APPLICATIONS OF GOLAY COMPLEMENTARY SEQUENCES IN MC-CDMA AND COMPRESSED SENSING

by

Xiao Bian

A Thesis

Presented to Lakehead University

in Partial Fulfillment of the Requirement for the Degree of

Master of Science

in

Electrical and Computer Engineering

Thunder Bay, Ontario, Canada

April 27, 2012

Abstract

This thesis consists of two separate topics involved with Golay complementary sequences. In the first part, we present results of an experimental investigation where the distribution of peak-to-average power ratio (PAPR) in downlink MC-CDMA systems is modeled by the generalized extreme value (GEV) distribution. Two orthogonal sets of sequences, Walsh-Hadamard and Golay complementary sequences, are used in spreading processes in the system. Then the parameters of the GEV distribution are estimated for the PAPR distribution. Through intensive numerical results, it is shown that the GEV distribution is an accurate model of the PAPR distribution of MC-CDMA systems. Also, the statistically estimated GEV distribution parameters for the PAPR reveal that when the number of subcarriers increases, the PAPR distributions converge to the Gumbel distribution.

In the second part of this thesis, a new (N, K) partial Fourier codebook is constructed, associated with a binary sequence obtained by an element-wise multiplication of a pair of binary Golay complementary sequences. In the codebook, $N = 2^m$ for a positive integer m, and K is approximately $\frac{N}{4}$. It is shown that the maximum magnitude of inner products between distinct code vectors is nontrivially bounded in the codebook, which is approximately up to $\sqrt{6}$ times the Welch bound equality for large $N = 2^m$ with odd m. Finally, the new codebook is employed as a deterministic sensing matrix for compressed sensing, where its recovery performance is tested through numerical experiments.

Acknowledgments

Hereby I would like to express my greatest gratitude to my supervisor Dr. Nam Yul Yu for his support and insightful guidance. I would like to thank my family for the love and support they provided during graduate school, and always. I also would like to thank the other members of my committee, Dr. Ruizhong Wei, Dr. Ali Manzak and Dr. Hassan Naser, for their words of wisdom and professional guidance.

Xiao Bian

Contents

7 Conclusions   **60**

List of Figures

List of Tables

List of Acronyms

M − PSK	–	M- phase-shift keying.
OFDM	–	Orthogonal frequency division multiplexing.
CDMA	–	Code division multiple access.
MC − CDMA	–	Multi-carrier CDMA.
CDF	–	Cumulative distribution function.
CCDF	–	Complementary cumulative distribution function.
WHS	–	Walsh-Hadamard sequences.
GCS	–	Golay complementary sequences.
EVT	–	Extreme value theory.
GEV	–	Generalized extreme value theory.
MLE	–	Maximum likelihood estimation.
IDFT	–	Inverse discrete Fourier transform.
FFT	–	Fast Fourier transform.
IFFT	–	Inverse fast Fourier transform.
StRIP	–	Statistical restricted isometry property.
OMP	–	Orthogonal matching pursuit.
MGCS	–	Multiplied Golay complementary sequences.

Part I

Modeling PAPR of MC-CDMA by Generalized Extreme Value Distribution

Chapter 1

Introduction I

Multicarrier code-division multiple access (MC-CDMA) [1] is a technique that combines the advantage of orthogonal frequency division multiplexing (OFDM) and code-division multiple access (CDMA) to offer its ability to combat against frequency-selective multipath fading and to utilize spectrum resource efficiently. However, the high peak-to-average power ratio (PAPR) inherited from OFDM requires stringent linearity specifications of the power amplifier and limits its applications. Therefore, many researches have been targeted on the PAPR reduction in MC-CDMA systems, e.g., [2]-[4].

Recently, studies in [5] and [6] derived PAPR upper bounds for MC-CDMA system employing Reed-Muller codes [7] and Golay complementary sequences [8], respectively. From a statistical point of view, the theoretical upper bound of PAPR is intrinsically a rare event, and as the number of carriers and users increases, the probability of the occurrence of the theoretically highest PAPR becomes negligible. On the other hand, it turned out that a statistical distribution which allows a more accurate and comprehensive characterization of the PAPR of multicarrier communications [9]. In [10], the extreme value theory (EVT) of Chi-square random processes was first employed to derive the peak-to-mean envelope power ratio (PMEPR) distribution of OFDM signals. Then, a general and accurate expression of the distribution of PAPR in OFDM systems with unequal power allocation to different subcarriers was presented in [11].

1.1 Motivations

Lately, [12] and [13] proposed numerical approximations of the PAPR distribution in MC-CDMA systems, utilizing Gaussian and Gamma distributions, respectively. Motivated by these previous works, we adopt a statistical approach to characterize the PAPR distribution of downlink MC-CDMA systems where new statistical models are employed. Since the MC-CDMA is essentially a pseudo-random coded OFDM system, it is simple logic that we extend the utilizing of the EVT family distributions for modeling PAPR of the MC-CDMA. The generalized extreme value (GEV) distribution is a powerful and robust model for studying the tail behavior of a distribution, which is the scenario for modeling the distribution of the PAPR. By extracting the three parameters of GEV distribution, we shall observe the trends of the PAPR distribution with different system configurations. Moreover, by proposing the PAPR model based on the GEV parameters, we may predict the PAPR distribution with high accuracy for various system configurations to assist the hardware designs.

1.2 Contributions

In this part of the thesis, we first statistically model the PAPR distribution of downlink MC-CDMA systems with the GEV distribution. Then we compare the estimation results with different spreading sequences in the MC-CDMA systems, namely, Golay complementary and Walsh-Hadamard sequences. Through intensive numerical experiments, it is shown that the GEV distribution is an accurate model to characterize the PAPR distribution of MC-CDMA. Based on the observed parameters' behaviors, we provide sequence-specific mathematical equations for modeling for the PAPR distribution, where the only variable in the model is the number of subcarriers, N_{sc}. The high closeness between the estimated PAPR and numerical PAPR provide evidences of the validation of the modeling. Moreover, the statistically estimated GEV distribution parameters for the PAPR reveal that when the number of subcarriers increases, both PAPR distributions converge to the Gumbel distribution [14].

The contributions in this part of the thesis can be summarized as follows.

- The GEV distribution is utilized to statistically model the PAPR distribution of downlink MC-CDMA systems.

- The parameters' trends are estimated in the GEV modeling of PAPR based on numerical

experiments, for Golay complementary and Walsh-Hadamard sequences spreading MC-CDMA.

- Sequence-specific mathematical expressions are established from the observed GEV parameters' patterns for the PAPR distributions with the variable of N_{sc}.

- The trend of the PAPR distributions converging to the Gumbel distribution is observed for large N_{sc}.

Chapter 2

Backgrounds I

2.1 M-PSK modulation scheme

A digital modulation scheme maps a binary sequence to a signal for transmission over a communication channel. The M- phase-shift keying (MPSK) is a memoryless digital modulation scheme. Specifically, it maps each k bits in the binary sequence into one of the M signal waveforms $s_m(t)$, $1 \leq m \leq M$, where $M = 2^k$, regardless of the previous mapped signals. In the digital phase modulation, the M signal waveform are represented as [15]

$$
\begin{aligned}
s_m(t) &= \mathrm{Re}[g(t)e^{j\frac{2\pi(m-1)}{M}}e^{j2\pi f_c t}] \\
&= g(t)\cos\left(2\pi f_c t + \frac{2\pi(m-1)}{M}\right) \\
&= g(t)\cos\left(\frac{2\pi(m-1)}{M}\right)\cos 2\pi f_c t - g(t)\sin\left(\frac{2\pi(m-1)}{M}\right)\sin 2\pi f_c t \quad (2.1)
\end{aligned}
$$

where $g(t)$ is the signal pulse,

$$
g(t) = \begin{cases} 1 & 0 \leq t \leq T_s, \\ 0 & \text{otherwise.} \end{cases}
$$

with the signal pulse energy ξ_g and the signaling interval T_s. We note that $g(t)\cos 2\pi f_c$ and $-g(t)\sin 2\pi f_c$ are orthogonal, and therefore we can use two orthogonal basis,

$$
\begin{aligned}
\phi_1(t) &= \sqrt{\frac{2}{\xi_g}}g(t)\cos 2\pi f_c t \\
\phi_2(t) &= -\sqrt{\frac{2}{\xi_g}}g(t)\sin 2\pi f_c t
\end{aligned}
$$
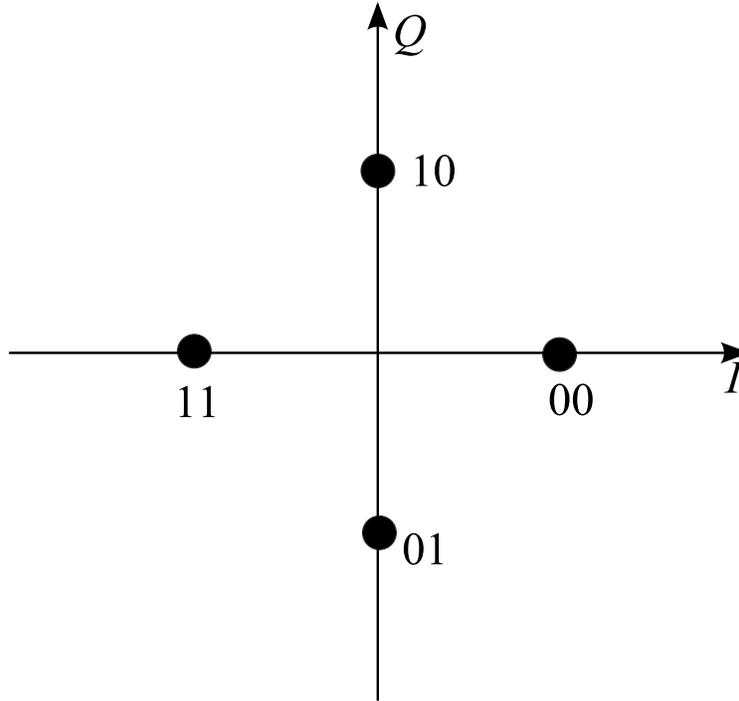
Figure 2.1: A QPSK constellation diagram.

to expand the signal $s_m(t)$, $1 \leq m \leq M$, as

$$s_m(t) = \sqrt{\frac{\xi_g}{2}} \cos\left(\frac{2\pi(m-1)}{M}\right) \phi_1(t) + \sqrt{\frac{\xi_g}{2}} \sin\left(\frac{2\pi(m-1)}{M}\right) \phi_2(t)$$

and the vector representations of $s_m(t)$ are [15]

$$\mathbf{s}_m = \left(\sqrt{\frac{\xi_g}{2}} \cos\left(\frac{2\pi(m-1)}{M}\right), \ \sqrt{\frac{\xi_g}{2}} \sin\left(\frac{2\pi(m-1)}{M}\right)\right) \quad m = 1, 2, \cdots, M. \qquad (2.2)$$

In this thesis, we modulate the user bits by the quadrature phase-shift keying signals (QPSK), where $M = 4$. The vector representations of each modulated signal take one of the values from $\{(\pm\sqrt{\xi_s}, 0), (0, \pm\sqrt{\xi_s})\}$, where $\xi_s = 1$ is the normalized symbol energy. The corresponding signal constellation is shown in Figure 2.1.

2.2 OFDM

Orthogonal frequency division multiplexing (OFDM) is a spectrally efficient parallel data transmission scheme. It transmits a single data stream over a number of low-rate subcarriers. The bandwidth of each subcarrier is much narrower than the system bandwidth, so each subcarrier experience only flat fading and robust against inter-symbol interference (ISI).

Therefore, the channel equalization is simplified. This robustness is very attractive in high speed data communications.

Historically, analogue OFDM design was first introduced in 1960s [16] [17]. In 1971 [18], discrete Fourier transform (DFT) version of OFDM was proposed for cost-effective implementations, and later in 1981 it was realized by fast Fourier transform (FFT) [19].

OFDM is the core component of many standards for communication systems, such as high-speed/asymmetric digital subscriber lines (HDSL/ADSL) for wired applications. In the 1990s, its wireless applications tended to focus on broadcast systems such as Digital Video Broadcasting (DVB) [20] and Digital Audio Broadcasting(DAB) [21], and relatively low-power system such as IEEE 802.11a [22]. Those applications benefit from the low complexity of the OFDM receiver, while not requiring a high-power transmitter in the consumer terminals [23]. This avoids one of the main disadvantages of OFDM, a much higher peak-to-average power ratio than that of single carrier systems, which needs stringent linearity specifications of the power amplifier and raise the cost of hardware implementation. Recently, it was in 3GPP Long Term Evolution (LTE) [24] that a cellular mobile communication standard is first based on OFDM. Since then, tremendous research and develop efforts enabled the OFDM to find its way into a mature and dominate modulation and multiple-access technique for modern telecommunications.

Figure 2.2 shows the typical block diagram of an OFDM system [25]. In each time interval T_s, the input modulated signal frame $[a_0, \ldots, a_{N-1}]$ is generated from N independent complex modulators and converted into N parallel data streams. Then each branch is carrier modulated with one of the N subcarriers. Finally, these sub-branch signals are added, in order to form a composite transmitted signal. Based on Figure 2.2, the baseband signal $s(t)$ is represented by

$$s(t) = \sum_{n=0}^{N-1} a_n e^{j2\pi n \cdot \Delta f t}, \quad 0 \le t \le T_s, \tag{2.3}$$

where T_s is an OFDM symbol duration, and $f_i = i \cdot \Delta f$, $0 \le i \le N - 1$ is the ith subcarrier frequency for $\Delta f = \frac{1}{T_s}$.
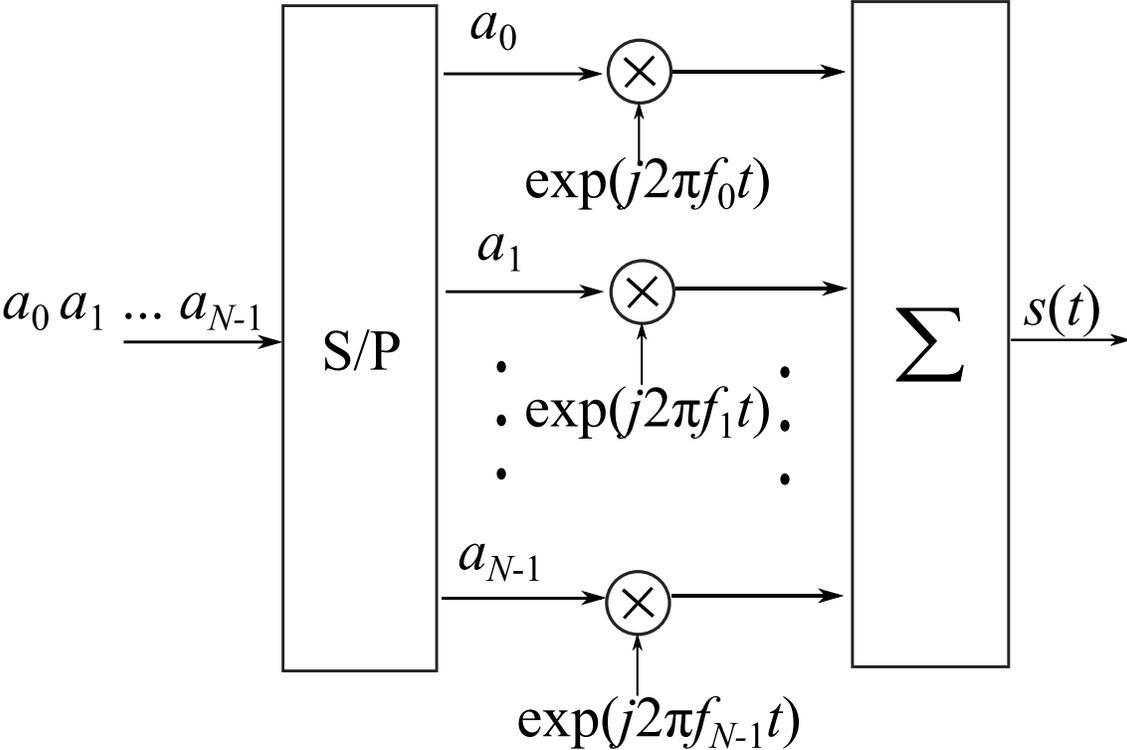
Figure 2.2: An OFDM transmitter block diagram.
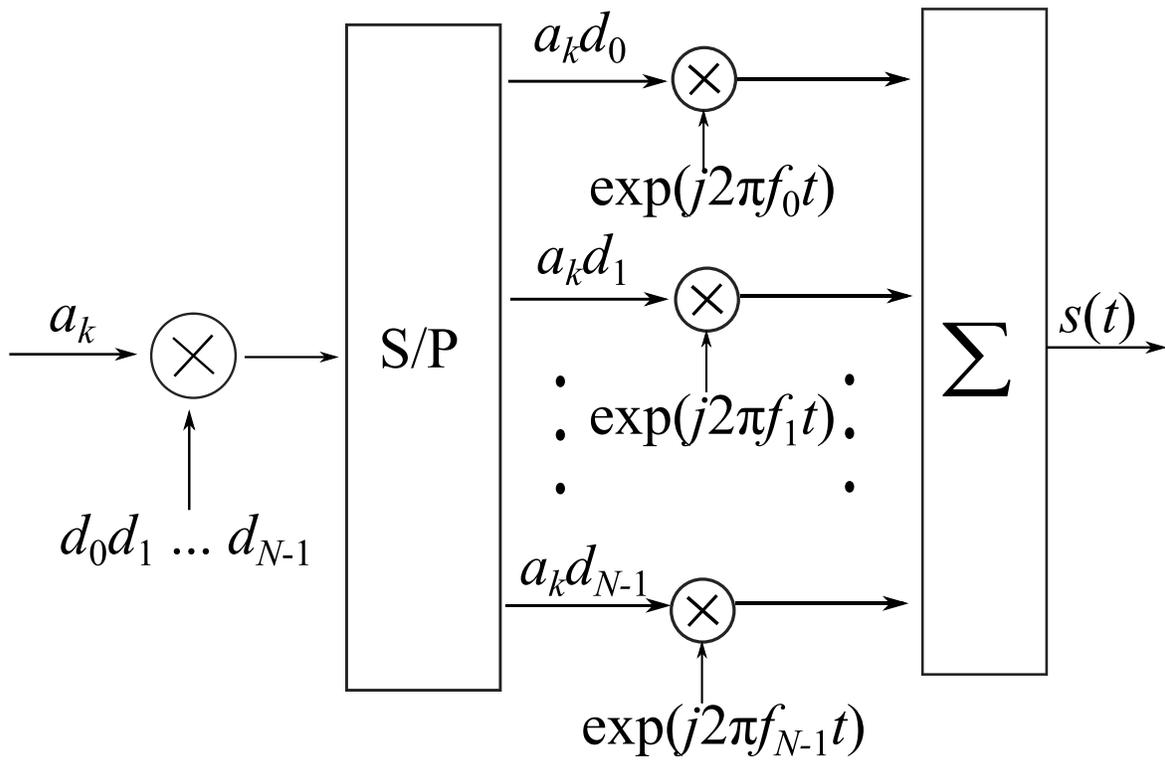
Figure 2.3: An MC-CDMA transmitter block diagram.

2.3 Multi-carrier CDMA

Multi-carrier code division multiple access (MC-CDMA) has been proposed as a promising multiple access scheme for the next generation mobile communications. It can be viewed as the combination of direct sequence (DS) CDMA and OFDM multiple access techniques. Generally, the combination can be categorized based on their signal-spreading models [25], Time (T)-domain spread MC-CDMA (MC-DS-CDMA) [26] - [28] and Frequency (F)-domain spread MC-CDMA [29] [30] [2]. The system we use here is F-domain spread MC-CDMA. More specifically, it uses orthogonal spreading sequences to spread the data in frequency domain before the subcarrier modulation process of OFDM. Because of using OFDM scheme, the MC-CDMA inevitably has some disadvantages as OFDM such as difficulty in subcarrier synchronization, sensitivity to frequency offset and high peak-to-average power ratio. However, this combination has major advantages that it can lower the symbol rate in each subcarrier so that a longer symbol duration makes it easier to quasi-synchronize the transmissions. Besides, the receiver can always employ all the received signal energy scattered in the frequency domain [1].

An MC-CDMA transmitter is shown in Figure 2.3, where we simplify the system to one user case. The user's kth data symbol a_k is first spread by a unique spreading sequences, $[d_0, d_1, \ldots, d_{N-1}]$. Then the spread signal $[a_k d_0, a_k d_1, \ldots, a_k d_{N-1}]$ is input to serial-to-parallel to continue the OFDM procedure. The baseband signal $s(t)$ for this simple MC-CDMA scheme is represented by

$$s(t) = \sum_{n=0}^{N-1} a_k d_n e^{j2\pi f_n t}, \quad 0 \leq t \leq T_s, \tag{2.4}$$

where T_s is an OFDM symbol duration and $f_i = i \cdot \Delta f$, $0 \leq i \leq N-1$ is the ith subcarrier frequency for $\Delta f = \frac{1}{T_s}$. For a general MC-CDMA transmitter diagram, please see Figure 3.1 in Chapter 3.

2.4 Peak-to-average power ratio (PAPR)

The peak-to-average power ratio (PAPR) is one measure of the high dynamic range of the signal waveforms [25]. The PAPR of a signal $s(t)$ in the interval of $0 \leq t \leq T_s$ is defined

as [31]

$$PAPR(s(t)) \triangleq \frac{\text{Peak power}}{\text{Average power}} = \frac{\max_{0 \le t \le T_s} |s(t)|^2}{E[|s(t)|^2]} = \frac{\max_{0 \le t \le T_s} |s(t)|^2}{\frac{1}{T_s} \int_0^{T_s} |s(t)|^2 dt} \qquad (2.5)$$

where $E[\cdot]$ denotes the ensemble average.

Example 1. Let $s(t) = \sin(t)$, according to the definition in (2.5) above, we can get

$$\max_{0 \le t \le 2\pi} |\sin(t)|^2 = 1.$$

Meanwhile,

$$\begin{aligned} E[|s(t)|^2] &= \frac{1}{2\pi} \int_0^{2\pi} |\sin(t)|^2 dt \\ &= \frac{1}{2\pi} \int_0^{2\pi} \frac{1 - \cos(2t)}{2} dt \\ &= \frac{1}{2}. \end{aligned}$$

Then,

$$PAPR(\sin(t)) = 3\,\text{dB}.$$

As mentioned in previous sections, one of the major drawbacks of OFDM and MC-CDMA systems is that the multi-carrier signals have potentially high PAPR with large number of subcarriers. As shown in (2.3) and (2.4), these multicarrier signals are essentially the sum of sinusoids. It is inevitable that the peaks of these sinusoids occur at the same time instance and cause large PAPR in the envelop of $s(t)$. When passed through a nonlinear device, such as a transmit power amplifier, the signal may suffer significant spectral spreading and in-band distortion [32].

There have been a large amount of research efforts to reduce the PAPR of a transmitted OFDM or MC-CDMA signal [33]. These techniques can be broadly categorized into three main concepts [23]: clipping and filtering [32] [34], selected mapping [35], and coding [2] [31].

From a statistical point of view, as the number of subcarriers and users increases, the probability of the occurrence of the theoretically highest PAPR becomes negligible [9]. Therefore, a statistical distribution which allows a more accurate and comprehensive characterization of the PAPR of OFDM and MC-CDMA has been taken into consideration. Several works on

theoretical approximations of the PAPR distribution of OFDM systems have been proposed [9]-[11]. In [10], the extreme value theory (EVT) of Chi-square random processes was first employed to derive the peak-to-mean envelope power ratio (PMEPR) distribution of OFDM signals. Then, a general and accurate expression of the distribution of PAPR in OFDM systems with unequal power allocation to different subcarriers was presented in [11]. To the best of our knowledge, the only works to date attempting to model the PAPR distribution in MC-CDMA system are [12] and [13], where Gaussian and Gamma distributions were respectively employed in their numerical approaches.

2.5 Complementary cumulative distribution function (CCDF)

Sometimes, it is useful to study how often the random variable is above a particular level. This is expressed as the tail distribution or the complementary cumulative distribution function (CCDF), defined as

$$\bar{F}(x) = P(X > x) = 1 - F(x).$$

It is clear that the CCDF curve gives us a more detailed focus on the upper tail of the distribution compared to the CDF (see Chapter 3). In the context of PAPR modeling, where the upper tail is more interesting, we adopt the CCDF to plot the PAPR curves in dB.

2.6 Spreading sequences

In the MC-CDMA, each user is assigned with a unique sequence to spread its data symbol in the frequency domain. Different user's spreading sequence should keep orthogonal to each other. If an MC-CDMA system is perfectly synchronized, the orthogonality allows for zero-correlation between the spreading codes and zero mutual interference among different user's data at the receiver side. In this section, we introduce two of the well-known classes of the orthogonal sequences, namely, Walsh-Hadamard sequences (WHS) and Golay complementary sequences (GCS). For detailed discussion on spreading sequences for MC-CDMA, we refer to [2] and [36].

An orthogonal set of WHS is generated by the Walsh-Hadamard matrix. A $2^m \times 2^m$ Walsh-Hadamard matrix is recursively constructed by

$$\mathbf{H}_{2^m} = \begin{bmatrix} \mathbf{H}_{2^{m-1}} & \mathbf{H}_{2^{m-1}} \\ \mathbf{H}_{2^{m-1}} & -\mathbf{H}_{2^{m-1}} \end{bmatrix}, \ \mathbf{H}_1 = [1].$$

Then, the WHS of length $N = 2^m$ are given by each row of the matrix $\mathbf{H}_{2^m}$, where a pair of rows are mutually orthogonal.

In a similar manner, an orthogonal set of GCS can be recursively obtained by

$$\mathbf{G}_{2^m} = \begin{bmatrix} \mathbf{G}_{2^{m-1}} & \overline{\mathbf{G}}_{2^{m-1}} \\ \mathbf{G}_{2^{m-1}} & -\overline{\mathbf{G}}_{2^{m-1}} \end{bmatrix}, \ \mathbf{G}_2 = \begin{bmatrix} +1 & +1 \\ +1 & -1 \end{bmatrix},$$

where $\overline{\mathbf{G}}_{2^{m-1}} = [\ \mathbf{A} \ \ -\mathbf{B} \ ]$ for $\mathbf{G}_{2^{m-1}} = [\ \mathbf{A} \ \ \mathbf{B} \ ]$ where $\mathbf{A}$ and $\mathbf{B}$ are $2^{m-1} \times 2^{m-2}$ submatrices [31]. Then, a pair of rows from matrix $\mathbf{G}_{2^m}$ are mutually orthogonal. The GCS of length $N = 2^m$ are given by each row of the matrix $\mathbf{G}_{2^m}$.

Example 2. $\mathbf{H}_8$ and $\mathbf{G}_8$ are recursively constructed as below.

$$\mathbf{H}_8 = \begin{bmatrix} +1 & +1 & +1 & +1 & +1 & +1 & +1 & +1 \\ +1 & -1 & +1 & -1 & +1 & -1 & +1 & -1 \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & -1 \\ +1 & -1 & -1 & +1 & +1 & -1 & -1 & +1 \\ +1 & +1 & +1 & +1 & -1 & -1 & -1 & -1 \\ +1 & -1 & +1 & -1 & -1 & +1 & -1 & +1 \\ +1 & +1 & -1 & -1 & -1 & -1 & +1 & +1 \\ +1 & -1 & -1 & +1 & -1 & +1 & +1 & -1 \end{bmatrix},$$

$$\mathbf{G}_8 = \begin{bmatrix} +1 & +1 & +1 & -1 & +1 & +1 & -1 & +1 \\ +1 & -1 & +1 & +1 & +1 & -1 & -1 & -1 \\ +1 & +1 & -1 & +1 & +1 & +1 & +1 & -1 \\ +1 & -1 & -1 & -1 & +1 & -1 & +1 & +1 \\ +1 & +1 & +1 & -1 & -1 & -1 & +1 & -1 \\ +1 & -1 & +1 & +1 & -1 & +1 & +1 & +1 \\ +1 & +1 & -1 & +1 & -1 & -1 & -1 & +1 \\ +1 & -1 & -1 & -1 & -1 & +1 & -1 & -1 \end{bmatrix}.$$

One can check that $\mathbf{H}_8 \cdot \mathbf{H}_8^T = 8 \cdot \mathbf{I}_8$ and $\mathbf{G}_8 \cdot \mathbf{G}_8^T = 8 \cdot \mathbf{I}_8$, where $\mathbf{I}_8$ is the 8×8 identity matrix. Hence, a pair of rows from each matrix are mutually orthogonal.

2.7 Generalized extreme value (GEV) distribution

2.7.1 The Fish-Tippett theorem

The extreme value theory (EVT) focuses on the statistics of rare events, e.g. the maximum value of samples. The main result of extreme value theory is called the Fisher-Tippett theorem [14], which states that the distribution of the maximum value in independent identically distribute (i.i.d.) samples, after shifted and scaled, tends to fall into one of the three families of distributions. Specifically, let M_n denote the maximum value of i.i.d. samples of size n. If there exist sequences a_n and b_n, such that the limit

$$F(x) = \lim_{n \to \infty} \Pr(\frac{M_n - b_n}{a_n} \leq x)$$

exists for all x, then this limit will be one of the following three forms

$$
\begin{aligned}
F_1(x) &= \exp(-\exp(-x)), & (2.6) \\
F_2(x) &= \begin{cases} 0, & \text{if } x \leq 0 \\ \exp(-x^{-\alpha}), & \text{if } x > 0 \end{cases} & (2.7) \\
F_3(x) &= \begin{cases} \exp(-(-x)^{-\alpha}), & \text{if } x \leq 0 \\ 1, & \text{if } x > 0 \end{cases} & (2.8)
\end{aligned}
$$

which are Gumbel, Fréchet and Weibull distributions [14], respectively, and $\alpha > 0$ is the tail index.

2.7.2 GEV distribution

The above three distributions can be unified into a single continuous one, known as the GEV distribution, which has the following cumulative distribution function (CDF)

$$G(x) = \exp\left\{ -\left[1 + \xi \left(\frac{x - \mu}{\sigma} \right) \right] \right\}^{-\frac{1}{\xi}}, \tag{2.9}$$

where ξ, σ, and μ are the shape, scale, and location parameters, respectively [37]. Note that if $\xi = 0$, (2.9) gives

$$G(x) = \exp\left[-\exp\left(-\frac{x - \mu}{\sigma} \right) \right], \tag{2.10}$$

which is the Gumbel distribution, or the type I extreme value distribution.

The probability density function (PDF) is, consequently

$$g(x) = \frac{1}{\sigma} \cdot \left[1 + \xi \left(\frac{x - \mu}{\sigma} \right) \right]^{-\frac{1}{\xi} - 1} \cdot \exp \left\{ - \left[1 + \xi \left(\frac{x - \mu}{\sigma} \right) \right] \right\}^{-\frac{1}{\xi}}. \tag{2.11}$$

Again, note that if $\xi = 0$, (2.11) gives

$$g(x) = \frac{1}{\sigma} \cdot \exp(-\frac{x - \mu}{\sigma}) \cdot \exp \left[- \exp \left(- \frac{x - \mu}{\sigma} \right) \right]. \tag{2.12}$$

Figure 2.4 shows the examples of probability density functions for the three basic forms of the generalized extreme value distribution, where $(\sigma, \mu)=(1, 0)$, ξ takes the values -0.5, 0 and 0.5, respectively.

2.8 Maximum likelihood estimation of GEV

2.8.1 Maximum likelihood estimation

In statistics, given a distribution model and a set of parameters, the corresponding CDF or PDF will show the probabilities of occurrence for certain data. In reality, however, it is often the case that we face a reversed problem: the model of distribution is known and we have observed samples and but we don't know the parameters of the distribution model. To solve this problem, we need find the parameters of the distribution model, i.e. PDF, that is most likely to produce the observed data. The procedure commonly used to estimate parameters is the maximum likelihood estimation (MLE).

Suppose there is an i.i.d sample of random variable X, x_1, x_2, $\cdots$, x_N of size N, coming from an unknown distribution function $f_0(x)$. However, we know that the function belongs to a certain family of distributions, e.g. $f(x|\theta), (\theta \in \Theta)$. So $f_0(x) = f(x|\theta_0)$. The value of θ_0 is unknown but referred to as the "true value" of the parameter. Note here θ can be a vector. The *joint density function* for all the observations, namely, x_1, x_2, $\cdots$, x_N, will be

$$f(x_1, x_2, \cdots x_N | \theta_0) = f(x_1|\theta_0) \cdot f(x_2|\theta_0) \cdots f(x_N|\theta_0). \tag{2.13}$$

By considering x_1, x_2, $\cdots$, x_N are "fixed parameters", whereas θ is a variable that can freely vary the function's value, we introduce the likelihood function, $L(\theta)$, defined as [38]

$$L(\theta) = f(x_1, x_2, \cdots x_N | \theta) = \prod_{i=1}^{N} f(x_i|\theta) \tag{2.14}$$
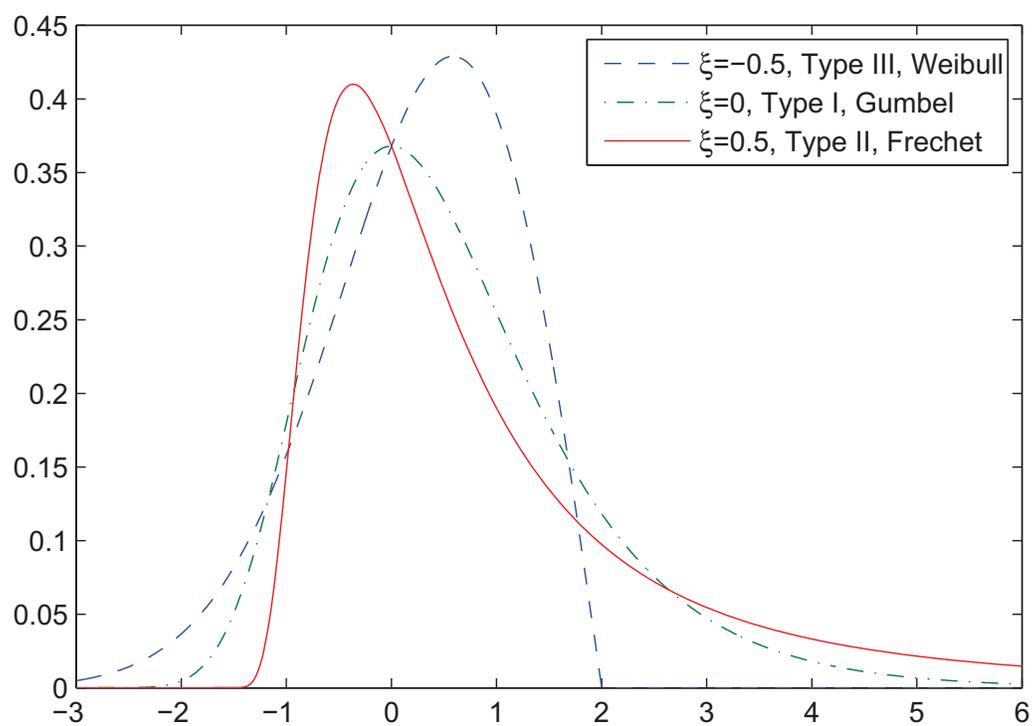
Figure 2.4: Probability density functions of GEV distribution, where $(\sigma, \mu)=(1, 0)$, ξ takes the values -0.5, 0 and 0.5.

The value $\hat{\theta}$ that maximizes the likelihood function is called the maximum likelihood estimator of θ_0. Because the logarithmic function $\ln x$ is a monotonically increasing function of x, maximizing $L(\theta)$ is equivalent to maximizing $\ln L(\theta)$, which is called the log-likelihood function. In practice, however, it is usually not possible to obtain an analytic form solution for the MLE estimation, especially when the model involves many parameters and its PDF is highly non-linear. In such situations, the MLE estimation must be solved numerically using nonlinear optimization algorithms [39]. This is the case for MLE in the GEV distribution as shown below.

2.8.2 Parameter estimation in GEV modeling

From (2.11) and (2.14), we may derive the log-likelihood function of the GEV distribution. Assume $\xi \neq 0$, let $u_i = 1 + \xi \left(\frac{x_i - \mu}{\sigma} \right)$, we have $\ln \left[L(\xi, \sigma, \mu) \right]$ as

$$
\begin{aligned}
\ln \left[L(\xi, \sigma, \mu | x_1, x_2, \cdots x_N) \right] &= \ln \left[\prod_{i=1}^{K} g(x_i) \right] \\
&= \ln \left[\prod_{i=1}^{N} \frac{1}{\sigma} \cdot (u_i)^{-\frac{1}{\xi}-1} \cdot \exp(-u_i^{-\frac{1}{\xi}}) \right] \\
&= -N \ln(\sigma) - (\frac{1}{\xi} + 1) \sum_{i=1}^{N} \ln(u_i) - \sum_{i=1}^{N} u_i^{-\frac{1}{\xi}}. \quad (2.15)
\end{aligned}
$$

When $\xi = 0$, the log-likelihood function will be

$$
\ln \left[L(\xi, \sigma, \mu | x_1, x_2, \cdots x_N) \right] = -N \ln(\sigma) - \sum_{i=1}^{N} \left[(\frac{x_i - \mu}{\sigma}) + \exp(\frac{x_i - \mu}{\sigma}) \right]. \quad (2.16)
$$

As previously mentioned, the log-likelihood function of the GEV distribution contains multiple parameters and hard to derive an analytic form for MLE. Thus, in the following chapters, we use numerical algorithm, specifically, function *gevfit* [40] in Matlab to search for the parameters ξ, σ, μ for the peak of the function (2.15) or (2.16) in Chapter 3.

Chapter 3

GEV Model of PAPR Distribution

3.1 System Model

A generalized downlink MC-CDMA system model is shown in Figure 3.1, where each of L users actively transmits K modulation symbols in an OFDM symbol. After a serial-to-parallel (S/P) conversion, the K modulated symbols $\mathbf{a}_l = [a_l^{(0)}, \ldots, a_l^{(K-1)}]$ of the lth user are spread by a user-specific sequence $\mathbf{d}_l = [d_l^{(0)}, \ldots, d_l^{(N-1)}]$ of length N, where $d_l^{(n)} \in \{+1, -1\}$. The spread data symbols of L users are added, and interleaved in the frequency domain to achieve frequency diversity. Then the $N \cdot K$ parallel data are input to IFFT of size $N \cdot K$ to generate an OFDM symbol. Finally, the baseband MC-CDMA signal $s(t)$ can be written as

$$s(t) = \sum_{k=0}^{K-1} \sum_{n=0}^{N-1} \sum_{l=0}^{L-1} a_l^{(k)} d_l^{(n)} e^{j2\pi(Kn+k)t/T_s}, \quad 0 \leq t \leq T_s,$$

where T_s is an OFDM symbol duration. The definition of the peak-to-average power ratio of $s(t)$ given by

$$PAPR(s(t)) = \frac{\max_{0 \leq t \leq T_s} |s(t)|^2}{E[|s(t)|^2]},$$

where $E[\cdot]$ denotes the ensemble average.
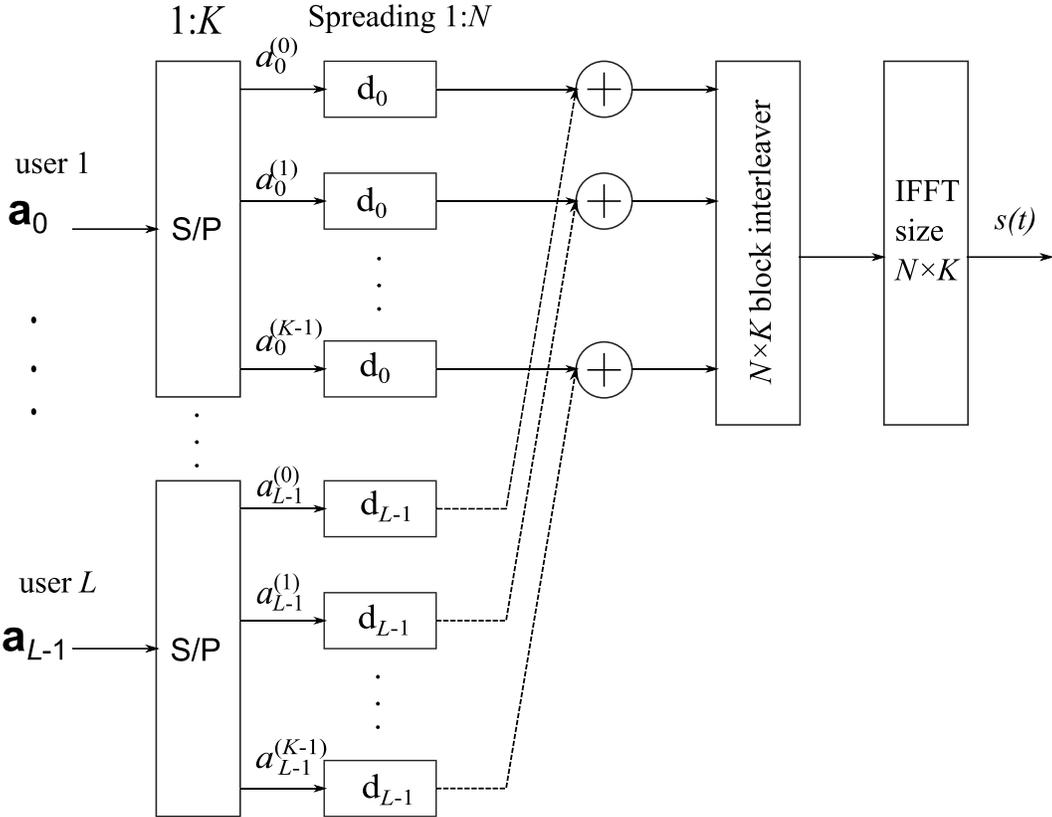
Figure 3.1: Downlink MC-CDMA transmitter.

3.2   GEV modeling results

In this section, we present experimental results for statistically modeling the PAPR distribution of MC-CDMA system where Monte Carlo method is used. For each spreading sequence of length $N = 2^m$, $5 \leq m \leq 12$, we tested the PAPR distribution of 10^5 OFDM symbols by generating random QPSK symbols for each user before the spreading scheme. We restricted our attention to a fully loaded MC-CDMA system, where the number of active users $L = N$.

In what follows, we first demonstrate that the GEV distribution may present a good model of PAPR of the MC-CDMA system. Then, we estimate the GEV parameters for various (N, K) pairs using maximum likelihood estimation (MLE) provided by *gevfit* function in Matlab. By exploiting the patterns of the empirical GEV parameters, an asymptotic GEV formula for the distribution model is proposed. Lastly, the comparison of numerical PAPR results and the estimated PAPR is given, demonstrating the proposed model favorably describes the PAPR distribution.

Figure 3.2 shows an example of complementary cumulative distribution function (CCDF) of a fully loaded MC-CDMA system. Using the MLE fitting, we estimate the GEV parameters of ξ, σ and μ in (2.9) from the empirical distribution and plot the GEV distribution with these parameters. We observe that the GEV CCDF curves almost overlap the original PAPR's CCDF, demonstrating they can accurately characterize the PAPR distribution. The idea we use the GEV distribution to fit the PAPR is inspired by [10] and [11]. However, due to the pseudo-random spreading before the IFFT scheme in MC-CDMA, the PAPR distributions should remain as a GEV style but may have different parameters than those of the OFDM.

To model the PAPR by the GEV distribution, we examine the PAPR distribution for various (N, K) pairs with given $N_{sc} = N \cdot K$, which is the number of subcarries. Then, we estimate the GEV parameters from each result in the same manner as in Figure 3.2. Figure 3.3 shows the trends of the GEV parameters as N_{sc} increases. In Figure 3.3(a), ξ approaches to 0, which implies the CDF of PAPR is close to the Gumbel distribution for large N_{sc}. This convergence verifies the assumption proposed in [10], which claimed the EVT can be employed to develop the CDF of the PMEPR in a coded OFDM signal. Figure 3.3(b) and 3.3(c) show the tendency of σ and μ as N_{sc} increases, respectively.
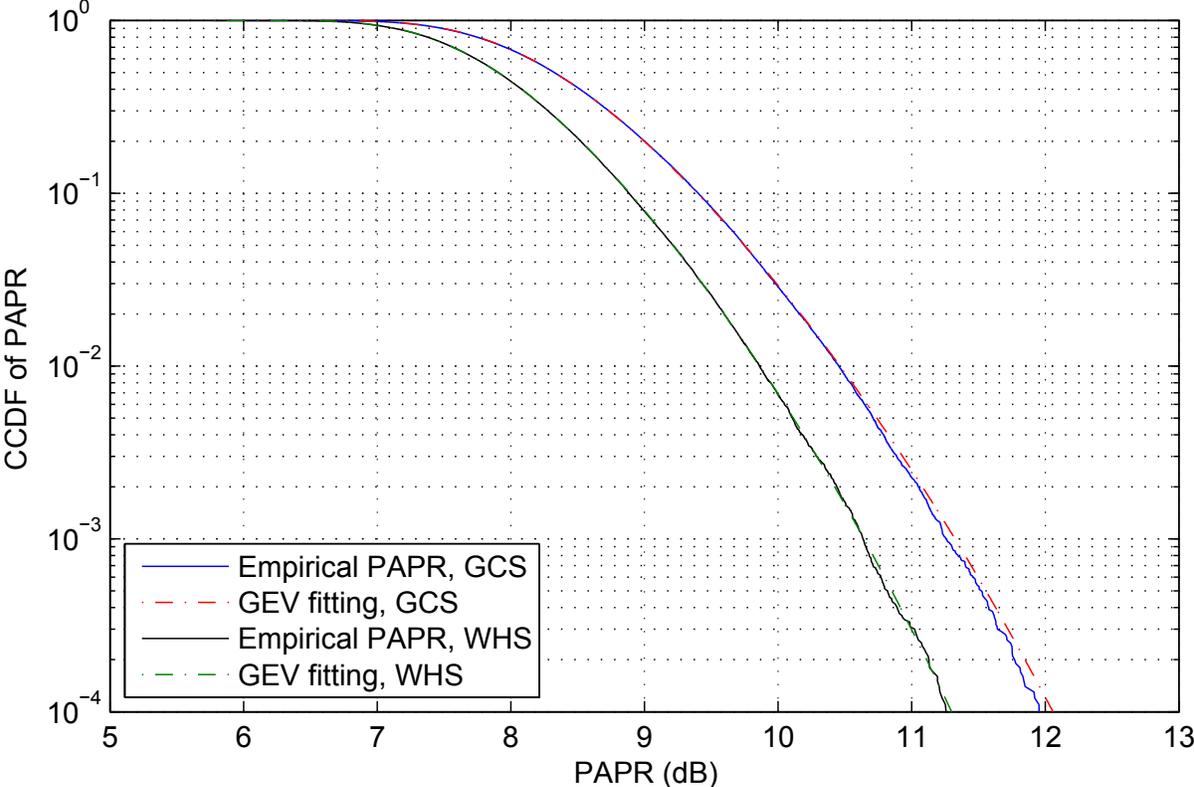
Figure 3.2: Empirical and GEV estimated PAPR distributions of a fully-loaded MC-CDMA, where N=256, L=256, K=1.
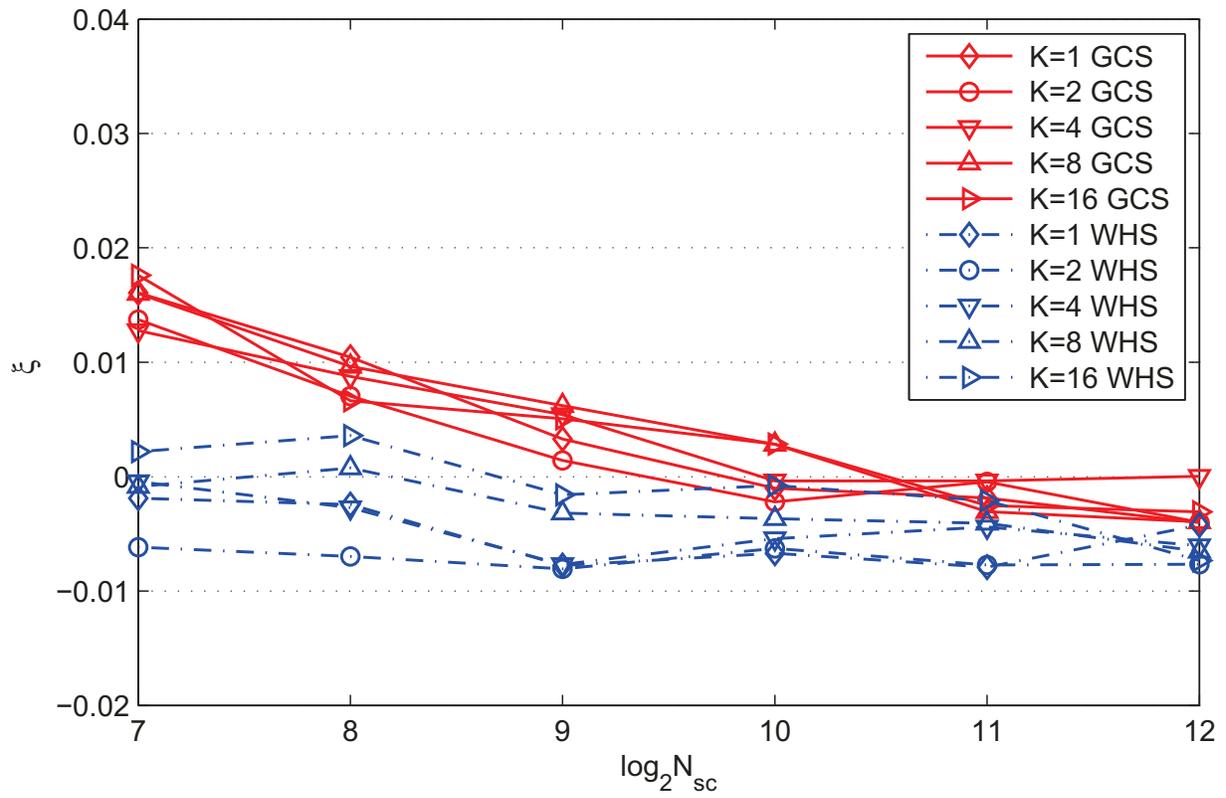
(a) ξ's trend

Figure 3.3: GEV parameters estimation in a fully loaded MC-CDMA system.

(b) σ's trend

Figure 3.3: GEV parameters estimation in a fully loaded MC-CDMA system.

(c) μ's trend
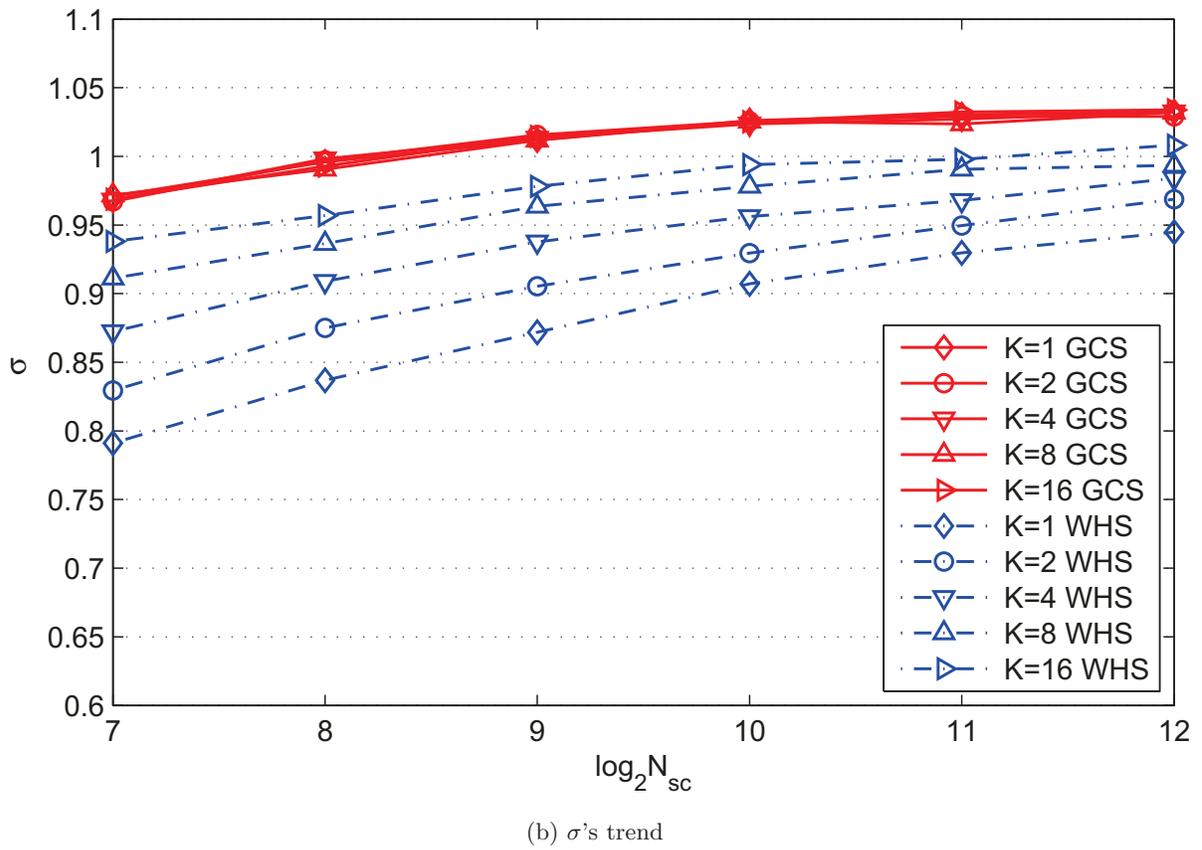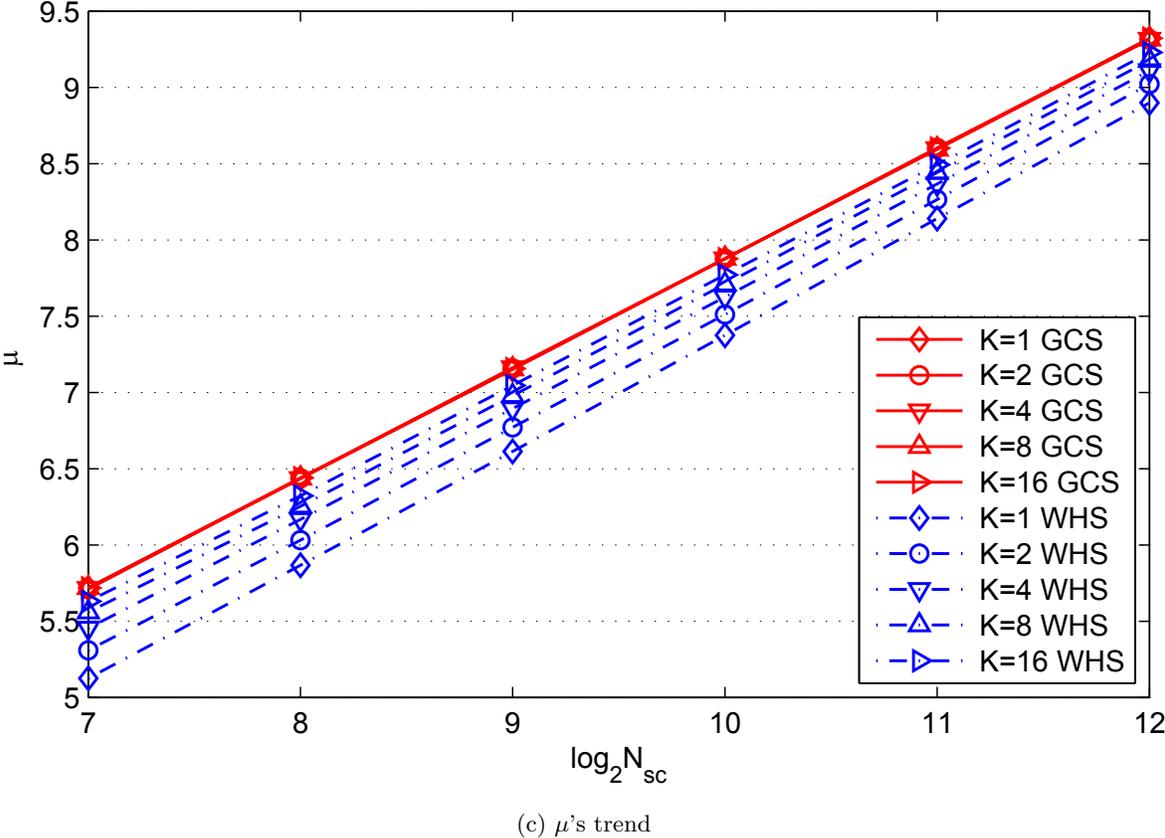
Figure 3.3: GEV parameters estimation in a fully loaded MC-CDMA system.

Note that each trend of the GEV distribution parameters has a similar pattern for various K. In particular, we observe that when the system is spread with GCS, the GEV parameters are overlapped for various (N, K) pairs, inferring the PAPR distributions are almost identical for the same number of subcarriers. On the other hand, when the system is spread with WHS, its PAPR will increase slightly by K as indicated by the trends in σ and μ.

Based on the aforementioned patterns of parameters from the GEV estimation, we propose a simple and asymptotic GEV model of the PAPR distribution for large N_{sc}. We assume $\xi = 0$, $\sigma = 1$ in both GCS and WHS cases. Then, we use linear functions of $\log_2 N_{sc}$ to represent μ, which is clear from Figure 3.3(c). We set $\mu_{GCS} = 0.717 \log_2 N_{sc} + 0.708$ and $\mu_{WHS} = 0.739 \log_2 N_{sc} - 0.014$ from $K = 1$ case, which shows good approximations to empirical results. To sum up, the proposed CCDF of PAPR is given as

$$Pr(PAPR \geq x) = \bar{F}(x) = 1 - \exp(-\exp(-x + \mu_s))$$

$$= \begin{cases} 1 - \exp(-\exp(-x + 0.717 \log_2 N_{sc} + 0.708), & \text{GCS spread} \\ 1 - \exp(-\exp(-x + 0.739 \log_2 N_{sc} - 0.014), & \text{WHS spread} \end{cases}$$

$$= \begin{cases} 1 - \exp(-e^{-x} \cdot 2.031 \cdot N_{sc}^{1.034}), & \text{GCS spread} \\ 1 - \exp(-e^{-x} \cdot 0.986 \cdot N_{sc}^{1.067}), & \text{WHS spread.} \end{cases} \quad (3.1)$$

For given x and N_{sc}, (3.1) implies that the overall PAPR in the WHS case is lower than the GCS case, which is confirmed by our numerical results. Figures 3.4 and 3.5 illustrate the CCDF of this model where N_{sc} equals to 256 and 1024, respectively. It is shown that the proposed model aligns well with the empirical CCDF curves, especially in GCS spread MC-CDMA. The GEV models are also compared to the EVT model for OFDM, given by equation (17) in [10], which gives a single estimation for coded OFDM, while (3.1) distinguishes the PAPR estimates for GCS and WHS. To further evaluate this model numerically, we compare the empirical 99.9% PAPR or $PAPR_0$ for which $Pr(PAPR > PAPR_0) = 10^{-3}$, and the estimated PAPR or $PAPR_e = \bar{F}^{-1}(10^{-3})$. In Table 3.1, the close agreement between the $PAPR_0$ and the $PAPR_e$ demonstrates that the GEV distribution can provide an accurate model for the PAPR distribution of MC-CDMA. Moreover, the table also demonstrates that when fully loaded, the WHS MC-CDMA shows better PAPR performance than the GCS MC-CDMA.
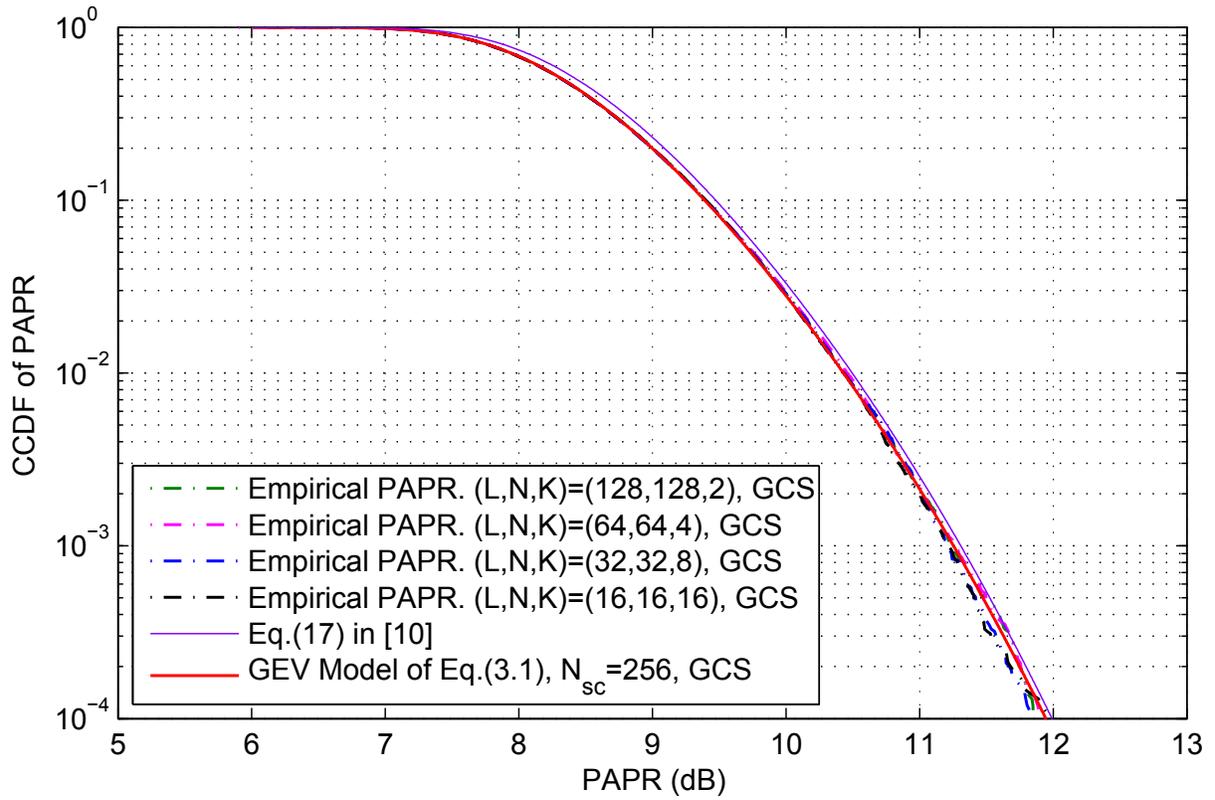
(a) GCS spreading

Figure 3.4: Comparison of the proposed GEV model and empirical PAPR distribution where $N_{sc} = 256$, $K = 2$, 4, 8 and 16.
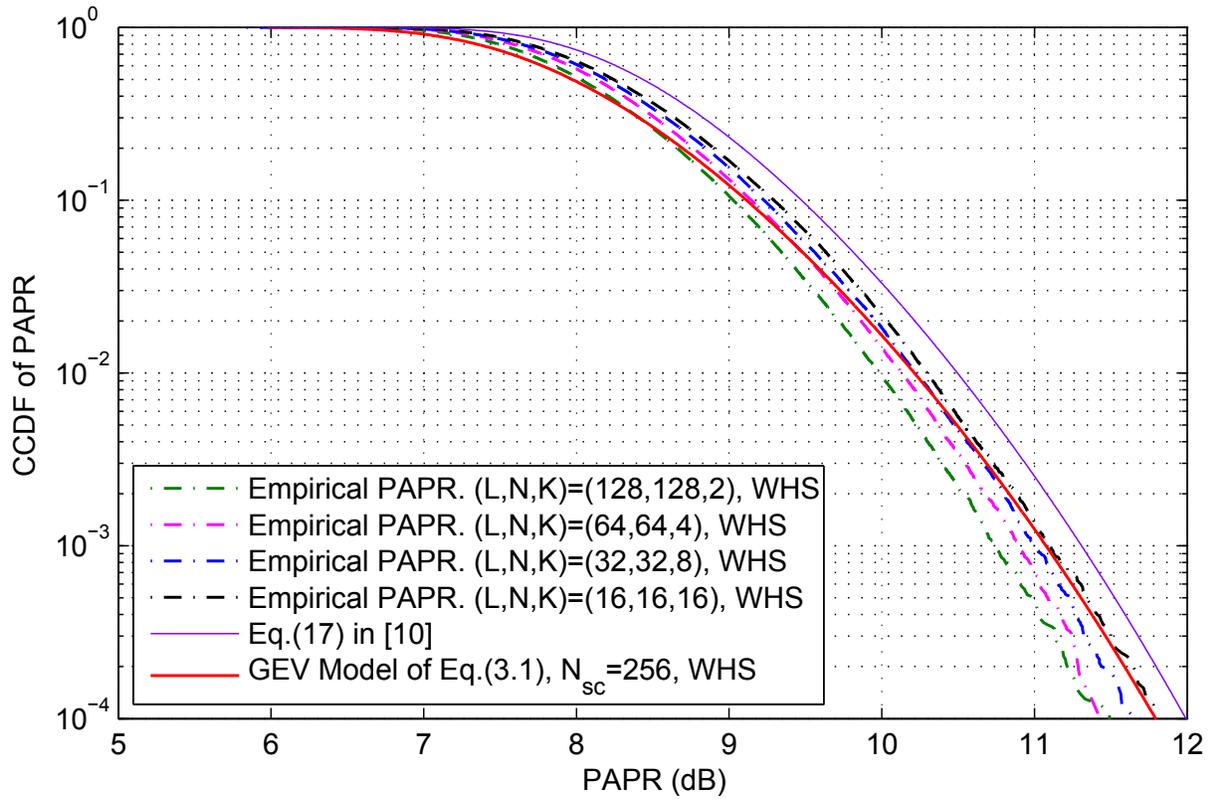
(b) WHS spreading

Figure 3.4: Comparison of the proposed GEV model and empirical PAPR distribution where $N_{sc} = 256$, $K = 2$, 4, 8 and 16.
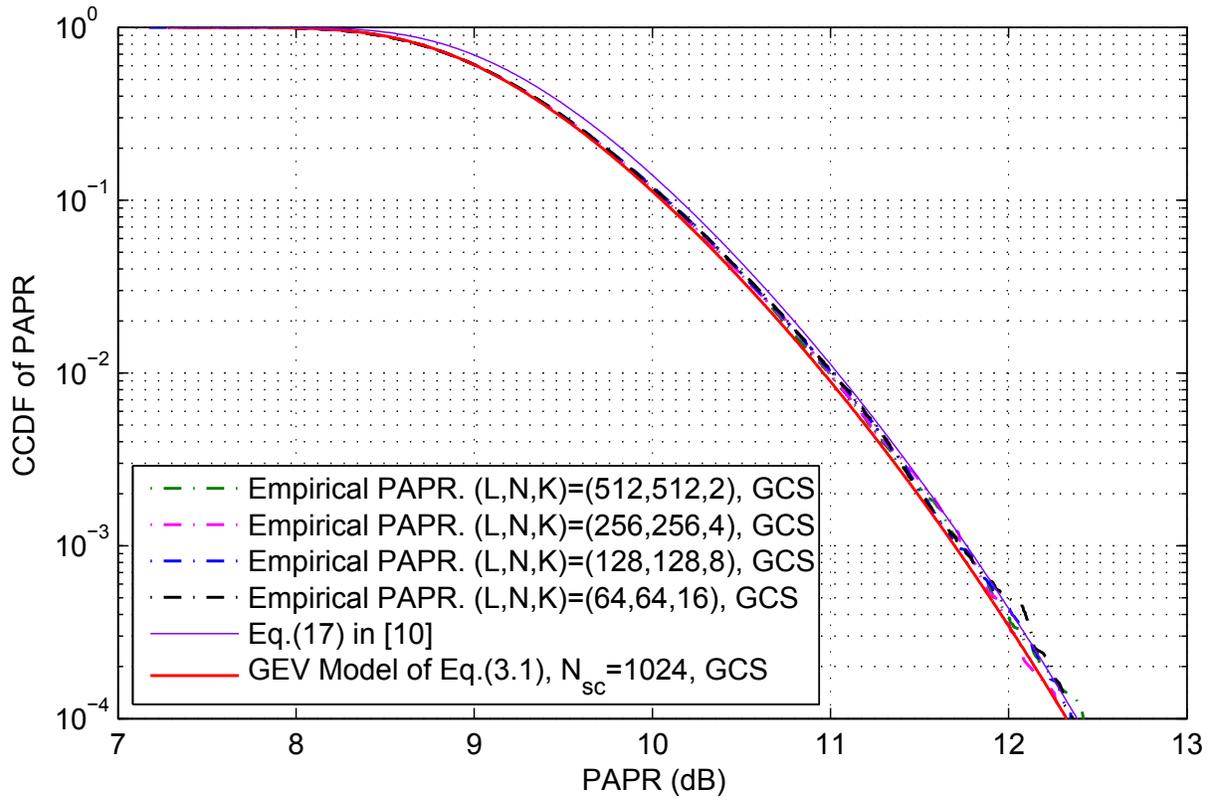
(a) GCS spreading

Figure 3.5: Comparison of the proposed GEV model and empirical PAPR distribution where $N_{sc} = 1024$, $K = 2, 4, 8$ and 16.

(b) WHS spreading
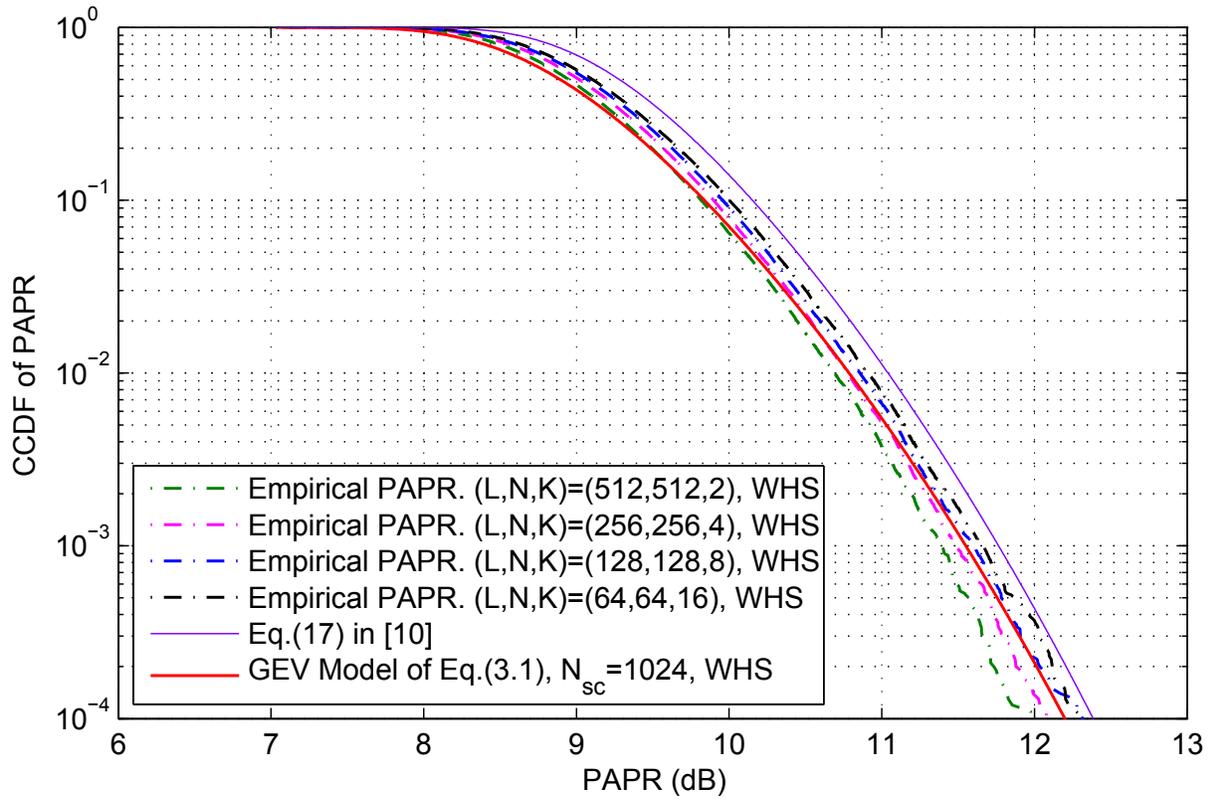
Figure 3.5: Comparison of the proposed GEV model and empirical PAPR distribution where $N_{sc} = 1024$, $K = 2$, 4, 8 and 16.

N_{sc}	$PAPR_0$					$PAPR_e$
	$K = 1$	$K = 2$	$K = 4$	$K = 8$	$K = 16$	
64	10.626	10.580	10.639	10.602	10.607	10.761
128	11.021	10.996	10.957	10.985	11.039	11.016
256	11.259	11.234	11.261	11.215	11.227	11.254
512	11.500	11.486	11.499	11.466	11.530	11.481
1024	11.694	11.741	11.751	11.706	11.734	11.697
2048	11.921	11.994	11.978	11.905	11.919	11.903
4096	12.129	12.168	12.179	12.163	12.182	12.099

(a) GCS spreading

N_{sc}	$PAPR_0$					$PAPR_e$
	$K = 1$	$K = 2$	$K = 4$	$K = 8$	$K = 16$	
64	9.708	9.939	10.082	10.287	10.425	10.543
128	10.205	10.364	10.519	10.648	10.787	10.817
256	10.637	10.740	10.891	11.000	11.105	11.076
512	10.956	11.101	11.222	11.297	11.367	11.319
1024	11.313	11.391	11.484	11.602	11.649	11.550
2048	11.605	11.664	11.791	11.786	11.835	11.769
4096	11.837	11.918	11.969	11.995	12.026	11.978

(b) WHS spreading

Table 3.1: Comparison of the empirical $PAPR_0$ and the estimated $PAPR_e$ in dB in a fully loaded MC-CDMA system.

Part II

Partial Fourier Codebooks Associated With Multiplied Golay Complementary Sequences For Compressed Sensing

Chapter 4

Introduction II

A complex $(N,\,K)$ codebook $\mathcal{C}$ is a set of N vectors in K-dimensional vector space. For its applications, we need a codebook $\mathcal{C}$ minimizing $I_{\max}(\mathcal{C})$ or the maximum magnitude of inner products between a pair of distinct code vectors. For instance, small $I_{\max}(\mathcal{C})$ guarantees low mutual interference in synchronous CDMA systems while a codebook $\mathcal{C}$ is used to provide N different *codes* for multiple users or channels [41]. Also a codebook $\mathcal{C}$ forms the *Grassmanian frame* with minimum achievable $I_{\max}(\mathcal{C})$ for the applications to multiple-input-multiple-output (MIMO) transmit beamforming [42]. Recently, compressed sensing [43] requires a measurement matrix with low *coherence* [44] that is defined as the maximum magnitude of inner products of the column vectors. Clearly, $(N,\,K)$ codebook $\mathcal{C}$ presents a $K \times N$ measurement matrix with low coherence, employing each code vector as a column of the matrix.

In particular, if $I_{\max}(\mathcal{C})$ meets the equality of the Welch bound [45], then $\mathcal{C}$ is called a *maximum-Welch-bound-equality (MWBE)* codebook. The MWBE codebook, also known as an *equiangular tight frame* [46], has been popular in a variety of research areas, e.g., communications, combinatorial designs, signal processing, and quantum computing.

Unfortunately, constructing the MWBE codebook in an analytic way is known to be extremely difficult [47]. Numerous attempts have been made to present a near-optimal codebook $\mathcal{C}$ where $I_{\max}(\mathcal{C})$ is very close to or slightly higher than the Welch bound equality. A number of construction examples based on codes and signal sets can be found in [47]. Ding and Feng also presented several near-optimal codebooks from almost difference sets [48][49].

4.1 Motivations

Recently, near-optimal partial Fourier and Hadamard codebooks associated with binary Sidelnikov sequences [50] have been presented in [51]. Besides, the author revealed that constructing a partial Fourier codebook $\mathcal{C}$ with low $I_{\max}(\mathcal{C})$ is equivalent to finding a binary sequence where the maximum magnitude of its N-point inverse discrete Fourier transform (IDFT) is as small as possible. In this sense, to find a near-optimal partial Fourier codebook with small $\frac{K}{N}$ ratio is also equivalent to find a binary sequence with small Hamming weight. Moreover, researches on deterministic compressed sensing matrix [52][53] raised requirement for constructing $K \times N$ near-optimal matrix where $K < \frac{N}{2}$. Inspired by this requirement, we are motivated to construct a new (N, K) partial Fourier codebook $\mathcal{C}$ associated with *multiplied* binary Golay complementary sequences. The new Fourier codebook can be directly used as a deterministic compressed sensing matrix, arranging each code vector as a column of the matrix. Note the idea behind this work is that we expect the multiplied binary Golay complementary sequences to inherit the low IDFT characters of the traditional Golay complementary sequences and additionally, their Hamming weights should be lower than those of the traditional Golay complementary sequences.

4.2 Contributions

In this part of the thesis, we first deliberately construct a new multiplied binary Golay complementary sequence. Specifically, for a pair of Golay complementary sequences $\mathbf{a}$ and $\mathbf{b}$ of length N, a multiplied Golay complementary sequence $\mathbf{u}$ is simply given by an element-wise multiplication, so the Hamming weight of $\mathbf{u}$ should be lower than those of the regular Golay complementary sequences. Then associated with $\mathbf{u}$, certain rows are selected from the N-point IDFT matrix to construct the new partial Fourier codebook, where the set of the selected row indices is equivalent to the index set of nonzero entries of the binary sequence $\mathbf{u}$. Using the N-point IDFT of $\mathbf{u}$, we show that $I_{\max}(\mathcal{C})$ is nontrivially bounded or at most $\sqrt{6}$ times the Welch bound equality for large $N = 2^m$ when m is odd and $K = \frac{N}{4}$. The codebook of $N = 2^m$ will be of interest since it allows efficient FFT techniques in practice.

Then the (N, K) partial Fourier codebook $\mathcal{C}$ associated with multiplied binary Golay complementary sequences is applied as a $K \times N$ deterministic sensing matrix $\mathbf{A}$ in compressed sensing [43], where each column of the sensing matrix is a code vector from $\mathcal{C}$. We

then show that the sensing matrix has the *statistical restricted isometry property* (StRIP) [53]. Finally, numerical results demonstrate the new sensing matrices, together with the orthogonal matching pursuit (OMP) algorithm [54], empirically achieve reliable recovery performance for sparsity level of $\mathcal{O}(K/\log N)$ from noiseless measurements. Therefore, the partial Fourier codebooks associated with multiplied Golay complementary sequences may be good candidates for deterministic sensing matrices, allowing efficient FFT processing with favorable parameter $N = 2^m$ and providing reliable recovery performance.

The contributions in this part of the thesis can be highlighted as follows.

- A binary sequence $\mathbf{u}$ of length $N = 2^m$ is constructed by element-wise multiplication of two Golay complementary sequences. The upper bound of the N-point IDFT of $\mathbf{u}$ is then theoretically derived.

- A new (N, K) partial Fourier codebook $\mathcal{C}$ is constructed associated with sequence $\mathbf{u}$. The upper bound of $I_{\max}(\mathcal{C})$ is also derived.

- The N-point IDFT value for sequence $\mathbf{u}$ for $K = \frac{N}{4}$ is searched by computer cluster for large m, and the codebook $\mathcal{C}$ associated with these sequences are displayed in Table 6.1.

- The codebook $\mathcal{C}$ is applied in compressed sensing as the sensing matrix $\mathbf{A}$, and it is shown that the codebook has the StRIP property.

- Numerical tests of the sensing matrix $\mathbf{A}$ with OMP recovery algorithm are conducted. The reliable recovery performance of the sensing matrix is demonstrated.

Chapter 5

Backgrounds II

5.1 Boolean functions

Let $\mathbf{x} = (x_0, \cdots, x_{m-1})$ be a binary vector where $x_i \in \{0, 1\}$, $0 \leq i \leq m-1$. A Boolean function $f(\mathbf{x})$ [7] is defined by

$$f(\mathbf{x}) = f(x_0, \cdots, x_{m-1}) = \sum_{i=0}^{2^m-1} c_i \prod_{l=0}^{m-1} x_l^{i_l} \tag{5.1}$$

where $c_i \in \{0, 1\}$ and i_l is obtained by the binary representation of $i = \sum_{l=0}^{m-1} i_l 2^l$, $i_l \in \{0, 1\}$. Note that the addition in (5.1) is computed modulo-2. In (5.1), the order of the ith monomial with nonzero c_i is given by $\sum_{l=0}^{m-1} i_l$, and the highest order of the monomials with nonzero c_i is called the *degree* of the Boolean function f. The *associated* binary sequence of length 2^m is given by

$$\mathbf{f} = (f_0, \cdots, f_{2^m-1}), \text{ where } f_i = f(i_0, \cdots, i_{m-1}) \text{ for } i = \sum_{l=0}^{m-1} i_l 2^l. \tag{5.2}$$

In other words, the associated codeword $\mathbf{f}$ of length 2^m is obtained by the Boolean function f_i while i increases from 0 to $2^m - 1$.

5.2 Reed-Muller codes

The rth-order Reed-Muller code $\mathrm{RM}(r, m)$ is defined by a set of binary codewords of length 2^m where each codeword is generated by a Boolean function of degree at most r [7]. In other words, each codeword in $\mathrm{RM}(r, m)$ is the associated codeword of length 2^m in (5.2) where the Boolean function f has the degree of at most r.

Example 3. To construct RM(1, 3), we can write a Boolean function has the degree of 1 as

$$f(\mathbf{x}) = f(x_0, \cdots, x_{m-1}) = c_0 x_0 + c_1 x_1 + c_2 x_2 + e \tag{5.3}$$

If we fix $e = 0$ for simplicity, and $[c_0, c_1, c_2]$ can be picked as one row from 8 possible combinations, i.e.,

$$\mathbf{c} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}. \tag{5.4}$$

On the other hand, from (5.2), a binary codeword from RM(1, 3) is

$$\mathbf{f} = (f(0,0,0),\ f(1,0,0),\ f(0,1,0),\ f(1,1,0),\ f(0,0,1),\ f(1,0,1),\ f(0,1,1),\ f(1,1,1)). \tag{5.5}$$

We then define

$$\mathbf{x} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix},$$

where each column corresponding the $[x_0, x_1, x_2]$ in (5.5). Clearly, by (5.3), each possible binary codeword is simply a row in $\mathbf{c} \cdot \mathbf{x}$. Totally,

$$\mathbf{c} \cdot \mathbf{x} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix},$$

where each row is a binary codeword in RM(1, 3). In the same way, by setting $e = 1$ in (5.3), we can derive the other 8 codewords of RM(1, 3).

5.3 Golay complementary sequences

In section 2.6, we have employed the recursive construction of Golay complementary sequences of length $N = 2^m$. Here we present the direct construction, which is more comprehensive.

Theorem 1. *[55] Let $N = 2^m$ for a positive integer m. Consider a Boolean function of m variables*

$$f(x_0, \cdots, x_{m-1}) = \sum_{r=0}^{m-2} x_{\pi(r)} x_{\pi(r+1)} + \sum_{r=0}^{m-1} c_r x_r + e \tag{5.6}$$

where $c_r, e \in \{0, 1\}$ and π is a permutation in $\{0, 1, \cdots, m-1\}$. Associated with the Boolean function f, a standard-form binary Golay complementary sequence of length N is given by $\mathbf{a} = (a_0, \cdots, a_{2^m-1})$, where $a_i = f(i_0, \cdots, i_{m-1})$ for $i = \sum_{l=0}^{m-1} i_l 2^l$, where $i_l \in \{0, 1\}$.

Clearly, (5.6) produces total $\frac{m!}{2} \cdot 2^{m+1} = m! \cdot 2^m$ distinct Golay complementary sequences of length 2^m, each of which belongs to the second order Reed-Muller code RM(2, m).

Example 4. Let $m = 3$, $\pi = \{1, 0, 2\}$ and $e = 0$. According to (5.6), the Boolean function for the Golay complementary sequence can be expressed as

$$a(\mathbf{x}) = a(x_0, x_1, x_2) = x_1 x_0 + x_0 x_2 + c_0 x_0 + c_1 x_1 + c_2 x_2 + 0 \tag{5.7}$$

and the binary Golay complementary sequence is given by

$$\mathbf{a} = (a(0,0,0), a(1,0,0), a(0,1,0), a(1,1,0), a(0,0,1), a(1,0,1), a(0,1,1), a(1,1,1)) \tag{5.8}$$

Similar to the previous example, we can get 8 possible Golay complementary sequences by taking coefficients $[c_0, c_1, c_2]$ values through rows in (5.4). So, if $[c_0, c_1, c_2] = [0, 0, 0]$, then
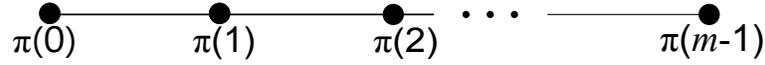
Figure 5.1: Graph structure of quadratic forms Q.

first row is $u_0 = [0, 0, 0, 1, 0, 1, 0, 0]$. Eventually, we have

$$
\begin{bmatrix}
u_0 \\
u_1 \\
u_2 \\
u_3 \\
u_4 \\
u_5 \\
u_6 \\
u_7
\end{bmatrix}
=
\begin{bmatrix}
0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 1
\end{bmatrix},
$$

where each row is a binary Golay complementary sequence. If we map these sequences into bipolar sequences, similar to Example 2, one can check a pair of rows from the matrix are mutually orthogonal.

5.4 Graph structure of quadratic forms

A quadratic form Q from a Boolean function of m variable x_0, x_1, $\cdots$, x_{m-1} is the sum of the second-order monomials. We can associate a graph $G(Q)$ on m vertices in the quadratic form Q, where each variable is depicted as a *vertex* and each monomial is depicted as an *edge*. In (5.6), we can depict the quadratic form $Q = \sum_{r=0}^{m-2} x_{\pi(r)} x_{\pi(r+1)}$ of a Golay complementary sequence as a *path* on m vertics in Figure 5.1.

5.5 Golay complementary set

With the concept of graph of a quadratic form, the Golay complementary set can be introduced.

Theorem 2. *[56] Suppose Q is a quadratic form in m variables. Suppose further that $G(Q)$ contains a set of $l \geq 0$ distinct vertices labelled j_1, j_2, $\cdots$, j_l with the property that deleting those l vertices and all their edges results in a path graph (necessarily on $m - l$ vertices).*

Let t be the label of either vertex of degree 1 in this path graph. Then for any choice of c, $c_k \in \{0, 1\}$

$$\left\{ Q + \sum_{k=0}^{m-1} c_k x_k + c + \sum_{k=1}^{l} d_k x_{j_k} + d x_t \mid d_k, d \in \{0, 1\} \right\} \tag{5.9}$$

is a Golay complementary set of size 2^{l+1}.

Example 5. [56] Let $m = 4$ and

$$Q = x_0 x_1 + x_0 x_2 + x_0 x_3 + x_1 x_1 + x_2 x_1 + x_2 x_3.$$

The graph $G(Q)$ is shown in Figure 5.2. We see that deleting the vertex labelled 0 and its edges results in a path graph on vertices 1, 2 and 3. Applying Theorem 2 with $l = 1$, we get, for each choice of c, $c_k \in \{0, 1\}$, the following Golay complementary set of size 4. Note here we choose $x_t = x_1$.

$$\left\{ \begin{array}{ll} Q + \sum_{k=0}^{3} c_k x_k + c, & (d_k = 0, \, d = 0) \\ Q + \sum_{k=0}^{3} c_k x_k + c + x_0, & (d_k = 1, \, d = 0) \\ Q + \sum_{k=0}^{3} c_k x_k + c + x_1, & (d_k = 0, \, d = 1) \\ Q + \sum_{k=0}^{3} c_k x_k + c + x_0 + x_1, & (d_k = 1, \, d = 1) \end{array} \right\}. \tag{5.10}$$

In other words, for given c, c_k, each one of the four Boolean functions in (5.10) is a Boolean function for a sequence lying in a Golay complementary set of size 4.

We denote the second-order Reed-Muller *coset* of $\mathrm{RM}(1, m)$ identified with quadratic form Q as "$Q + \mathrm{RM}(1, m)$". To put it another way, for a given quadratic form Q, this coset consists of all the Boolean functions with the form of $Q + \sum_{k=0}^{m-1} c_k x_k + c$, for c, $c_k \in \{0, 1\}$. We will use this interpretation in the following chapters. In Example 5, one can check that any $f \in Q + \mathrm{RM}(1, 4)$ is a Boolean function lying in (5.10) for certain c, c_k. Thus, f is Boolean function for a sequence lying in a Golay complementary set of size 4.

5.6 Codebooks and frames

Let $\mathbf{x} \in \mathbb{C}^K$ be a K-dimensional vector, i.e., $\mathbf{x} = (x_0, \cdots, x_{K-1})^T$ where $x_k \in \mathbb{C}$. Throughout this part of thesis, $\|\mathbf{x}\|$ denotes l_2-norm, i.e., $\|\mathbf{x}\| = \left(\sum_{k=0}^{K-1} |x_k|^2 \right)^{\frac{1}{2}}$. In particular, if $\|\mathbf{x}\| = 1$, then it is called a *unit-norm* vector.
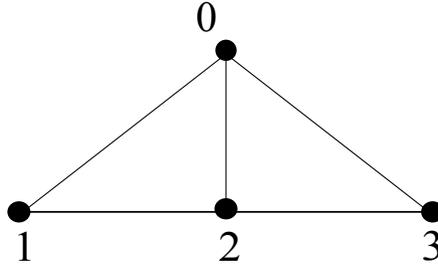
Figure 5.2: Graph structure of quadratic form $Q = x_0x_1 + x_0x_2 + x_0x_3 + x_1x_1 + x_2x_1 + x_2x_3$.

A complex (N, K) codebook $\mathcal{C} = \{\mathbf{c}_0, \ldots, \mathbf{c}_{N-1}\}$ is a set of N vectors in K-dimensional vector space, where $\mathbf{c}_l$, $0 \leq l \leq N - 1$, is a unit-norm $K \times 1$ code vector. The *Welch bound* [45] provides a well known lower bound on $I_{\max}(\mathcal{C})$, i.e.,

$$I_{\max}(\mathcal{C}) = \max_{0 \leq l \neq m \leq N-1} |\mathbf{c}_l^H \mathbf{c}_m| \geq \sqrt{\frac{N - K}{K(N - 1)}} \tag{5.11}$$

with equality if and only if for all pairs of (l, m) with $l \neq m$, $|\mathbf{c}_l^H \mathbf{c}_m| = \sqrt{\frac{N-K}{K(N-1)}}$, where $\mathbf{c}_l^H$ is the conjugate transpose of $\mathbf{c}_l$.

In frame theory, a complex (N, K) codebook $\mathcal{C}$ is equivalent to a *frame* [46] in $\mathbb{C}^K$, and the *coherence* [57] of the frame is equivalent to $I_{\max}(\mathcal{C})$. In particular, if $\|\mathcal{C}^H v\|^2 = \frac{N}{K}\|v\|^2$ for every vector $v \in \mathbb{C}^K$, then $\mathcal{C}$ is called a *tight frame* with *redundancy* $\frac{N}{K}$ [57].

5.7   Inverse discrete Fourier transform matrix

The N-point inverse discrete Fourier transform (IDFT) of an discrete signal $X(n)$ is defined by [58]:

$$x(k) = \sum_{n=0}^{N-1} e^{\frac{2\pi jkn}{N}} X(n), \quad k = 0, 1, \cdots, N - 1. \tag{5.12}$$

where $j = \sqrt{-1}$. Equivalently, the matrix form of IDFT can be written compactly as follows.

$$\mathbf{x} = \mathbf{A}_N \cdot \mathbf{X},$$

where $\mathbf{A}_N$ is the N-point IDFT matrix. The nth column of $\mathbf{A}_N$ is denoted as $\mathbf{a}_n$ and the kth row of $\mathbf{a}_n$, denoted as $\mathbf{a}_n(k)$, is $e^{\frac{2\pi jkn}{N}}$.

Example 6. The 4-point IDFT matrix $\mathbf{A}_4$ is shown below,

$$\mathbf{A}_4 = \begin{bmatrix} e^{j\frac{2\pi 0 \cdot 0}{4}} & e^{j\frac{2\pi 0 \cdot 1}{4}} & e^{j\frac{2\pi 0 \cdot 2}{4}} & e^{j\frac{2\pi 0 \cdot 3}{4}} \\ e^{j\frac{2\pi 1 \cdot 0}{4}} & e^{j\frac{2\pi 1 \cdot 1}{4}} & e^{j\frac{2\pi 1 \cdot 2}{4}} & e^{j\frac{2\pi 1 \cdot 3}{4}} \\ e^{j\frac{2\pi 2 \cdot 0}{4}} & e^{j\frac{2\pi 2 \cdot 1}{4}} & e^{j\frac{2\pi 2 \cdot 2}{4}} & e^{j\frac{2\pi 2 \cdot 3}{4}} \\ e^{j\frac{2\pi 3 \cdot 0}{4}} & e^{j\frac{2\pi 3 \cdot 1}{4}} & e^{j\frac{2\pi 3 \cdot 2}{4}} & e^{j\frac{2\pi 3 \cdot 3}{4}} \end{bmatrix}. \tag{5.13}$$

5.8 Partial Fourier codebooks associated with binary sequences

Let $D = \{d_0, \ldots, d_{K-1}\}$ be a set of K distinct integers, where $0 \leq d_k \leq N - 1$. Consider a $K \times N$ partial Fourier matrix selecting K rows from the N-point IDFT matrix, where the selected row indices are from D. With a scaling factor of $\frac{1}{\sqrt{K}}$, the l-th column vector of the partial Fourier matrix is given as

$$\mathbf{c}_l = \frac{1}{\sqrt{K}} \left(e^{j\frac{2\pi d_0 l}{N}}, \, e^{j\frac{2\pi d_1 l}{N}}, \, \ldots, \, e^{j\frac{2\pi d_{K-1} l}{N}} \right)^T, \quad 0 \leq l \leq N - 1. \tag{5.14}$$

Then $\mathcal{C} = (\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{N-1})$ is an (N, K) partial Fourier codebook. Associated with the partial Fourier codebook $\mathcal{C}$, we define a binary sequence $\mathbf{u} = (u_0, \ldots, u_{N-1})$ of length N and Hamming weight K, where

$$u_i = \begin{cases} 1, & \text{if } i \in D, \\ 0, & \text{if } i \notin D. \end{cases}$$

Example 7. Let $N = 8$, $\mathbf{u} = [01011011]$, then $K = 5$, $D = \{1, 3, 4, 6, 7\}$. The partial Fourier codebook $\mathcal{C}$ is constructed as below. We first present the 8-point IDFT matrix $\mathbf{A}_8$ aligned with the binary sequence $\mathbf{u}$,

$$\begin{bmatrix} 0 \\ \boxed{1} \\ 0 \\ \boxed{1} \\ \boxed{1} \\ 0 \\ \boxed{1} \\ \boxed{1} \end{bmatrix} \begin{bmatrix} e^{j\frac{2\pi 0 \cdot 0}{8}} & e^{j\frac{2\pi 0 \cdot 1}{8}} & e^{j\frac{2\pi 0 \cdot 2}{8}} & e^{j\frac{2\pi 0 \cdot 3}{8}} & e^{j\frac{2\pi 0 \cdot 4}{8}} & e^{j\frac{2\pi 0 \cdot 5}{8}} & e^{j\frac{2\pi 0 \cdot 6}{8}} & e^{j\frac{2\pi 0 \cdot 7}{8}} \\ \boxed{e^{j\frac{2\pi 1 \cdot 0}{8}} & e^{j\frac{2\pi 1 \cdot 1}{8}} & e^{j\frac{2\pi 1 \cdot 2}{8}} & e^{j\frac{2\pi 1 \cdot 3}{8}} & e^{j\frac{2\pi 1 \cdot 4}{8}} & e^{j\frac{2\pi 1 \cdot 5}{8}} & e^{j\frac{2\pi 1 \cdot 6}{8}} & e^{j\frac{2\pi 1 \cdot 7}{8}}} \\ e^{j\frac{2\pi 2 \cdot 0}{8}} & e^{j\frac{2\pi 2 \cdot 1}{8}} & e^{j\frac{2\pi 2 \cdot 2}{8}} & e^{j\frac{2\pi 2 \cdot 3}{8}} & e^{j\frac{2\pi 2 \cdot 4}{8}} & e^{j\frac{2\pi 2 \cdot 5}{8}} & e^{j\frac{2\pi 2 \cdot 6}{8}} & e^{j\frac{2\pi 2 \cdot 7}{8}} \\ \boxed{e^{j\frac{2\pi 3 \cdot 0}{8}} & e^{j\frac{2\pi 3 \cdot 1}{8}} & e^{j\frac{2\pi 3 \cdot 2}{8}} & e^{j\frac{2\pi 3 \cdot 3}{8}} & e^{j\frac{2\pi 3 \cdot 4}{8}} & e^{j\frac{2\pi 3 \cdot 5}{8}} & e^{j\frac{2\pi 3 \cdot 6}{8}} & e^{j\frac{2\pi 3 \cdot 7}{8}}} \\ \boxed{e^{j\frac{2\pi 4 \cdot 0}{8}} & e^{j\frac{2\pi 4 \cdot 1}{8}} & e^{j\frac{2\pi 4 \cdot 2}{8}} & e^{j\frac{2\pi 4 \cdot 3}{8}} & e^{j\frac{2\pi 4 \cdot 4}{8}} & e^{j\frac{2\pi 4 \cdot 5}{8}} & e^{j\frac{2\pi 4 \cdot 6}{8}} & e^{j\frac{2\pi 4 \cdot 7}{8}}} \\ e^{j\frac{2\pi 5 \cdot 0}{8}} & e^{j\frac{2\pi 5 \cdot 1}{8}} & e^{j\frac{2\pi 5 \cdot 2}{8}} & e^{j\frac{2\pi 5 \cdot 3}{8}} & e^{j\frac{2\pi 5 \cdot 4}{8}} & e^{j\frac{2\pi 5 \cdot 5}{8}} & e^{j\frac{2\pi 5 \cdot 6}{8}} & e^{j\frac{2\pi 5 \cdot 7}{8}} \\ \boxed{e^{j\frac{2\pi 6 \cdot 0}{8}} & e^{j\frac{2\pi 6 \cdot 1}{8}} & e^{j\frac{2\pi 6 \cdot 2}{8}} & e^{j\frac{2\pi 6 \cdot 3}{8}} & e^{j\frac{2\pi 6 \cdot 4}{8}} & e^{j\frac{2\pi 6 \cdot 5}{8}} & e^{j\frac{2\pi 6 \cdot 6}{8}} & e^{j\frac{2\pi 6 \cdot 7}{8}}} \\ \boxed{e^{j\frac{2\pi 7 \cdot 0}{8}} & e^{j\frac{2\pi 7 \cdot 1}{8}} & e^{j\frac{2\pi 7 \cdot 2}{8}} & e^{j\frac{2\pi 7 \cdot 3}{8}} & e^{j\frac{2\pi 7 \cdot 4}{8}} & e^{j\frac{2\pi 7 \cdot 5}{8}} & e^{j\frac{2\pi 7 \cdot 6}{8}} & e^{j\frac{2\pi 7 \cdot 7}{8}}} \end{bmatrix}.$$

Then, $\mathcal{C}$ is formed by picking the rows by index D in the matrix (highlighted in the boxes) and scaled by $\frac{1}{\sqrt{5}}$,

$$
\mathcal{C} = \frac{1}{\sqrt{5}} \cdot \begin{bmatrix}
e^{j\frac{2\pi 1 \cdot 0}{8}} & e^{j\frac{2\pi 1 \cdot 1}{8}} & e^{j\frac{2\pi 1 \cdot 2}{8}} & e^{j\frac{2\pi 1 \cdot 3}{8}} & e^{j\frac{2\pi 1 \cdot 4}{8}} & e^{j\frac{2\pi 1 \cdot 5}{8}} & e^{j\frac{2\pi 1 \cdot 6}{8}} & e^{j\frac{2\pi 1 \cdot 7}{8}} \\
e^{j\frac{2\pi 3 \cdot 0}{8}} & e^{j\frac{2\pi 3 \cdot 1}{8}} & e^{j\frac{2\pi 3 \cdot 2}{8}} & e^{j\frac{2\pi 3 \cdot 3}{8}} & e^{j\frac{2\pi 3 \cdot 4}{8}} & e^{j\frac{2\pi 3 \cdot 5}{8}} & e^{j\frac{2\pi 3 \cdot 6}{8}} & e^{j\frac{2\pi 3 \cdot 7}{8}} \\
e^{j\frac{2\pi 4 \cdot 0}{8}} & e^{j\frac{2\pi 4 \cdot 1}{8}} & e^{j\frac{2\pi 4 \cdot 2}{8}} & e^{j\frac{2\pi 4 \cdot 3}{8}} & e^{j\frac{2\pi 4 \cdot 4}{8}} & e^{j\frac{2\pi 4 \cdot 5}{8}} & e^{j\frac{2\pi 4 \cdot 6}{8}} & e^{j\frac{2\pi 4 \cdot 7}{8}} \\
e^{j\frac{2\pi 6 \cdot 0}{8}} & e^{j\frac{2\pi 6 \cdot 1}{8}} & e^{j\frac{2\pi 6 \cdot 2}{8}} & e^{j\frac{2\pi 6 \cdot 3}{8}} & e^{j\frac{2\pi 6 \cdot 4}{8}} & e^{j\frac{2\pi 6 \cdot 5}{8}} & e^{j\frac{2\pi 6 \cdot 6}{8}} & e^{j\frac{2\pi 6 \cdot 7}{8}} \\
e^{j\frac{2\pi 7 \cdot 0}{8}} & e^{j\frac{2\pi 7 \cdot 1}{8}} & e^{j\frac{2\pi 7 \cdot 2}{8}} & e^{j\frac{2\pi 7 \cdot 3}{8}} & e^{j\frac{2\pi 7 \cdot 4}{8}} & e^{j\frac{2\pi 7 \cdot 5}{8}} & e^{j\frac{2\pi 7 \cdot 6}{8}} & e^{j\frac{2\pi 7 \cdot 7}{8}}
\end{bmatrix}.
$$

We have the following observations on an $N \times K$ partial Fourier codebook $\mathcal{C}$. Note $\mathbf{c}_n(k)$ denotes the kth row, nth column element in $\mathcal{C}$.

- Each column has the unit-norm.

- The sum of each row is 0, as long as the first element in $\mathbf{u}$ is 0.

- Every distinct pair of rows in $\mathcal{C}$ is orthogonal. Specifically, $\mathcal{C}\mathcal{C}^H = \frac{N}{K}\mathbf{I}_N$, where $\mathbf{I}_N$ is the N-dimensional identity matrix. Moreover, $\mathcal{C}$ is a tight frame in $\mathbb{C}^K$ with redundancy $\frac{N}{K}$ [53].

- For any $n, n' \in \{1, \cdots, N\}$, there exists an $n'' \in \{1, \cdots, N\}$, such that $\mathbf{c}_n(k) \cdot \mathbf{c}_{n'}(k) = \frac{1}{\sqrt{K}}\mathbf{c}_{n''}(k)$, for $k = 1, \cdots, K$.

- For all $n \in \{1, \cdots, N\}$, there exists an $n' \in \{1, \cdots, N\}$, such that $\mathbf{c}_n(k) = \overline{\mathbf{c}_{n'}(k)}$, for $k = 1, \cdots, K$. Thus, the columns of $\mathcal{C}$ are closed under complex conjugation.

5.9   Compressed sensing with deterministic matrices

One of the most important foundations in digital revolution is the development and utilization of the sensing system that can translate nature informations into digital forms [59]. It is well known that original data can be exactly recovered from the samples taken at least at *Nyquist rate* or twice of the highest frequency of the signal. However, the data acquisition and processing of signals in applications such as medical imaging, remote surveillance, spectroscopy, astronomy, meteorology continue to pose a tremendous challenge because of the cost and physical limitation in the sensing systems.

To address these challenges, we depend on data compression, which aims for capturing the concise representation of the original signal and introduces acceptable distortion in the

data. One of the most popular techniques for signal compression is known as *transform coding*, and typically relies on finding a basis or frame that provides *sparse* or *compressible* representations for signals in a class of interest [59]. By sparse representation, we can represent the length N signal with $K \ll N$ nonzero coefficients. Both sparse and compressible signals can be represented with high fidelity by preserving only the values and locations of the largest coefficients of the signal. This process is called *sparse approximation*, and forms the foundation of transform coding schemes that exploit signal sparsity and compressibility, including the JPEG, JPEG2000, MPEG, and MP3 standards [59]. Since most of sampled data (not "information") of the signals will be discarded during the data compression process, one may ask, "Can we capture, or sample the original signal in a *compressed* manner, which combine the sampling and compressing together ?"

The compressed sensing [43] answered this question by establishing a new *framework* for data acquisition. In short, it is a novel technique of signal processing that can recover sparse signals of high dimension from few measurements. In practice, one of the imperative applications of compressed sensing is the magnetic resonance imaging (MRI), because the patient must hold still while an image is formed. Ordinary after-the-fact compression is no help in this respect, but compressive sensing offers hope of faster scanning without loss of resolution or contrast [60].

In compressed sensing, measuring an N-dimensional signal $\mathbf{x} \in \mathbb{R}^N$ with a $K \times N$ measurement matrix $\mathbf{A}$ produces a K-dimensional vector $\mathbf{y} = \mathbf{A}\mathbf{x}$, where $K < N$. In recovering $\mathbf{x}$ from $\mathbf{y}$, it seems impossible to solve K linear equations with N indeterminates by traditional linear algebra. However, imposing an additional requirement that $\mathbf{x}$ is s-sparse or the number of the nonzero entries in $\mathbf{x}$ is at most s, one can recover $\mathbf{x}$ exactly with high probability by l_1-minimization or greedy algorithms, which are computationally tractable.

The research efforts on compressed sensing revealed that a measurement matrix $\mathbf{A}$ plays a crucial role in sparse signal recovery. A typical choice of the matrix is a Gaussian or Bernoulli random matrix where the entries are generated by the Gaussian or Bernoulli process. Also, a partial Fourier random matrix is of particular interest, since it allows an efficient FFT algorithm in recovery of signals. However, such random matrices have the drawbacks of large storage, high complexity, and low efficiency in the implementation [53]. To overcome the

drawbacks, *deterministic* matrices have been studied in many literatures, where well known codes and sequences are employed to construct the sensing matrix, e.g., chirp sequences [61], Alltop sequences [62][63], Kerdock and Delsarte-Goethals codes [64][53], second order Reed-Muller codes [65], and dual BCH codes [66]. Other techniques for deterministic construction, based on finite fields, representation theory and additive characters, can be found in [67], [52] and [68].

5.10 Restrict isometry property and StRIP

The restricted isometry property (RIP) [69] of a compressed sensing matrix is an important necessary condition to guarantee the sparse signal recovery.

Definition 1. *[43] For each integer $s = 1, 2, \cdots$, define the isometry constant $\delta_s \in (0, 1)$ of a matrix $\mathbf{A}$ as the smallest number such that*

$$(1 - \delta_s) \|\mathbf{x}\| \leq \|\mathbf{A}\mathbf{x}\| \leq (1 + \delta_s) \|\mathbf{x}\| \tag{5.15}$$

holds for all s-sparse vectors $\mathbf{x}$.

A matrix $\mathbf{A}$ obeys the RIP of order s if δ_s is not too close to one [43]. When this property holds, $\mathbf{A}$ approximately preserves the Euclidean length of the s-sparse vector $\mathbf{x}$, which is necessary for reconstruction. The RIP can be interpreted in another perspective that all the subsets of s columns taken from $\mathbf{A}$ are in fact nearly orthonormal [43]. The RIP is a very restrictive condition and current known matrices that satisfying the RIP fall into 2 categories [70]: 1) A Gaussian or Bernoulli random matrix where the entries are generated by a probability distribution of the Gaussian or Bernoulli process. 2) Random partial Fourier matrix or Hadamard transform matrix obtained by choosing K rows uniformly from an $N \times N$ Fourier transform matrix or Hadamard transform matrix. Since it is impossible to test all the s-sparse vectors $\mathbf{x}$ for the deterministic sensing matrix $\mathbf{A}$ for the RIP, a statistical version of the RIP was formulated in [53]. Before we introduce the statistical restricted isometry property (StRIP), we need to introduce the concept of η-StRIP-able [53], the sufficient conditions for the StRIP.

Definition 2. *[53] A $K \times N$ matrix $\mathbf{A}$ is said to be η-StRIP-able, where $0 < \eta \leq 1$, if the following three conditions are satisfied.*

1). The rows of $\mathbf{A}$ are orthogonal, and all the row sums are zero.

2). For any $n, n' \in \{1, \cdots, N\}$, there exists an $n'' \in \{1, \cdots, N\}$, such that $\mathbf{a}_n(k) \cdot \mathbf{a}_{n'}(k) = \frac{1}{\sqrt{K}} \mathbf{a}_{n''}(k)$, for $k = 1, \cdots, K$.

3). For any $n \in \{2, \cdots, N\}$,

$$\left| \sum_k \mathbf{a}_n(k) \right|^2 \leq K^{1-\eta} \tag{5.16}$$

Remark 1. The third condition is a bound for the absolute value of the column sum of the matrix. For a partial Fourier matrix $\mathbf{A}$ that has the first column of $(\frac{1}{\sqrt{K}}, \frac{1}{\sqrt{K}}, \cdots, \frac{1}{\sqrt{K}})^T$, denoted as $\mathbf{a}_1$, one can check that

$$\left| \sum_k \mathbf{a}_n(k) \right| = \left| \sqrt{K} \mathbf{a}_1^H \mathbf{a}_n \right|.$$

Thus, the column sum is actually close related to the coherence of the partial Fourier matrix.

With the above conditions, the following theorem is presented.

Theorem 3. *[53] Suppose the $K \times N$ matrix $\mathbf{A}$ is η-StRIP-able, and suppose $s < 1 + (N-1)\epsilon$ and $\eta > \frac{1}{2}$. Then there exists a constant c such that, if $K \geq (\frac{cs \log N}{\epsilon^2})^{\frac{1}{\eta}}$, then $\mathbf{A}$ has the statistical restricted isometry property (StRIP) with probability exceeding $1 - \delta$, or*

$$\Pr(\left| \|\mathbf{A}\mathbf{x}\|^2 - \|\mathbf{x}\|^2 \right| \leq \epsilon \|\mathbf{x}\|^2) \geq 1 - \delta.$$

Additionally, the unique sparse reconstruction is guaranteed with probability exceeding $1 - \delta$, where $\delta = 4 \exp\left[-\frac{(\epsilon - (\frac{s-1}{N-1}))^2 \cdot K^\eta}{32s} \right]$.

5.11 Orthogonal matching pursuit algorithm

This section introduces the orthogonal matching pursuit (OMP) algorithm proposed in [54]. This is a useful and general algorithm for sparse signal recovery. This algorithm is used in the compressed sensing numerical experiments in Chapter 6.

Input:

- A $K \times N$ measurement matrix $\mathbf{A}$

- A K-dimensional measurement vector $\mathbf{y}$

- The sparsity level s

Output:

- An index set Λ containing s elements

- A signal estimate $\hat{\mathbf{x}} \in \mathbb{R}^N$

Procedure (OMP):

1). Initialize a residual vector $\mathbf{r}_0 = \mathbf{y} = (y_0, , \cdots, y_{K-1})^T$ and $\Lambda = \phi$ at iteration $i = 0$.

2). At iteration i, compute $\mathbf{f} = \mathbf{A}^H \mathbf{r}_i = (f_0, \cdots, f_{N-1})^T$, find the peak of $|\mathbf{f}|$, and record its position as n_i, i.e.,

$$n_i = \mathrm{argmax}_{t=0, \cdots, N-1} |f_t|.$$

3). Update the index set $\Lambda \leftarrow \Lambda \cup \{n_i\}$ and the submatrix $\mathbf{A}_{i+1} = [\mathbf{A}_i \ \mathbf{a}_{n_i}]$. Note that $\mathbf{A}_0$ is an empty matrix.

4). Solve a least-square problem to obtain

$$\mathbf{b}_i = \mathrm{argmax}_{\mathbf{b}} ||\mathbf{y} - \mathbf{A}_{i+1} \mathbf{b}_i||.$$

5). Update the residual by

$$\mathbf{r}_{i+1} = \mathbf{y} - \mathbf{A}_{i+1} \mathbf{b}_i.$$

6). If $i < s - 1$, then $i \leftarrow i + 1$ and repeat 1) $-$ 4). If $i = s - 1$, stop the iteration. The nonzero entry of $\hat{\mathbf{x}}$ is set by $\hat{x}_{nj} = b_j$ for $n_j \in \Lambda$, where b_j is the jth element of $\mathbf{b}_{s-1}$.

Note the measurement procedure in the compressed sensing, i.e., $\mathbf{Ax}$, is a linear combination of s columns in $\mathbf{A}$. In recovery, we need to determine *which columns* of $\mathbf{A}$ participated in this measurement and the *coefficients* of these columns contributed in the measurement. The idea behind this algorithm is to pick columns in a greedy fashion [54]. At each iteration, we choose the column of $\mathbf{A}$ that is the most strongly correlated with the remaining part of vector $\mathbf{y}$ (step 2). Then the coefficients of the picked columns are calculated in a least-square manner (step 4). Finally, we subtract off these columns' contribution to $\mathbf{y}$ (step 5) and iterate on the residual. One hopes that, after s iterations, the algorithm will have identified the correct set of columns together with their corresponding coefficients.

Chapter 6

Partial Fourier Codebooks Associated with Multiplied Golay Complementary Sequences

6.1 Multiplication of Golay complementary sequences

Let $N = 2^m$ for a positive integer m. Let $\mathbf{a} = (a_0, \cdots, a_{N-1})$ and $\mathbf{b} = (b_0, \cdots, b_{N-1})$ be two binary Golay complementary sequences of length N, where $a_i, b_i \in \{0, 1\}$. Note that $\mathbf{a}$ and $\mathbf{b}$ must not form a Golay complementary pair. Let $f = f(x_0, \cdots, x_{m-1})$ and $g = g(x_0, \cdots, x_{m-1})$ be the Boolean functions of m variables that represent $\mathbf{a}$ and $\mathbf{b}$, respectively, where we denote $f \leftrightarrow \mathbf{a}$ and $g \leftrightarrow \mathbf{b}$. Define $\mathbf{c} = \mathbf{a} + \mathbf{b} = (c_0, \cdots, c_{N-1})$ for which $c_i = a_i + b_i$, where the addition is computed modulo-2.

Lemma 1. *Let π_a and π_b be the permutations for f and g, respectively, in $\{0, 1, \cdots, m-1\}$, where $m \geq 3$ is odd. Assume that π_a is given. If π_b is defined by*

$$\pi_b(i) = \begin{cases} \pi_a(i+1), & \text{if } i \text{ is even } (i \neq m-1) \\ \pi_a(i-1), & \text{if } i \text{ is odd} \\ \pi_a(i), & \text{if } i = m-1, \end{cases}$$

then $h = f + g$ is also a Boolean function for a Golay complementary sequence. Therefore, $\mathbf{c} = \mathbf{a} + \mathbf{b}$ is a binary Golay complementary sequence of length N with $h \leftrightarrow \mathbf{c}$. Hence, the

(a)Path of Q_{π_a} (b)Path of Q_{π_b} (c)Path of Q_{π_c}
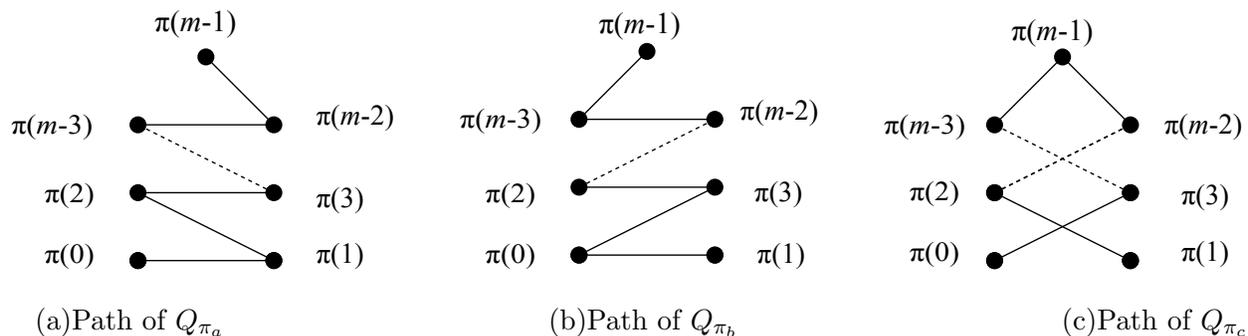
Figure 6.1: Graph structure of quadratic forms, where $m \geq 3$ is odd.

N-point IDFT of **c** *is bounded by*

$$|\widehat{c_l}| = \left| \sum_{i=0}^{N-1} (-1)^{c_i} e^{j\frac{2\pi il}{N}} \right| \leq \sqrt{2N}, \quad 0 \leq l \leq N-1.$$

Proof. Consider a quadratic form

$$Q_\pi = x_{\pi(0)}x_{\pi(1)} + x_{\pi(1)}x_{\pi(2)} + \cdots + x_{\pi(m-2)}x_{\pi(m-1)}$$

in the Boolean function of a Golay complementary sequence, where π is a permutation of $\{0, 1, \ldots, m-1\}$. According to the graph structure of Golay complementary sequences in section 5.4, Q_π can be illustrated as a path where each edge represents a monomial in the quadratic form, i.e., $x_{\pi(i)}x_{\pi(i+1)}$, and each vertex represents a variable, i.e., $x_{\pi(i)}$. Figure 6.1(a) and 6.1(b) illustrate the graph structure of Q_{π_a} and Q_{π_b} of f and g, respectively. Then the addition $h = f + g$ will cancel out all the second order monomials simultaneously existing in both f and g, specifically every $x_{\pi(k)}x_{\pi(k+1)}$, where k is even. Correspondingly, the quadratic form Q_{π_c} of h is illustrated in Figure 6.1(c), resulting a new path on m vertices. According to Theorem 1, $h \in Q_{\pi_c} + \mathrm{RM}(1, m)$ is a Boolean function for a Golay complementary sequence, and **c** is a binary Golay complementary sequence of length N with $\mathbf{c} \leftrightarrow h$. $\qquad\square$

If m is even, we derive a similar permutation π_b for g, such that $h = f + g$ is a Boolean function of a Golay complementary set.

Lemma 2. *Let π_a and π_b be the permutations for f and g, respectively, in $\{0, 1, \cdots, m-1\}$,*

(a)Path of Q_{π_a} (b)Path of Q_{π_b} (c)Path of Q_{π_c}
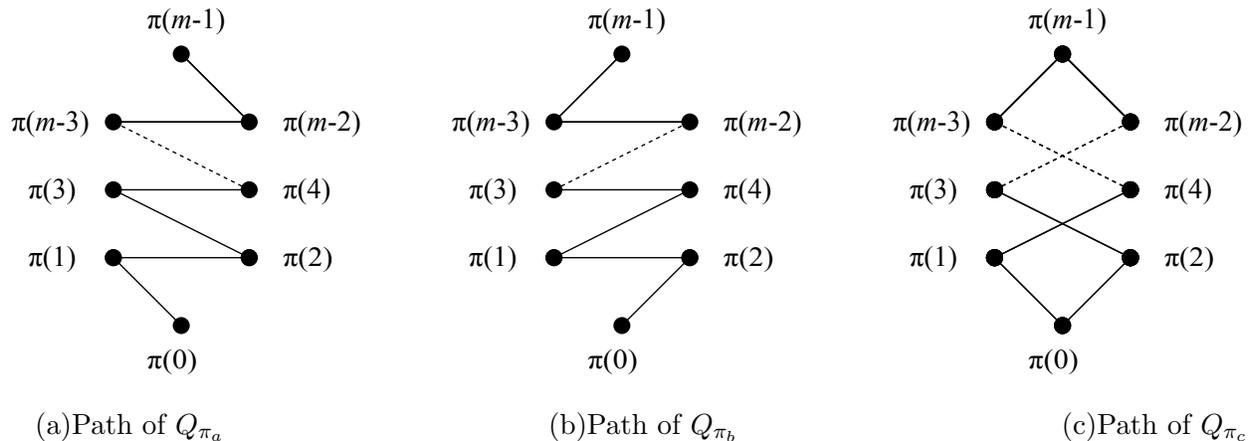
Figure 6.2: Graph structure of quadratic forms, where $m \geq 4$ is even.

where $m \geq 4$ is even. Assume that π_a is given. If π_b is defined by

$$\pi_b(i) = \begin{cases} \pi_a\left(i - 1\right), & \text{if } i \text{ is even } (i \neq 0) \\ \pi_a\left(i + 1\right), & \text{if } i \text{ is odd } (i \neq m - 1) \\ \pi_a(i), & \text{if } i = 0 \text{ or } i = m - 1, \end{cases}$$

*then $h = f + g$ is a Boolean function for a Golay complementary set of size 4. Therefore,
$\mathbf{c} = \mathbf{a} + \mathbf{b}$ is a binary sequence of length N from a Golay complementary set with $h \leftrightarrow \mathbf{c}$.
Hence, the N-point IDFT of $\mathbf{c}$ is bounded by [56]*

$$|\widehat{c}_l| = \left| \sum_{i=0}^{N-1} (-1)^{c_i} e^{j\frac{2\pi il}{N}} \right| \leq \sqrt{4N}, \quad 0 \leq l \leq N - 1.$$

Proof. Similar to the proof of Lemma 1, the addition $h = f + g$ will cancel out all the second
order monomials simultaneously existing in both f and g, specifically every $x_{\pi(k)}x_{\pi(k+1)}$,
where k is odd. Correspondingly, as shown in Figure 6.2 the graph structure of quadratic
form of h is a closed loop on m vertices. According to the Theorem 2, each second order
coset of RM(1, m) identified with this quadratic form consists of sequences lying in a Golay
complementary set of size 4. Hence, $\mathbf{c}$ is a binary sequence from a Golay complementary set
of length N with $\mathbf{c} \leftrightarrow h$. □

In what follows, we define a multiplied Golay complementary sequence using the Golay
complementary sequences $\mathbf{a}$ and $\mathbf{b}$.

$$\pi(i+2) \quad\quad \pi(i+3) \quad\quad \pi(i+2) \quad\quad \pi(i+3)$$

$$\pi(i) \quad\quad \pi(i+1) \quad\quad \pi(i) \quad\quad \pi(i+1)$$

(a) (b)
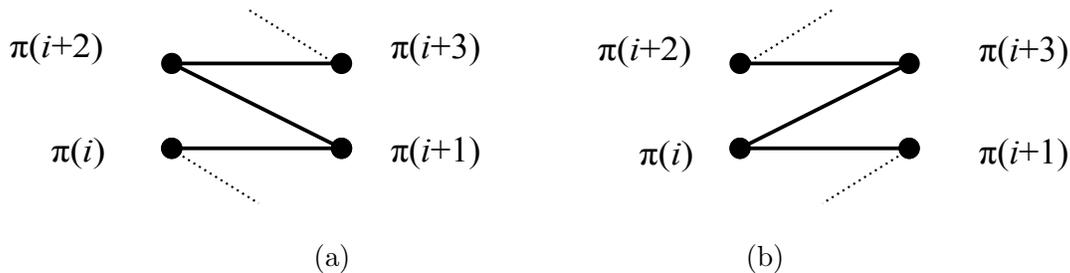
Figure 6.3: Graph of quadratic form of f and g.

Definition 3. *For a positive integer $m \geq 3$, let* **a** *and* **b** *be a pair of Golay complementary sequences of length $N = 2^m$ defined in Lemmas 1 and 2. A multiplied Golay complementary sequence (MGCS) of length N is defined as*

$$\mathbf{u} = (u_0, \cdots, u_{N-1}) = \mathbf{a} \otimes \mathbf{b} \ \text{where } u_i = a_i \cdot b_i, \ \ 0 \leq i \leq N-1 \tag{6.1}$$

where $a_{i,}, b_i, u_i \in \{0, 1\}$.

To avoid a trivial case, we need to ensure that **u** will not be degenerated to a Golay complementary sequence for $m > 4$ in Definition 3.

Lemma 3. **u** *is not a Golay complementary sequence for $m > 4$.*

Proof. For odd $m > 4$, let $p \leftrightarrow \mathbf{u}$. From Lemma 1, we have

$$p = f \cdot g = \quad (\cdots + x_{\pi(i)}x_{\pi(i+1)} + x_{\pi(i+1)}x_{\pi(i+2)} + x_{\pi(i+2)}x_{\pi(i+3)} + \cdots)$$

$$\cdot (\cdots + x_{\pi(i)}x_{\pi(i+1)} + x_{\pi(i)}x_{\pi(i+3)} + x_{\pi(i+2)}x_{\pi(i+3)} + \cdots),$$

where $i < m - 3$ is *even*. The corresponding graph of quadratic form of f and g are partial displayed in Figure 6.3. Expanding the right-hand side of the equation, we eventually have a fourth order monomial $x_{\pi(i)}x_{\pi(i+1)}x_{\pi(i+2)}x_{\pi(i+3)}$, which cannot be eliminated by the rest parts of p. In sum, $\mathbf{u} \subset \mathrm{RM}(4, m)$ is not a Golay complementary sequence [55].

On the other hand, for even $m > 4$ and odd $i < m - 3$, we can develop a similar proof that **u** is not a Golay complementary sequence, which we omit here. $\square$

Before we investigate the Hamming weight of MGCS **u**, we present the following useful relationship between the Hamming weight of a binary sequence and its N-point IDFT.

Let w be the Hamming weight of the binary sequence $\mathbf{u}$. Then,

$$\widehat{u}_0 = \sum_{i=0}^{N-1}(-1)^{u_i}e^{j\frac{2\pi i \cdot 0}{N}} = \sum_{i=0}^{N-1}(-1)^{u_i} = N - 2w. \tag{6.2}$$

Lemma 4. *For odd $m \geq 3$, the Hamming weight of $\mathbf{u}$ is given by*

$$\frac{N - 3\sqrt{2N}}{4} \leq w_u \leq \frac{N + 3\sqrt{2N}}{4}. \tag{6.3}$$

On the other hand, for even $m \geq 4$,

$$\frac{N - (2 + \sqrt{2})\sqrt{2N}}{4} \leq w_u \leq \frac{N + (2 + \sqrt{2})\sqrt{2N}}{4}. \tag{6.4}$$

Proof. Let w_a, w_b, w_c denote the Hamming weights of binary sequences $\mathbf{a}$, $\mathbf{b}$, and $\mathbf{c}$ in Definition 3, respectively. It is easy to find that $w_c = w_a + w_b - 2w_u$, since $\mathbf{c} = \mathbf{a} + \mathbf{b}$ and $\mathbf{u} = \mathbf{a} \otimes \mathbf{b}$. Meanwhile, recall (6.2), a binary sequence lying in a Golay complementary set of size 2^{t+1} has the Hamming weight $\frac{N-\sqrt{2^{t+1}N}}{2} \leq w \leq \frac{N-\sqrt{2^{t+1}N}}{2}$ from the bounded N-point IDFT of $\sqrt{2^{t+1}N}$ [56]. For odd m, the Golay complementary sequence $\mathbf{c}$ is lying in a Golay complementary set of size 2, where $t = 0$, giving $\frac{N-\sqrt{2N}}{2} \leq w_c \leq \frac{N+\sqrt{2N}}{2}$. The range of w_a and w_b is the same as w_c. Then, using $w_u = \frac{w_a+w_b-w_c}{2}$, a simple math yields (6.3). For even m, w_a and w_b have the same range as in odd m. However, $\mathbf{c}$ is from a Golay complementary set of size 4, where $t = 1$, giving $\frac{N-2\sqrt{N}}{2} \leq w_c \leq \frac{N+2\sqrt{N}}{2}$. Thus the range of w_u is given by (6.4). $\qquad\square$

We now investigate the N-point IDFT of the MGCS.

Lemma 5. *Let $\mathbf{u}$ be a binary MGCS of length $N = 2^m$, defined in Definition 3. Then, if m is odd, we have*

$$|\widehat{u}_l| \leq \frac{3\sqrt{2N}}{2}, \quad 1 \leq l \leq N - 1.$$

On the other hand, if m is even, then

$$|\widehat{u}_l| \leq \frac{(2 + \sqrt{2})\sqrt{2N}}{2}, \quad 1 \leq l \leq N - 1.$$

Proof. First of all, we have

$$|\widehat{a}_l| = \left|\sum_{i=0}^{N-1}(-1)^{a_i}e^{j\frac{2\pi il}{N}}\right| = \left|\sum_{i=0}^{N-1}(1 - 2a_i)e^{j\frac{2\pi il}{N}}\right| = 2\left|\sum_{i=0}^{N-1}a_i e^{j\frac{2\pi il}{N}}\right| \tag{6.5}$$

where we used $\sum_{i=0}^{N-1} e^{j\frac{2\pi il}{N}} = 0$ for $l \neq 0$. Similarly, $|\widehat{b_l}| = 2\left|\sum_{i=0}^{N-1} b_i e^{j\frac{2\pi il}{N}}\right|$. Meanwhile, from $\mathbf{c} = \mathbf{a} + \mathbf{b}$,

$$
\begin{aligned}
\widehat{c_l} &= \sum_{i=0}^{N-1}(-1)^{(a_i+b_i)}e^{j\frac{2\pi il}{N}} \\
&= \sum_{i=0}^{N-1}(1-2a_i)(1-2b_i)e^{j\frac{2\pi il}{N}} \\
&= \sum_{i=0}^{N-1}(1-2a_i-2b_i+4a_ib_i)e^{j\frac{2\pi il}{N}}
\end{aligned}
$$

where

$$
4\sum_{i=0}^{N-1} a_ib_i e^{j\frac{2\pi il}{N}} = \widehat{c_l} + 2\sum_{i=0}^{N-1} a_i e^{j\frac{2\pi il}{N}} + 2\sum_{i=0}^{N-1} b_i e^{j\frac{2\pi il}{N}}, \quad 1 \leq l \leq N-1. \tag{6.6}
$$

By (6.1), (6.5), and (6.6), we have

$$
\left|\sum_{i=0}^{N-1} u_i e^{j\frac{2\pi il}{N}}\right| \leq \frac{|\widehat{c_l}| + |\widehat{a_l}| + |\widehat{b_l}|}{4}, \quad 1 \leq l \leq N-1.
$$

Finally, if m is odd, then $|\widehat{c_l}| \leq \sqrt{2N}$ from Lemma 1, and thus

$$
|\widehat{u_l}| = 2\left|\sum_{i=0}^{N-1} u_i e^{j\frac{2\pi il}{N}}\right| \leq \frac{3\sqrt{2N}}{2}, \quad 1 \leq l \leq N-1.
$$

On the other hand, if m is even, then $|\widehat{c_l}| \leq \sqrt{4N}$ from Lemma 2, and thus

$$
|\widehat{u_l}| = 2\left|\sum_{i=0}^{N-1} u_i e^{j\frac{2\pi il}{N}}\right| \leq \frac{(2+\sqrt{2})\sqrt{2N}}{2}, \quad 1 \leq l \leq N-1. \qquad \square
$$

Before we construct partial Fourier codebooks associated with MGCS, we present below theorem for partial Fourier codebooks associated with binary sequences.

Theorem 4. [51] *Let $\mathcal{C}$ be an (N, K) partial Fourier codebook associated with a binary sequence $\mathbf{u}$. Then,*

$$
I_{\max}(\mathcal{C}) = \frac{1}{2K} \cdot \max_{1 \leq l \leq N-1} |\widehat{u_l}|
$$

where $\widehat{u_l} = \sum_{i=0}^{N-1}(-1)^{u_i} e^{j\frac{2\pi il}{N}}$ is the N-point IDFT of the sequence $\mathbf{u}$.

Now we present Theorem 5, the main contribution of this thesis, where the proof is straightforward from Theorem 4 and Lemma 5.

Theorem 5. *Let $\mathcal{C}$ be an (N, K) partial Fourier codebook associated with MGCS $\mathbf{u}$ in Definition 3, where $N = 2^m$ and K is determined by the Hamming weight of $\mathbf{u}$ in Lemma 4. For odd m, we have*

$$I_{\max}(\mathcal{C}) \le \frac{3\sqrt{2N}}{4K},$$

and for even m,

$$I_{\max}(\mathcal{C}) \le \frac{(2 + \sqrt{2})\sqrt{2N}}{4K}.$$

Remark 2. A binary sequence from a Golay complementary set of size 4 has the bounded N-point IDFT of $\sqrt{2} \cdot \sqrt{2N}$, which is slightly smaller than $\frac{3}{2} \cdot \sqrt{2N}$ of the MGCS $\mathbf{u}$ ($l \ne 0$). However, its Hamming weight w approaches to $\frac{N}{2}$ for large N with $\frac{N-2\sqrt{N}}{2} \le w \le \frac{N+2\sqrt{N}}{2}$, while the MGCS $\mathbf{u}$ has the Hamming weight approaching to $\frac{N}{4}$ for large N from Lemma 4. Therefore, the smaller Hamming weight of the MGCS $\mathbf{u}$ makes its associated codebooks more suitable for the applications to compressed sensing that generally requires $K < \frac{N}{2}$.

6.2 Search for partial Fourier codebooks associated with MGCS

For each m, there are $m! \cdot 2^{2m+1}$ possible MGCS in Definition 3, which is a huge search space as m increases. The following restriction is adopted to reduce our search scope for codebooks with large m. We set $\pi_a(i) = i$ for $0 \le i \le m-1$, $f = Q_{\pi_a} = x_0 x_1 + x_1 x_2 + \cdots + x_{m-2} x_{m-1}$, and $g = Q_{\pi_b} + \mathrm{RM}(1, m)$ where π_b is defined in Lemmas 1 and 2. Then for each $7 \le m \le 15$, we searched partial Fourier codebooks over 2^{m+1} MGCS $\mathbf{u}$. Table 6.1 shows the parameters for several (N, K) partial Fourier codebooks from this search scope. In the table, I_{Welch} denotes the Welch bound equality in (5.11), while $I_{\mathrm{upper}}(\mathcal{C})$ denotes the theoretical upper bound in Theorem 5. We present the codebooks with smallest $I_{\max}(\mathcal{C})/I_{\mathrm{Welch}}$ ratio, where $N = 4K$. For odd m, note the ratio $I_{\max}(\mathcal{C})/I_{\mathrm{Welch}}$ will be at most $\sqrt{6}$ for $N = 4K$, since $I_{\max}(\mathcal{C}) \le 3\sqrt{\frac{2}{N}}$ and $I_{\mathrm{Welch}} \gtrsim \sqrt{\frac{3}{N}}$.

Remark 3. Note here $f = x_0 x_1 + x_1 x_2 + \cdots + x_{m-2} x_{m-1}$, recall (5.2) of associated sequences of Boolean function, one can check that the first element of $\mathbf{u}$ is always 0, which means that the first row of IDFT matrix will not be selected in this construction.

Table 6.1: Search results for (N, K) partial Fourier codebooks $\mathcal{C}$ associated with MGCS $\mathbf{u} \leftrightarrow f \cdot g$ where $f = x_0 x_1 + x_1 x_2 + \cdots + x_{m-2} x_{m-1}$. The listed codebooks have the smallest $I_{\max}(\mathcal{C})/I_{\text{Welch}}$ ratio with $N = 4K$.

(N, K)	$I_{\max}(\mathcal{C})$	$I_{\text{upper}}(\mathcal{C})$	I_{Welch}	$I_{\max}(\mathcal{C})/I_{\text{Welch}}$
(128, 32)	0.250000	0.375000	0.153695	1.626602
(256, 64)	0.190033	0.301777	0.108465	1.752016
(512, 128)	0.138621	0.187500	0.076621	1.809169
(1024, 256)	0.105765	0.150888	0.054153	1.953083
(2048, 512)	0.076891	0.093750	0.038283	2.008511
(4096, 1024)	0.058582	0.075444	0.027067	2.164375
(8192, 2048)	0.040625	0.046875	0.019138	2.122767
(16384, 4096)	0.031510	0.037722	0.013532	2.328529
(32768, 8192)	0.021148	0.023438	0.009568	2.210203

6.3 Applications to deterministic compressed sensing matrices

In this section, we apply an (N, K) partial Fourier codebook $\mathcal{C}$ associated with an MGCS as a $K \times N$ deterministic sensing matrix $\mathbf{A}$ in compressed sensing, where each code vector of $\mathcal{C}$ forms a column of $\mathbf{A}$. The coherence of the sensing matrix $\mathbf{A}$ is then equivalent to $I_{\max}(\mathcal{C})$ with the upper bound in Theorem 5. Each column of the $K \times N$ matrix also forms a tight frame, since a pair of distinct row vectors is mutually orthogonal. Besides, the partial Fourier sensing matrix with $N = 2^m$ is favorable in practice, allowing an efficient FFT technique for recovery of sparse signals.

Since the first element in sequence $\mathbf{u}$ is 0 (Remark 3), let $\mathbf{A} = \mathcal{C}$, one can check that a partial Fourier sensing matrix $\mathbf{A}$ associated with $\mathbf{u}$ achieves the three conditions in Definition 2. Moreover,

$$\left| \sum_k \mathbf{a}_n(k) \right|^2 = K \cdot \left| \mathbf{a}_1^H \mathbf{a}_n \right|^2 \leq K \cdot I_{\max}(\mathcal{C})^2.$$

With the condition $N = 4K$, the following is derived from Theorem 3.

Corollary 1. *For odd $m \geq 7$, let $N = 2^m$. Let $\frac{s-1}{N-1} < \epsilon < 1$, and $C_\epsilon = \frac{2\epsilon^2}{9c}$ for a constant c. If the sparsity level s satisfies $s \leq C_\epsilon \cdot \frac{K}{\log N}$, then the matrix $\mathbf{A}$ has the statistical restricted isometry property (StRIP) with probability exceeding $1 - \delta$, or*

$$\Pr(| \, \|\mathbf{A}\mathbf{x}\|^2 - \|\mathbf{x}\|^2 \, | \leq \epsilon \, \|\mathbf{x}\|^2) \geq 1 - \delta$$

with respect to a uniform distribution of the vectors $\mathbf{x}$ among all s-sparse vectors in $\mathbb{R}^N$, where $\delta = 4 \exp\left[-\frac{(\epsilon - (\frac{s-1}{N-1}))^2 \cdot K}{144s} \right]$. Additionally, the unique sparse reconstruction is guaranteed with probability exceeding $1 - \delta$.

Proof. Recall Remark 1, let

$$\left| \sum_k \mathbf{a}_n(k) \right|^2 \leq K^{1-\eta} = K \cdot I_{\max}(\mathcal{C})^2.$$

Then, by $N = 4K$, and Theorem 5 for odd m

$$\frac{K}{K^\eta} = K \cdot I_{\max}(\mathcal{C})^2 = K \cdot \frac{18N}{16K^2} = \frac{9}{2}. \tag{6.7}$$

Note that only for $m \geq 7$, there exist some $\frac{1}{2} < \eta \leq 1$ such that $\frac{K}{K^\eta} = \frac{9}{2}$. Finally, we may substitute K^η by $\frac{2K}{9}$ in Theorem 3. $\qquad \square$

We present a similar corollary for even $m \geq 8$ without the proof, as shown below.

Corollary 2. *For even $m \geq 8$, let $N = 2^m$. Let $\frac{s-1}{N-1} < \epsilon < 1$, and $C_\epsilon = \frac{\epsilon^2}{(3+2\sqrt{2})c}$ for a constant c. If the sparsity level s satisfies $s \leq C_\epsilon \cdot \frac{K}{\log N}$, then the matrix $\mathbf{A}$ has the StRIP with probability exceeding $1 - \delta$, or*

$$\Pr(|\, \|\mathbf{Ax}\|^2 - \|\mathbf{x}\|^2 \,| \leq \epsilon \|\mathbf{x}\|^2) \geq 1 - \delta$$

with respect to a uniform distribution of the vectors $\mathbf{x}$ among all s-sparse vectors in $\mathbb{R}^N$, where $\delta = 4 \exp\left[-\frac{(\epsilon - (\frac{s-1}{N-1}))^2 \cdot K}{(96+64\sqrt{2})s}\right]$. Additionally, the unique sparse reconstruction is guaranteed with probability exceeding $1 - \delta$.

6.4 Recovery performance

To examine the empirical recovery performance from noiseless measurements, we took numerical experiments for several $K \times N$ partial Fourier matrices selected from the codebooks in Table 6.1. For recovery of s-sparse signals, we employed the OMP algorithm described in section 5.11, where total 2000 sample vectors were tested for each sparsity level. Each nonzero entry of an s-sparse signal $\mathbf{x}$ has the magnitude of 1, and its sign and position are chosen uniformly at random. A success is declared in the reconstruction if the squared error is reasonably small for the estimate $\hat{\mathbf{x}}$, i.e., $||\mathbf{x} - \hat{\mathbf{x}}||^2 < 10^{-6}$.

Figure 6.4 displays the recovery performance of some partial Fourier sensing matrices $\mathbf{A}$ as sparsity level increases. Figure 6.5 displays the maximum sparsity level, or $s_{\max}$ for which the partial Fourier sensing matrix achieves more than 99% successful recovery rates by the OMP reconstruction algorithm. The linear regression shows $s_{\max} \approx 1.3 \cdot \frac{K}{\log N} - 5.2$, indicating reliable recovery performance for sparsity level of $\mathcal{O}(K/\log N)$. Therefore, with the reliable recovery performance as well as the efficient FFT technique in OMP recovery process, the partial Fourier codebooks associated with MGCS present good candidates for deterministic compressed sensing matrices.
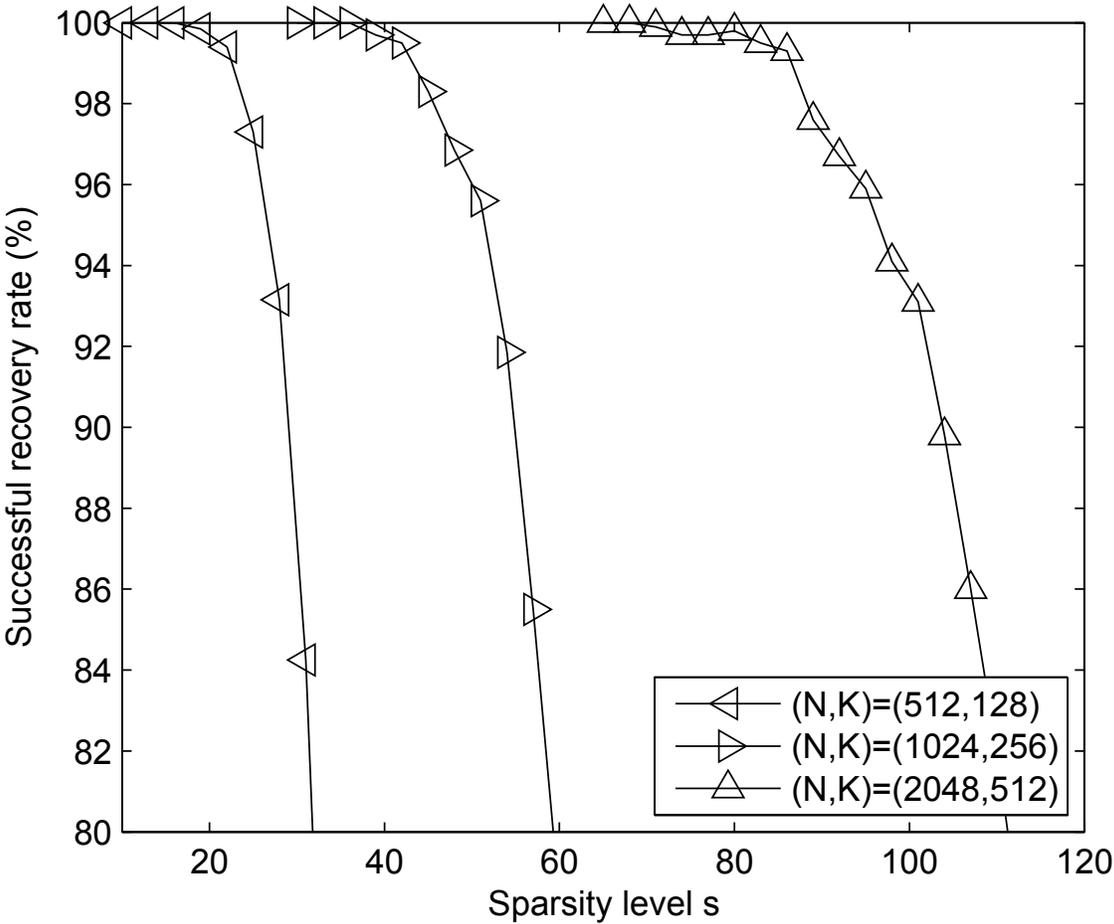
Figure 6.4: Successful recovery rates for partial Fourier matrices associated with MGCS.
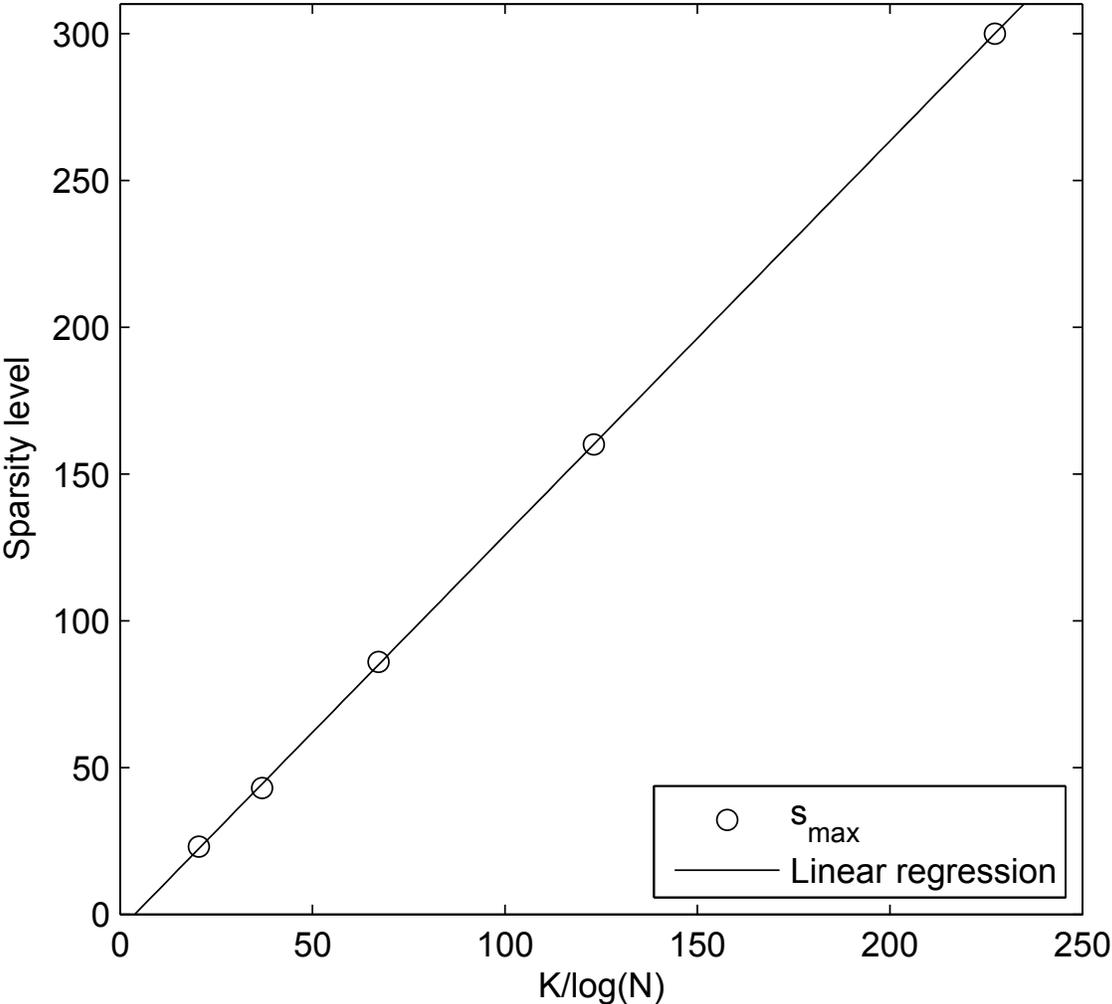
Figure 6.5: Empirically maximum sparsity levels achieving more than 99% recovery rate for partial Fourier sensing matrices, where $N = 4K = 2^m$ for $9 \leq m \leq 13$. The equation of the linear regression is $1.3K/\log N - 5.2$.

Chapter 7

Conclusions

In the first part of thesis, we have examined the PAPR distribution of the downlink MC-CDMA systems spread by Walsh-Hadamard and Golay complementary sequences. We employed the GEV distribution to model the PAPR distribution, and found the patterns of the GEV parameters. Exploiting the patterns, we proposed numerical-based sequence-specific mathematical expressions for the PAPR distributions with the variable of N_{sc}. The good agreement between the GEV model and the empirical PAPR indicates that the GEV distribution is well-suited for modeling the PAPR distribution in MC-CDMA system. We also observed the trend of the PAPR distributions converging to the Gumbel distribution for large N_{sc}. This is the first work applying the GEV distribution for modeling of the PAPR in downlink MC-CDMA systems, which presented the simple but novel GEV model of (3.1) for predicting the PAPR distribution.

In the second part of the thesis, we deliberately constructed a pair of Golay complementary sequences with the concept of graph structure of quadratic forms. Then we introduced a new class of sequences by the element-wise multiplication of the two Golay complementary sequences. We derived the upper bound of the N-point IDFT of the new sequences. The Hamming weight of the sequence was also studied. We constructed new partial Fourier codebook associated with these sequences for $N = 2^m$, which is favorable in practice, and K is approximately $\frac{N}{4}$. The upper bound of the maximum magnitude of inner products between distinct code vectors was also developed from the N-point IDFT property from the sequence. Next, assisted by the computer cluster, we searched the sequences over a restricted space.

The codebooks associated with sequences from the search results were displayed in Table 6.1. For its application, the new (N, K) partial Fourier codebooks with $N = 4K$ were employed as deterministic sensing matrices in compressed sensing. Numerical results demonstrated that the new partial Fourier sensing matrices have reliable recovery performance with the FFT-enabled OMP recovery algorithm, indicating the new codebook can be a suitable choice for compress sensing. In the future work, we will focus on the application of these codebook in the imagine processing area, and test recovery performances of these matrices with other recovery algorithms.

Bibliography

[1] S. Hara and R. Prasad, "Overview of multicarrier CDMA," *IEEE Commun. Mag.*, vol. 35, no. 12, pp. 126–133, Dec. 1997.

[2] B. M. Popovic, "Spreading sequences for multicarrier CDMA systems," *IEEE Trans. Commun.*, vol. 47, no. 6, pp. 918–926, Jun. 1999.

[3] N. Ruangsurat and R. Rajatheva, "An investigation of peak to average power ratio in MC-CDMA combined with partial transmit sequence," *IEEE 53rd VTC*, vol. 1, no. 53, pp. 761–765, 2001.

[4] K. Choi, K. Kang, and S. Kim, "Peak power reduction scheme based on subcarrier scrambling for MC-CDMA systems," *Communications, IEE Proceedings*, vol. 151, pp. 39–43, 2004.

[5] N. Y. Yu, "A theoretical study of peak-to-average power ratio in Reed-Muller coded multicarrier CDMA," in *Proc. of Conf. Inf. Sci. Syst.*, Princeton, NJ, Mar. 2010, pp. 1–6.

[6] L. Dong and N. Y. Yu, "Peak power analysis of MC-CDMA employing Golay complementary sequences," in *Proc. of 12th Canadian Workshop on Information Theory*, Kelowna, Canada, May 2011, pp. 38–41.

[7] F. J. MacWillams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, Amsterdam, The Netherlands: North Holland, 1986.

[8] M. J. E. Golay, "Complementary series," *IRE Trans. Inform. Theory*, vol. 7, no. 2, pp. 82–87, 1961.

[9] H. Ochiai and H. Imai, "On the distribution of the peak to average power ratio in OFDM signals," *IEEE Trans. on. Commun.*, vol. 49, no. 2, pp. 282–289, Feb. 2001.

[10] S. Q. Wei, D. L. Goeckel, and P. E. Kelly, "A modern extreme value theory approach to calculating the distribution of the peak-to-average power ratio in OFDM systems," in *IEEE International Conferences on Communications (ICC02)*, Apr. 2002, vol. 3, pp. 1686–1690.

[11] T. Jiang, M. Guizani, H. Chen, W. Xiang, and Y. Wu, "Derivation of PAPR distribution for OFDM wireless systems based on extreme value theory," *IEEE Trans. on Wireless Comm.*, vol. 7, no. 4, pp. 1298–1305, Apr. 2008.

[12] D. Yang, X. Yu, K. Liu, and Q. Zhang, "Performance analysis of PAPR in MC-CDMA system," in *Proc. Information Science and Engineering (ICISE)*, 2009, pp. 2676 – 2679.

[13] Z. Fedra and J. Blumenstein, "PAPR and amplitude distribution in MC-CDMA system," in *IEEE Region 8 International Conference on Computational Technologies in Electrical and Electronics Engineering (SIBIRCON)*, Jul. 2002, pp. 247 – 250.

[14] R. A. Fisher and L. H. C. Tippet, "Limiting forms of the frequency distribution of the largest or smallest member of a sample," in *Proc. Cambridge Philosoph. Soc.*, 1928, vol. 24, pp. 180–190.

[15] J. G. Proakis and M. Salehi, *Digital Communications. 5th ed*, McGraw-Hill, 2008.

[16] R. W. Chang, "Synthesis of bandlimited orthogonal signals for multichannel data transmission," *Bell System Technical Journal.*, vol. 46, pp. 1775–1796, Dec. 1966.

[17] B. R. Saltzberg, "Performance of an efficient paralled data transmission system," *IEEE Trans. Comm.*, vol. 15, pp. 805–811, Dec. 1967.

[18] S. B. Weinstein and P. M. Ebert, "Data transmission by frequency-division multiplexing using the discrete Fourier transform," *IEEE Trans. Comm.*, vol. 19, pp. 628–634, Oct. 1971.

[19] A. Peled and A. Ruiz, "Frequency domain data transmission using reduced computational complexity algorithms," in *IEEE Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Apr. 1980, pp. 964–967.

[20] ETSI, "*v1.5.1 - Digital Video Broadcasting (DVB)*," 2004.

[21] ETSI, "*v1.4.1 - Original DAB specification*," 2006.

[22] IEEE., "*802.11a-1999 High-speed Physical Layer in the 5 GHz band*," 1999.

[23] S. Sesia, I. Toufik, and M. Baker, *LTE, The UMTS Long Term Evolution: From Theory to Practice*, Wiley, 2009.

[24] TS 36.300 3GPP, "Evolved Universal Terrestrial Radio access (EUTRA) and Evolved Universal Terrestrial Radio Access Network (EUTRAN) Overall Description; Stage 2 (release 8) v8.10.0," Sep. 2009.

[25] L. L. Yang, *Multicarrier Communication*, Wiley, 2009.

[26] Y. H. Kim, I. Song, H. G. Kim, and J. Lee, "Design and performance analysis of a convolutionally coded overlapping multicarrier DS/CDMA system," *IEEE Trans. Veh. Tech.*, vol. 49, no. 7, pp. 1950–1967, Sept. 2000.

[27] S. Kondo and L. B. Milstein, "On the use of multicarrier direct sequence spread spectrum systems," in *Proc. IEEE Milcom*, Oct. 1993, pp. 52–56.

[28] S. Kondo and L. B. Milstein, "Performance of multicarrier DS-CDMA systems," *IEEE Trans. Commun.*, vol. 44, no. 7, pp. 238–246, Feb. 1996.

[29] A. Chouly, A. Brajal, and S. Jourdan, "Orthogonal multicarrier techniques applied to direct sequence spread spectrum CDMA systems," in *Proc. IEEE GLOBECOM*, Houston, TX, 1993, pp. 1723–1728.

[30] N. Yee, J. Linnartz, and G. Fettweis, "Multi-carrier CDMA in indoor wireless radio networks," in *Proc. IEEE PIMRC*, Sept. 1993, pp. 109–113.

[31] H. Ochiai and H. Imai, "OFDM-CDMA with peak power reduction based on the spreading sequences," in *IEEE International Conferences on Communications*, Apr. 1998, vol. 3, pp. 1299–1303.

[32] X. Li and L. J. Cimini, "Effect of clipping and filtering on the performance of OFDM," *IEEE Commun.Lett.*, vol. 2, no. 5, pp. 131–133, May 1998.

[33] S. H. Han and J. H. Lee, "An overview of peak-to-average power ratio reduction techniques for multicarrier transmission," *IEEE Wireless Commun.*, vol. 12, no. 2, pp. 56–65, Apr. 2005.

[34] J. Armstrong, "Peak-to-average power reduction for OFDM by repeated clipping and frequency domain filtering," *Elect. Lett.*, vol. 38, no. 8, pp. 246–247, Feb. 2002.

[35] R. W. Buml, R. F. H. Fisher, and J. B. Huber, "Reducing the peak-to-average power ratio of multicarrier modulation by selected mapping," *Elect. Lett.*, vol. 32, no. 22, pp. 2056–2057, Oct. 1996.

[36] B. J. Choi, E. L. Kuan, and L. Hanzo, "OFDM-CDMA with peak power reduction based on the spreading sequences," in *IEEE Proc. Vehicular Technology Conf.*, Sept. 1999, pp. 233–237.

[37] S. Kotz and S. Nadarajah, *Extreme Value Distributions: Theory and Applications*, Singapore: World Scientific, 2001.

[38] M. Barkat, *Signal detection and estimation. 2nd ed*, Artech-House, 2005.

[39] I. J. Myung, "Tutorial on maximum likelihood estimation," *Journal of Mathematical Psychology*, vol. 1, no. 47, pp. 90–100, 2003.

[40] Mathworks Inc., "R2012a documentation statistics toolbox : gevfit," 2012.

[41] J. L. Massey and T. Mittelholzer, "Welch's bound and sequence sets for code-division multiple-access systems," in *Sequences II: Methods in Communication, Security, and Computer Science*, 1993, pp. 63–78.

[42] D. J. Love, R. W. Heath, and T. Strohmer, "Grassmannian beamforming for multiple-input multiple-output wireless systems," *IEEE Trans. Inform. Theory*, vol. 49, pp. 2735–2747, 2003.

[43] E. J. Candes and M. B. Wakin, "An introduction to compressive sampling," *IEEE Sig. Proc. Mag.*, pp. 21–30, March 2008.

[44] D. L. Donoho and M. Elad, "Optimally sparse representation in general (non-orthogonal) dictionaries via l_1 minimization," in *Proc. Natl Acad. Sci.*, 2003, pp. 2197–2202.

[45] L. R. Welch, "Lower bounds on the maximum cross correlation of signals," *IEEE Trans. Inf. Theory*, vol. 20, no. 3, pp. 397–399, 1974.

[46] J. Kovacevic and A. Chebira, "An introduction to frames," *Foundations and Trends in Signal Processing*, vol. 2, no. 1, 2008.

[47] D. V. Sarwate, "Meeting the Welch bound with equality," in *Sequences and Their Applications, C. Ding, T. Helleseth, and H. Niederreiter Eds., DMTCS Series Springer-Verlag*, 1999, pp. 79–102.

[48] C. Ding, "Complex codebooks from combinatorial designs," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 4229–4235, 2006.

[49] C. Ding and T. Feng, "Codebooks from almost difference sets," *Des. Codes Cryptogr.*, vol. 46, pp. 113–126, 2008.

[50] V. M. Sidelnikov, "Some k-valued pseudo-random sequences and nearly equidistant codes," *Probl. Inf. Transm.*, vol. 5, pp. 12–16, 1969.

[51] N. Y. Yu, "A construction of codebooks associated with binary sequences," *IEEE Trans. Inform. Theory, to appear*, 2012.

[52] R. A. DeVore, "Deterministic constructions of compressed sensing matrices," *J. Complexity*, vol. 28, pp. 918–925, 2007.

[53] R. Calderbank, S. Howard, and S. Jafarpour, "Construction of a large class of deterministic matrices that satisfy a statistical isometry property," *IEEE J. Selected Topics in Signal Processing*, vol. 4, no. 2, pp. 358–374, 2010.

[54] J. A. Tropp and A. C. Gilbert., "Signal recovery from random measurements via orthogonal matching pursuit," *IEEE Trans. Inf. Theory*, vol. 53, no. 12, pp. 4655–4666, 2007.

[55] J. A. Davis and J. Jedwab, "Peak-to-mean power control for OFDM, Golay complementary sequences, and Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2397–2417, 1999.

[56] K. G. Paterson, "Generalized Reed-Muller codes and power control in OFDM modulation," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 104–120, 2000.

[57] J. A. Tropp, "The sparsity gap: uncertainty principle proportional to dimension," in *Conf. Information Sciences and Systems (CISS)*, Princeton, NJ, 2010, pp. 1–6.

[58] S. Orfanidis, *Introduction to Signal Processing*, Prentice Hall, 1995.

[59] M. Davenport, M. Duarte, Y. Eldar, and G. Kutyniok, *Compressed Sensing: Theory and Applications*, Cambridge University Press, 2012.

[60] B. Hayes, "The best bits - a new technology called compressive sensing slims down data at the source," *American scientist*, vol. 97, no. 4, pp. 276, Jul.-Aug. 2009.

[61] L. Applebaum, S. Howard, S. Searle, and R. Calderbank, "Chirp sensing codes: deterministic compressed sensing measurements for fast recovery," *Appl. and Comput. Harmon. Anal.*, vol. 26, 2009.

[62] W. Alltop, "Complex sequences with low periodic correlations," *IEEE Trans. Inf. Theory*, vol. 26, no. 3, pp. 350–354, 1980.

[63] T. Strohmer and R. Heath, "Grassmanian frames with applications to coding and communication," *Appl. and Comput. Harmon. Anal.*, vol. 14, no. 3, pp. 257–275, 2003.

[64] R. Calderbank, S. Howard, and S. Jafarpour, "A sublinear algorithm for sparse reconstruction with l_2/l_2 recovery guarantees," in *Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP), 3rd IEEE International Workshop on*, 2009, pp. 209 – 212.

[65] S. Howard, R. Calderbank, and S. Searle, "A fast reconstruction algorithm for deterministic compressive sensing using second order Reed-Muller codes," in *Conference on Information Systems and Sciences (CISS)*, Princeton, NJ, 2008, pp. 11–15.

[66] N. Ailon and E. Liberty, "Fast dimension reduction using Rademacher series on dual BCH codes," in *Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, 2008., pp. 215–224.

[67] Z. Xu, "Deterministic sampling of sparse trigonometric polynomials," *Journal of Complexity*, vol. 27, no. 2, 2011.

[68] N. Y. Yu, "Additive character sequences with small alphabets for compressed sensing matrices," in *IEEE Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Prague, Czech Republic, 2011, pp. 2932–2935.

[69] E. Candes and T. Tao, "Decoding by linear programming," *IEEE Trans. Inf. Theory*, vol. 51, pp. 4203–4215, 2005.

[70] M. Rudelson and R. Vershynin, "On sparse reconstruction from Fourier and Gaussian measurements," *Communications on Pure and Applied Mathematics*, vol. 61, pp. 1025–1045, 2008.