Research Article
Blind Estimation of GPS M-Code Signals under Noncooperative Conditions

Zixuan Rui, Xiaofeng Ouyang, Fangling Zeng, and Xu Xu

College of Electronic Engineering, National University of Defense Technology, 230037, China

Correspondence should be addressed to Zixuan Rui; ruizixuan17@nudt.edu.cn

Received 27 August 2022; Accepted 27 September 2022; Published 12 October 2022

1. Introduction

Although the Global Positioning System (GPS) has been widely used in military and civilian applications over the past three decades, its accuracy, continuity, and anti-jamming capabilities still need further improvement [1]. To establish effective warfare navigation capabilities while further improving system performance for both authorized and unauthorized users, the GPS modernization program has been implemented. The first phase of the GPS modernization program was the launch of the Block IIR-M satellites, which added a civilian L2C signal in the L2 band and broadcast a new military M-code signal in both the L1 and L2 bands [2]. The first GPS IIR-M satellite was launched on September 2, 2005. The second phase was the launch of the Block IIF satellites, which further enhanced the transmission power of the M-code signal and added a new civil signal in the L5 band [3]. The third phase is the launch of the Galileo-compatible Block III satellites, which will eventually replace all Block II satellites, thereby significantly improving GPS performance. As the next generation of military signals, M-code signals are the most critical content of the GPS modernization program and the primary means of achieving future warfare navigation objectives.

As the military signals currently in use, P(Y) signals have provided high-accuracy navigation and positioning services for military users. The length of their pseudocode sequences, with a cycle time of up to seven days, and their complex encryption methods make them almost impossible to decipher, but P(Y) signals also have the following inherent defects [4]. First, in the signal acquisition process, the long pseudocode sequences are challenging to capture directly, so the P(Y) signals are typically captured with the aid of the C/A code. The C/A code has shorter code sequences but poorer anti-interference capabilities. Therefore, this approach weakens the anti-interference and anti-spoofing capabilities of P(Y) signals. Second, the P(Y) signals use binary phase shift keying (BPSK) modulation. Their spectrum significantly overlaps with that of the C/A code, which means that C/A-code and P(Y) signals may interfere with each other, thus limiting the ability to improve anti-interference capabilities through power enhancement. To overcome these flaws of P(Y) signals, Betz proposed a new signal modulation scheme, binary offset carrier (BOC)
modulation [5]. This modulation scheme is specifically designed for the characteristics of satellite navigation signals. It allows a new signal to be added to the current band without causing interference with the original signal components. M-code signals are gradually replacing P(Y) signals to provide more secure, accurate, and highly robust military navigation and positioning services.

Because M-code signals are the next generation of military navigation signals, their pseudocode sequences and generation mechanism are highly classified [3]. This presents significant difficulties in estimating pseudocode sequences. Satellite selection and the pseudorange calculation depend on the replication of the pseudocode sequence. When the signal generation mechanism is unknown, the ranging performance and sequence characteristics cannot be accurately evaluated.

For this reason, research institutions in Germany and Austria have carried out monitoring projects on GPS M-code signals. These projects focus on receiving GPS signals and separating the M codes from the composite signals to achieve the blind estimation of GPS M-code sequences [6]. Research teams from Austria and Ireland have developed a blind sequence generator for this purpose, using a 1.8-meter turntable antenna to extract the code sequences of GPS M-code signals on the ground for tracking and measurement. To perform code sequence estimation for signals with unknown signal properties, the modulation of signals, code rate, center frequency,(4,6),(994,993)
BPSK signals. Multiple secondary peaks are present simultaneously, which can enable highly accurate code tracking and good multipath resolution due to the narrow prominent peaks of the autocorrelation functions of BOC-modulated signals. In the case of Gaussian white noise, the pseudorange measurement error of M codes is approximately 1/2.6 that of P(Y) codes; thus, the former has the potential to provide better navigation performance [14]. Figure 4 plots the autocorrelation function of BOC-modulated signals at different bandwidths, and it can be seen that the peak change of the autocorrelation function tends to flatten out as the bandwidth increases. Additionally, as the order of the BOC signal increases, the slope of the central peak of the autocorrelation function increases, and the signal becomes more sensitive to the time offset.

3. Algorithm Description

The first GPS III satellite, SVN-74, was built by Lockheed Martin Space and launched on December 23, 2018, from Cape Canaveral, Florida. It started transmitting signals in 2019 [15]. To acquire the latest M-code signal, this satellite is selected as the signal source. Satellite orbit data provided by the International GNSS Service (IGS) global monitoring network are used to control the high-gain antenna to maintain continuous tracking and signal locking on the dynamic satellite signal.

The optimal detector at the GPS signal receiving end samples the received GPS signal after matching the filter at the receiving end to make a judgment. Taking a BPSK signal as an example, the input signal $s(t)$ is defined as

$$ s(t) = A \times \sum_{n=-\infty}^{\infty} a_n \mu(t - nT_b), $$

where $a_n$ is a pseudorandom noise (PRN) sequence with values of ±1; $\mu(t)$ is the modulation pulse of the signal; $T_b$ is the chip period; $n(t)$ is additive Gaussian white noise with variance $\delta_n^2$, and $A$ is the amplitude of the received signal. The impulse response of the matched filter is

$$ h(t) = s(T_b - t). $$

The output $y(t)$ after passing through the matched filter is

$$ y(t) = \int_{0}^{T_b} [s(t) + n(t)]h(t - \tau)d\tau = \int_{0}^{T_b} [s(\tau) + n(\tau)]s(T_b - t + \tau)d\tau. $$

(8)

$y(t)$ is sampled with a sampling interval $T_b$,

$$ y(T_b) = \int_{0}^{T_b} [s(\tau) + n(\tau)]s(\tau)d\tau = E_b + Z, $$

(9)

where $E_b$ is the bit energy, and $Z$ is the noise energy. $y(T_b)$ obeys a Gaussian distribution with mean $E_b$ and variance $\delta_n^2$. The bit error rate (BER) of the signal is

$$ p_e = \frac{1}{2} \text{erfc} \left( \sqrt{\frac{E_b}{\delta_n^2}} \right). $$

(10)

The carrier-to-noise ratio is often used as a measure of signal quality in satellite communication systems. It is independent of the noise bandwidth of the receiver, thus allowing a more intuitive comparison of the performance of different receivers. With this concept, the BER can be written as

$$ p_e = \frac{1}{2} \text{erfc} \left( \sqrt{\frac{C}{N_0 \times R_c}} \right). $$

(11)

Figure 5 shows that the higher the code rate of the PRN code is, the greater the carrier-to-noise ratio that is needed to reach the same level of chip error rate (CER). This is because the higher the code rate is, the less energy is available for estimation, which reduces the CER. In the worst case of the carrier-to-noise ratio, the CER reaches 50% because only random guesses can be made on the PRN code. To guarantee the correct verdict for a code sequence, it is necessary to ensure that the CER is better than 10% so that the carrier-to-noise ratio is greater than 59 dB Hz for L1 C/A signals and greater than 69 dB Hz for P(Y) signals [16].

Considering the effect of noise on M-code sequence identification, the receiver antenna needs to have a significant signal gain to ensure that the M-code sequence is not obscured by noise. Under the conditions that the temperature is 290K, and the receiver bandwidth is 20 MHz, the noise power $N$ within this bandwidth is

$$ N = kTB_N = 1.38 \times 10^{-23} \times 290 \times 20 \times 10^6 = -131(\text{dBW}), $$

(12)

where $k$ is the Boltzmann constant; $T$ is the noise temperature, and $B_N$ is the noise bandwidth. Based on the minimum received power of -158 dBW when the M code reaches the ground, the ambient thermal noise is higher than the M-code signal by 27 dB [17]. At the same time, no spreading gain can be obtained through correlation if the M code cannot be generated locally. Therefore, a high gain of the
antenna system is needed to improve the signal-to-noise ratio of the received signal. In this study, the high-gain antenna system has a 37 dB gain and a low-noise amplifier with a 50 dB gain, which is sufficient to separate the GPS signal from the noise. Table 1 shows the characteristics of GPS III L1 signal components, including signal modulation, minimum received power, signal multiplexing mode, chipping rate, and other parameters. It can be seen that there are M-code signals on both signal channels.

The GPS signal is sampled at a sampling rate of 125 MHz after downconversion. Since the receiver cannot generate a replica of the M code, it cannot carry out M-code signal acquisition and tracking by searching for the code in two dimensions [18]. However, the M-code signal is broadcast with a C/A-code signal and a P(Y)-code signal in the L1 and L2 bands, respectively; accordingly, it has the same Doppler offset as the accompanying signal in the same band. Thus, M-code acquisition can be achieved with the help of

---

**Figure 2:** Spectra of the GPS L1 signals. The L1-band signal contains three kinds of signals: C/A-code, P(Y)-code, and M-code signals. These signals use different types of modulation. The bandwidth of the M code reaches 30 MHz, which is larger than the 20 MHz bandwidth of the P code.

**Figure 3:** Autocorrelation functions for different signals. The autocorrelation functions of BPSK signals and BOC signals with different code rates are compared.
Figure 4: M-code autocorrelation function at different bandwidths.

Figure 5: CERs for BPSK signals at different code rates. Differently colored curves represent the CERs for different code rates.

Table 1: GPS III L1 signal components.

<table>
<thead>
<tr>
<th>Component</th>
<th>Modulation</th>
<th>Chipping rate (MHz)</th>
<th>Phase I/Q</th>
<th>Minimum received power (dBW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>L1C data</td>
<td>BOC (1, 1)</td>
<td>1.023</td>
<td>I</td>
<td>-163.0</td>
</tr>
<tr>
<td>L1C pilot</td>
<td>TMBOC (6, 1, 4/33)</td>
<td>1.023</td>
<td>I</td>
<td>-158.25</td>
</tr>
<tr>
<td>C/A</td>
<td>BPSK (1)</td>
<td>1.023</td>
<td>Q</td>
<td>-158.5</td>
</tr>
<tr>
<td>P(Y)</td>
<td>BPSK (10)</td>
<td>10.23</td>
<td>I</td>
<td>-161.5</td>
</tr>
<tr>
<td>M</td>
<td>BOC (10, 5)</td>
<td>5.115</td>
<td>I and Q</td>
<td>-158</td>
</tr>
</tbody>
</table>
the C/A code. The M-code signal is moved to the baseband together with the other signals. Then, the auxiliary signal is filtered out in accordance with the different characteristics of the M-code signal and other signals in different signal taps to obtain the baseband M-code sequence. The complete signal recording and processing process is shown in Figure 6.

Figures 7 and 8 show the results of the acquisition and tracking using the GPS software receiver. The results show that the receiver successfully acquired the signal, and the tracking loop runs normally; the navigation message is demodulated, and the baseband satellite signal is obtained.

4. L1-Band GPS Signal Analysis

To improve spectrum utilization, GPS adopts quadrature modulation to modulate the signals in the in-phase and quadrature channels separately. In addition, GPS satellites generate pseudorandom sequences with the asymmetric rise and fall times of the code elements, which is considered one of the primary sources of positioning errors. To overcome the problem of digital distortion, the GPS Block IIF and GPS Block IIR satellites adopt coherent adaptive subcarrier modulation (CASM), which splits the multiple signals on the carrier in either the time or phase domain such that the synthesized signals have constant envelope characteristics. In the Block III satellites, the P(Y)-code signals are combined with the L1CP and L1CD signals in the in-phase channel using weighted voting modulation. Analysis of the spectrograms of the in-phase and quadrature channels shows that in the L1 band, the M code is modulated together with the C/A code in the quadrature channel, whereas the M code is modulated together with the P code in the in-phase channel. In the in-phase channel, two narrow peaks appear in the signal at the center frequency of the spectrum, which can be distinguished as the L1C signal with BOC (1, 1) modulation. The M-code signal with BOC (10, 5) modulation appears at a distance of 10 MHz from the center frequency. The M-code signal and the C/A-code signal in the quadrature channel can also be observed at the center frequency.

Figures 9 and 10 show the spectrum of the in-phase and quadrature channel of the GPS L1 band received by the high gain antenna, respectively.
In the following, the M-code sequences will be identified from the in-phase (I) channel and the quadrature channel individually. In the I channel, the P(Y)-code and M-code signals are linearly combined; the P(Y) code is modulated by BPSK (10) with a code rate of 10.23 MHz, and the M-code signal is modulated by BOC (10, 5), so the spreading code rate is 5.115 MHz, and the length of each chip period is $4T_s$. Each spreading code chip contains four subcarriers. After subcarrier modulation, the square-wave rate becomes $20.46$ MHz, corresponding to two M-code chips within the

Figure 8: Tracking and demodulation of navigation messages. This figure contains the delay-locked loop (DLL) and phase-locked loop (PLL) parameters and shows that the signal loop gradually converges.

Figure 9: Spectrogram of the SV4 in-phase channel. The waveform in the middle represents the C/A code, and the waveforms on both sides represent the M code.
width of one P-code chip. The P-code and M-code signals are linearly superimposed and modulated to the same phase channel, and the signal \( S_I(t) \) is expressed as follows:

\[
S_I(t) = \sqrt{P_P} d_P(t) c_P(t) + \sqrt{P_M} d_M(t) c_M(t) + n(t).
\]

(13)

Here, \( P_P \) and \( P_M \) denote the signal power levels of the P(Y)-code and M-code signals, respectively, in the I channel. \( d_P(t) \) and \( d_M(t) \) are the modulated navigation data. \( c_P(t) \) is the PRN sequence of the P-code signal. \( c_M(t) \) is the square-wave signal obtained by multiplying the PRN sequence of the M-code signal by the square-wave subcarrier. \( f_c \) is the carrier frequency of the GPS satellite signal; \( \theta \) is the carrier phase, and \( n(t) \) is Gaussian white noise. Under the assumptions that the amplitude of the P-code signal is 1 and the amplitude ratio of the M-code signal to the P-code signal is \( m \), the linear combination of the baseband signals of the P-code and M-code signals can be expressed as

\[
S_I(t) = S_P(t) \pm m \cdot S_M(t) + n(t).
\]

(14)

When the P-code is 1, the corresponding M code can be \((1, -1)\) or \((-1, 1)\); when the P code is -1, the corresponding M code can be \((-1, 1)\) or \((1, -1)\). Thus, there are four possible cases for the amplitude of the superimposed code: \(\{1, m(-1, 1)\}, \{1, m(1, -1)\}, \{-1, m(1, -1)\}, \{-1, m(-1, 1)\}\). Figure 11 shows the time domain waveform of the L1 signal.

Table 1 shows that the M-code signal reaches the ground with a minimum power of -158 dBW, whereas the minimum
received power of the P-code signal at the ground is -161.5 dBW, meaning that the power of the M-code signal is greater than that of the P-code signal. Theoretically, it should be 2.24 times the P-code power. In a histogram of the received signal levels from Figures 12 and 13, it can be seen that the ratio between the maximum- and minimum-level amplitudes is approximately 4:1; from this, it is possible to calculate that the actual amplitude ratio, $m$ between the M-code and P-code signals is approximately 1.66. The amplitude relationship between the P-code and M-code signals can be used for the blind identification of the M-code signal.

5. Implementation and Testing

A GPS software-defined receiver is used for signal acquisition and tracking. Figures 6 and 7 show that the signal from GPS PRN4 is acquired successfully, and that the code-tracking loop and the carrier-tracking loop converge. The signal can be used to properly demodulate the navigation message. Figure 14 shows the algorithm of blind M-code estimation.

Each chip period $T_p$ of the Q-channel baseband signal contains a combination of P-code chips and M-code chips. In accordance with the relationship between the sampling rate and the P-code rate and the numerical size of the sampling point, the position of the starting point of the code can be found. Then, the sampled data are chunked in accordance with the P-code and M-code sampling rates. In this paper, the sampling rate of the GPS PRN4 satellite signal is 125 MHz; the P-code chipping rate is 10.23 MHz, and the M-code chipping rate is equivalent to 20 MHz; thus, every 12 sampling points correspond to one P-code chip, and every six sampling points correspond to one M-code chip.

The analysis of four cases shows that two M-code chips corresponding to the value of a sampling point must have opposite (positive and negative) signs. If the first M-code chip corresponding to the value of the sampling point is negative, this means that the P code and M code take values of $\{1, m(-1, 1)\}$ and $\{-1, m(-1, 1)\}$. Then, the absolute values of the first M-code chip and the second M-code chip should be compared. If the absolute value of the first chip is smaller than that of the second one, this means that the P

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{I_channel_signal_histogram}
\caption{Histogram of I-channel signals. The amplitude ratio of the I-channel signal component can be visualized from the histogram. The horizontal band represents the level of the superimposed I-channel signal, and the vertical band represents the frequency of the level.}
\end{figure}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{Q_channel_signal_histogram}
\caption{Histogram of Q-channel signals. The amplitude ratio of the Q channel signal component can be visualized from the histogram. The horizontal band represents the level of the superimposed Q-channel signal, and the vertical band represents the frequency of the level.}
\end{figure}
The code takes a value of 1, and the two M codes take values of \((-1, 1)\). The same is true for the case in which the first M-code chip has a negative value. Therefore, the M-code and P-code values can be identified simultaneously by using the different positive and negative signs of the corresponding sampling points due to the power of the P code and M code. The identified M-code and P-code signals are shown in Figure 15.

To verify whether the separated P-code and M-code signals are correct, the waveform distribution is used to check the code sequence. The obtained P-code and M-code sequences are superimposed in accordance with the power ratio \(m = 1.6\) and compared with the original sampled Q-channel signal to observe whether the signal waveforms are consistent with the original signal. From the results for the time-domain waveform of the original signal and the signal waveform of the recovered signal after superposition in accordance with the power ratio, it is seen that the signal waveform matches. Figure 16 shows the waveforms of the original signal and the recovered signal.

At the same time, the M-code signal is modulated in both the I and Q channels, so the M-code sequence recovered from the Q-channel can also be used to perform...
Figure 16: Raw signal and recovered signal. The extracted code sequences are superimposed in proportion to the original power and compared with the original waveform to verify correct extraction.

Figure 17: Cross-correlation function for the M-code and I-channel signal.
Figure 18: I-channel signal and identified signal. The horizontal coordinate indicates the number of code pieces of M code. The identified M-code waveform is aligned with the I branch signal and then compared, and the M code corresponds well to the waveform of the I channel signal.

Figure 19: M-code and C/A-code signals recovered from the raw signal. Since the M and C/A codes have different code rates, one C/A code will correspond to multiple M-code chips.
correlation operations with the signal from the I channel. If there is a correlation peak, the M-code sequence recovered from the Q-channel is consistent with the M-code sequence in the I channel, indicating that the recovered sequence is correct. The correlation peaks are shown in Figure 17.

In the I-channel, the M code and C/A code are modulated together in a linear combination; however, the two pseudorandom codes correspond to different code rates, so the blind M-code identification algorithm above cannot be applied in this situation. It can be seen from the figure that the frequencies occupied by the C/A-code and M-code signals are different; therefore, a filtering method can be considered to filter the C/A code, and then, the sign function can be applied to achieve blind identification of the M-code sequence. The expression for the Q-channel signal is

\[
S_Q(t) = \sqrt{P_{CA}d_{CA}(t)c_{CA}(t)} \cos(2\pi f_c t + \theta) + \sqrt{P_{M}d_{M}(t)c_{M}(t)} \cos(2\pi f_c t + \theta') + n(t),
\]

where \( P_{CA} \) is the C/A-code power in the quadrature channel; \( d_{CA}(t) \) is the navigation message; \( c_{CA}(t) \) is the C/A-code sequence, and \( \theta \) and \( \theta' \) denote the initial phases of the C/A code and M code, respectively. Blind estimation of the M-code sequence in the orthogonal branch also requires capturing and tracking the C/A-code signal to remove the Doppler frequency in order to obtain the baseband signal. The baseband signal is passed through a bandpass filter with a passband frequency designed to filter out the C/A code signal; then, the filtered signal from the same-phase branch no longer contains the C/A code signal at the frequency of 1.023 MHz. Finally, the sign of the filtered signal is taken. Blind identification of the M-code sequence can be realized by applying the sign function to the filtered signal. Through this filtering method, the C/A code signal can be obtained simultaneously with the M-code sequence so that the local C/A code can be used to check the M-code sequence. A comparison of the time domain waveforms of the identified signal and the I-channel signal is shown in Figure 18.

It can be seen from Figures 19 and 20 that the C/A-code signal extracted via the filtering method is the same as the local C/A-code signal generated in accordance with IS-GPS-200J, indicating that the C/A-code and M-code signals have been successfully separated.

6. Conclusion

This paper has presented a method for the blind estimation of M-code sequences based on the amplitudes of different signal components and spectral distribution characteristics. A ground-based high-gain antenna receives the GPS III satellite signal as the data source. After downsampling, the M-code signal is captured with the aid of the C/A-code signal to obtain the offset of carrier frequency and code phase. The blind identification of M-code sequences requires different approaches depending on the signal components. For the Q channel, the P-code and M-code signals are separated chips by chips using the waveform matching technique. In the I channel, the two signals are separated by means of a filtering method using the different spectral distributions of
the M-code and C/A-code signals. The results show that the blind estimation of M-code sequences under noncooperative conditions is achieved. This paper provides a new idea for the study of noncooperative signals in GNSS systems. Authorized sequences extracted from GPS signals can be used to study and conduct performance assessments under the condition that the encryption algorithm is unknown.

In future work, the internal characteristics of the identified M-code sequences can be further studied, and the possibility of using M-code signals for localization under noncooperative conditions can be considered.

Data Availability

The GPS SV4 signal data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

Acknowledgments

This study is supported by the Navigation Center of the National University of Defense Technology. The research and publication of this article were funded by the Graduate Training Program of the National University of Defense Technology.

References


