $\exp j(\frac{\pi k}{T_d} t + \theta)$  is the residual Doppler ambiguity.

If  $k$  is an odd number, the signals in different periods cancel out, and the stacking result appears to be all noise. If this happens, we modulate each period of data with  $(-1)^i$ ,  $i=0, 1, 2, \dots$ , and restack.

Figures 4.8 and 4.9 show the inphase and quadrature channels of  $T_d = 1$  ms stack of baseband signal with Doppler compensation and secondary code wiped off.  $N = 100$  code periods are stacked in the two figures.

### 4.1.7 Wipeoff of Doppler Ambiguity

The signal stack has two parts as shown in Figures 4.8 and 4.9. The first part appears to have a sinusoidal envelope, while the second part looks like noise. The first part, described by (4.13), shows the PRN code energy boosted  $N$  times. The code  $C(t - \tau_d)$  is modulated by the initial secondary code bit  $d_0$  and a sinusoidal wave  $\exp j(\frac{\pi k}{T_d} t + \theta)$ . The second part of the stacked signal is described by (4.14). If we assume the secondary code to be independent identically distributed (i.i.d.) random variables with zero mean, then  $\sum_{i=0}^{N-1} d_i d_{i+1}$  also has zero mean. This second part of the signal stack is thus dominated by noise.

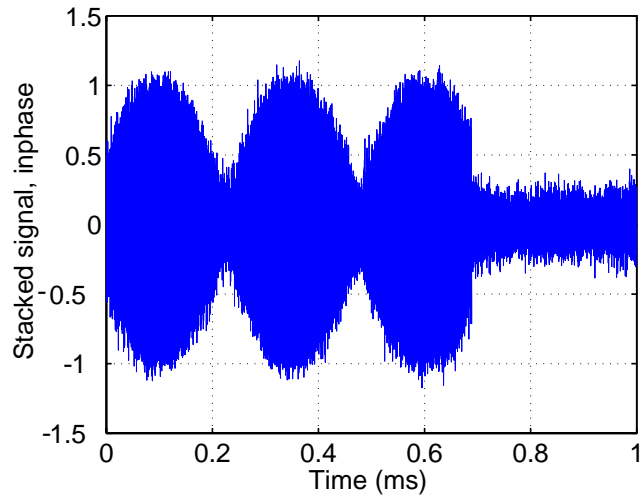


Figure 4.8: Multiple periods of signal stacked, inphase channel

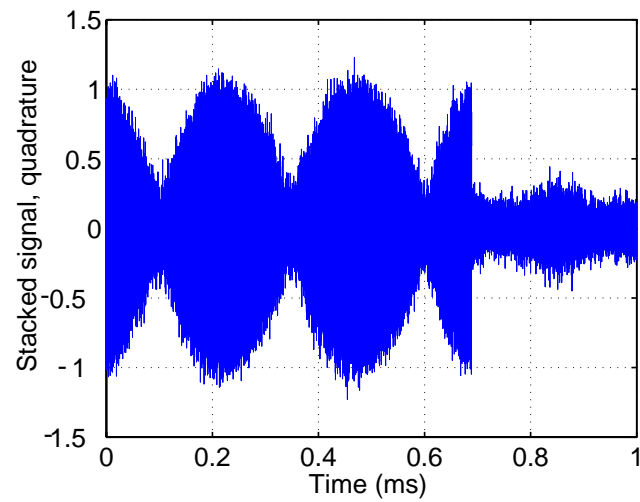


Figure 4.9: Multiple periods of signal stacked, quadrature channel



We solve the Doppler ambiguity problem by estimating the frequency of the sinusoidal envelope in the first part of the signal stack. In the collected data, the Doppler ambiguity is 2000 Hz.

After the Doppler ambiguity is resolved and the Doppler is wiped off completely, the noiseless part of the signal becomes

$$D(t - \tau_d)C(t - \tau_d) \exp j\theta. \quad (4.15)$$

We then restack the signal. The inphase and quadrature parts of the 1 ms stack of the data are shown in Figures 4.10 and 4.11. Now the signal envelope becomes constant.

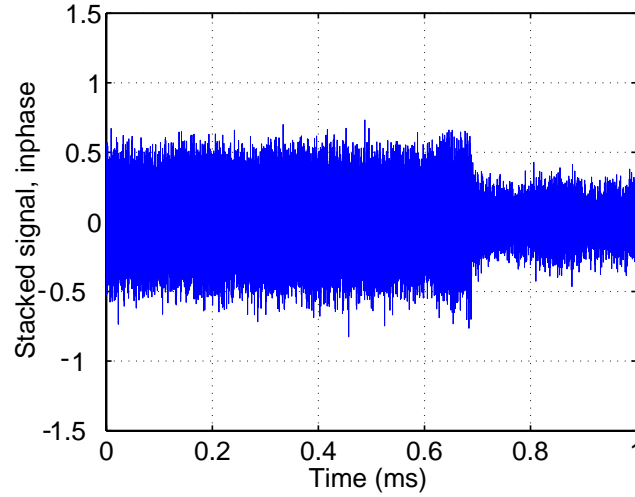


Figure 4.10: Stacked signal with no Doppler ambiguity, inphase channel

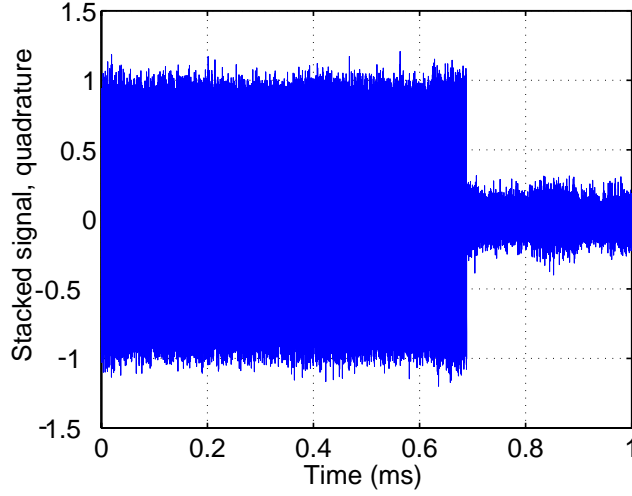


Figure 4.11: Stacked signal with no Doppler ambiguity, quadrature channel

#### 4.1.8 Zeroing Initial Phase

Figures 4.10 and 4.11 show signals in both inphase and quadrature channels, even though there is only one PRN code of interest. This is because of the initial phase shift  $\theta$ . Figure 4.12 shows the I-Q plot of the 1 ms stack before phase adjustment. The I-Q plot is generated by plotting inphase values versus quadrature values in a 2-D plot. Each complex time-domain sample becomes a dot in the I-Q plot. In our case, only the inphase channel is active at values  $\pm 1$ . So, we expect to see two clusters of dots separated horizontally if the initial phase is zero. Hence, we adjust the initial phase shift  $\theta$  so that the axis of the time-domain scatter points is aligned with the inphase axis, as shown in Figure 4.13.

Figures 4.14 and 4.15 show the inphase and quadrature part of the 1 ms stack of baseband signal with complete Doppler wipeoff, secondary code wipeoff and initial phase adjustment. After the initial phase is set to zero, the signal energy concentrates in the inphase channel. The quadrature channel has no signal but noise and interference.

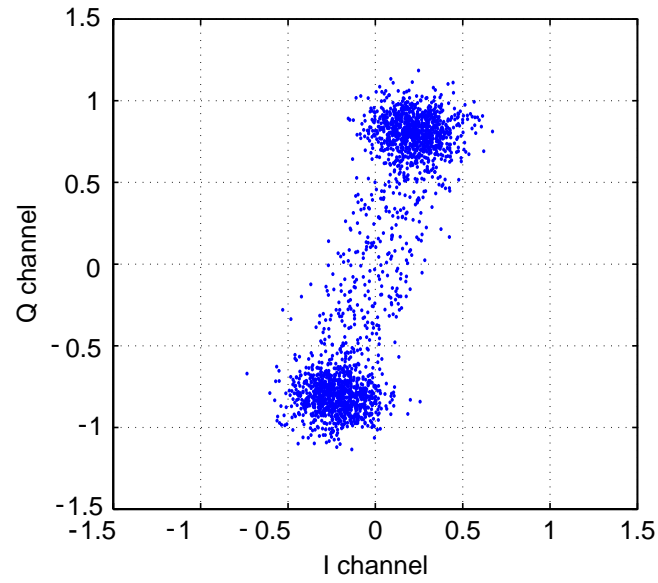


Figure 4.12: The I-Q plot of the stacked signal before phase adjustment

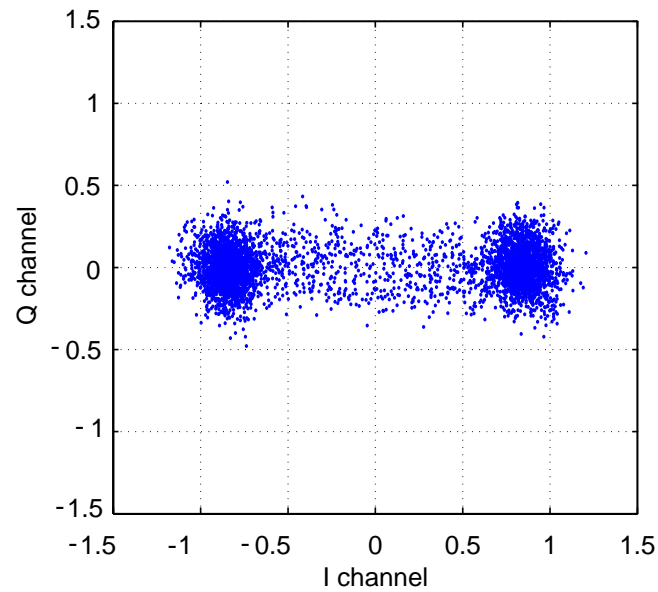


Figure 4.13: The I-Q plot of the stacked signal after phase adjustment

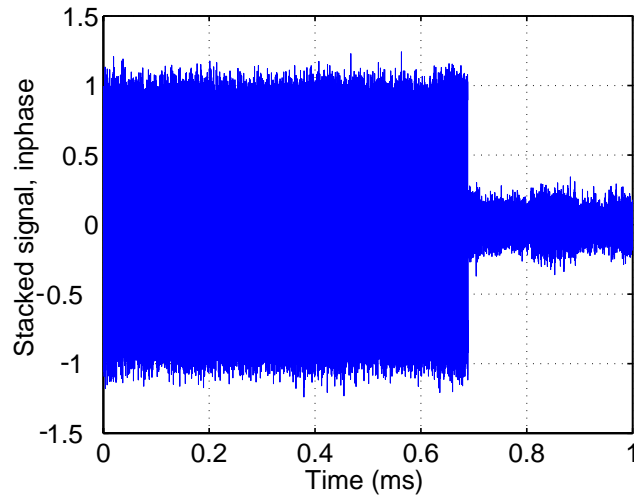


Figure 4.14: Stacked signal with initial phase adjusted, inphase channel

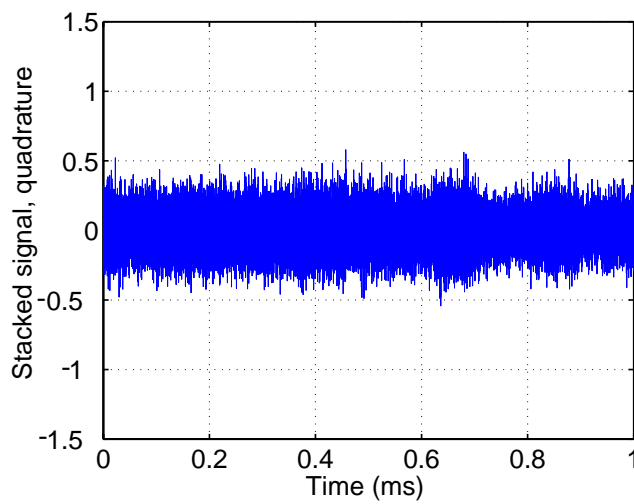


Figure 4.15: Stacked signal with initial phase adjusted, quadrature channel

### 4.1.9 Start of the Code and Shifting the Whole Data Set

The next step is to determine the start of the code  $\tau_d$ . According to (4.13) and (4.14),  $\tau_d$  is the transition point in the stacked signal from boosted PRN code to noise. If we zoom in, the transition region of the stacked signal is shown in Figure 4.16. We determine the start of the PRN code by estimating this transition point.

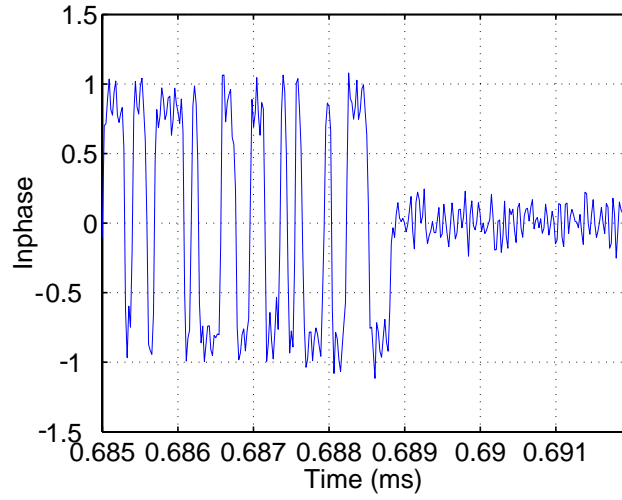


Figure 4.16: Stacked signal with initial phase adjusted, zoom in

We then shift the whole data to the start of the PRN code. The noiseless part of the signal now becomes

$$d_0 C(t). \quad (4.16)$$

### 4.1.10 Code Chips up to Overall Polarity

With the start of the PRN code sequence determined, we restack the whole data into one code period. The individual code chips are now visible over the noise. Figure 4.17 shows the first  $5 \mu s$ . The whole code sequence is thus revealed.

After downsampling, the code bits are obtained. The E6 I-channel PRN code is 10230 bits long and lasts for one millisecond. Figure 4.18 shows the first 50 bits of the code.

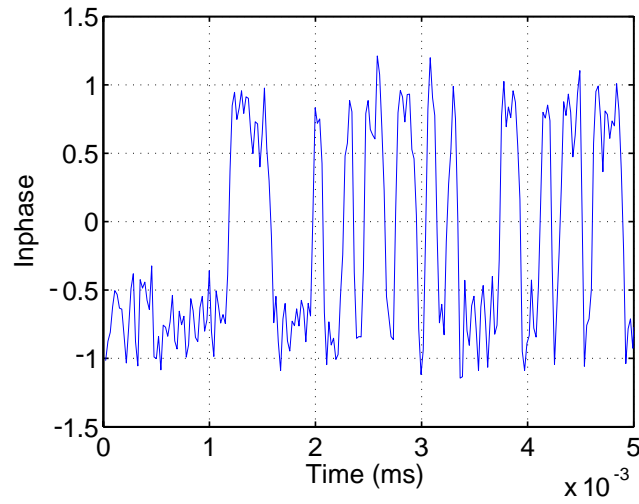


Figure 4.17: Stacked signal with code start determined, zoom in

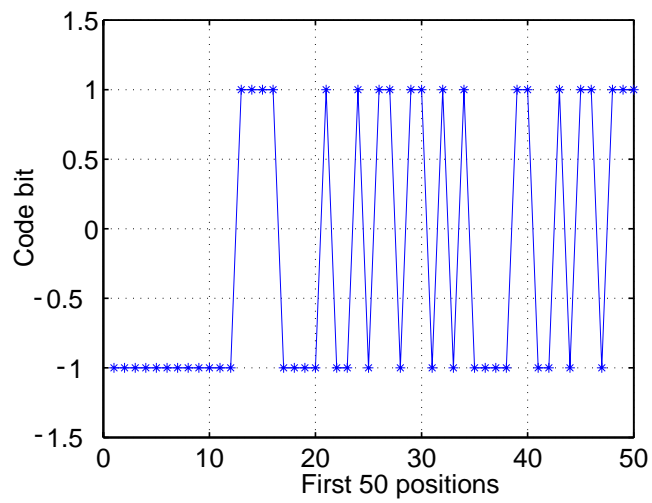


Figure 4.18: First 50 bits of E6 I-channel PRN code

Note that the overall polarity of the PRN code is ambiguous, because the sign of the first bit of the secondary code  $d_0$  is not determined yet. This may cause the sign of the whole PRN code sequence to flip. The sign ambiguity problem can be solved once we derive the code generator in the next section.

## 4.2 E6 Code Generator

With the code sequence obtained, we can implement this PRN sequence in a receiver for acquisition and tracking. However, we would also like to study the code structure, which will help us understand the effects of this code on other signals in the frequency band. This motivates us to seek the underlying code generator.

Furthermore, determining the PRN code generator helps minimize the code representation. This dramatically reduces the memory requirement for receivers. Storing thousands of bits in receivers is expensive in terms of flash memory and even more expensive in digital signal processing (DSP) units.

We consider linear codes as likely candidates for the Compass code design, because they have good correlation performance, and can be generated by LFSRs, which require only tens of bits to specify [5].

The schematic of an LFSR is shown in Figure 4.19. Its outputs are linear combinations of the previous bits. In other words, the entire output sequence  $u_i$  is completely determined by its tap weights  $(a_1, \dots, a_N)$  and initial state  $(u_1, \dots, u_N)$ . The LFSR arithmetic is modulo 2. It is conventional to describe this LFSR as a polynomial,  $a_1X^N + a_2X^{N-1} + \dots + a_NX + 1$ .

The algorithm in Figure 4.20 searches for a linear code representation. It loops through values of  $N$ , the length of the LFSR, until tap weights consistent with the demodulated code sequence are found. For example if  $N = 10$ , we can form the following 10 equations with 10 unknown tap weights,  $a_1, \dots, a_{10}$ .

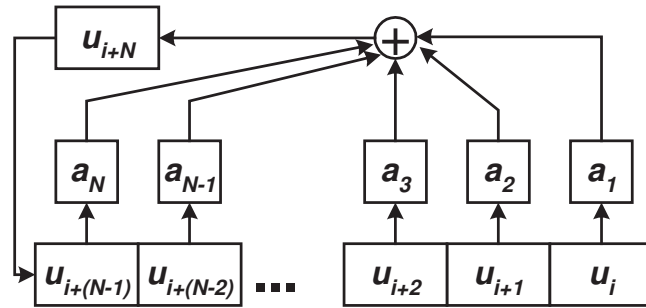


Figure 4.19: Linear feedback shift register (LFSR)

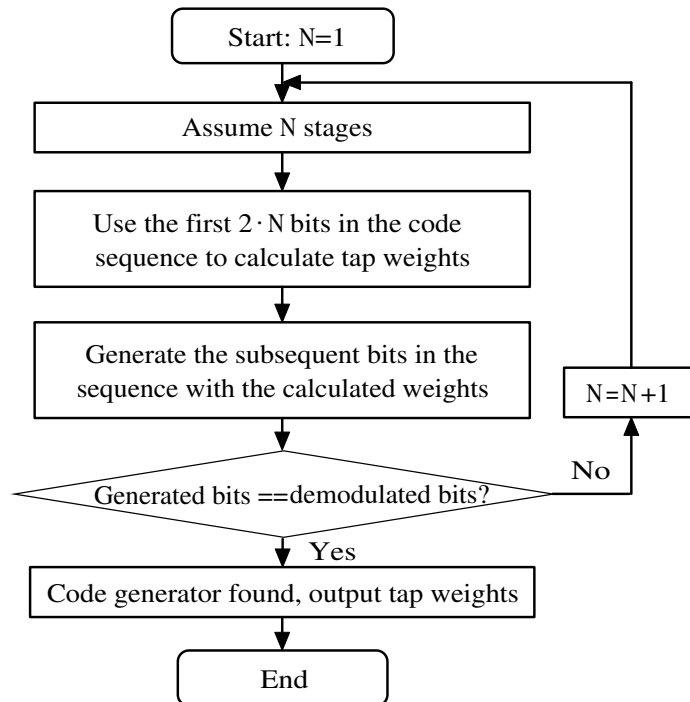


Figure 4.20: Search algorithm for linear code representation



$$\left\{ \begin{array}{lcl} u_{11} & = & a_{10} \cdot u_{10} \oplus a_9 \cdot u_9 \oplus \cdots \oplus a_1 \cdot u_1 \\ u_{12} & = & a_{10} \cdot u_{11} \oplus a_9 \cdot u_{10} \oplus \cdots \oplus a_1 \cdot u_2 \\ & \vdots & \\ u_{20} & = & a_{10} \cdot u_{19} \oplus a_9 \cdot u_{18} \oplus \cdots \oplus a_1 \cdot u_{10} \end{array} \right. \quad (4.17)$$

The above set of equations is solved modulo 2 to obtain the tap weights. The subsequent bits in the sequence are then generated. If the generated bits and the demodulated bits match, the code generator is deemed correct. If not, we increment  $N$  and repeat. To accommodate possible chip estimation errors, we define a successful match to be a 90% agreement between the generated bits and the demodulated bits.

Our method of finding the shortest LFSR for a given output sequence is closely related to the Berlekamp-Massey algorithm in [50, 55]. The Berlekamp-Massey algorithm is more efficient because it speeds up the solution of the set of equations by re-using the results of previous solutions. For deriving short LFSRs (tens of bits), the time savings are not significant. On the other hand, the Berlekamp-Massey algorithm is not robust to errors. A single incorrect bit will cause the algorithm to discard the correct tap weights. In contrast, our method only requires us to find a string of correctly demodulated bits of length equal to twice the length of the LFSR. Discrepancies in the rest of the sequence are allowed. In case there is a chip error in the test segment, we recognize the error by failing to obtain a generator. We then shift to the next segment and repeat until a clean segment is found.

With our algorithm, the Compass-M1 E6 code is proven to be linear. When we derived the code generators for the E6 code, only first 8190 bits of the generated sequence matched the demodulated sequence. We found out that the following 2040 bits are generated by a different generator. So the E6 code is a concatenated code composed of two segments, denoted as E6\_head and E6\_tail. E6\_head provides the first 8190 bits of the code sequence. E6\_tail contains the 8191st bit to the 10230th bit in the sequence. Both E6\_head and E6\_tail are generated by 26th-order LFSRs. The 26th-order polynomials can be further factorized into two 13th-order polynomials. This means that both the head and tail parts of the E6 code sequence can be generated by modulo 2 summing the outputs of pairs of 13 stage LFSRs. In fact, the head and

tail parts share the same two 13th-order polynomials, which form the preferred pair of a Gold code [56]. The initial states are also identical, except in a single bit position.

The code generators and initial conditions for the E6\_head and E6\_tail sequence are presented in Tables 4.1 and 4.2, respectively.

E6_head I channel code	
Polynomial_1	$X^{13} + X^{12} + X^{10} + X^9 + X^7 + X^6 + X^5 + X + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 0]
Polynomial_2	$X^{13} + X^4 + X^3 + X + 1$
Initial State_2	[1 1 1 1 1 1 1 1 1 1 1 1]

Table 4.1: Code generator polynomials and initial states for generating the first 8190 bits of the Compass E6 I-channel code

E6_tail I channel code	
Polynomial_1	$X^{13} + X^{12} + X^{10} + X^9 + X^7 + X^6 + X^5 + X + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{13} + X^4 + X^3 + X + 1$
Initial State_2	[1 1 1 1 1 1 1 1 1 1 1 1]

Table 4.2: Code generator polynomials and initial states for generating bits 8191-10230 (last 2040 bits) of the Compass E6 I-channel code

The code sequence sign ambiguity of the previous section can be solved after deriving the PRN code polynomials. If the PRN code polynomial can be factorized by  $1 + X$ , then the derived code should be flipped to remove this factor from the polynomial. Otherwise, the derived code is correct. This is because the polynomial  $1 + X$  generates a sequence of all ones. If it is added modulo 2 to the code sequence, all the resultant code bits flip sign.

Now we have solved the sign ambiguity for the secondary code sequence. The secondary code turns out to be a 20-bit Neuman-Hoffman code with the following sequence: [-1 -1 -1 -1 -1 1 -1 -1 1 1 -1 1 -1 1 -1 -1 1 1 -1 ], as defined in [57].

### 4.3 E2 and E5b Codes and Generators

We decoded the E2 and E5b codes using the technique described above for decoding the E6 code. The E2 signal uses QPSK(2) modulation. The Compass E2 I-channel primary code is 1 ms long and has 2046 bits. The E2 Q-channel has a long military code that is not studied in this work. Our analysis has proven that the E2 short code is linear and can be generated by a 22nd-order LSFR. The 22nd-order LSFR polynomial can be further factorized into two 11th-order polynomials. This indicates that the Compass E2 I-channel PRN code is an 11 stage Gold code.

The code generator polynomials and initial states are shown in Table 4.4. The PRN code generator schematic is shown in Figure 4.21.

E2 I channel code	
Polynomial_1	$X^{11} + X^{10} + X^9 + X^8 + X^7 + X + 1$
Initial State_1	[0 1 0 1 0 1 0 1 0 1 0]
Polynomial_2	$X^{11} + X^9 + X^8 + X^5 + X^4 + X^3 + X^2 + X + 1$
Initial State_2	[0 0 0 0 0 0 1 1 1 1]

Table 4.3: Code generator polynomials and initial states for generating the Compass E2 I-channel code

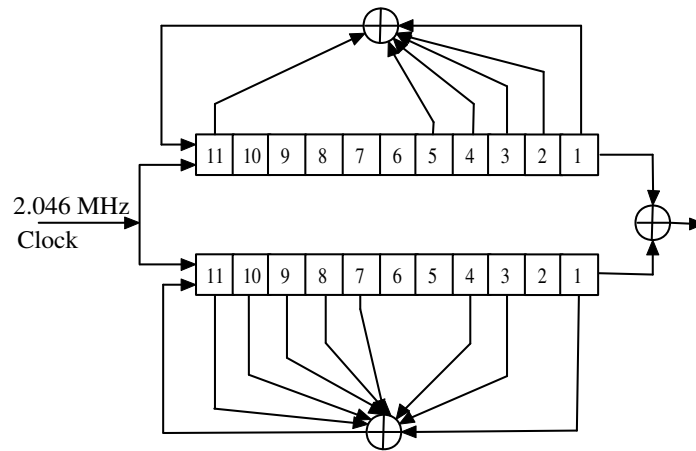


Figure 4.21: Code generator schematic of the Compass E2 I-channel signal

Two signals occupy the E5b band: one modulated with BPSK(2) in the I-channel and one with BPSK(10) in the Q-channel. The BPSK(2) code is a 1 ms short code. The BPSK(10) code is a long military code, also not studied in this work.

The Compass E5b short code turns out to be the same as the E2 code. Many observers have noted that the E2 I-channel and E5b BPSK(2) codes are identical [3, 49]. Furthermore, the E2 and E5b I-channel also have a 20-bit secondary code sequences identical to the one used in E6 band.

## 4.4 Summary

This chapter described the deciphering of the broadcast Compass-M1 codes following the flow chart presented in Chapter 3. We not only demonstrated the algorithms to reveal PRN code chips, but also designed an algorithm for analyzing the decoded PRN codes and their generation structures. The algorithm was a substantial modification of the well-known Berlekamp-Massey algorithm, to be robust against a high probability of code chip error. The code generation schematic in return resolved the overall polarity ambiguity of the PRN code sequences to complete and validate the deciphering process.

We applied the algorithms of our design to the Compass-M1 broadcast I-channel codes in all frequency bands, namely E2, E5b and E6 bands. All three PRN primary codes are linear codes with a period of 1 ms. The E2 and E5b codes are identical; they are truncated 11th-order Gold codes of 2046 bits. The E6 code has 10230 bits, a concatenation of two Gold code segments. Both segments are truncated 13th-order Gold codes with the same code polynomials but different initial states. The E2, E5b and E6 primary codes are modulated with 20-bit Neuman-Hoffman codes as secondary codes. The secondary codes in the three frequency bands are identical.

Table 4.4 summarizes the Compass-M1 decoding results.

Frequency band	Modulation type	Primary code period	Code generators	Secondary code period
E2	BPSK(2)	1 ms	11 stage Gold code	20 ms
E5b	BPSK(2)	1 ms	11 stage Gold code	20 ms
E6	BPSK(10)	1 ms	13 stage Gold code	20 ms

Table 4.4: Summary of Compass-M1 broadcast code results (civil signal only)



# Chapter 5

## Decoding Galileo GIOVE-A and GIOVE-B

### 5.1 Galileo Preliminaries

Galileo, like GPS, is a CDMA system. Compared with the widely used GPS civil signal in the L1 band, Galileo signals differ in many ways. The Galileo L1 signals use BOC modulation. Galileo E5a and E5b signals also suffer from pulsed interference from existing aeronautical systems. So will the future GPS L5 signal. This section describes the new modulation scheme and the challenging signal environment for Galileo.

#### Binary Offset Carrier (BOC)

The GPS L1 Coarse Acquisition (C/A) signal uses BPSK modulation [4], in which the PRN code chip shape is a square wave. So do the Galileo civilian signals in E6, E5a and E5b bands [45]. In contrast, Galileo L1 signals use BOC modulation [45]. The concept of BOC modulation is based on Manchester encoding [58]. Spilker *et al* generalized the Manchester coded technique in baseband communications to higher square wave clock rates [59], and named it split spectrum modulation. The terminology BOC modulation or BOC coding came later starting with Betz *et al* [60, 61]. In

BOC( $n,m$ ) modulation, the PRN code chip shape is a square subcarrier of frequency  $n$  multiples of 1.023 MHz, where the BPSK chip rate is  $m$  multiples of 1.023 MHz [62]. The Galileo open service signal in L1 band has BOC(1,1) modulation. Figure 5.1 compares a PRN code chip of the GPS L1 C/A signal using BPSK modulation with the Galileo L1 signal using BOC(1,1) modulation.

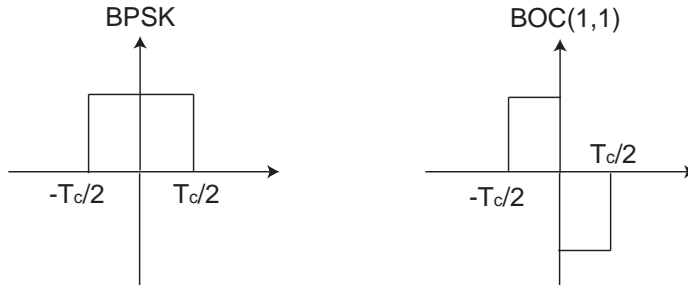


Figure 5.1: PRN code chip with BPSK and BOC(1,1) modulation, respectively

A feature of BOC(1,1) modulation is that it splits the spectrum from one main lobe in the center into two side lobes as shown in Figure 5.2. The dashed curve shows the GPS C/A signal with BPSK modulation, while the solid curve is the Galileo L1 signal with BOC(1,1) modulation. Although GPS and Galileo share the same L1 frequency band, the split spectrum of the Galileo BOC(1,1) signal mitigates interference with the GPS L1 signal by using different spectral occupation.

BOC modulation also increases the Gabor bandwidth [63] by pushing the signal energy to the edges of the bandwidth. This has the effect of sharpening the correlator peak. Figure 5.3 shows the correlation function of BPSK and BOC(1,1) modulation. The sharper correlation peak improves tracking sensitivity, but the side peaks may confuse the receiver tracking loops in noisy environments.

### Pulsed Aeronautical Interference

The Galileo E5a and E5b signals at 1176.45 MHz and 1207.14 MHz are exposed to a unique pulsed environment created by existing aeronautical system emitters, especially Distance Measuring Equipment (DME) and Tactical Air Navigation (TACAN) systems. DME provides distance measurement between aircraft and a ground station.



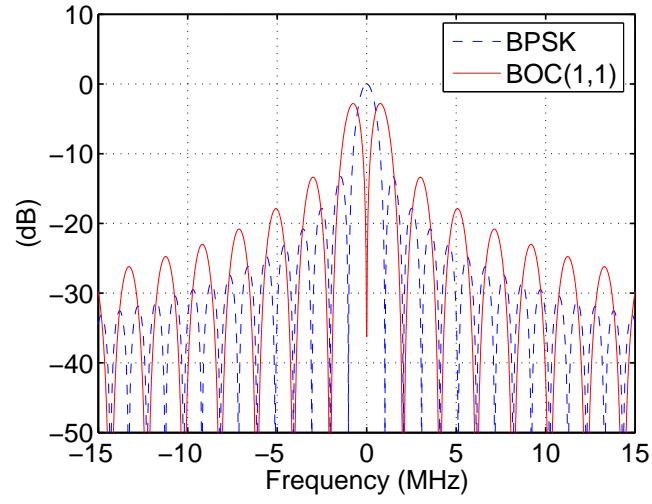


Figure 5.2: The spectrum of BPSK and BOC(1,1) modulation

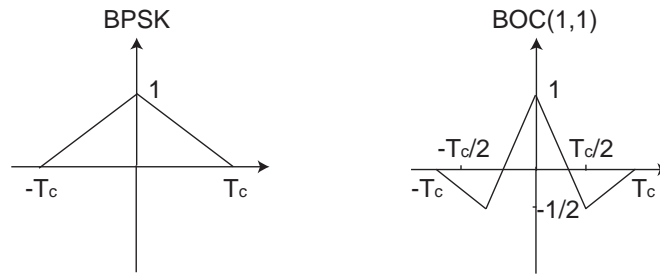


Figure 5.3: Correlation functions of BPSK and BOC(1,1) modulation, respectively

TACAN additionally provides azimuth information and is a military system. These navigation systems consist of an airborne interrogator and a ground-based transponder. DME/TACAN operate in four modes (X, Y, W and Z) between 960 MHz and 1215 MHz in an Aeronautical Radionavigation Services (ARNS) band [30]. Figure 5.4 illustrates the overlap between the DME/TACAN frequency band and the E5 band. Only the X mode replies in the 1151-1213 MHz frequency band.

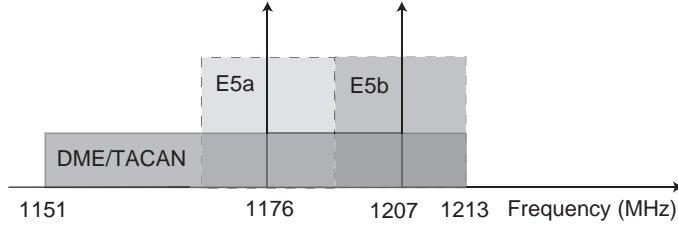


Figure 5.4: Overlap of DME/TACAN band and E5 band

The DME/TACAN signals are composed of pulse pairs with an inter-pulse interval of  $12 \mu\text{s}$ , each pulse lasting  $3.5 \mu\text{s}$  [31]. Each pulse can be modeled as a Gaussian function. A pulse pair has the following expression [64], which is illustrated in Figure 5.5:

$$p(t) = \exp\left(\frac{\alpha}{2}\left(t + \frac{\Delta t}{2}\right)^2\right) + \exp\left(-\frac{\alpha}{2}\left(t - \frac{\Delta t}{2}\right)^2\right), \quad (5.1)$$

where  $\alpha = 4.5 \times 10^{11} \text{ s}^{-2}$ ,  $\Delta t = 12 \times 10^{-6} \text{ s}$ . An observation of an actual pulse pair was shown in Figure 2.12.

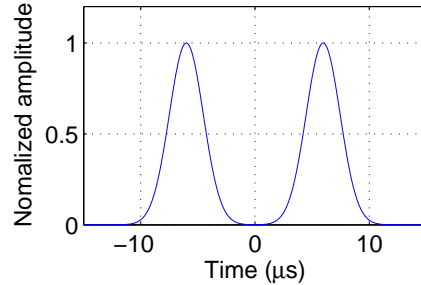


Figure 5.5: A DME/TACAN pulse pair

The DME/TACAN interference degrades the signal to interference plus noise ratio

(SINR), and makes the E5 decoding process more difficult than decoding L1 and E6 codes.

## 5.2 GIOVE-A E5b Codes

We describe the decoding of the E5b signal in detail, because it is the most challenging to decode. The E5b signal we collected at Stanford suffers from DME/TACAN interference from multiple nearby transponders, as shown in Figures 2.7 to 2.12. Moreover, the E5b code has bandwidth as wide as 20 MHz and consequently a high PRN code chip rate.

### 5.2.1 Interference Mitigation

Since the received GIOVE-A E5b signal suffers from narrow band DME/TACAN interference, we condition the received signal by notch filtering in the frequency domain. For convenience, we repeat Figures 2.8 and 2.10 as Figures 5.6 and 5.7 below to recall the DME/TACAN interference in time and frequency domain.

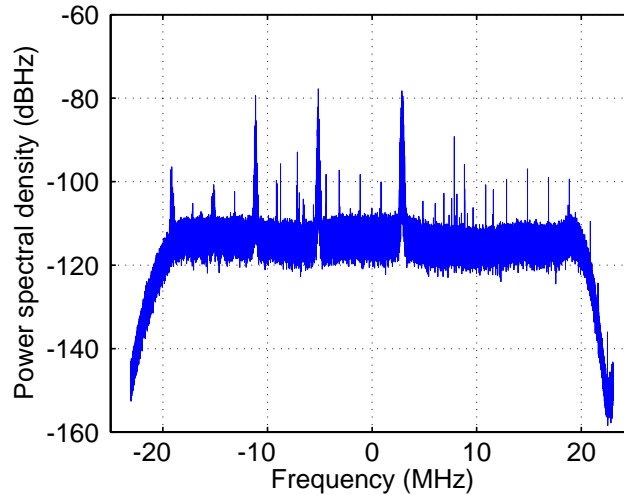


Figure 5.6: The GIOVE-A E5b band spectrum observed by the SGMS dish. There are three strong narrow-band tones attributed to DME/TACAN. (Same as Figure 2.8)

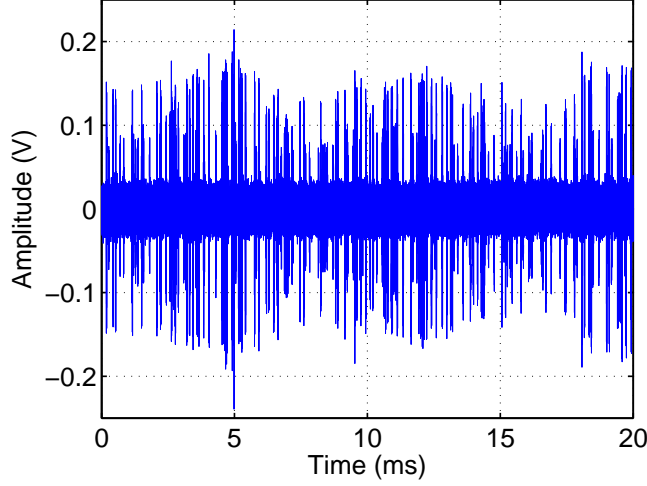


Figure 5.7: The time-domain GIOVE-A E5b signal observed by the SGMS dish. The DME/TACAN pulses in time domain are 5 to 100 times greater in amplitude than the noise, while the E5 signals are even weaker than noise. (Same as Figure 2.10)

We transfer the time domain signal to frequency domain by Fast Fourier Transform (FFT). We null the spike frequency components above the threshold of -102 dBHz, and then return the frequency expression to the time domain. Since this is post-processing, we apply digital filtering rather than analog filtering. In this way, the complexity is not limited in terms of number of notches or order of filter. Figures 5.8 and 5.9 show the frequency and time domain signals after notch filtering. For this data set, three nulls are applied to the signal spectrum. Narrow-band spikes in the spectrum and pulses in the time domain disappear from Figures 5.6 and 5.7. Note that when we apply notch filtering, we filter out about 10% of signal energy as well. Nevertheless, we obtain a net gain in SINR.

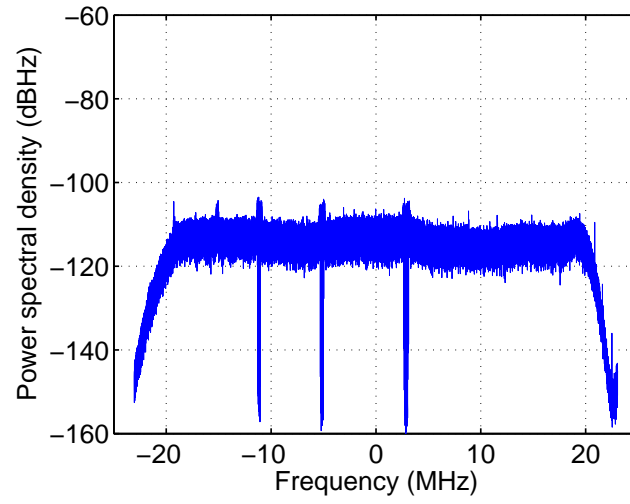


Figure 5.8: Signal spectrum after notch filtering

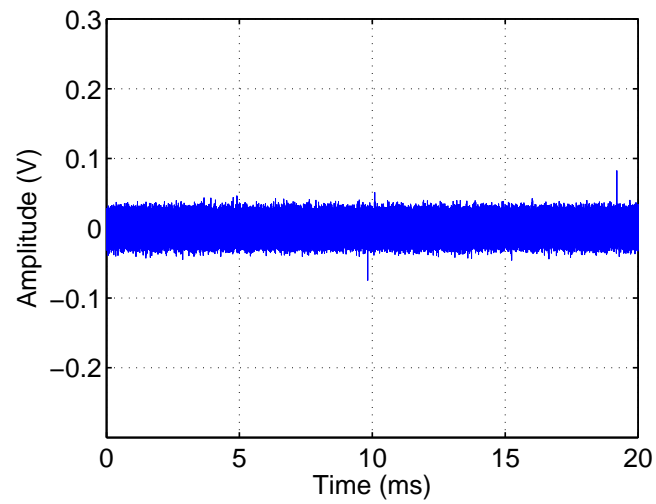


Figure 5.9: Time-domain signal after notch filtering

### 5.2.2 Code Period

We correlate the whole code sequence with a small slice of itself. The correlation plots for inphase and quadrature parts are shown in Figures 5.10 and 5.11. The intervals between peaks are multiples of 1 ms, and this indicates that the PRN codes have period 1 ms. To avoid bit transitions within the small slice of data, we take two consecutive slices of 0.5 ms and use the one that makes relatively larger peaks in the correlation.

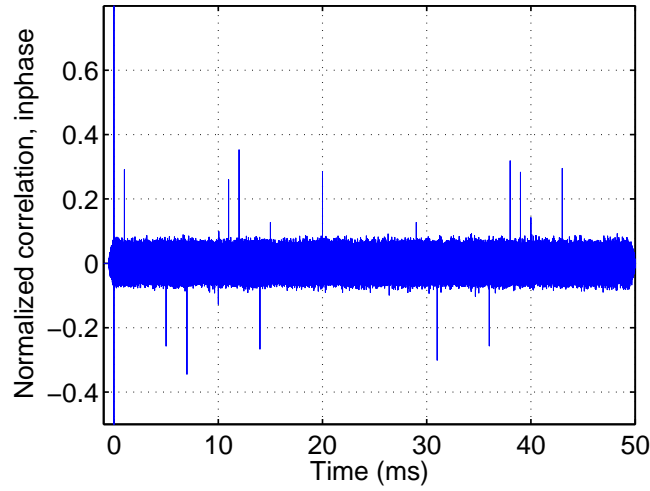


Figure 5.10: Correlation of the whole code sequence with a small slice of itself, inphase. The intervals between pairs of peaks are used to compute the code length. As the peaks occur at multiples of 1 ms, the PRN codes have period of 1 ms.

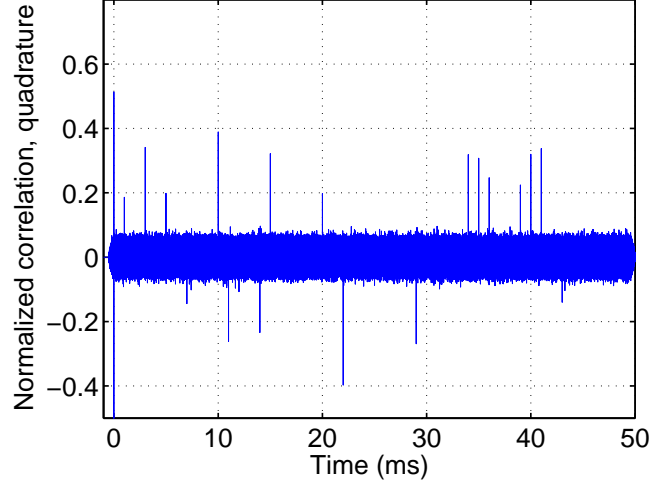


Figure 5.11: Correlation of the whole code sequence with a small slice of itself, quadrature

### 5.2.3 Wipeoff of Doppler Frequency up to Half of the Code Repetition Rate

The Doppler offset results in constant phase variation, modulating the correlation peak heights sinusoidally in inphase and quadrature channels. We estimate the Doppler offset as the value that minimizes the peak variation after compensation. Since the correlation peaks are 1 ms apart and their polarity is unknown, the estimate has the ambiguity up to half the code repetition rate. In other words, the real Doppler offset is the estimate plus a multiple of 500 Hz. This Doppler ambiguity is resolved later. After wiping off the Doppler offset up to half of the code repetition rate, we see peaks with more uniform heights in the inphase channel and no peak in the quadrature channel as shown in Figures 5.12 and 5.13.

### 5.2.4 Wipeoff of Secondary Codes up to Overall Polarity

In Figure 5.12, there are positive and negative peaks at multiples of 1 ms. We deduce null peaks where no positive or negative peaks appear. These null peaks indicate that there are two signals canceling. Each signal contains a PRN code with 1 ms period

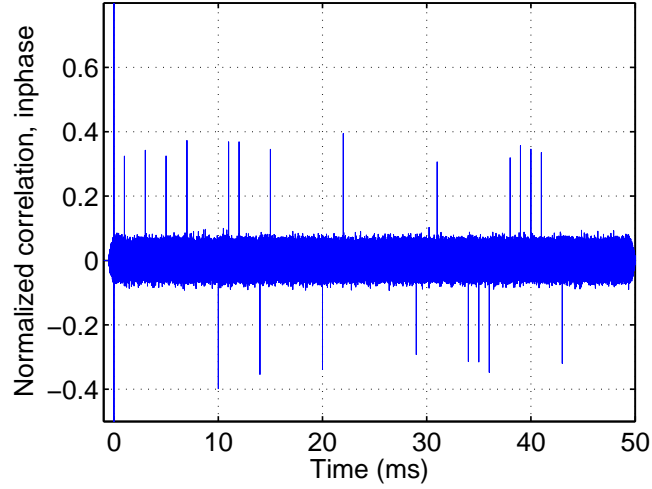


Figure 5.12: Correlation of the whole code sequence with a small slice of itself, inphase, after Doppler offset removal. The correlation peaks have more uniform heights in the inphase channel. There are positive and negative peaks at multiples of 1 ms. Null peaks are deduced where no positive or negative peaks exist. The null peaks indicate that there are two signals superposed.

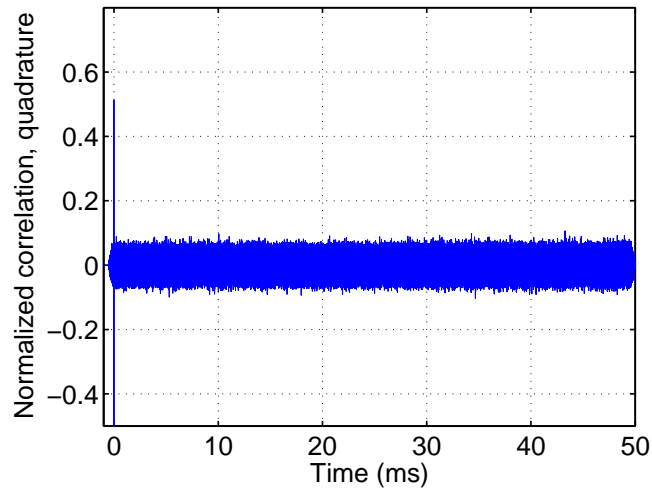


Figure 5.13: Correlation of the whole code sequence with a small slice of itself, quadrature, after Doppler removal. No correlation peaks appear in the quadrature channel.



	Period	Secondary code
E5b-I code	1 ms	$[1, 1, 1, 1, -1, 1, 1, 1, -1, -1, -1, 1, 1, \dots]$
E5b-Q code	1 ms	$[1, 1, -1, 1, 1, 1, 1, -1, 1, 1, 1, -1, 1, 1, \dots]$

Table 5.1: Secondary code reading of E5b-I and E5b-Q based on Figure 5.14

modulated by a secondary code with code bit duration of 1 ms. This matches the description in the Galileo ICD, which names the two PRN codes E5b-I and E5b-Q codes [45].

We now assume the small slice of code used for correlation contains  $(E5b-I) + (E5b-Q)$  in order to extract the secondary code; this assumption introduces ambiguity in the overall polarity of the codes. We resolve the ambiguity of the overall polarity after we derive the code generators. Then the positive peaks represent  $(E5b-I) + (E5b-Q)$ , the negative peaks represent  $-(E5b-I) - (E5b-Q)$ , while the null peaks are either  $(E5b-I) - (E5b-Q)$  or  $-(E5b-I) + (E5b-Q)$ . In this way, Figure 5.12 partially reveals the secondary code.

To distinguish between the null peaks, we correlate the whole sequence with another slice of data that corresponds to a null peak. In this example, the second slice of data starts at 2 ms. We again see positive and negative peaks and null peaks, as shown in the dashed red curve in Figure 5.14. Assuming this second slice of data contains  $(E5b-I) - (E5b-Q)$ , the positive peaks stand for  $(E5b-I) - (E5b-Q)$  and the negative peaks for  $-(E5b-I) + (E5b-Q)$ . The null peaks are either  $(E5b-I) + (E5b-Q)$  or  $-(E5b-I) - (E5b-Q)$ .

The solid blue curve in Figure 5.14 is the same curve in Figure 5.12. Taking both curves together reveals the secondary codes. The positive blue peaks and positive red peaks correspond to +1 in the E5b-I secondary code; the negative blue peaks and negative red peaks correspond to -1 for E5b-I secondary code. The positive blue peaks and negative red peaks correspond to +1 in the E5b-Q secondary code; the negative blue peaks and positive red peaks correspond to -1 for E5b-Q secondary code. Table 5.1 shows the reading of the secondary codes in the example shown in Figure 5.14.

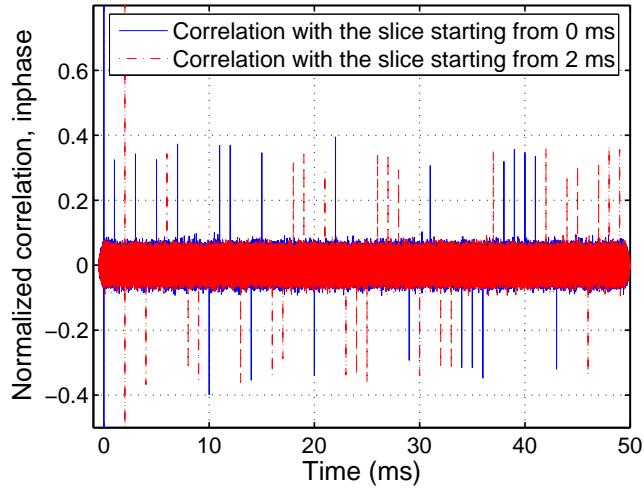


Figure 5.14: Extracting secondary code bits according to correlation peaks. For the solid blue curve, the positive and negative peaks reveal the secondary code bits at the peak locations, while the secondary code bits corresponding to the null peaks are unknown. The ambiguity of null peaks are solved by correlating another slice of data that corresponds to a null peak as shown by the dashed red curve. All the original nulls are filled with dashed peaks.

### 5.2.5 Wipeoff of Doppler Ambiguity

After wiping off the secondary code, the next step is to stack multiple periods of the whole data to increase the SNR. Figures 5.15 and 5.16 show the inphase and quadrature channels of the signal stack for the E5b-I code. The first 0.84 ms has a sinusoidal envelope due to the Doppler residual of an integer multiple of 500 Hz. In this example, the Doppler ambiguity is 1000 Hz. The data in inphase and quadrature channels after wiping off the Doppler residual are shown in Figures 5.17 and 5.18 respectively. The signal now has a constant envelope instead of a sinusoidal one in both inphase and quadrature channels.

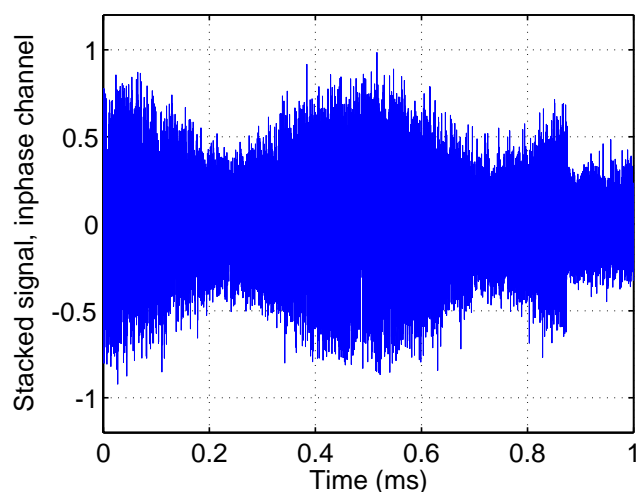


Figure 5.15: Multiple periods of signal stacked, inphase channel. The first 0.84 ms appears to have a sinusoidal envelope and the rest looks like noise. The sinusoidal envelope is due to the Doppler residual of an integer multiple of 500 Hz. The transition between the sinusoidal part and the noise-like part is the boundary between PRN code periods.

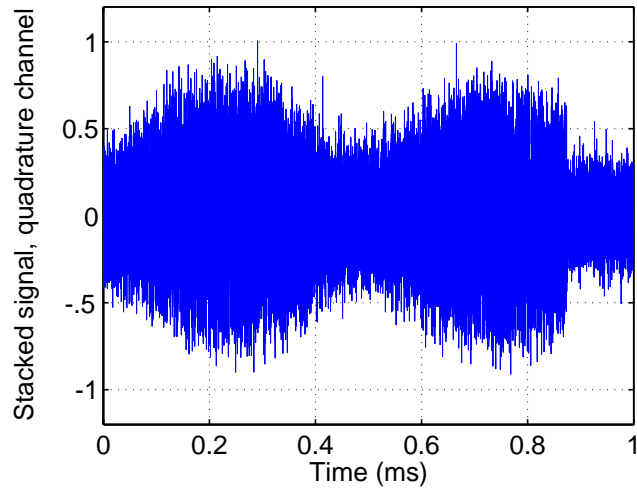


Figure 5.16: Multiple periods of signal stacked, quadrature channel

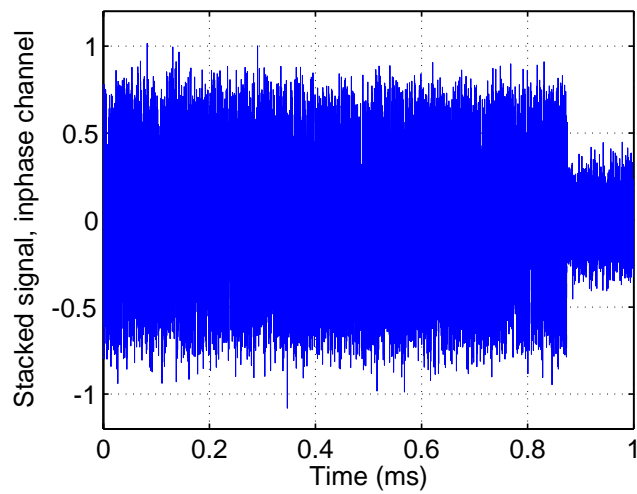


Figure 5.17: Stacked signal with no Doppler ambiguity, inphase channel. The signal now has a constant envelope instead of a sinusoidal one.

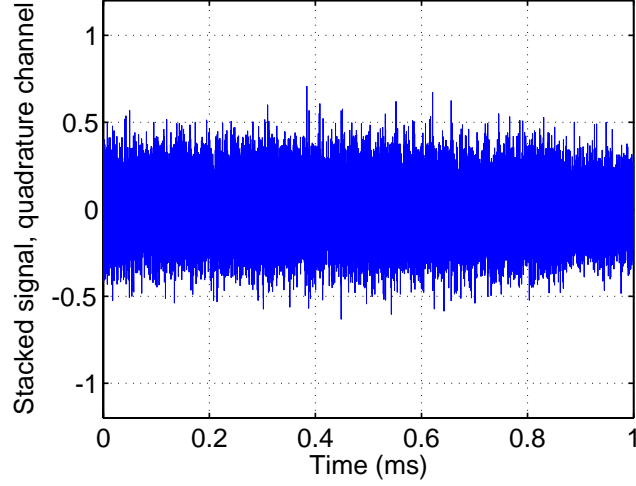


Figure 5.18: Stacked signal with no Doppler ambiguity, quadrature channel

### 5.2.6 Zeroing the Initial Phase

Figure 5.19 shows the I-Q scatter plot of the 1 ms stack after Doppler residual wipeoff, with inphase values versus quadrature values. In our case, we are only interested in the inphase channel, because it contains civil signals, while the quadrature channel is for military use. So, the initial phase estimate is the angle between the axis of the scatter points and the horizontal axis.

### 5.2.7 Start of the Code and Shifting the Whole Data Set

The 1 ms signal stack in Figure 5.17 is coherent only for the first 0.84 ms. This is because the transition marks the boundary between PRN code periods. After the transition, the secondary code bits do not correspond to those wiped off earlier. The whole data are now shifted to make the entire 1 ms of the signal stack coherent. In this way, the signal stack matches one period of the PRN code.

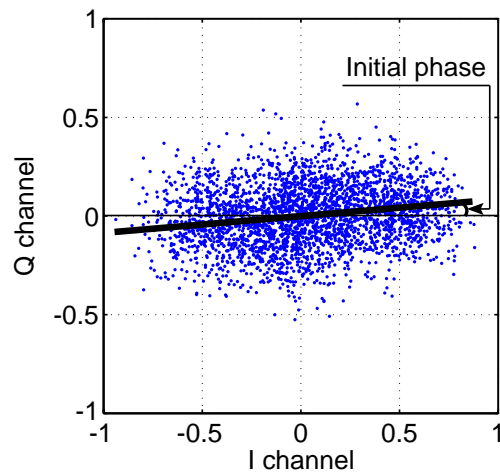


Figure 5.19: The I-Q plot of the stacked signal

### 5.2.8 Code Chips up to Overall Polarity

Figure 5.20 shows the first 100 chips of the E5b-I code. The E5b-Q code is decoded similarly. Both of these PRN codes are found to be 10230 bits long. The overall polarity of these codes is still ambiguous, but will be resolved once the code generators are derived in the next section.

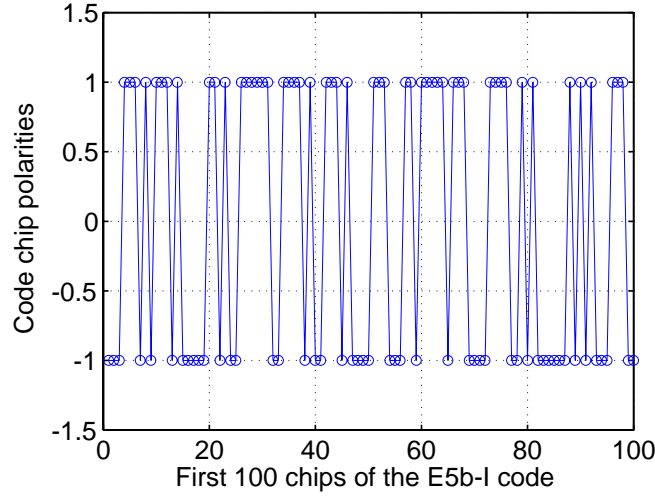


Figure 5.20: The first 100 chips of the E5b-I code

### 5.3 GIOVE-A E5b Codes and Code Generators

The code generators are derived using the method described in Section 4.2. Our analysis shows that the E5b codes are linear and can be generated by 28th-order LFSRs. Each 28th-order LSFR polynomial can be further factorized into two 14th-order polynomials. This indicates that the GIOVE-A broadcast E5b codes are 14 stage Gold codes. Since the E5b code length (10230 bits) is shorter than that of a 14 stage Gold code (16383 bits), the E5b codes are truncated Gold codes.

The ambiguity in overall polarity arose, because we assumed one small slice of code used for correlation contained  $(E5b-I) + (E5b-Q)$ , and another slice of code contained  $(E5b-I) - (E5b-Q)$ . The codes with true polarity should have the simplest code generators. As in Section 4.2, if any of the PRN code polynomials can be factorized by  $1 + X$ , then the derived code should be flipped to remove this factor from the polynomial.

The code generator polynomials and initial states for E5b-I and E5b-Q codes are shown in Tables 5.2 and 5.3, respectively. The two codes have the same generator polynomial but different initial states. The PRN code generator schematic for both codes is shown in Figure 5.21.

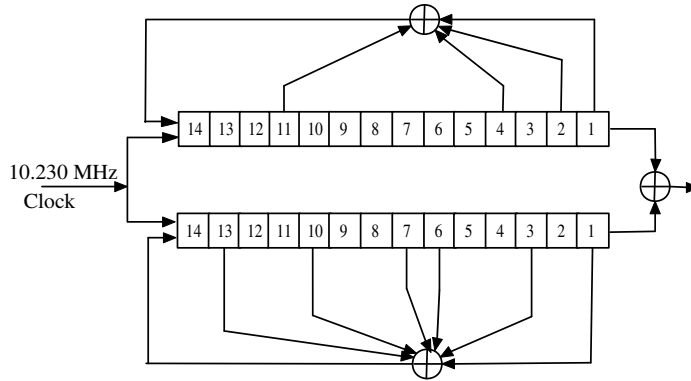


Figure 5.21: The E5b code generator

E5b-I code (10230 bits, 1msec, 14 stage Gold code)	
Polynomial_1	$X^{14} + X^{13} + X^4 + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{14} + X^{12} + X^9 + X^8 + X^5 + X^2 + 1$
Initial State_2	[1 1 1 0 0 0 1 0 1 0 0 0 1 0]

Table 5.2: Code generator polynomials and initial states for GIOVE-A E5b-I PRN code

E5b-Q code (10230 bits, 1msec, 14 stage Gold code)	
Polynomial_1	$X^{14} + X^{13} + X^4 + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{14} + X^{12} + X^9 + X^8 + X^5 + X^2 + 1$
Initial State_2	[1 1 0 0 0 0 0 0 0 0 0 0 1 0]

Table 5.3: Code generator polynomials and initial states for GIOVE-A E5b-Q PRN code



## 5.4 GIOVE-A E5a Codes and Code Generators

Decoding the GIOVE-A E5a codes follows the same procedure as decoding the E5b codes. The E5a band also has two PRN codes superimposed, namely E5a-I and E5a-Q codes. Our analysis shows that the E5a-I and E5a-Q codes are truncated 14 stage Gold codes. The polynomials and initial states are shown in Tables 5.4 and 5.5, respectively.

E5a-I code (10230 bits, 1msec, 14 stage Gold code)	
Polynomial_1	$X^{14} + X^8 + X^6 + X + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{14} + X^{12} + X^8 + X^7 + X^5 + X^4 + 1$
Initial State_2	[1 1 1 0 1 0 1 0 1 1 1 1 1]

Table 5.4: Code generator polynomials and initial states for GIOVE-A E5a-I PRN code

E5a-Q code (10230 bits, 1msec, 14 stage Gold code)	
Polynomial_1	$X^{14} + X^8 + X^6 + X + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{14} + X^{12} + X^8 + X^7 + X^5 + X^4 + 1$
Initial State_2	[0 1 1 0 1 1 0 0 1 0 1 0 1 0]

Table 5.5: Code generator polynomials and initial states for GIOVE-A E5a-Q PRN code

## 5.5 GIOVE-A L1 Codes and Code Generators

Decoding the GIOVE-A L1 codes is also similar to decoding E5 codes except for three differences. First, the Galileo L1 band overlaps with the GPS L1 band, so it is quite possible to obtain an interfering GPS signal if a GPS satellite falls in the antenna main lobe. Figure 5.22 shows the skyplot on February 6, 2006, observing from Stanford. Two GPS satellites, NAVSTAR 36 and NAVSTAR 32 fall in the antenna main lobe of GIOVE-A. Second, there are two GIOVE-A L1 codes superimposed, namely L1-B

and L1-C codes, with different code periods. Third, the Galileo L1 signal uses BOC modulation, while the E5b signal does not.

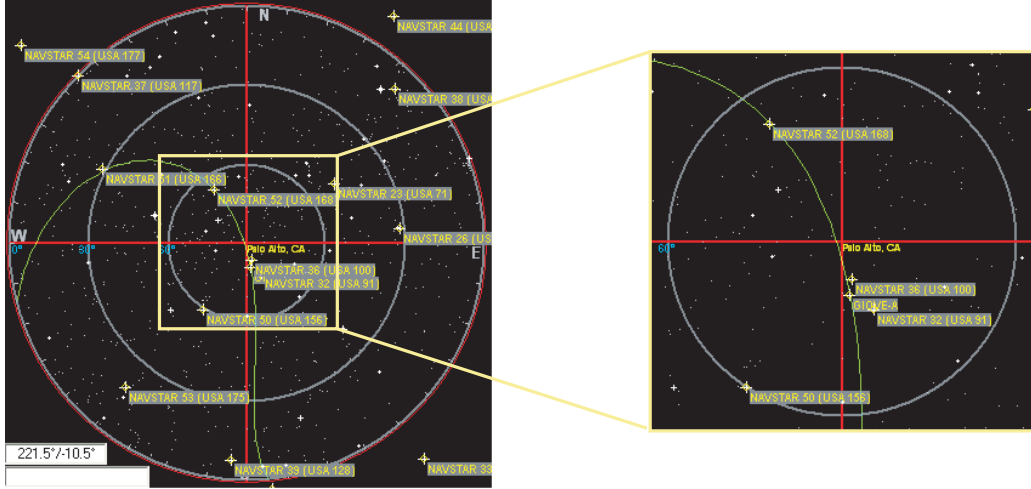


Figure 5.22: A skyplot of GIOVE-A and GPS NAVSTAR satellites, in which GPS NAVSTAR 36 and 32 fall in the antenna main lobe of GIOVE-A.

The GIOVE-A L1 correlation after Doppler wipeoff is shown in Figure 5.23. The interfering GPS signal appears in this correlation result. It consists of small triangular peaks 1 ms apart in a sinusoidal envelope. The peaks are smaller than the GIOVE-A peaks because the dish antenna is pointed directly at GIOVE-A. The triangular shape is characteristic of the GPS signal's BPSK modulation, as opposed to the BOC correlation shape of GIOVE-A shown in Figure 5.3. The sinusoidal envelope modulates the GPS peaks because only the GIOVE-A Doppler frequency was wiped off. There are two approaches to deal with such GPS interference. One is to subtract the GPS interference from the collected data after acquiring and tracking the GPS signal. The other way, which we adopt, is to treat the GPS signal as interference and stack the GIOVE-A signal for a longer period of time.

The presence of two GIOVE-A L1 codes of different periods is also apparent in the correlation plot Figure 5.23. GIOVE-A correlation peaks (shaped as in Figure 5.3) occur at some multiples of 4 ms. Among them, the peaks double in height of the others occur at some multiples of 8 ms. This suggests one code (L1-B) has period of

4 ms, and the other superimposed code (L1-C) has period of 8 ms. We also deduce the presence of null peaks at multiples of 8 ms, where the L1-B and L1-C code peaks cancel out.

The final difference in decoding the L1 codes is the wipeoff of the BOC modulation from the stacked signal, as shown in Figure 5.24. We align the BOC(1, 1) carrier with the stacked signal, and then multiply them together, as shown in Figure 5.24, which uses different vertical scales for clarity.

The GIOVE-A L1-B and L1-C codes are shown to be truncated 13 stage Gold codes. The polynomials and initial states are shown in Tables 5.6 and 5.7, respectively.

L1-B code (4092 bits, 4msec, 13 stage Gold code)	
Polynomial_1	$X^{13} + X^{10} + X^9 + X^7 + X^5 + X^4 + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{13} + X^{12} + X^8 + X^7 + X^6 + X^5 + 1$
Initial State_2	[1 1 0 1 1 1 00 0 0 0 1 1]

Table 5.6: Code generator polynomials and initial states for GIOVE-A L1-B PRN code

L1-C code (8184 bits, 8msec, 13 stage Gold code)	
Polynomial_1	$X^{13} + X^{10} + X^9 + X^7 + X^5 + X^4 + 1$
Initial State_1	[1 1 0 0 1 1 0 0 0 0 0 1 1]
Polynomial_2	$X^{13} + X^4 + X^3 + X + 1$
Initial State_2	[1 1 1 1 1 1 1 1 1 1 1 1 1]

Table 5.7: Code generator polynomials and initial states for GIOVE-A L1-C PRN code

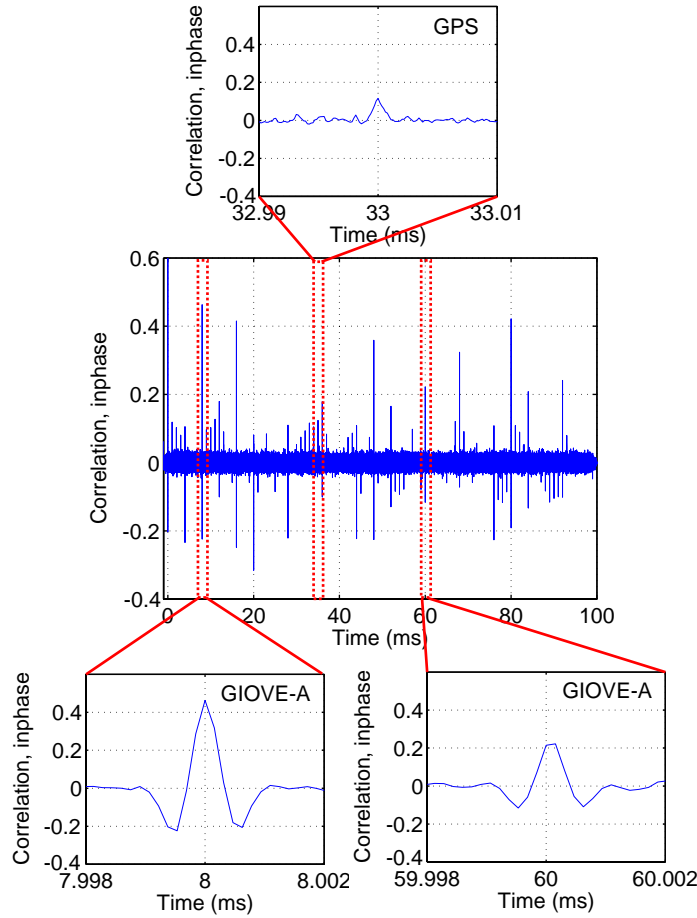


Figure 5.23: Extracting secondary code bits according to correlation peaks. Since the GIOVE-A L1 band overlaps with the GPS L1 band, the GPS L1 signal is received as well, which is indicated by the small triangular correlation peaks (top). The correlation peaks of the GIOVE-A L1 signal have shapes consistent with typical BOC modulation. The double-in-height peaks (bottom left) and single-in-height peaks (bottom right) indicate two PRN codes are superimposed. One PRN code is twice as long as the other.

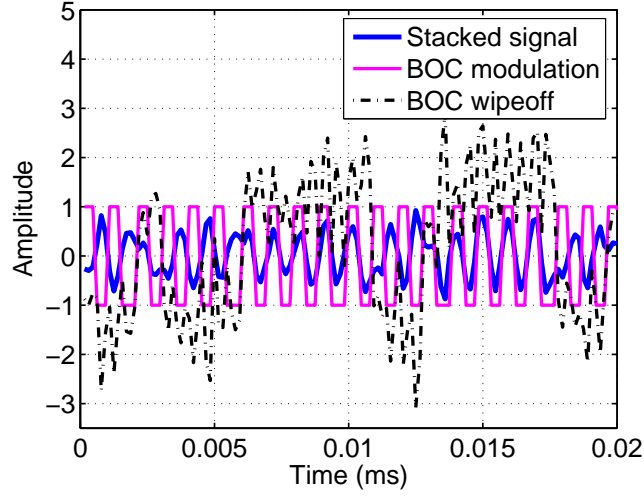


Figure 5.24: BOC modulation wipeoff. We align the BOC(1, 1) carrier with the stacked signal, and then multiply them together.

## 5.6 GIOVE-A E6 Codes and Generators

Decoding the GIOVE-A E6 codes is similar to decoding the E5b codes as shown in Figure 3.3, except for two differences. First, the E6 band does not contain DME/TACAN pulses, so there is no need to apply interference mitigation. Second, the E6 band has two PRN codes of different periods. The E6-B and E6-C codes have periods of 1 ms and 2 ms, respectively. The procedure for decoding them is similar to that for decoding the L1-B and L1-C codes.

Both E6 codes are shown to be truncated Gold codes, 13 stage for the E6-B code and 14 stage for the E6-C code. The polynomials and initial states are shown in Tables 5.8 and 5.9, respectively.

E6-B code (5115 bits, 1msec, 13 stage Gold code)	
Polynomial_1	$X^{13} + X^{10} + X^8 + X^5 + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{13} + X^{12} + X^{11} + X + 1$
Initial State_2	[0 1 0 1 0 1 1 1 0 0 0 0]

Table 5.8: Code generator polynomials and initial states for GIOVE-A E6-B PRN code

E6-C code (10230 bits, 2msec, 14 stage Gold code)	
Polynomial_1	$X^{14} + X^{11} + X^6 + X + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{14} + X^8 + X^7 + X^4 + X^3 + X^2 + 1$
Initial State_2	[0 1 1 0 1 0 0 0 0 1 1 1 0 1]

Table 5.9: Code generator polynomials and initial states for GIOVE-A E6-C PRN code

## 5.7 GIOVE-B Codes and Generators

Using a similar process to decoding the GIOVE-A codes, we also successfully decode the GIOVE-B codes and obtain their generators. GIOVE-B and GIOVE-A codes also share the same generator polynomials, only the initial states are different. Tables 5.10 to 5.15 show the GIOVE-B code generator polynomials and initial states in current transmission bands of L1, E5a and E5b. Just like GIOVE-A codes, the GIOVE-B L1 PRN codes are both truncated 13 stage Gold codes, and the GIOVE-B E5a and E5b codes are truncated 14 stage Gold codes.

L1-B code (4092 bits, 4msec, 13 stage Gold code)	
Polynomial_1	$X^{13} + X^{10} + X^9 + X^7 + X^5 + X^4 + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{13} + X^{12} + X^8 + X^7 + X^6 + X^5 + 1$
Initial State_2	[1 0 0 1 1 1 1 1 1 1 1 0]

Table 5.10: Code generator polynomials and initial states for GIOVE-B L1-B PRN code

L1-C code (8184 bits, 8msec, 13 stage Gold code)	
Polynomial_1	$X^{13} + X^{10} + X^9 + X^7 + X^5 + X^4 + 1$
Initial State_1	[0 1 0 0 0 1 0 1 1 1 1 1 1]
Polynomial_2	$X^{13} + X^4 + X^3 + X + 1$
Initial State_2	[1 1 1 1 1 1 1 1 1 1 1 1 1]

Table 5.11: Code generator polynomials and initial states for GIOVE-B L1-C PRN code

E5a-I code (10230 bits, 1msec, 14 stage Gold code)	
Polynomial_1	$X^{14} + X^8 + X^6 + X + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{14} + X^{12} + X^8 + X^7 + X^5 + X^4 + 1$
Initial State_2	[1 0 0 1 1 0 0 1 0 0 0 0 0 0]

Table 5.12: Code generator polynomials and initial states for GIOVE-B E5a-I PRN code

E5a-Q code (10230 bits, 1msec, 14 stage Gold code)	
Polynomial_1	$X^{14} + X^8 + X^6 + X + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{14} + X^{12} + X^8 + X^7 + X^5 + X^4 + 1$
Initial State_2	[1 0 0 0 1 1 1 0 1 0 1 1 0 0]

Table 5.13: Code generator polynomials and initial states for GIOVE-B E5a-Q PRN code

E5b-I code (10230 bits, 1msec, 14 stage Gold code)	
Polynomial_1	$X^{14} + X^{13} + X^4 + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{14} + X^{12} + X^9 + X^8 + X^5 + X^2 + 1$
Initial State_2	[0 0 0 0 1 0 1 0 1 1 0 0 1 0]

Table 5.14: Code generator polynomials and initial states for GIOVE-B E5b-I PRN code

E5b-Q code (10230 bits, 1msec, 14 stage Gold code)	
Polynomial_1	$X^{14} + X^{13} + X^4 + 1$
Initial State_1	[1 1 1 1 1 1 1 1 1 1 1 1 1 1]
Polynomial_2	$X^{14} + X^{12} + X^9 + X^8 + X^5 + X^2 + 1$
Initial State_2	[0 1 0 1 0 0 0 0 0 1 0 1 1 1]

Table 5.15: Code generator polynomials and initial states for GIOVE-B E5b-Q PRN code

## 5.8 Summary

Chapter 5 described in detail the deciphering of the Galileo GIOVE-A and GIOVE-B broadcast codes in all frequency bands. The GIOVE codes are more complicated to decode than their Compass counterparts. First, there are two codes with different code periods superimposed in each channel. Thus, there is an additional challenge in separating them. Second, the Galileo civil signals in E5 band suffer from more DME/TACAN interference, because the bandwidth covers more DME/TACAN frequencies. Third, the Galileo L1 band overlaps with GPS L1, so the GPS signals behave as additional noise when decoding Galileo GIOVE codes.

All PRN primary codes are truncated Gold Codes. All GIOVE-B broadcast codes have the same structure as their GIOVE-A counterparts, with the same generator polynomials, but different initial states. The GIOVE-A and GIOVE-B L1 codes have the chip rate of 1.023 MHz. L1-B code is 4 ms long and L1-C is twice as long. Both L1-B and L1-C codes are truncated 13-stage Gold codes. The E6 chip rate is 5.115 MHz, faster than that of L1 codes. E6-B code is a truncated 13-stage Gold code of 1 ms period. E6-C code is a truncated 14-stage Gold code of 2 ms period. All E5a and E5b codes are 10230-bit truncated 14-stage Gold codes of period 1 ms.

Table 5.16 provides a summary of the codes that we have currently determined for GIOVE-A and GIOVE-B. As of August 2008, GIOVE-B is transmitting in L1, E5a and E5b bands, but not in E6 band.

Frequency band	Modulation type	Code	Length	Period	Code type (Gold code)
L1	BOC	L1-B	4092	4 ms	13-stage
		L1-C	8184	8 ms	13-stage
E6	BPSK	E6-B	5115	1 ms	13-stage
		E6-C	10230	2 ms	14-stage
E5a	BPSK	E5a-I	10230	1 ms	14-stage
		E5a-Q	10230	1 ms	14-stage
E5b	BPSK	E5b-I	10230	1 ms	14-stage
		E5b-Q	10230	1 ms	14-stage

Table 5.16: Summary of GIOVE-A and GIOVE-B broadcast codes



## Chapter 6

# How Many Satellites Are Too Many?

The growing number of GNSS satellites and signals enable greater redundancy for positioning. On the other hand, the signals interfere with each other due to overlapping frequency bands. In this chapter, we answer the question: how many satellites are too many? We begin by studying various properties of the GIOVE and Compass PRN codes as well as statistical properties of random sequences. As GIOVE-A and GIOVE-B codes are similar, for brevity, we only show the results for GIOVE-A. We ultimately establish the multiple access capacity of GNSS.

### 6.1 Correlation Properties of Random Sequences

The auto- and cross-correlations of the PRN codes determine their system's robustness to noise and interference. In a noisy environment, the auto-correlation side peaks or the cross-correlation peaks with other PRN codes can exceed the main auto-correlation peak and thus confuse receiver acquisition and tracking loops. In this section, we analyze the statistical correlation properties of random sequences, modulated by BPSK and BOC(1,1). Let  $X = (x_1, x_2, \dots, x_N)$  and  $Y = (y_1, y_2, \dots, y_N)$  be sequences of independent and identically distributed (i.i.d.) random variables, taking values  $\pm 1$  equiprobably.

### 6.1.1 Auto-correlation of BPSK random sequence

Suppose that  $X$  is modulated by BPSK with chip duration  $T_c$ , so that the overall period of the code  $T_{code} = NT_c$ . The auto-correlation  $R_X(t)$  of this signal has the following properties, derived in [4].  $R_X(0) = 1$  deterministically and  $R_X(iT_c)$  (where  $i \neq 0$ ) has mean 0 and variance  $\frac{1}{N}$ . The mean and variance of this auto-correlation are plotted in Figures 6.1 and 6.2. Note that, between integer multiples of  $T_c$ , the mean and variance are linear [4]. Since the auto-correlation mean is zero away from the main peak, the variance characterizes the robustness of a random sequence used as a PRN code. Reducing the variance away from the main peak (by increasing the length  $N$ ) improves the likelihood that the main peak will be found by the receiver.

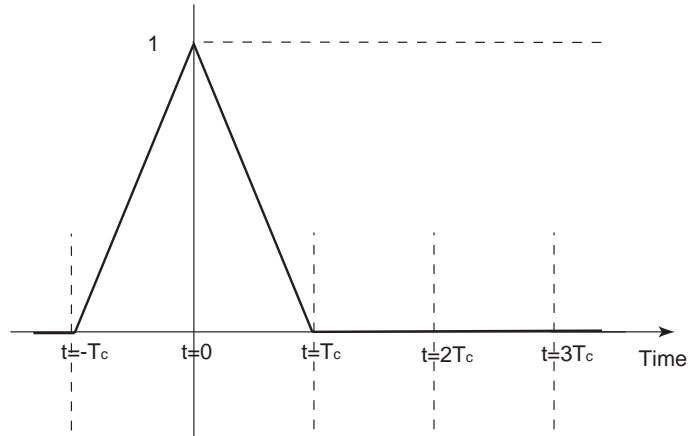


Figure 6.1: Auto-correlation mean of a random sequence of length  $N$  with BPSK modulation.

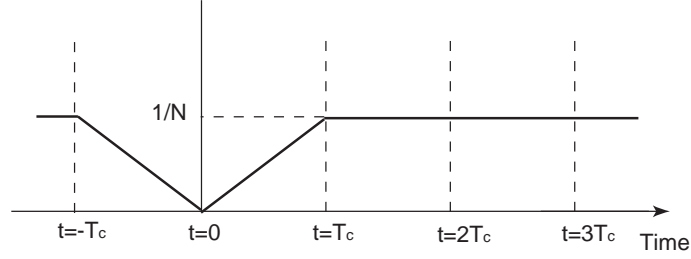


Figure 6.2: Auto-correlation variance of a random sequence of length  $N$  with BPSK modulation.

### 6.1.2 Cross-correlation of BPSK random sequences

Now suppose that  $X$  and  $Y$  are both modulated by BPSK. The mean of the cross-correlation  $R_{XY}(t)$  is 0, since the sequences are i.i.d. and zero mean. We now derive the cross-correlation variance at integer multiples of the chip duration  $T_c$ .

$$\begin{aligned}
 E\{(R_{XY}(iT_c) - E\{R_{XY}(iT_c)\})^2\} &= E\{(R_{XY}(iT_c))^2\} \\
 &= \frac{T_c^2}{T_{code}^2} E\left\{\sum_{m=0}^{N-1} x_m y_{m+i} \sum_{n=0}^{N-1} x_n y_{n+i}\right\} \\
 &= \frac{1}{N^2} \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} E\{x_m x_n y_{m+i} y_{n+i}\} \\
 &= \frac{1}{N},
 \end{aligned} \tag{6.1}$$

since

$$E\{x_m x_n y_{m+i} y_{n+i}\} = \begin{cases} 1, & \text{if } m = n \\ 0, & \text{otherwise} \end{cases}. \tag{6.2}$$

The cross-correlation variance is plotted in Figure 6.3, and its value is the same as the auto-correlation variance away from the main peak.

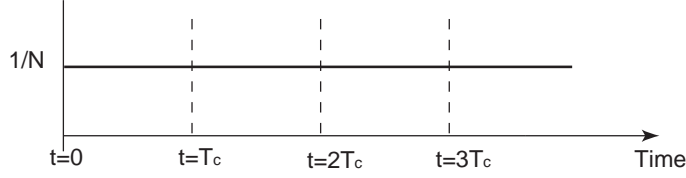


Figure 6.3: Cross-correlation variance of random sequences of length  $N$ , both modulated by BPSK.

### 6.1.3 Cross-correlation of BOC(1,1) and BPSK random sequences

The BPSK cross-correlation variance characterizes the level of self-interference within the GPS system. However, the Galileo L1 signal uses BOC(1,1) modulation. So, we now consider the cross-correlation between BOC(1,1) and BPSK random sequences. Suppose that  $X$  is modulated by BOC(1,1) to produce the signal  $X_{BOC}(t)$  and that  $Y$  is modulated by BPSK to produce the signal  $Y(t)$ , as illustrated in Figure 6.4. We represent  $X_{BOC}(t)$  as  $X_1(t) + X_2(t)$ , where  $X_1(t)$  captures the first halves of the chips and  $X_2(t)$  captures the second halves of the chips.

As in the case of BPSK cross-correlation, the cross-correlation mean is zero since the random sequences are i.i.d. and zero mean. The cross-correlation variance is

$$\begin{aligned} E\{(R_{XY}(t))^2\} &= E\left\{\left(\frac{1}{T_{code}} \int_0^{T_{code}} X_{BOC}(t)Y(t-\tau)d\tau\right)^2\right\} \\ &= E\left\{\left(\frac{1}{T_{code}} \int_0^{T_{code}} X_1(t)Y(t-\tau) + X_2(t)Y(t-\tau)d\tau\right)^2\right\}. \end{aligned} \quad (6.3)$$

When the signals are offset by an integer multiple of  $T_c$ , the chips of  $X_1(t)$  cancel out the chips of  $X_2(t)$  within each chip duration of  $Y(t)$ . So, the variance becomes

$$\begin{aligned} E\{(R_{XY}(iT_c))^2\} &= \frac{(T_c/2)^2}{T_{code}^2} E\left\{\left(\sum_{m=0}^{N-1} x_m y_{m+i} + (-x_m) y_{m+i}\right)^2\right\} \\ &= 0. \end{aligned} \quad (6.4)$$

When the signals are offset by an additional half a chip, the correlated chips of  $X_1(t)$

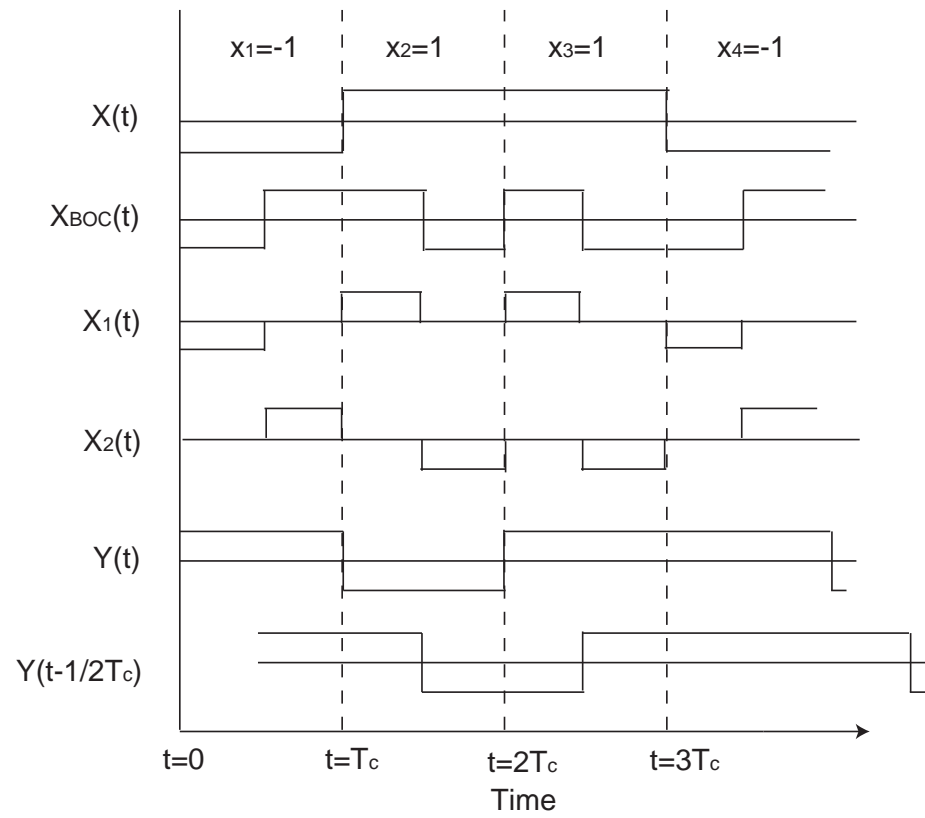


Figure 6.4: Illustration of a BOC modulated random sequence  $X_{BOC}(t)$  and a BPSK modulated random sequence  $Y(t)$ .

and  $X_2(t)$  overlap different chips of  $Y(t)$ . The variance is

$$\begin{aligned}
& E\{(R_{XY}((i + \frac{1}{2})T_c))^2\} \\
&= \frac{(T_c/2)^2}{T_{code}^2} E\{(\sum_{m=0}^{N-1} x_m y_{m+i} + (-x_m) y_{m+i+1})^2\} \\
&= \frac{1}{(2N)^2} E\{(\sum_{m=0}^{N-1} x_m y_{m+i})^2 + (\sum_{m=0}^{N-1} (-x_m) y_{m+i+1})^2 + 2 \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} x_m y_{m+i} (-x_n) y_{n+i+1}\} \\
&= \frac{1}{(2N)^2} E\{(\sum_{m=0}^{N-1} x_m y_{m+i})^2 + (\sum_{m=0}^{N-1} (-x_m) y_{m+i+1})^2\} \\
&= \frac{1}{2N}.
\end{aligned} \tag{6.5}$$

In the third step,  $x_m y_{m+i}$  and  $(-x_n) y_{n+i+1}$  are independent because either  $x_m$  and  $(-x_n)$  are independent or  $y_{m+i}$  and  $y_{n+i+1}$  are independent or both.

The cross-correlation variance of BOC(1,1) and BPSK modulated random sequences is plotted in Figure 6.5. Compared to BPSK versus BPSK, the maximum variance is halved, which indicates that BOC(1,1) interference to BPSK is 3 dB lower than the BPSK interference. This result is consistent with the BOC(1,1) and BPSK spectra, shown in Figure 6.6. The split spectrum of BOC(1,1) modulation does not fully overlap with the BPSK spectrum, thus reducing interference.

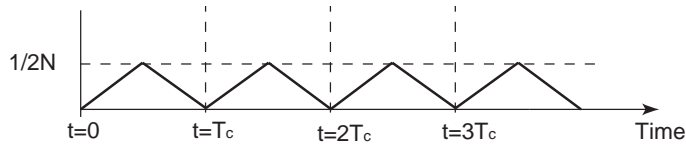


Figure 6.5: Variation of cross-correlation of random sequences of length  $N$ , BOC(1,1) vs. BPSK

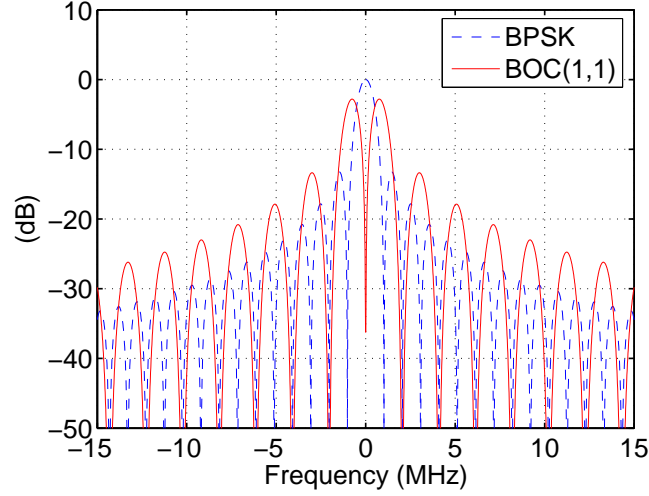


Figure 6.6: The spectra of BPSK and BOC(1,1) modulation, same as Figure 5.2.

#### 6.1.4 Cross-correlation of BOC(1,1) random sequences

The cross-correlation variance between two BOC(1,1) modulated random sequences  $X_{BOC}(t)$  and  $Y_{BOC}(t)$  is shown in Figure 6.7. This characterizes the self-interference within the Galileo system in L1 band. When the signals are offset by an integer multiple of  $T_c$ , the cross-correlation is equivalent to that of two BPSK modulated signals. In this case, the variance is  $\frac{1}{N}$ . When the signals are offset by an additional half a chip, the correlated chips of  $X_1(t)$  and  $X_2(t)$  overlap different chips of  $Y_{BOC}(t)$ . Similar to the derivation in (6.5), the variance is  $\frac{1}{2N}$ .

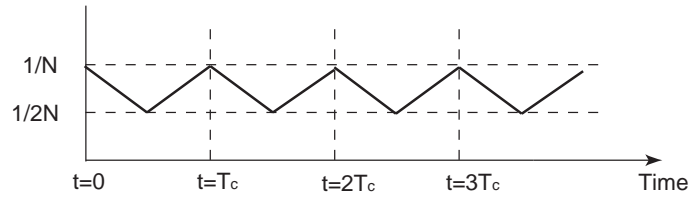


Figure 6.7: cross-correlation variance of random sequences of length  $N$ , both modulated by BOC(1,1).

The results in this section show that auto- and cross-correlation variances of random sequences are inversely proportional to the length of the random sequences.

## 6.2 Auto- and Cross-correlation within a System

We now consider the correlation properties of the actual broadcast PRN codes within the Galileo and Compass systems. For GIOVE-A, there are two codes in each frequency band, so each code acts as interference to its counterpart. The cross-correlation function characterizes how one PRN code interferes with the other code in the same band. For both auto- and cross-correlation functions, the lower the side lobes are, the lower SNR the system can tolerate. Tables 6.1 and 6.2 show the GIOVE-A maximum auto- and cross-correlation side lobes relative to the main peak. Based on our discussion of random codes, the correlation side peak variance is inversely proportional to the code length. The GIOVE-A L1-C and E6-C codes have lower maximum side lobes than their B counterparts, because they are twice as long and thus have longer integration time. When computing cross-correlation, two periods of the B codes are used to accommodate the C code lengths. Table 6.3 shows the Compass-M1 maximum auto-correlation side lobes. We also compare the maximum auto-correlation side lobes with random code side lobe variances as computed in the previous section. Side lobe variance represents an average behavior, while maximum auto-correlation side lobe is the worst case. It is shown that the worst case self-interference is about 10 to 12 dB higher than the average case.

GIOVE-A code	Maximum auto-correlation side lobes (dB)	Random code side lobe variance (dB)
L1-B	-25.39	-36.12
L1-C	-29.19	-39.13
E5a-I	-28.20	-40.10
E5a-Q	-28.38	-40.10
E5b-I	-28.20	-40.10
E5b-Q	-28.74	-40.10
E6-B	-26.32	-37.09
E6-C	-28.11	-40.10

Table 6.1: Maximum side lobes of GIOVE-A auto-correlation



GIOVE-A codes	Maximum cross-correlation side lobes (dB)	Random code side lobe variance (dB)
L1-B with L1-C	-27.94	-39.13
E5a-I with E5a-Q	-28.07	-40.10
E5b-I with E5b-Q	-28.88	-40.10
E6-B with E6-C	-29.27	-40.10

Table 6.2: Maximum side lobes of cross-correlation

Compass-M1 code	Maximum auto-correlation side lobes (dB)	Random code side lobe variance (dB)
E2/E5b	-23.68	-33.11
E6	-29.83	-40.10

Table 6.3: Maximum side lobes of Compass-M1 auto-correlation

Doppler residuals always exist in satellite signals. This causes frequency offset between the incoming signal and the local replica. Therefore, we need to investigate the correlation performance not only at zero frequency, but also at all frequency offsets ranging from -10 kHz to 10 kHz. The auto-correlation performance of the GIOVE-A L1, E6, E5a and E5b codes is shown in Figures 6.8 to 6.11. The auto-correlation performance of the Compass-M1 E2/E5b and E6 codes is shown in Figure 6.12. For the GIOVE-A L1 and E6 bands, the C codes have 3 dB better performance than the B codes, since the C codes are twice as long as the B codes. The Compass E6 code has roughly 7 dB better performance than the Compass E2/E5b code, because the length of the E6 code is 5 times that of the E2/E5b code.

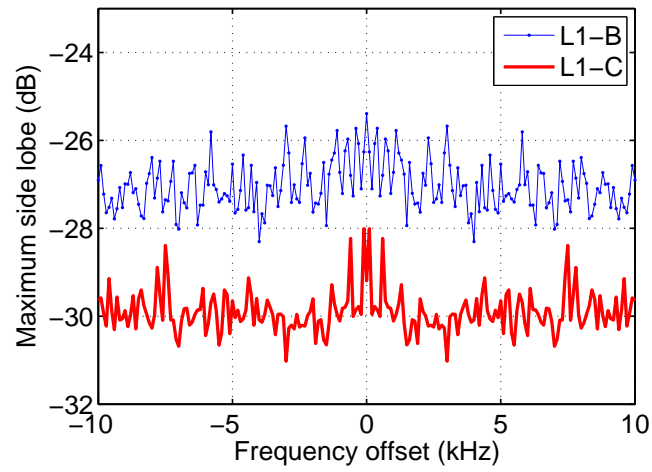


Figure 6.8: Maximum correlation side lobes of GIOVE-A L1 code auto-correlation

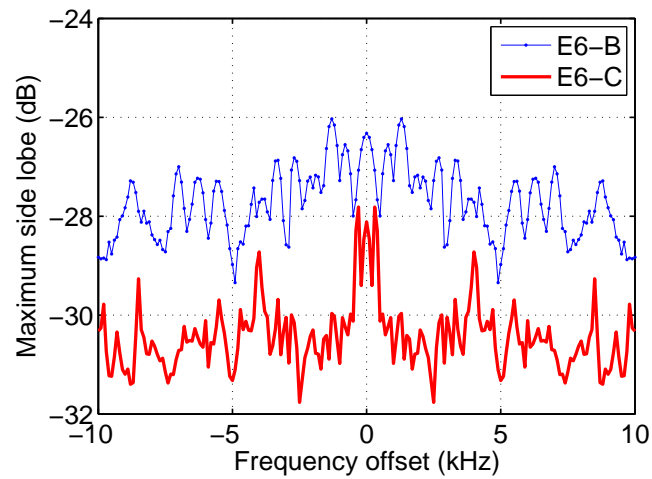


Figure 6.9: Maximum correlation side lobes of GIOVE-A E6 code auto-correlation

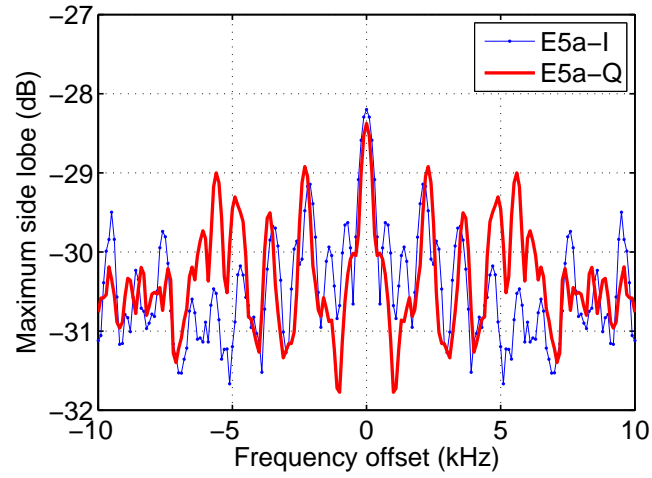


Figure 6.10: Max correlation side lobes of GIOVE-A E5a code auto-correlation

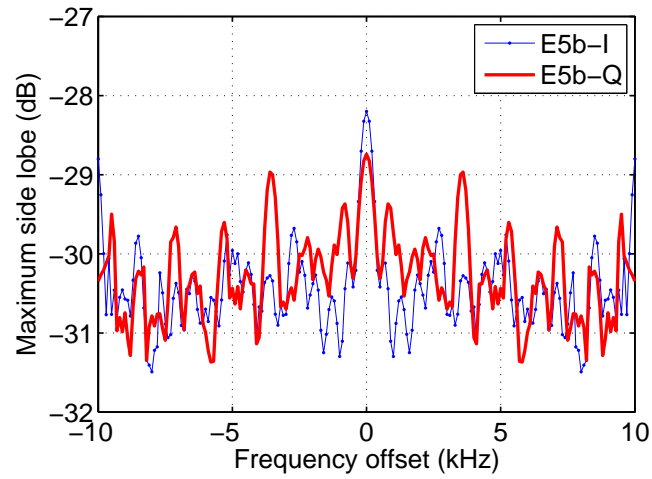


Figure 6.11: Maximum correlation side lobes of GIOVE-A E5b code auto-correlation

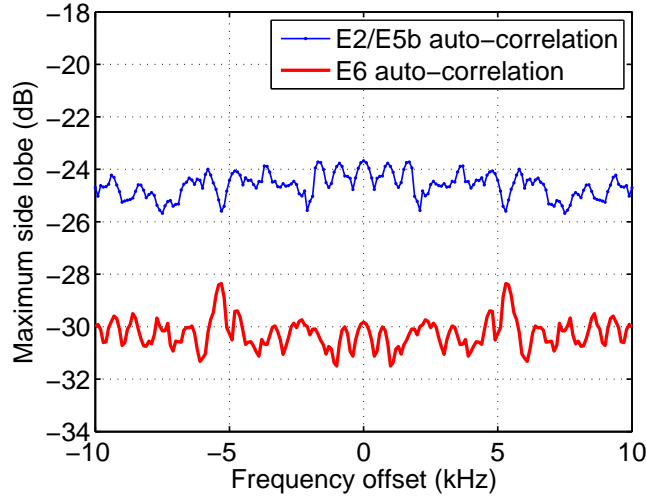


Figure 6.12: Maximum correlation side lobes of Compass E2/E5b and E6 code auto-correlation

### 6.3 Cross-correlation between Systems

The Galileo L1 band overlaps with that of GPS, and the Galileo E5b band overlaps with that of Compass as described in Chapter 1. When acquiring or tracking a Galileo signal, the signals from other satellites in the same frequency bands behave as interference. In return, the Galileo signals in the common frequency bands also interfere with other GNSS systems. The coexistence of Galileo and either GPS or Compass is characterized by the cross-correlation functions between the GIOVE-A PRN codes and the GPS or Compass PRN codes. In addition, since the satellites are orbiting, the relative velocity between two satellites results in a frequency offset between the PRN code of one incoming satellite signal and the PRN code of the local replica of another satellite. This frequency offset ranges from -10 kHz to 10 kHz.

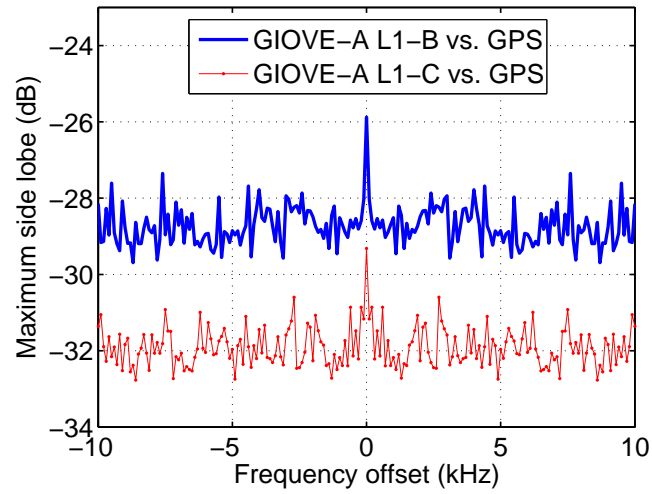


Figure 6.13: Maximum side lobes of cross-correlation between GIOVE-A L1 codes and GPS codes

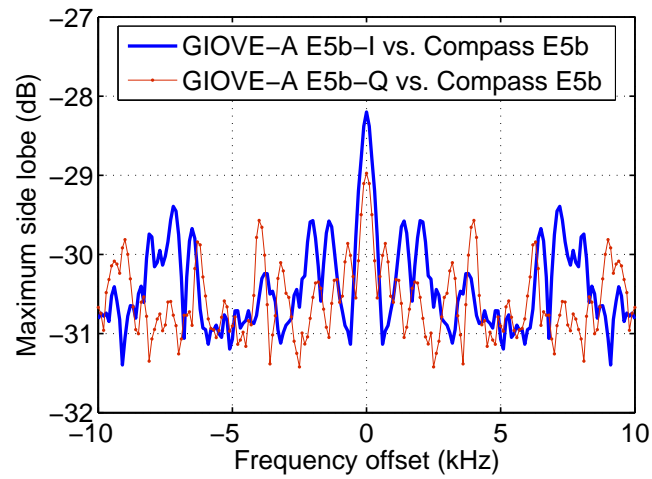


Figure 6.14: Maximum side lobes of cross-correlation between GIOVE-A E5b codes and Compass E5b code

Figure 6.13 shows the maximum side lobes of cross-correlation between the GIOVE-A and GPS PRN codes in L1 band. Since there are 32 PRN codes assigned for the GPS L1 C/A signal, the maximum side lobe is plotted among all 32 correlation functions at each frequency offset. BOC modulation of the GIOVE-A signal is considered, and the GPS C/A codes are repeated 4 and 8 times to accommodate the length of the GIOVE-A L1-B and L1-C codes, respectively. The performance of the L1-B code is 3 dB worse than that of the L1-C code, because the L1-B code is half the length of the L1-C code.

The maximum side lobes of cross-correlation between the GIOVE-A and Compass PRN codes in E5b band is shown in Figure 6.14.

## 6.4 Multiple Access Capacity of GNSS

Although the new satellites and signals provide greater redundancy for positioning, it is not always a case of “the more, the merrier.” The previous section showed that the GNSS satellites interfere with each other, because they share the frequency bands. When a receiver processes the signal from a particular satellite, other satellite signals contribute to the correlation side lobes. If there are too many satellites, the correlation side peaks may exceed the main peak, confuse the receiver, and cause the positioning to fail.

Beyond what number of satellites would a receiver fail? The question is not easy to answer, because receiver performance depends on a variety of parameters, such as integration time, coherent or non-coherent integration, receiver filters, LNA noise figure, etc. We choose to measure the level of the satellite self-interference relative to the thermal noise floor. This metric is thus general and independent of receiver design.

The GNSS satellite transmission power is estimated based on GPS transmission power and the similarity among the GPS, Galileo and Compass systems. The GPS L1 C/A signal power available from an isotropic antenna is shown in Figure 6.15. The power is not flat over the whole range of elevation angles in order to accommodate non-isotropic patch antenna gains. Patch antennas are the most popular antenna for

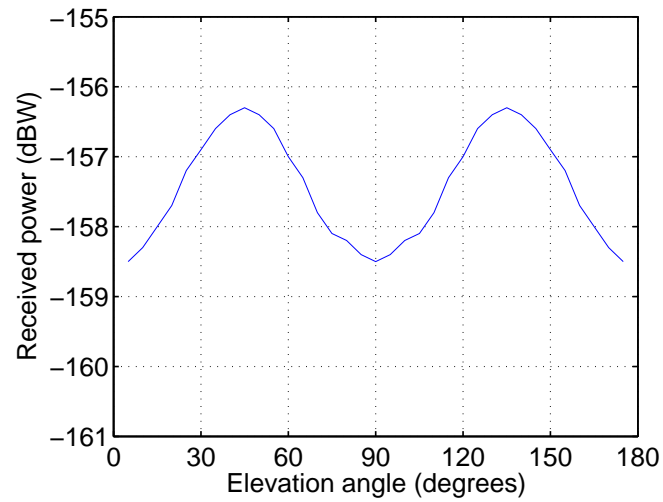


Figure 6.15: Received C/A code signal power available from an isotropic antenna as a function of elevation angle for a user on the surface of the earth [4].

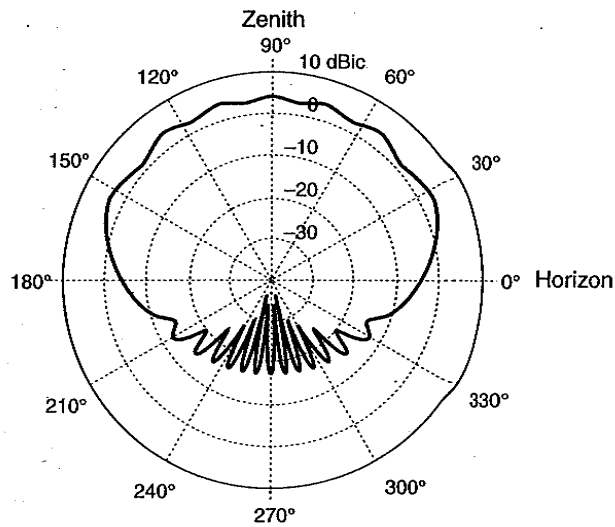


Figure 6.16: Commercial L1 antenna gain pattern. Predicted pattern for a standard patch antenna mounted on a four-wavelength-diameter circular ground plane (Courtesy of Frank Bauregger, Novariant, Inc.)

commercial receivers due to their low cost and small size. An example of a patch antenna gain is shown in Figure 6.16. It reaches a maximum towards zenith, an elevation of  $90^\circ$ . The received GPS L1 signal power, shown in Figure 6.17, is roughly flat from  $20^\circ$  to  $160^\circ$ , after being subject to the commercial patch antenna gain.

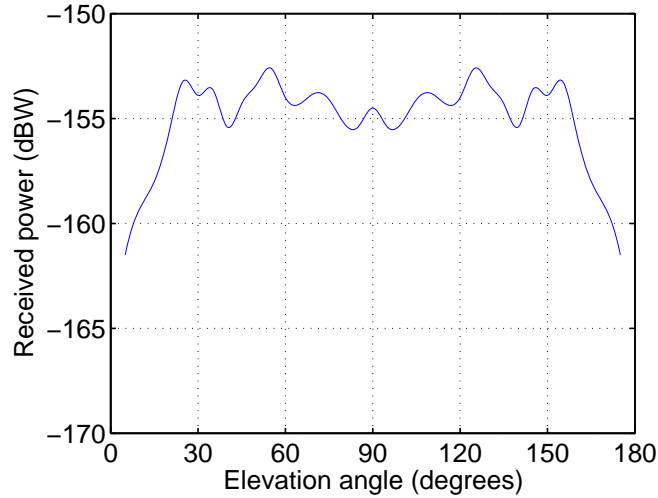


Figure 6.17: Received C/A code signal power subject to the gain of a patch antenna

To model the interference, we assume that GNSS satellites are uniformly distributed around the earth. We also assume that the PRN codes are random sequences. According to our discussion in Section 6.1, correlation side lobe variance is upper bounded by  $10 \log_{10} 1/N$  dB for both BPSK and BOC(1,1) modulation, where  $N$  is the code sequence length. We use the upper bound for our computations for two reasons. First, we consider up to 2000 satellites in the future, and it is uncertain how many of them will use BOC(1,1) and how many use BPSK modulation. Second, for a GPS L1 receiver with sampling rate 1.023 MHz, the incoming Galileo L1 BOC signal is down sampled and appears to be BPSK modulated. Figures 6.18 and 6.19 show the average-case GNSS satellite self-interference power level with respect to the thermal noise power level. In L1 band, the satellite self-interference power reaches that of thermal noise when there are 329 GNSS satellites. In L5 band, the self-interference power will not exceed the noise floor until there are 817 GNSS satellites. The L5 band



can tolerate larger number of satellites than the L1 band, because the L5 band is 10 times as wide as the L1 band. When both Galileo and Compass systems are fully deployed, there will be about 120 satellites. Even for L1 band, the self-interference then is still 4.5 dB below the thermal noise power level. So, we conclude that 120 satellites can coexist.

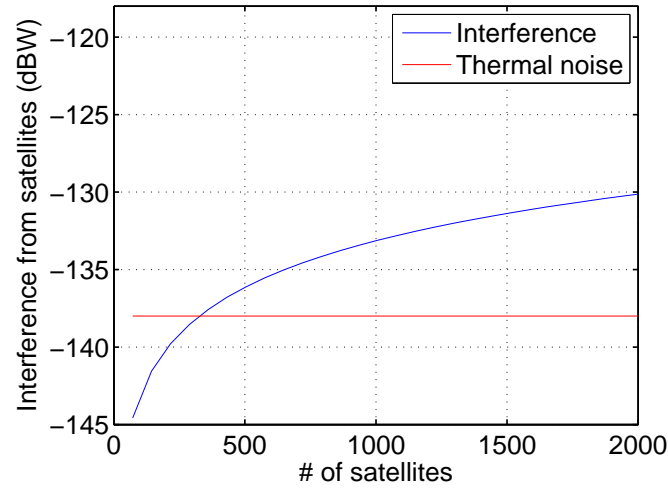


Figure 6.18: Average-case multiple satellite self-interference, L1 band

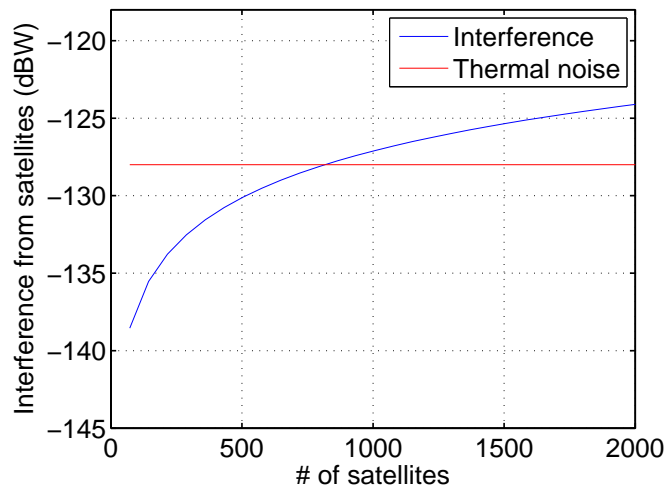


Figure 6.19: Average-case multiple satellite self-interference, L5 band

## 6.5 Summary

The code properties are analyzed with respect to correlation. Correlation performance is evaluated at different frequency offsets. On average, the C codes are better than the corresponding B codes by 3 dB because they are twice as long. The self-interference among the GNSS satellites with respect to the number of GNSS satellites is studied, and compared with the thermal noise level for both GPS L1 and L5 bands. When Galileo and Compass are completely deployed, we conclude that the total 120 navigation satellites from all GNSS systems can coexist.

## Chapter 7

# Satellite Acquisition and Tracking Results

In this chapter, we implement the Compass and Galileo code generators in a multi-signal all-in-view GNSS software receiver developed by David De Lorenzo [65–67] to acquire and track the broadcast Compass-M1 and GIOVE-A signals. We show results in the absence and in presence of DME/TACAN interference. We also investigate and propose methods of interference mitigation for better acquisition and tracking.

### 7.1 Frequency Bands without DME/TACAN

We first show the acquisition and tracking results in frequency bands that do not suffer from DME/TACAN, namely the Compass E2 and E6, and the Galileo L1 and E6 bands. Acquisition is implemented as a parallel code-phase search using FFT-based processing to correlate over code phase shift. Several milliseconds of data may be combined to increase weak-signal sensitivity or to provide more accurate estimates of carrier Doppler frequency, although at a trade-off in execution time. The 3-D acquisition plot in Figure 7.1 shows the normalized correlation function output of the Compass-M1 E2 signal as a function of code phase on one axis and carrier Doppler frequency on the other axis. A small amount of averaging (2 ms) is used. We read the code phase and Doppler estimate based on the location of the main peak in the

code phase and Doppler domain.

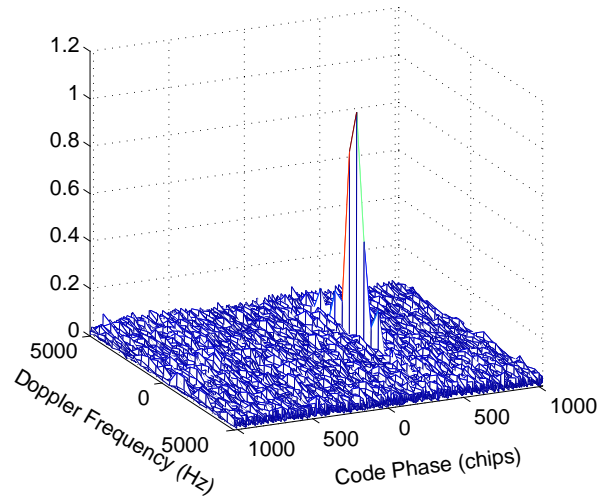


Figure 7.1: Acquisition plot of Compass-M1 E2 I-channel

Immediately after acquisition, the code-phase and carrier frequency estimates are used to initialize the code and carrier numerically-controlled oscillators (NCOs). The receiver refines the estimates of carrier frequency, carrier phase, and code phase through a succession of tracking modes, where the phase-lock and delay-lock loop (PLL and DLL, respectively) noise bandwidths are successively reduced.

The tracking output in Figure 7.2 shows four subplots as follows, each as a function of elapsed tracking time along the horizontal axis:

- Upper-left: PLL discriminator output in degrees
- Upper-right: DLL discriminator output in meters
- Lower-left: carrier Doppler frequency estimate
- Lower-right: code phase estimate with respect to the receiver's on-board millisecond counter

Since one of the tracking objectives is the estimation of the secondary code length and sequence, integration times are kept to 1 ms for all tracking modes (the length

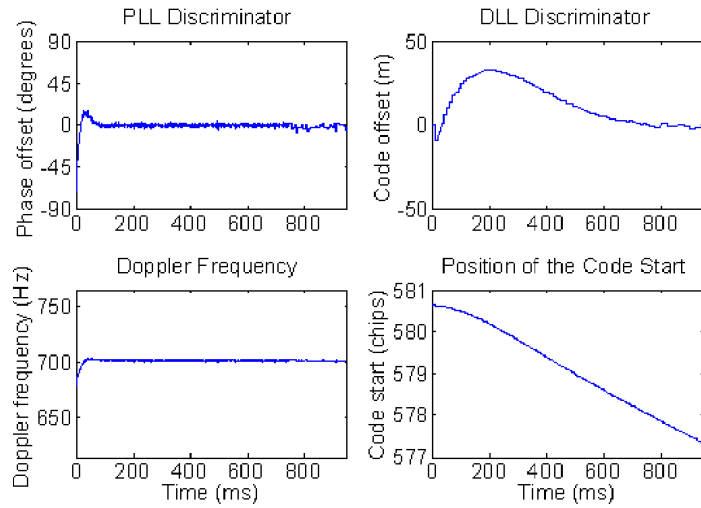


Figure 7.2: Tracking results of Compass-M1 E2 I-channel

of the primary PRN code sequence). This is because carrier polarity may change at each millisecond, and this sequence is unknown until the secondary decoding has occurred.

All tracking outputs converge, such as phase offset, code offset and Doppler frequency. The PLL converges quickly. However, the DLL discriminators take a bit longer to settle to roughly zero offset. This is caused by the acquisition algorithm estimating the code phase to the nearest sample, while there are only two-and-a-half samples per chip due to the choice of sampling rate. The result is that our initial estimate may be off by as much as a quarter of a chip. This is confirmed by the plot as our estimate is never greater than  $1/4$  chip (about 40 m) during convergence. The Doppler frequency is locked at 700 Hz as shown in the lower-left plot in Figure 7.2.

In addition to the Compass E2 signal, we are also able to successfully acquire and track the Compass E5b and E6, and the GIOVE-A L1 and E6 signals. For brevity, we only show the acquisition and tracking results for the E2 channel.

## 7.2 Frequency Bands with DME/TACAN

Although acquisition and tracking in bands without DME/TACAN are successful, they can fail in E5 band where DME/TACAN interference exists.

Figure 7.3 shows the acquisition and tracking results for GIOVE-A E5a Q channel. Although we can see an acquisition peak, there is a lot of noise. The correlation peak to next peak ratio (CPPR) is only 6.24 dB. This indicates a low SINR. The Doppler estimate is -700 Hz. Due to the low CPPR, this estimate is in fact inaccurate and later causes convergence failure in the tracking module.

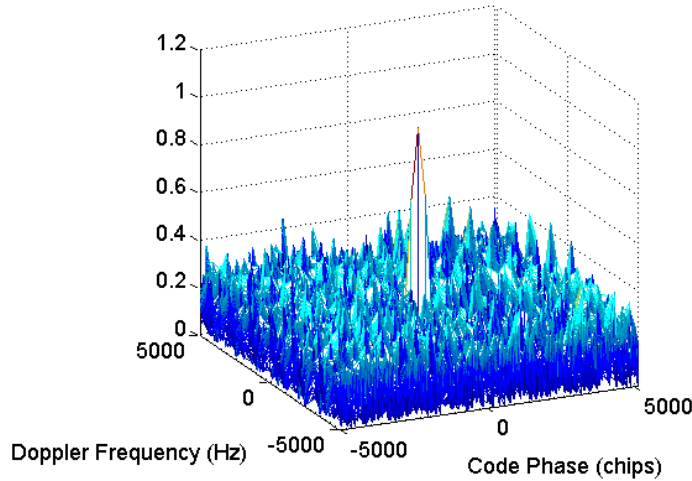


Figure 7.3: Acquisition plot of Galileo GIOVE-A E5a Q-channel

We initiate the tracking mode with a rough estimate of the code phase and carrier frequency from the acquisition results. Figure 7.4 shows the tracking results. Unfortunately, the PLL and DLL are not locked. We observe excessive jumps in the estimates of phase offset and code offset. This is caused by inaccurate Doppler offset and code phase output from the acquisition module. The Doppler offset should be -450 Hz, but the PLL incorrectly locks onto -700 Hz.

In this example, the reason for tracking failure is DME/TACAN interference, which degrades the SINR and causes the tracking loops to diverge. This motivates us to investigate algorithms to mitigate such interference.

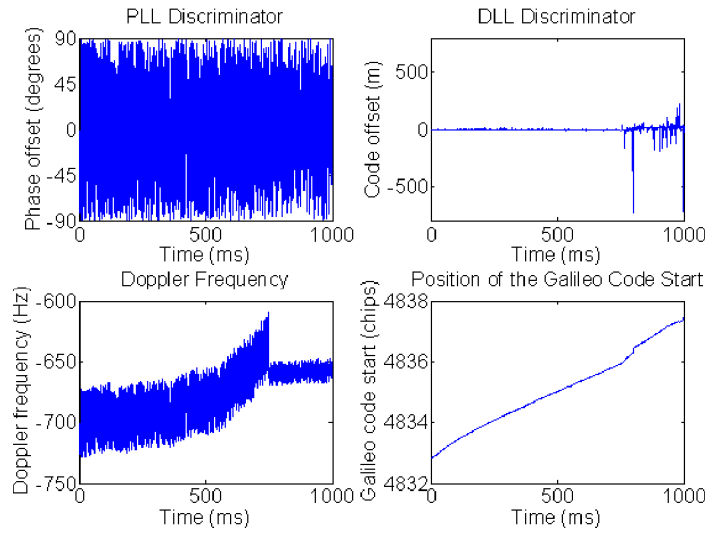


Figure 7.4: Tracking results of Galileo GIOVE-A E5a Q-channel

## 7.3 DME/TACAN Interference Mitigation

### 7.3.1 Pulse Blanking in Time Domain

Pulse blanking is suggested by [30, 31] as a time domain approach for mitigating DME/TACAN interference. It blanks the signal if the norm of its amplitude exceeds a certain threshold level, as shown in Figure 7.5.

Figures 7.6 and 7.7 show the time domain E5a signal before and after pulse blanking. Figure 7.8 shows the power spectrum after pulse blanking. In this example, pulse blanking mitigates 22 dB of DME/TACAN interference, reducing the spikes from -70 dB to -92dB. However, smaller spikes still exist at 17 dB above the noise floor.

Pulse blanking is effective and simple to implement but not thorough due to the bell shape of the DME/TACAN pulses. Their tails stretch below the noise floor, and thus cannot be removed by pulse blanking alone. Furthermore, the E5 signal that coincides with the pulses is also blanked out. In this example, since DME/TACAN pulses occur 10-14% of the time, pulse blanking reduces the E5 signal power by a similar amount.

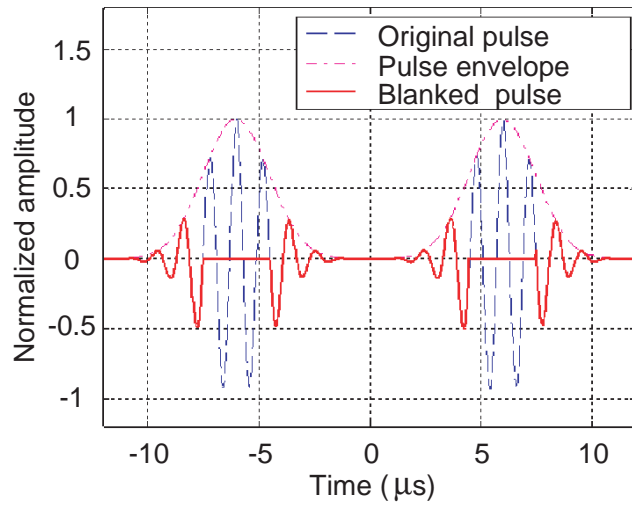


Figure 7.5: Pulse blanking

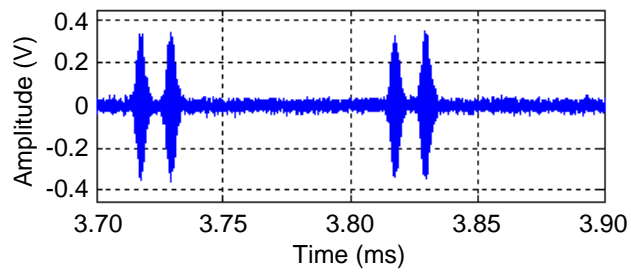


Figure 7.6: Time domain E5a signal before pulse blanking

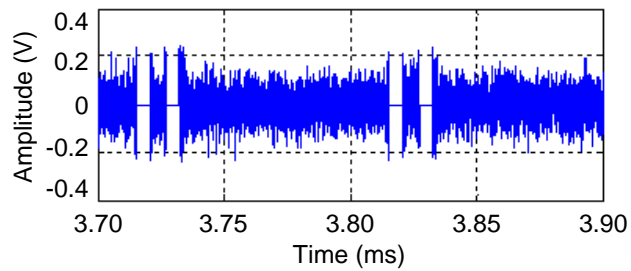


Figure 7.7: Time domain E5a signal after pulse blanking



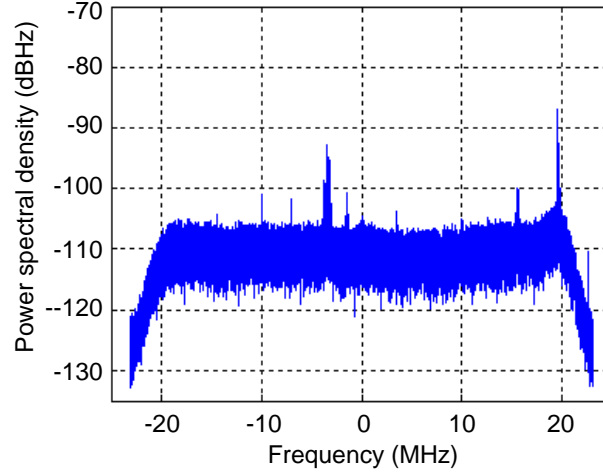


Figure 7.8: E5a power spectral density estimate, after pulse blanking

### 7.3.2 Notch Filtering In Frequency Domain

The DME/TACAN signals have pulse characteristics not only in time domain, but also in frequency domain. In the frequency spectrum, the DME/TACAN signals appear as narrow band frequency tones. Each frequency tone represents the signal from a nearby airport beacon. Therefore, another method to mitigate the DME/TACAN interference is notch filtering [68]. Notch filtering removes the frequency components that exceed a certain level of the noise spectral density as shown in Figure 7.9.

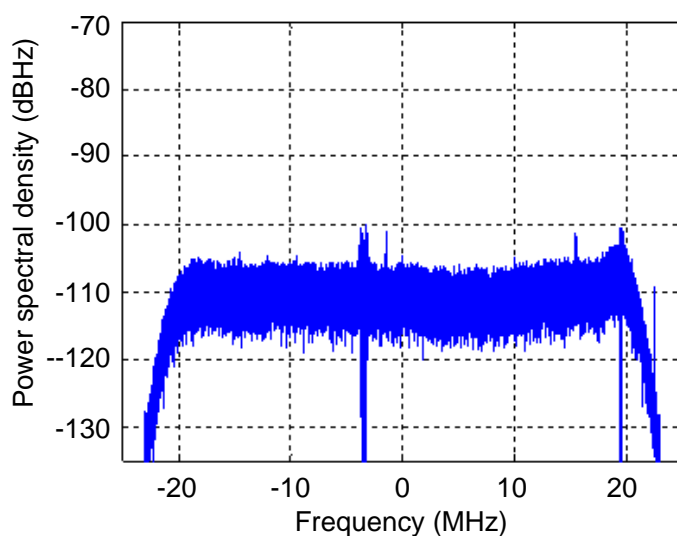


Figure 7.9: E5a power spectral density estimate after notch filtering

Notch filtering has two merits. First, it can completely suppress the DME/TACAN interference, including both the central part and the tails of the Gaussian pulses. As the DME/TACAN signals only occur at certain frequencies, if the signal power at these frequency components is filtered out, DME/TACAN interference can be eliminated. Second, compared to time domain pulse blanking, it preserves more of the energy of the E5 signal coincident with the interference pulses in time domain. Figure 7.10 shows the notch filtered data from the same time period as in Figure 7.6. The interference pulses disappear, while the E5 signal along with thermal noise remains.

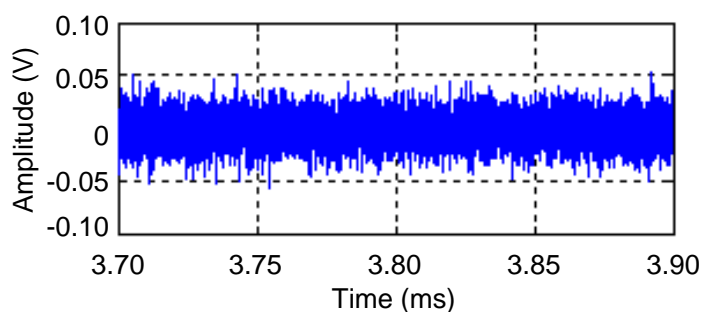


Figure 7.10: Time domain E5a signal, after notch filtering

However, notch filtering also has its drawbacks. Besides the interference, it also removes the E5 signal energy at the DME/TACAN frequencies. Since each nearby airport is mapped as a spike in the spectrum, a large number of airports in the surrounding area will result in many spikes in the spectrum. When filtering the frequency components regarding to the spikes, a large portion of the GNSS signal will be also filtered out. Even during the time period when there are no DME/TACAN pulses, the E5 signal at these frequencies is still filtered. Moreover, the design of the notch filter will become complicated as the number of nulls increases.

### 7.3.3 Hybrid Blanking in Time-Frequency Domain

Pulse blanking and notch filtering both have advantages and disadvantages. Pulse blanking only functions when pulse interference occurs, but it can not eliminate the pulses completely. It also has the side effect of blanking the E5 signal superposed with the pulses. Notch filtering can suppress pulse interference thoroughly and preserve most of the energy of the E5 signal energy coincident with the pulses, but it degrades the signal power even when there are no DME/TACAN pulses. The notch filter design becomes difficult when there are several notches in the filter due to the number of DME/TACAN transponders.

We propose another DME/TACAN interference mitigation technique, hybrid blanking, which combines the advantages of pulse blanking and notch filtering. The schematic of this technique is shown in Figure 7.11. The incoming signal is passed through a sliding window first. The next step is time domain pulse detection. In the time domain, if the amplitude of the incoming complex signal exceeds a certain level of the noise floor, a DME/TACAN pulse is detected. The pulse position is then estimated based on the center of mass of the signal in the segment. The pulse detection and the pulse center estimation trigger notch filtering. A  $12\ \mu\text{s}$  segment of data centered at the estimated pulse position is converted into frequency domain and is fed into a notch filter. The choice of  $12\ \mu\text{s}$  is due to the  $12\ \mu\text{s}$  interpulse interval and the Gaussian tailing effect. The filtered piece of data is then converted back to the time domain and replaces the original portion as the output.

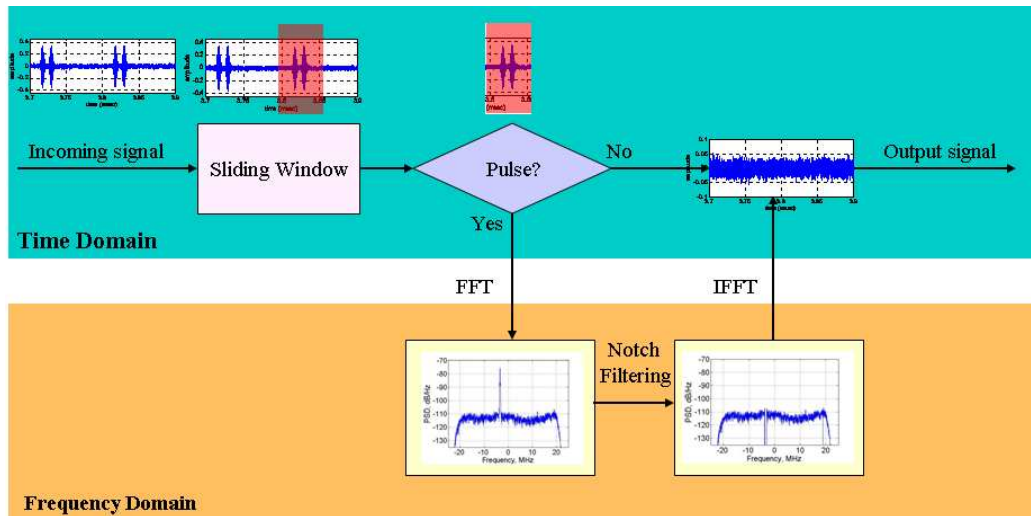


Figure 7.11: Hybrid blanking schematic

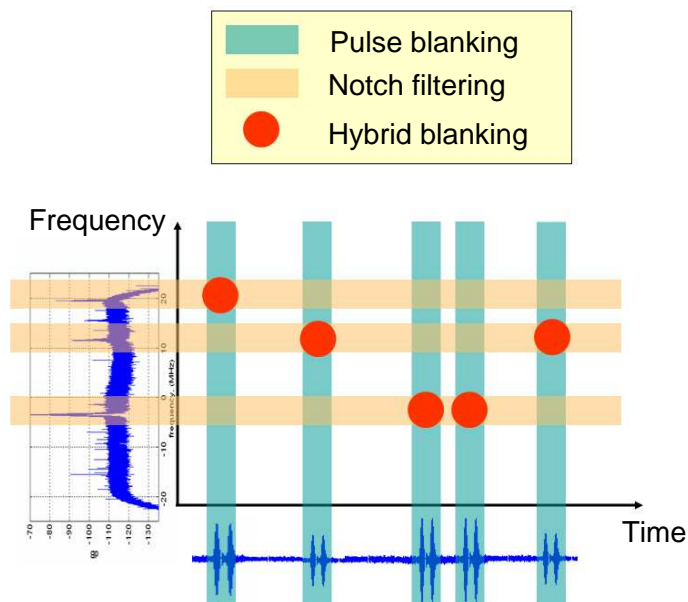


Figure 7.12: Selectivity of pulse blanking, notch filtering and hybrid blanking

Figure 7.12 shows the selectivity of the three mitigation techniques, pulse blanking, notch filtering and hybrid blanking. Hybrid blanking is shown as the red dots. Hybrid blanking is only implemented when DME/TACAN pulses exist. As shown in Figure 7.13, it overcomes the disadvantage of regular notch filtering, which always suppresses the corresponding frequency components of the signal even when there is no interference. For the slices of the data that are covered by DME/TACAN pulses, hybrid blanking preserves most of the signal energy as shown in Figure 7.14. This overcomes the disadvantage of time domain pulse blanking.

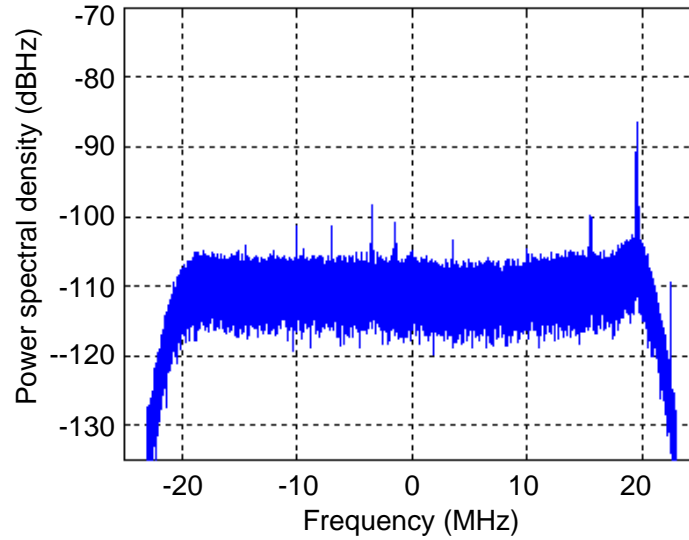


Figure 7.13: E5a power spectral density estimate, after hybrid blanking

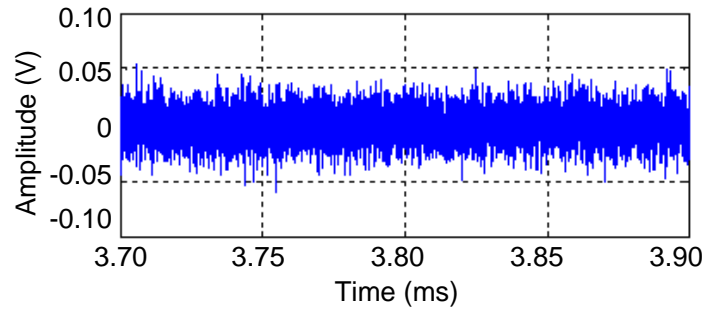


Figure 7.14: Time domain E5a signal, after hybrid blanking

## 7.4 DME/TACAN Mitigation at Stanford

In the previous section, we introduced pulse blanking and notch filtering, and proposed hybrid filtering for mitigating DME/TACAN interference for GNSS receivers. To evaluate these three methods, we first study the case at Stanford, CA. Signals from the Galileo GIOVE-A and Compass-M1 satellites are conditioned by these techniques respectively and acquired with a multi-signal all-in-view GNSS software receiver implemented in MATLAB [65–67]. We implemented the broadcast codes we decoded in Chapters 4 and 5. We have two figures of merit to evaluate the mitigation techniques, the correlation peak to next peak ratio (CPPR) and the correlation peak to mean peak ratio (CPPM). These two figures reflect the post-processing signal to noise plus interference ratio.

The real broadcast GNSS signals are acquired as a parallel code-phase search using FFT-based processing. We acquire 1 ms of data. The 3-D acquisition plots in Figures 7.15 to 7.18 show the normalized correlation function output as a function of code phase on one axis and carrier Doppler frequency on the other axis.

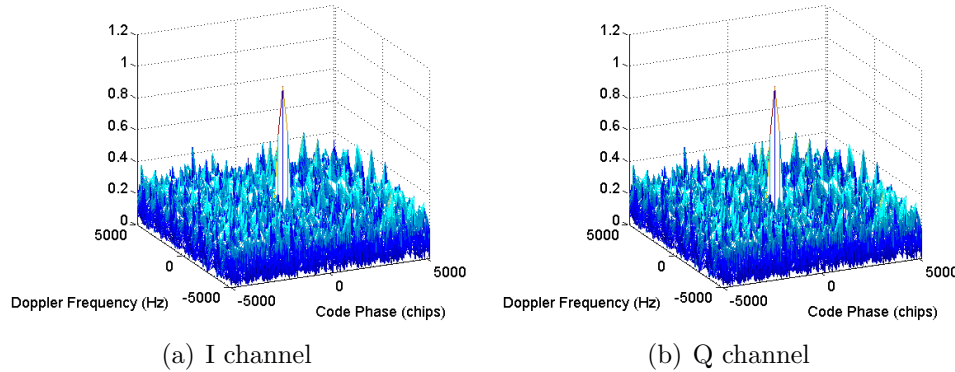


Figure 7.15: Acquisition plot of the Galileo E5a signal, raw data without DME/TACAN interference mitigation

Figure 7.15 shows the acquisition plots of the Galileo E5a-I and E5a-Q channels without any mitigation. The CPPRs and CPPMs are shown in Table 7.1. These low peak ratios are due to the high DME/TACAN interference.

	CPPR (dB)	CPPM (dB)
E5a-I	6.77	16.90
E5a-Q	5.93	16.65

Table 7.1: Acquisition results of the E5a, raw data

	CPPR (dB)	CPPM (dB)
E5a-I	16.99	28.35
E5a-Q	16.78	28.37

Table 7.2: Acquisition results of the E5a, pulse blanking

Next we apply pulse blanking before sending the raw data into the acquisition module. Figure 7.16 shows the acquisition results for E5a-I and E5a-Q channels. The integration time remains unchanged. This time we see less noisy plots. The CPPRs, shown in Table 7.2, increase from around 6 dB to 17 dB due to the pulse blanking technique. Figure 7.17 shows the tracking results. Compared with Figure 7.4, the tracking loops converge after pulse blanking is applied to mitigate the DME/TACAN pulses.

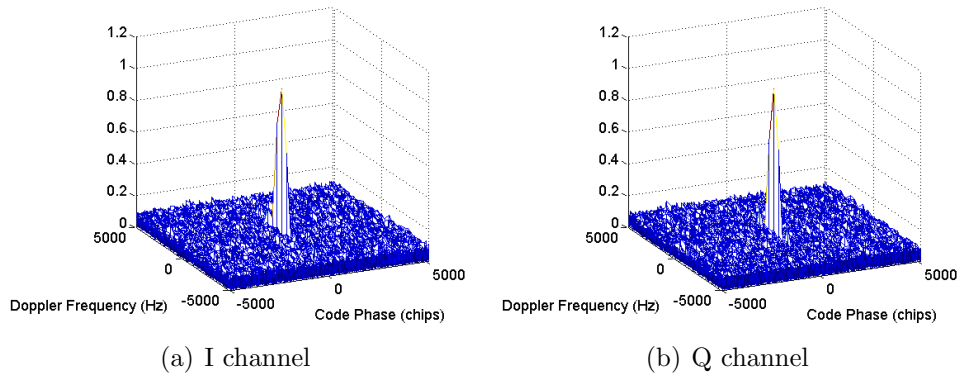


Figure 7.16: Acquisition plot of the Galileo E5a signal, with pulse blanking.

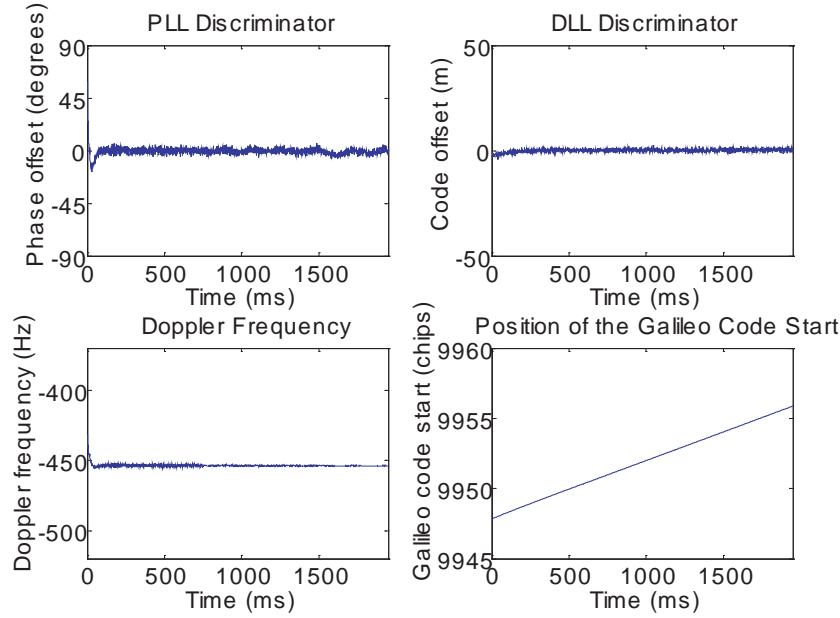


Figure 7.17: Tracking results of GIOVE-A E5a Q-channel, after pulse blanking

We also apply notch filtering to the raw data. Figure 7.18 shows the acquisition results for E5a-I and E5a-Q signals after notch filtering. The CPPRs and CPPMs, shown in Table 7.3, are only slightly better than those of pulse blanking. The similar CPPRs and CPPMs of notch filtering and pulse blanking indicate that the loss of notch filtering from suppressing the E5a signal where there are no interference pulses cancels out the gain from preserving the signal covered by these pulses.

	CPPR (dB)	CPPM (dB)
E5a-I	17.50	28.93
E5a-Q	17.35	28.90

Table 7.3: Acquisition results of the E5a, notch filtering



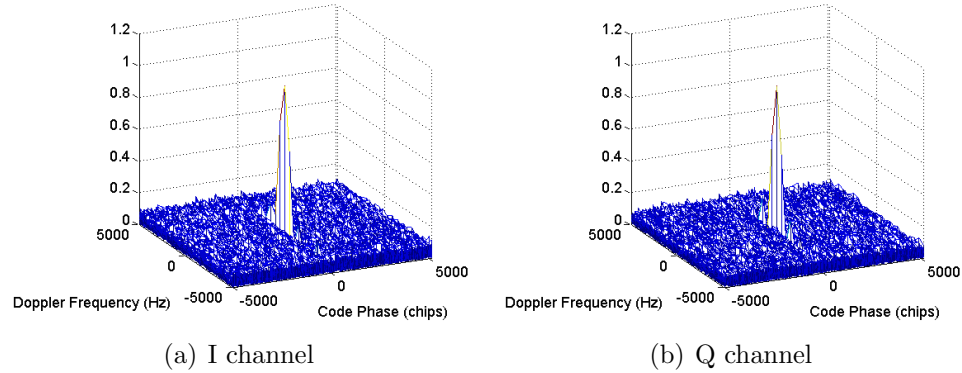


Figure 7.18: Acquisition plot of the Galileo E5a signal, with notch filtering

We then evaluate the hybrid blanking technique. Figure 7.19 shows the acquisition results for E5a-I and E5a-Q signals after hybrid blanking. The CPPRs and CPPMs in Table 7.4 improve, but by less than 1 dB. This indicates that hybrid blanking has slightly better performance than pulse blanking or notch filtering. The benefit is marginal since the DME/TACAN pulses occur about 10% of the time in this example. Thus, the improvement in SINR is limited to 10%, which converts to 1 dB. Hybrid blanking would be important when DME/TACAN pulses are denser in time and frequency domains. As for the interference environment of Stanford, California, the three mitigation methods have similar performance.

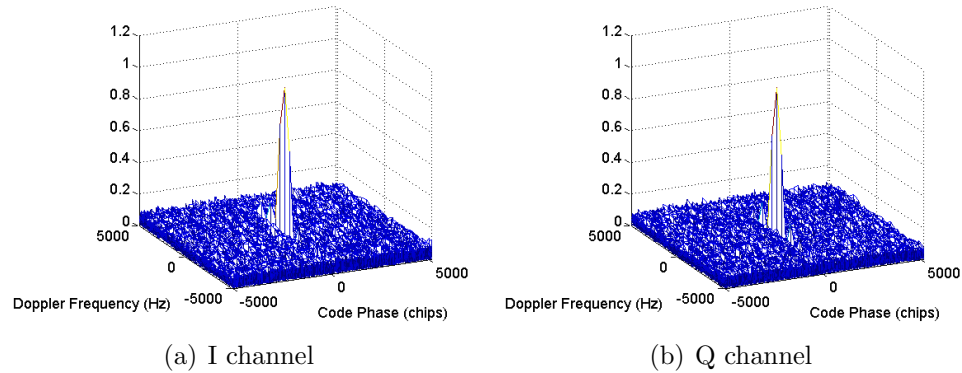


Figure 7.19: Acquisition plot of the Galileo E5a signal, with hybrid blanking

	CPPR (dB)	CPPM (dB)
E5a-I	17.70	29.15
E5a-Q	17.48	29.19

Table 7.4: Acquisition results of the E5a, hybrid blanking

## 7.5 Summary

In this chapter, we implemented the Compass and GIOVE code generators in a multi-signal all-in-view GNSS software receiver to acquire and track the broadcast Compass-M1 and GIOVE-A signals. We showed results in the absence and in the presence of DME/TACAN interference. We investigated existing interference mitigation techniques, pulse blanking in time domain and notch filtering in frequency domain, proposed a time and frequency domain combined technique, hybrid blanking. We used the acquisition and tracking results of the real broadcast signals to analyze the pulsed DME/TACAN interference environment at Stanford, CA, and to evaluate the different methods of interference mitigation. We showed that mitigation of pulsed interference is beneficial to receiver performance.

# Chapter 8

## Conclusions

### 8.1 Results and Contributions

This dissertation deciphered the new test satellite signals from the Galileo and Compass satellite systems, where the signal definition had not been published. All broadcast spread spectrum PRN codes of the Galileo GIOVE-A and GIOVE-B, and Compass-M1 satellites were decoded based on observation alone. The codes were shown to be Gold codes, and the code generators were also derived. The properties and interaction of these PRN codes were examined, and the multiple access capacity of GNSS established. We also implemented these PRN codes in our software receiver and used the acquisition and tracking results to analyze aeronautical interference to GNSS. We recap our contributions in more detail below.

#### **Designed Algorithms for Deciphering Unknown PRN Codes Chips**

Chapter 3 built a mathematical model for received Galileo and Compass signals that represented their components and parameters. This model provided the foundation for the decoding process, which involved stripping off all other components from the received signals, leaving only the PRN codes. The fundamental technique to reveal the unknown PRN code chips was to raise the SNR level by coherently combining multiple periods of the received signal. There were four main challenges in deciphering the codes. First, the received Galileo and Compass signals were very weak due to

the path loss. The received signal power was on the order of  $10^{-16}$  W, assuming an omnidirectional antenna. Second, the signal structure was complicated and unknown. Third, the data collection apparatus was asynchronous with respect to the satellite transmission. Fourth, the Galileo and Compass test signals were subject to strong interfering pulses from nearby aeronautical radio systems.

### **Modified the Berlekamp-Massey Algorithm in an Error-tolerant Manner**

The dissertation also designed an algorithm for analyzing the decoded PRN codes and their generation structures. The algorithm was a substantial modification of the well-known Berlekamp-Massey algorithm, to be robust against a high probability of code chip error. The code generation schematic in return resolved the overall polarity ambiguity of the PRN code sequences to complete and validate the deciphering process.

### **Characterized Galileo and Compass Test Satellite Signals**

Chapter 4 applied the algorithms of our design to the Compass-M1 broadcast I-channel codes in all frequency bands, namely E2, E5b and E6 bands. We not only extracted the code bits, but also derived the code generators. All three PRN primary codes are linear codes with a period of 1 ms. The E2 and E5b codes are identical; they are truncated 11th-order Gold codes of 2046 bits. The E6 code has 10230 bits, a concatenation of two Gold code segments. Both segments are truncated 13th-order Gold codes with the same code polynomials but different initial states. The E2, E5b and E6 primary codes are modulated with 20-bit Neuman-Hoffman codes as secondary codes. The secondary codes in the three frequency bands are identical.

Chapter 5 described in detail the decoding of the Galileo GIOVE-A and GIOVE-B broadcast codes in all frequency bands. There are two PRN codes superimposed in each frequency band. We not only extracted the code bits, but also derived the code generators. All PRN primary codes are truncated Gold Codes. All GIOVE-B broadcast codes have the same structure as their GIOVE-A counterparts, with the same generator polynomials, but different initial states.

Our Compass and GIOVE PRN code results have been implemented in software and hardware and independently verified by receiver companies. For example, Trimble Navigation, Ltd. tracked GIOVE-A in March 2007, and GIOVE-B in May 2008. Javad GNSS Inc. have applied our decoding results in their receivers since May 2007. W. Dewilde *et al.* from Septentrio Satellite Navigation N.V., a Belgian company, were able to track Compass-M1 E2 and E5b signals in real-time through a hemispherical antenna using the codes we supplied.

### **Established Multiple Access Capacity of GNSS**

Chapter 6 assessed the self-interference within GNSS, and hence established their multiple access capacity, by examining the code interactions between satellites. The code properties were analyzed with respect to and correlation at different frequency offsets. On average for GIOVE-A, the C codes were better than the corresponding B codes by 3 dB because they are twice as long. The self-interference among the GNSS satellites with respect to the number of GNSS satellites was studied in both GPS L1 and L5 bands. We concluded that when Galileo and Compass are completely deployed, a total of 120 navigation satellites from all GNSS systems can coexist.

### **Analyzed Pulsed Interference Mitigation**

In Chapter 7, we implemented the Compass and GIOVE code generators in a multi-signal all-in-view GNSS software receiver to acquire and track the broadcast Compass-M1 and GIOVE-A signals. We showed results in the absence and in the presence of DME/TACAN interference. We investigated existing interference mitigation techniques, pulse blanking in time domain and notch filtering in frequency domain, proposed a time and frequency domain combined technique, hybrid blanking. We used the acquisition and tracking results of the real broadcast signals to analyze the pulsed DME/TACAN interference environment at Stanford, CA, and to evaluate the different methods of interference mitigation.

## 8.2 Directions for Future Work

In this section, we briefly discuss a number of promising directions for future research.

### Analyzing New Signals of Upcoming Satellites

So far, only two satellites from Galileo and one satellite from Compass have been launched. More satellites will be launched to complete the whole constellation of the Galileo and Compass system. We are excited at the prospect of decoding and tracking many more new satellite signals using the methods described in this dissertation.

### Designing Optimal PRN Codes for Modernized GPS

The GPS, Compass-M1, GIOVE-A and GIOVE-B satellites all use Gold Codes as their broadcast spread spectrum codes, although with different numbers of stages and different generator polynomials and initial states. Gold codes have good correlation properties and are easy to generate. Are Gold codes optimal? Are there better code sets, which provides better auto- and cross-correlation performance for all Doppler frequency offsets? We have learned a lot from our European and Chinese colleagues. We hope their code design insights could help us find better PRN codes for modernized GPS.

### Using Real Data to Assess Self-interference

When establishing the multiple access capability of the whole GNSS family, we used simulated data and a few assumptions. Currently, the real data available are limited, because there are only a small number of Galileo and Compass satellites in orbit. We look forward to a more solid analysis of GNSS self-interference using real data when the constellations of Galileo and Compass are more complete.

### Analyzing DME/TACAN Interference in Other Environments

This dissertation analyzes the DME/TACAN interference environment at Stanford, CA. We would like to study other environments, especially Harrisburg, PA, where

DME/TACAN interference is the most severe in the US due to its proximity to several major airports.

### **Designing Integrated GPS/Galileo/Compass Hardware Receiver with Pulsed Interference Mitigation**

Finally, we would like to design an integrated GPS/Galileo/Compass receiver in hardware, which would provide a real platform to assess different pulsed interference mitigation techniques, the interoperability among the GPS, Galileo and Compass systems, and so on.





# Appendix A

## Acronyms

ARNS	Aeronautical Radionavigation Services
BOC	Binary Offset Carrier
BPSK	Binary Phase Shift Keying
C/A	Coarse Acquisition
CDMA	Code Division Multiple Access
CNES	Centre National d'Etudes Spatiales, the French Space Agency
CNSS	Compass Navigation Satellite System
CPPM	Correlation Peak to mean Peak Ratio
CPPR	Correlation Peak to next Peak Ratio
DLL	Delay Lock Loop
DME	Distance Measuring Equipment
DSP	Digital Signal Processing
EC	European Commission
ESA	European Space Agency
FAA	Federal Aviation Administration
FDMA	Frequency Division Multiple Access
FFT	Fast Fourier Transform
GEO	Geostationary Orbit

GLONASS	GLObal'naya Navigatsionnaya Sputnikovaya Sistema, translated as Global Navigation Satellite System
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
HP	High Precision
IGEB	Interagency GPS Executive Board
ITU	International Telecommunication Union
LFSR	Linear Feedback Shift Register
LNA	Low Noise Amplifiers
MEO	Medium Earth Orbit
NCO	Numerically-Controlled Oscillator
OS SIS ICD	Open Service Signal In Space Interface Control Document
PLL	Phase Lock Loop
PRN	Pseudo Random Noise
PRS	Public Regulated Service
QPSK	Quadrature Phase Shift Keying
RDSS	Radio Determination Satellite Service
RTCA	Radio Technical Commission for Aeronautics
SGMS	Stanford GNSS Monitor System
SINR	Signal to Interference plus Noise Ratio
SNR	Signal to Noise Ratio
SP	Standard Precision
TACAN	TACTical Air Navigation
VSA	Vector Signal Analyzer

# Bibliography

- [1] “The GPS constellation: Now and future,” *Defense Industry Daily*, August 24, 2005.
- [2] “ESA’s most advanced navigation satellite launched tonight,” *ESA Press Release*, April 27, 2008.
- [3] T. Grelier, J. Dantepal, A. Delatour, A. Ghion, and L. Ries, “Initial observations and analysis of Compass MEO satellite signal,” *Inside GNSS*, May/June 2007.
- [4] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*. Ganga-Jamuna Press, 2006.
- [5] B. W. Parkinson and J. J. Spilker, Jr., *Global Positioning System: Theory and Applications*. American Institute of Aeronautics and Astronautics (AIAA), 1996.
- [6] G. W. Hein and S. Wallner, “Development and design of Galileo,” in *Proceedings of ION Annual Meeting*, Cambridge, MA, USA, June 2005.
- [7] “First Galileo satellites named ‘GIOVE’,” *ESA Press Release*, November 9, 2005.
- [8] J. Amos, “Europe launches Galileo satellite,” *BBC News*, December 28, 2005.
- [9] “China’s state company obtains contract to develop Galileo technologies,” *People’s Daily*, March 30, 2005.
- [10] “China to build global satellite navigation system,” *People’s Daily*, 16 April, 2007.

- [11] U. Roßbach, "Positioning and navigation using the Russian satellite system GLONASS," Bundeswehr University Munich, Germany, 2000.
- [12] P. Daly, "Review of GLONASS system characteristics," in *Proceedings of the ION GPS Conference*, Colorado Springs, CO, USA, September 1990.
- [13] —, "GLONASS approaches full operational capability (FOC)," in *Proceedings of the ION GPS Conference*, Palm Springs, CA, USA, September 1995.
- [14] P. Silvestrin, S. Riley, N. Howard, E. Aardoom, and P. Daly, "A combined GPS/GLONASS high precision receiver for space applications," in *Proceedings of the ION GPS Conference*, Palm Springs, CA, USA, September 1995.
- [15] R. B. Langley, "GLONASS: Review and update," *GPS World*, July 2007.
- [16] G. L. Cook, "GLONASS: The next generation?" in *Proceedings of ION GPS conference*, Portland, OR, USA, September 2002.
- [17] "GLONASS constellation status by russian space agency," accessed July 29, 2008. [Online]. Available: {<http://www.glonass-ianc.rsa.ru/pls/htmldb/f?p=202:20:17421293520707003964::NO>}
- [18] "GLONASS interface control document, version 5.0," accessed July 29, 2008. [Online]. Available: [http://www.glonass-ianc.rsa.ru/i/glonass/ICD02\\_e.pdf](http://www.glonass-ianc.rsa.ru/i/glonass/ICD02_e.pdf)
- [19] J. Benedicto, S. E. Dinwiddy, G. Gatti, R. Lucas, and M. Lugert, "GALILEO: Satellite system design and technology developments," *ESA Documentation*, July 17, 2007.
- [20] "How to build up a constellation of 30 navigation satellites," *ESA Documentation*, July 17, 2007.
- [21] "GIOVE-B transmitting its first signals," *ESA Press Release*, May 7, 2008.
- [22] G. W. Hein, J. Godet, J.-L. Issler, J.-C. Martin, R. Lucas-Rodriguez, and T. Pratt, "The GALILEO frequency structure and signal design," in *Proceedings of ION GPS conference*, Salt Lake City, UT, USA, September 2001.

- [23] Z. F. Shaofeng Bian, Jihuang Jin, “The Beidou satellite positioning system and its positioning accuracy,” in *Navigation*, vol. 52, no. 3, 2005.
- [24] S. A. Dale, P. Daly, and I. D. Kitching, “Understanding signals from GLONASS navigation satellites,” *International Journal of Satellite Communications*, 7:1122 1989.
- [25] G. R. Lennen, “The USSRs Glonass P-Code determination and initial results,” in *Proceedings of the ION GPS Conference*, Colorado Springs, CO, USA, September 1989.
- [26] “Implementation of a third civil GPS signal: Final report,” *Interagency GPS Executive Board*, November 1999.
- [27] C. Hegarty, A. V. Dierendonck, D. Bobyn, M. Tran, and J. Grabowski, “Suppression of pulsed interference through blanking,” in *Proceedings of the ION Annual Meeting*, San Diego, CA, USA, June 2000.
- [28] J. Grabowski and C. Hegarty, “Characterization of L5 receiver performance using digital pulse blanking,” in *Proceedings of the ION GPS Conference*, Portland, OR, USA, September 2002.
- [29] F. Bastide, C. Macabiau, D. Akos, and B. Roturier, “Assessment of L5 receiver performance in presence of interference using a realistic receiver simulator,” in *Proceedings of the ION GPS Conference*, Portland, OR, USA, September 2003.
- [30] T. Kim and J. Grabowski, “Validation of GPS L5 coexistence with DME/TACAN and Link-16 system,” in *Proceedings of ION GNSS conference*, Portland, OR, USA, September 2003.
- [31] F. Bastide, E. Chatre, C. Macabiau, and B. Roturier, “GPS L5 and Galileo E5a/E5b signal-to-noise density ratio degradation due to DME/TACAN signals: Simulation and theoretical derivation,” in *Proceedings of ION NTM Conference*, San Diego, CA, USA, January 2004.

- [32] R. J. Erlandson, T. Kim, C. Hegarty, and A. J. V. Dierendonck, "Pulsed RFI effects on aviation operations using GPS L5," in *Proceedings of the ION NTM Conference*, San Diego, CA, USA, January 2004.
- [33] "Assessment of radio frequency interference relevant to the GNSS L5/E5A frequency band," *RTCA DO-292*, July 2004.
- [34] J. Owen, "Results of an investigation into the use of 1175 MH and 1202 MHz for GNSS signals in European airspace," in *Proceedings of the ION NTM Conference*, San Diego, CA, USA, January 2002.
- [35] M. Powe and J. I. R. Owen, "The European GNSS L5/E5 interference environment and the performance of pulsed interference mitigation techniques," in *Proceedings of the ION GNSS Conference*, Long Beach, CA, USA, September 2004.
- [36] G. W. Hein, J. Godet, J.-L. Issler, J.-C. Martin, P. Erhard, R. Lucas-Rodriguez, and T. Pratt, "Galileo broadcast E5 codes and their application to acquisition and tracking," in *Proceedings of ION GPS conference*, Portland, OR, USA, September 2002.
- [37] J.-L. Issler, G. W. Hein, J. Godet, T. Pratt, P. Erhard, R. Lucas-Rodriguez, and J.-C. Martin, "Galileo frequency and signal design," *GPS World*, June 2003.
- [38] G. X. Gao, J. Spilker, Jr., T. Walter, P. Enge, and A. R. Pratt, "Code generation scheme and property analysis of broadcast Galileo L1 and E6 signals," in *Proceedings of ION GNSS conference*, Fort Worth, TX, USA, September 2006.
- [39] M. M. M. C. E. R. C. J. M. T. M. Falcone, M. Lugert, "GIOVE-A in orbit testing results," in *Proceedings of the ION GNSS Conference*, Fort Worth, TX, USA, September 2006.
- [40] E. Rooney, M. Unwin, G. Gatti, M. Falcone, S. Binda, M. Malik, and D. Hannes, "GIOVE-A and GIOVE-A2 orbit testing results," in *Proceedings of the ION GNSS Conference*, Fort Worth, TX, USA, September 2007.

- [41] M. L. Psiaki, T. E. Humphreys, S. Mohiuddin, S. P. Powell, A. P. Cerruti, and J. Paul M. Kintner, "Reception and analysis of signals from GIOVE-A," *GPS World*, June 2006.
- [42] —, "Searching for Galileo," in *Proceedings of ION GNSS conference*, Fort Worth, TX, USA, September 2006.
- [43] O. Montenbruck, C. Günther, S. Graf, M. Garcia-Fernandez, J. Furthner, and H. Kuhlen, "GIOVE-A initial signal analysis," *GPS Solutions*, May 2006.
- [44] G. X. Gao, D. S. De Lorenzo, A. Chen, S. C. Lo, D. M. Akos, T. Walter, and P. Enge, "Galileo broadcast E5 codes and their application to acquisition and tracking," in *Proceedings of ION NTM conference*, San Diego, CA, USA, January 2007.
- [45] "GIOVE-A navigation signal-in-space interface control document," *ESA Galileo Documentation*, November 2000.
- [46] "Galileo open service signal in space interference control document (OS SIS ICD)," published May 23, 2006, accessed Feb 18, 2007.
- [47] G. X. Gao, D. Akos, T. Walter, and P. Enge, "GIOVE-B on the air, understanding Galileo's new signals," *Inside GNSS*, May/June 2008.
- [48] T. Grelier, A. Ghion, J. Dantepal, L. Ries, A. DeLatour, J.-L. Issler, and G. H. J.A. Avila-Rodriguez, S. Wallner, "Compass signal structure and first measurements," in *Proceedings of the ION GNSS Conference*, Fort Worth, TX, USA, September 2007.
- [49] G. X. Gao, A. Chen, S. Lo, D. De Lorenzo, and P. Enge, "GNSS over China, the Compass MEO satellite codes," *Inside GNSS*, July/August 2007.
- [50] E. R. Berlekamp, *Algorithmic Coding Theory*. New York: McGraw-Hill, 1968.
- [51] W. D. Wilde, F. Boon, J.-M. Sleewaegen, and F. Wilms, "More Compass points: Tracking Chinas MEO satellite on a hardware receiver," *Inside GNSS*, July/August 2007.

- [52] G. Parks, "Large antennas," *IRE Professional Groups on Antennas and Propagation Newsletter*, Jan 1962.
- [53] S. Lo, A. Chen, P. Enge, G. X. Gao, D. Akos, J.-L. Issler, L. Ries, T. Grelier, and J. Dantepal, "GNSS album: Images and spectral signatures of the new GNSS signals," *Inside GNSS*, May/June 2006.
- [54] S. Ford, "Short takesNova for Windows 32," *QST Magazine*, April 2000.
- [55] J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, January 1969.
- [56] S. W. Golomb and G. Gong, *Signal Design for Good Correlation*. Cambridge University Press, 2005.
- [57] J. Spilker, Jr., *Digital Communications by Satellite*. Prentice-Hall Information Theory Series, 1977.
- [58] W. Stallings, *Data and Computer Communications (7th ed.)*. Prentice Hall, 2004.
- [59] J. J. Spilker, Jr., E. Martin, and B. W. Parkinson, "A family of split spectrum GPS civil signals," in *Proceedings of the 11th International Technical Meeting of the Satellite Division of the Institute of Navigation ION GPS*, Nashville, TN, USA, September 1998.
- [60] J. W. Betz, "A note on offset carrier signals," *MITRE Product MP98B14*, March 1998.
- [61] —, "The offset carrier modulation for GPS modernization," in *Proceedings of the ION NTM Conference*, San Diego, CA, USA, Jan 1999.
- [62] A. R. Pratt and J. I. R. Owen, "BOC modulation waveforms," in *Proceedings of ION GPS conference*, Portland, OR, USA, September 2003.
- [63] L. R. Weill, "Multipath mitigation, how good can it get with new signals?" *GPS World*, June 2003.



- [64] M. Kayton and W. R. Fried, *Avionics Navigation Systems, Second Edition*. John Wiley and Sons, Inc., 1997.
- [65] D. S. De Lorenzo, J. Rife, P. Enge, and D. M. Akos, "Navigation accuracy and interference rejection for an adaptive GPS antenna array," in *Proceedings of the ION GNSS Conference*, Fort Worth, TX, USA, September 2006.
- [66] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen, *A Software-Defined GPS and Galileo Receiver: A Single-Frequency Approach*. Birkhäuser Boston, 2006.
- [67] D. S. De Lorenzo, *Navigation Accuracy and Interference Rejection for GPS Adaptive Antenna Arrays*. Ph.D. Thesis, Stanford University, 2007.
- [68] B. Widrow and S. Stearns, *Adaptive Signal Processing*. Prentice Hall, 1985.